



EuropaInstitut

AN DER UNIVERSITÄT ZÜRICH

Fabio Andreotti

Dezentrale Handelsplattformen im Schweizer Finanzmarktrecht

Eine Analyse unter Erarbeitung eines Rechtsprinzips
der Dezentralität

Dezentrale Handelsplattformen im Schweizer Finanzmarktrecht

**Eine Analyse unter Erarbeitung eines Rechtsprinzips der
Dezentralität**

Dissertation
der Rechtswissenschaftlichen Fakultät
der Universität Zürich

zur Erlangung der Würde eines Doktors der Rechtswissenschaft

vorgelegt von

Fabio Andrea Andreotti
von Gambarogno TI

genehmigt auf Antrag von

Prof. Dr. Rolf Sethe
und
Prof. Dr. Corinne Zellweger-Gutknecht

Die Rechtswissenschaftliche Fakultät gestattet hierdurch die Drucklegung der vorliegenden Dissertation, ohne damit zu den darin ausgesprochenen Anschauungen Stellung zu nehmen.

Zürich, den 5. Oktober 2022

Der Dekan: Prof. Dr. Thomas Gächter



Dezentrale Handelsplattformen im Schweizer Finanzmarktrecht Copyright © by Fabio Andreotti is licensed under a [Creative Commons Namensnennung-Nicht kommerziell-Keine Bearbeitung 4.0 International](https://creativecommons.org/licenses/by-nc-nd/4.0/), except where otherwise noted.

© 2024 – CC BY-NC-ND (Werk), CC BY-SA (Text)

Autor: Fabio Andreotti

Verlag: EIZ Publishing (eizpublishing.ch)

Produktion, Satz & Vertrieb: buch & netz (buchundnetz.com)

ISBN:

978-3-03805-679-9 (Print – Softcover)

978-3-03805-680-5 (Print – Hardcover)

978-3-03805-681-2 (PDF)

978-3-03805-682-9 (ePub)

DOI: <https://doi.org/10.36862/eiz-680>

Version: 1.03 – 20240523

Die Dissertation wurde publiziert mit Unterstützung des Schweizerischen Nationalfonds zur Förderung der wissenschaftlichen Forschung.

Die vorliegende Dissertation wurde von Fabio Andreotti eingereicht und von der Rechtswissenschaftlichen Fakultät der Universität Zürich abgenommen.

Sie wurde betreut von Prof. Dr. Rolf Sethe, Zweitgutachten von Prof. Dr. Corinne Zellweger-Gutknecht.

Das Werk ist als gedrucktes Buch und als Open-Access-Publikation in verschiedenen digitalen Formaten verfügbar: <https://eizpublishing.ch/publikationen/dezentrale-handelsplattformen-im-schweizer-finanzmarktrecht/>.

Die Publikation ist auch auf der Webseite der Zentralbibliothek Zürich abrufbar: <https://www.zb.uzh.ch/de/>

The life of the law has not been logic: it has been experience.

– Oliver Wendell Holmes, Jr.,
The Common Law, Boston 1881, 1

Vorwort

«Aller Anfang ist schwer! Das mag in einem gewissen Sinne wahr sein; allgemeiner aber kann man sagen: aller Anfang ist leicht, und die letzten Stufen werden am schwersten und seltensten erstiegen.»

Folgt man Johann Wolfgang von Goethe (Wilhelm Meisters Wanderjahre, 1821), hätte die vorliegende Arbeit vermutlich kaum je ein Ende gefunden. Sie wurde überwiegend in meiner Zeit als wissenschaftlicher Assistent an der Universität Zürich, als Mitarbeiter des Staatssekretariats für internationale Finanzfragen (SIF) in Bern, als Substitut einer Zürcher Wirtschaftskanzlei, als Assistenzstaatsanwalt im Bereich der Wirtschaftskriminalität des Kantons Aargau und als Head of Legal & Compliance einer Schwyzer und Zuger Investmentfirma verfasst. Dazwischen habe ich noch einen Forschungsaufenthalt am Mercatus Center der George Mason University, Virginia, USA, einschieben dürfen.

Vielen Menschen darf, ja muss ich danken, denn eine Dissertation ist selten ein Sololauf. Die Liste der Beitragenden wäre endlos, mit Namen erwähnen möchte ich vor allem meine Eltern Katalin und Mario Andreotti-Schneuwly, meine Schwestern Flavia und Celina und ganz besonders Anna Züst und Flor; dank ihnen konnte ich meine «Wanderjahre» zu einem guten Ende bringen.

Ein spezieller Dank gilt sodann meinem Doktorvater, Prof. Dr. Rolf Sethe. Er hat mich während meiner lehrreichen Assistenzzeit in ganz humanistischer Weise gefördert und gefordert. Ein grosses Dankeschön gilt auch Prof. Dr. Corinne Zellweger-Gutknecht für den prompten Abschluss der Zweitbegutachtung. Ferner möchte ich mich auch bei den Verantwortlichen des Issekutz-Preises bedanken, den ich für die Arbeit im Frühling 2023 entgegennehmen durfte. Beim Schweizerischen Nationalfonds bedanke ich mich schliesslich für die Übernahme der Kosten der Publikation im Open-Access-Format, beim Europa Institut der Universität Zürich (EIZ Publishing) für die unkomplizierte Unterstützung der Veröffentlichung der Arbeit.

Die vorliegende Arbeit wurde im Herbstsemester 2022 von der Rechtswissenschaftlichen Fakultät der Universität Zürich als Dissertation angenommen. Der Stand der letzten Bearbeitung ist der 29. Februar 2024. Kaum ein Thema des

Finanzmarktrechts hat in den letzten Jahren derart weitgehende Kontroversen ausgelöst wie die Welt rundum Bitcoin und Co. Entsprechend wurde die Arbeit seit der Einreichung im November 2021 nochmals stark überarbeitet.

Zürich, im März 2024

Fabio Andreotti

Inhaltsübersicht

Vorwort	VII
Inhaltsübersicht	IX
Inhaltsverzeichnis	XI
Literaturverzeichnis	XXIII
Materialienverzeichnis	CLVI
Abkürzungsverzeichnis	CLXXI
I. Einführung	1
1. Einleitung	1
2. Untersuchungsgegenstand	5
3. Forschungsfrage	10
4. Aufbau der Arbeit	12
II. Intermediation und Disintermediation	15
1. Grundlagen der Intermediation und Disintermediation	15
2. Ökonomische Begründung der Finanzintermediation	28
3. Formen der Disintermediation in Finanzmärkten	44
4. Decentralized Finance (DeFi)	62
5. Netzwerkbasierte Intermediation	90
6. Reintermediation als Gegenbewegung?	124
7. Zusammenfassung Kapitel II	135
III. Technische Grundlagen	139
1. Begriffliches: dezentral vs. verteilt	139
2. Dezentrale Systeme	142
3. Dezentrale Netzwerke (sog. Abwicklungsebene)	151
4. Dezentrale Applikationen (sog. Applikationsebene)	161
5. Skalierungslösungen	166
6. Zusammenfassung Kapitel III	173
IV. Dezentrale Handelsplattformen	175
1. Vorbemerkungen zur Begriffsverwendung	175
2. Einleitung und kurzer historischer Rückblick	178
3. Plattformkategorien	185
4. Gemeinsamkeiten und Unterschiede dezentraler Handelsplattformen	230
5. Chancen und Risiken	240
6. Definition einer dezentralen Handelsplattform	340
7. Zusammenfassung Kapitel IV	342
V. Rechtliche Einordnung dezentraler Handelsplattformen in das Schweizer Finanzmarktrecht	345
1. Vorbemerkungen	345
2. Geldwäschereirecht	358

3.	Finanzmarktinfrastrekturrecht	433
4.	Bankenrecht	461
5.	Finanzinstitutsrecht	479
6.	Finanzdienstleistungsrecht	488
7.	Zusammenfassung Kapitel V	509
VI.	Ansätze für die Regulierung dezentraler Handelsplattformen	515
1.	Herausforderungen für Aufsicht und Regulierung	515
2.	Unmöglichkeit eines Technologieverbots	520
3.	Anleger- und Funktionsschutz	527
4.	Marktorientierung in der Finanzmarktregulierung	535
5.	Zusammenfassung Kapitel VI	564
VII.	Dezentralität als neues Rechtsprinzip	567
1.	Dezentralität als soziotechnisches Phänomen	567
2.	Anerkennung von Dezentralität als Ordnungsprinzip	572
3.	Konkretisierung von Dezentralität in Form eines Rechtsprinzips	590
4.	Dezentralitätstest für Handelsplattformen	612
5.	Diskussion	639
6.	Zusammenfassung Kapitel VII	644
VIII.	Schlussthesen	647
1.	Dezentrale Systeme sind ein Phänomen, das zwischen Markt und Finanzmarktpolitik eingepfercht zu sein scheint	647
2.	Die Wechselhaftigkeit von Intermediation und Disintermediation bestätigt sich auch für dezentrale Systeme	649
3.	Dezentrale Systeme basieren auf eigenständigen Regelungs- und Handlungsstrukturen, weshalb sie mit der Rechtsordnung bis zu einem gewissen Grad in Konkurrenz stehen	651
4.	Der von der Finanzmarktaufsicht verfolgte funktionale Ansatz ist grundsätzlich auch für DeFi angemessen, muss aber den anders gearteten Risiken dezentraler Handelsplattformen Rechnung tragen	653
5.	Die grosse Eigenverantwortung der Nutzer macht den Einsatz von Intermediären in gewissen Situationen sinnvoll	655
6.	Das Rechtsprinzip der Dezentralität kann heute als grundsätzlich anerkannt betrachtet werden; dessen langfristige Beständigkeit ist aber fraglich	657
7.	Regulierung kann ein wichtiger Treiber der Dezentralisierung von Protokollen sein, was bei zurückhaltenden Eingriffen letztlich im Interesse der Nutzer ist	659
	Curriculum Vitae	662

Inhaltsverzeichnis

Vorwort	VII
Inhaltsübersicht	IX
Inhaltsverzeichnis	XI
Literaturverzeichnis	XXIII
Materialienverzeichnis	CLVI
Abkürzungsverzeichnis	CLXXI
I. Einführung	1
1. Einleitung	1
2. Untersuchungsgegenstand	5
3. Forschungsfrage	10
4. Aufbau der Arbeit	12
II. Intermediation und Disintermediation	15
1. Grundlagen der Intermediation und Disintermediation	15
1.1. Begriff der Intermediation	15
1.2. Intermediation und Disintermediation als ubiquitäre Phänomene	16
1.3. Finanzintermediation im Besonderen	21
1.4. Intermediation als historische Gesetzmässigkeit	24
1.5. Zentralisierung von Entscheidungsgewalt und Kontrolle	25
2. Ökonomische Begründung der Finanzintermediation	28
2.1. Begriff der Finanzintermediation	28
2.2. Eigenschaften und Bedeutung der Finanzintermediation	30
2.3. Organisationsformen	32
a. Einleitung	32
b. Markt vs. Hierarchie	32
c. ... vs. Netzwerk	35
2.4. Vorteile und Nachteile der Finanzintermediation	36
a. Kosten- und Informationsvorteile	36
b. Kontroll- und Vertrauensrisiken	39
c. Mittel zur Verringerung von Kontroll- und Vertrauensrisiken	42
3. Formen der Disintermediation in Finanzmärkten	44
3.1. Begriff der Disintermediation	44
3.2. Beispiele von Disintermediation	45
a. Asset Securitization	46
b. Crowdfunding bzw. Peer-to-Peer-Lending	47
c. Robo-Advice	48
d. DLT-Handelssysteme	49
e. Central Bank Digital Currency (CBDC)	50
3.3. Technologische Innovation als Treiberin von Disintermediation	53
a. Digitalisierung und Intermediation	53
b. FinTech im Allgemeinen	54

c.	FinTech 3.0	58
d.	Ausbleiben vollständiger Disintermediation	59
4.	Decentralized Finance (DeFi)	62
4.1.	Vorgeschichte und Vorläufer	62
a.	Cypherpunks und Hightech-Hayekians	62
b.	Digital Cash und Smart Contracts	66
i.	Kryptowährungen	66
ii.	Smart Contracts und DAOs	71
4.2.	Begriff von Decentralized Finance	75
4.3.	Abgrenzung	77
a.	Begriff der Centralized Finance	77
b.	Web 3.0	78
c.	Open Finance und Open Banking	81
4.4.	Inhalt und Umfang	82
4.5.	Dezentrale Handelsplattformen im Besonderen	86
5.	Netzwerkbasierte Intermediation	90
5.1.	Einleitung	90
5.2.	Ökonomische Eigenschaften	90
a.	Neuartige Form der wirtschaftlichen Organisation	90
b.	Überwindung kollektiver Handlungsprobleme	94
c.	Reduktion traditioneller Kontroll- und Vertrauensrisiken	97
d.	Unmittelbare Zuordnung von Handlungs- und Verfügungsrechten	98
e.	Offener Plattformwettbewerb	100
5.3.	Soziotechnische Eigenschaften	102
a.	Dezentrale Governance	102
i.	Verteiltheit des Konsenses	102
ii.	Formen dezentraler Governance	103
iii.	Bazar Governance in der Softwareentwicklung	104
iv.	Proof of Human	105
b.	Regelbasierte Systeme	106
i.	Code is Law	106
ii.	Cryptoeconomics	108
iii.	Kybernetische Dimension	111
iv.	Konstitutionelle Dimension	112
c.	Vertrauen und Komplexität	114
i.	Technologievertrauen	114
ii.	Entwicklervertrauen	116
iii.	Komplexität	118
5.4.	Fazit	122
6.	Reintermediation als Gegenbewegung?	124
6.1.	Begriff der Reintermediation	124
6.2.	Ebene der peripheren Dienstleister, insb. Hosted Wallets	125
a.	Wallet-Typen	125
b.	Wallet-Anbieter	126
6.3.	Ebene des dezentralen Netzwerks, insb. Mining Pools	128
6.4.	Ebene der traditionellen Finanzintermediation, insb. treuhänderische Strukturen	129

6.5.	Ursachen und Kritik	131
7.	Zusammenfassung Kapitel II	135
III.	Technische Grundlagen	139
1.	Begriffliches: dezentral vs. verteilt	139
2.	Dezentrale Systeme	142
2.1.	Einleitung	142
2.2.	Verteilte, gemeinschaftliche Verwaltung	142
2.3.	Offene, interoperable Protokolle	144
2.4.	Kryptografisch abgesicherte Vermögenswerte	146
a.	Kryptografische Absicherung	146
b.	Kryptowährungen (bzw. Coins)	147
c.	Token	148
3.	Dezentrale Netzwerke (sog. Abwicklungsebene)	151
3.1.	Aufbau und Struktur	151
a.	Bitcoin	151
b.	Ethereum	152
3.2.	Beteiligte Personen	153
3.3.	Konsensmechanismus	155
a.	Konsensalgorithmus	155
b.	Ablauf am Beispiel des «Nakamoto-Konsens»	156
3.4.	Governance und die Rolle von Kryptowährungen	159
4.	Dezentrale Applikationen (sog. Applikationsebene)	161
4.1.	Aufbau und Struktur	161
4.2.	Beteiligte Personen	163
a.	Im Allgemeinen	163
b.	DAOs im Besonderen	164
5.	Skalierungslösungen	166
5.1.	Layer-1-Netzwerk und ihre Trade-offs	166
5.2.	Layer-2-Netzwerke	168
a.	Einleitung	168
b.	State Channels	169
c.	Sidechains	170
d.	Rollups	171
6.	Zusammenfassung Kapitel III	173
IV.	Dezentrale Handelsplattformen	175
1.	Vorbemerkungen zur Begriffsverwendung	175
1.1.	Generische Begriffsverwendung	175
1.2.	Abweichungen zu den Publikationen des Bundesrates	175
1.3.	Synopsis	176
2.	Einleitung und kurzer historischer Rückblick	178
2.1.	Dezentrale Handelsplattformen als dezentrale Applikationen	178
2.2.	Abriss über den Meinungsstand in der Literatur	178
2.3.	Protokoll und/oder Anwendung	179
2.4.	Dezentrale Handelsplattformen als Antwort auf die Mängel zentraler Handelsplattformen	181
2.5.	Evolution dezentraler Handelsplattformen	184

3.	Plattformkategorien	185
3.1.	Einleitung	185
3.2.	Zentrale Handelsplattformen	185
a.	Custodial Handelsplattformen	185
b.	Custodial OTC-Handelsplattformen	188
3.3.	Non-custodial P2O-Handelsplattformen	188
a.	Hintergrund	188
b.	Funktionsweise am Beispiel von Shapeshift und Changelly	189
c.	Beteiligte Parteien am Beispiel von Shapeshift und Changelly	189
d.	Weiterentwicklungen	190
3.4.	Escrow-basierte P2P-Handelsplattformen	191
a.	Hintergrund	191
b.	Funktionsweise am Beispiel von Bisq	192
c.	Beteiligte Parteien am Beispiel von Bisq	194
d.	Weiterentwicklungen	194
3.5.	Atomic Swap-basierte P2P-Handelsplattformen	195
a.	Hintergrund	195
b.	Funktionsweise am Beispiel von AtomicDEX	196
c.	Beteiligte Parteien am Beispiel von AtomicDEX	197
d.	Weiterentwicklungen	198
3.6.	Smart Contract-basierte P2P-Handelsplattform	199
a.	Hintergrund	199
b.	Funktionsweise am Beispiel von EtherDelta und OasisDEX	200
c.	Beteiligte Parteien am Beispiel von EtherDelta und OasisDEX	202
d.	Weiterentwicklungen	203
3.7.	Smart Contract-basierte Liquiditätspools	206
a.	Hintergrund	206
b.	Funktionsweise am Beispiel von Uniswap	207
c.	Beteiligte Parteien am Beispiel von Uniswap	210
d.	Weiterentwicklungen	212
3.8.	Smart Contract-basierte Aggregatoren (Exkurs)	215
3.9.	Layer-2-Handelsplattformen	215
a.	Hintergrund	215
b.	Funktionsweise am Beispiel von Loopring	216
c.	Beteiligte Parteien am Beispiel von Loopring	218
d.	Weiterentwicklungen	219
3.10.	On-chain-Handelsplattformen	221
a.	Hintergrund	221
b.	Funktionsweise am Beispiel von Serum	222
c.	Beteiligte Parteien am Beispiel von Serum	223
d.	Weiterentwicklungen	224
3.11.	Hybride Handelsplattformen	225
a.	Hintergrund	225
b.	Funktionsweise am Beispiel von IDEX	225
c.	Beteiligte Parteien am Beispiel von IDEX	227
d.	Weiterentwicklungen	227
3.12.	Übersicht der Plattformkategorien	228

4.	Gemeinsamkeiten und Unterschiede dezentraler Handelsplattformen	230
4.1.	Gemeinsamkeiten	230
a.	Kontrolle über Kryptovermögenswerte	230
b.	On-chain-Handelsabwicklung	230
c.	Handelbare Vermögenswerte	231
4.2.	Unterschiede	233
a.	Orderbuch vs. Liquiditätspools	233
b.	On-chain- vs. Off-chain-Orderbuch	234
c.	Matching-Modelle	235
d.	Kassa- vs. Termingeschäfte	237
e.	Weitere Unterschiede	238
5.	Chancen und Risiken	240
5.1.	Chancen	240
a.	Einleitung	240
b.	Freie Zugänglichkeit	240
i.	Beschränkter Zugang für Retailanleger	240
ii.	Dezentrale Handelsplattformen	241
c.	Verringerung von traditionellen Gegenpartei- und Systemrisiken	242
i.	Ubiquität von Gegenparteiisiken	242
ii.	Erfüllungs-, Wiederbeschaffungs- und Liquiditätsrisiken	244
iii.	Delivery versus Payment (DvP)	245
iv.	Dezentrale Handelsplattformen	247
v.	Gegenparteiisiko bei Tokenisierung	252
d.	Gleichlauf von Verfügungsrechten und faktischer Kontrolle	252
i.	Intermediatisierte Wertpapierverwahrung	252
ii.	Direct Ownership- vs. Multi-Tiered Entitlement-Modell	255
iii.	Verwahrungsrisiken und Eigentümerintransparenz im Besonderen	257
iv.	Intermediatisierter Zahlungsverkehr	259
v.	Dezentrale Handelsplattformen	261
e.	Globale Liquidität und Transparenz	263
i.	Fragmentierter Handel	263
ii.	Fragmentierte Liquidität	264
iii.	Fragmentierte Transparenz	265
iv.	Dezentrale Handelsplattformen	266
f.	Reduktion von Rent Seeking	270
i.	Rent Seeking und Regulatory Capture	270
ii.	Dezentrale Handelsplattformen	274
5.2.	Risiken	277
a.	Einleitung	277
b.	Produktrisiken	277
c.	Transparenzrisiken	279
i.	Öffentlichkeit verteilter Register	279
ii.	Privacy by Design-Technologien	283
iii.	Frontrunning und MEV über dezentrale Handelsplattformen	289
iv.	Anti-Frontrunning-Technologien	292
d.	Informationsrisiken	297
i.	Informationsasymmetrien als Ausgangspunkt	297

ii.	Admin Keys	299
iii.	Wash Trading über dezentrale Handelsplattformen	306
iv.	Vertrauen in Benutzeroberflächen	308
e.	Smart Contract- und Plattformrisiken	308
i.	Programmierfehler	308
ii.	Hacking von Smart Contracts	310
iii.	Re-Zentralisierung von Mining und Staking	312
iv.	Kollusion von Softwareentwicklern	316
f.	Neuartige Systemrisiken	319
i.	Composability Risiko	319
ii.	Black Thursday-Risiken	324
iii.	Interdependenzen zwischen dezentralen Systemen	325
iv.	Probabilistische Finalität	326
g.	Kollektive Handlungsprobleme	329
i.	Ostroms «drei Rätsel»	329
ii.	Bereitstellung des Netzwerks	330
iii.	Governance-Risiko von dezentralen Applikationen	332
iv.	Softwareentwicklung	332
v.	Governance i.w.S.	336
h.	Rechtsunsicherheit	337
6.	Definition einer dezentralen Handelsplattform	340
6.1.	Vorbemerkungen	340
6.2.	Definitionsversuch	340
7.	Zusammenfassung Kapitel IV	342
V.	Rechtliche Einordnung dezentraler Handelsplattformen in das Schweizer Finanzmarktrecht	345
1.	Vorbemerkungen	345
1.1.	Einleitung	345
1.2.	Wirtschaftskollisionsrechtliche Aspekte	347
1.3.	Anknüpfung an den Finanzintermediär	349
1.4.	Anknüpfung an den ausländischen Finanzintermediär	352
1.5.	Anknüpfung an die arbeitsteilig vorgehende Gruppe	355
2.	Geldwäschereirecht	358
2.1.	Einleitung	358
2.2.	Geldwäscherei- und Terrorismusfinanzierungsrisiko	358
a.	Kryptowährungen	358
b.	Dezentrale Handelsplattformen	360
2.3.	FATF-Empfehlungen	362
a.	Einleitung zu VAs und VASPs	362
b.	Empfehlung Nr. 15	363
c.	Travel Rule (Exkurs)	364
d.	VASP-Guidance	370
i.	Guidance vom Juni 2019	370
ii.	Draft Guidance vom März 2021	372
iii.	Updated Guidance vom Oktober 2021	378
2.4.	Aufgreifkriterien der Finanzintermediation	382

2.5.	Dezentrale Handelsplattformen	385
a.	Definition virtueller Währungen	385
b.	Definition dezentraler Handelsplattformen	387
c.	Vorliegen einer finanzintermediären Tätigkeit?	387
d.	Keine alleinige Verfügungsmacht über fremde Vermögenswerte	391
2.6.	Analyse des revidierten Art. 4 Abs. 1 lit. b GwV	393
a.	Einleitung und Wortlaut	393
b.	Verzicht auf das Kriterium der alleinigen Verfügungsmacht über fremde Vermögenswerte	394
c.	Hilfe zur Übertragung von virtuellen Währungen	396
d.	Dauernde Geschäftsbeziehung	399
e.	Reine Vermittlungstätigkeit	402
f.	Vollständig autonome Systeme vs. reine Vermittlungstätigkeit	403
2.7.	Bereitstellung von Liquidität über dezentrale Handelsplattform	405
a.	Einleitung	405
b.	Kassageschäft	405
c.	Bargeschäft	406
d.	Handelsgeschäft	407
e.	Bemerkungen zur Technologieneutralität von Art. 51a GwV-FINMA (Exkurs)	408
2.8.	Wallet-Anbieter (Exkurs)	409
a.	Hosted Wallets	409
b.	Multisig-Wallets und verschlüsselte Wallets	409
c.	Self-Hosted Wallets	410
2.9.	Zwischenfazit	412
2.10.	Teilnahme an dezentralen Netzwerken	414
a.	Einleitung	414
b.	Netzwerkteilnehmer als Gruppe?	414
c.	Netzwerkteilnahme als Finanzintermediation?	416
d.	Lightning Netzwerk	419
2.11.	Softwareentwicklung	420
2.12.	Fazit	421
a.	Einleitung	421
b.	Bargeld, Inhaberaktien und virtuelle Währungen	421
c.	Ausdehnung des Finanzintermediationsbegriffs	422
d.	Handlungsmacht der Rechtsunterworfenen	423
e.	Überregulierung	424
f.	Wirksamkeit des heutigen Geldwäschereiregimes?	426
g.	Mögliche Handlungsalternativen	427
h.	Datenschutz und Privatsphäre	430
i.	Risiko der Bifurkation des Finanzsystems	432
3.	Finanzmarktinfrastrukturrecht	433
3.1.	Einleitung	433
3.2.	Begrifflichkeiten	433
a.	Finanzmarktinfrastruktur	433
b.	Effekten und DLT-Effekten	434

3.3.	Dezentrale Handelsplattformen als DLT-Handelssysteme?	436
a.	Vorbemerkung	436
b.	DLT-Handelssysteme	436
i.	Begriff und Konzept	436
ii.	Bemerkungen zur Technologieneutralität von Art. 73a ff. FinfraG	438
c.	Funktionale Parallelen und Unterschiede zwischen dezentralen Handelsplattformen und DLT-Handelssystemen	439
d.	Abgrenzung zu DLT-Handelssystemen	443
i.	Kein Handelssystem	443
ii.	Kein OHS (Exkurs)	445
iii.	Multilateraler Handel nach nichtdiskretionären Regeln	445
iv.	Kein Betreiber	447
v.	Keine Einrichtung	448
vi.	Keine Gewerbsmässigkeit	449
vii.	Fazit	451
3.4.	Emittenten-betriebene Handelslösungen (Exkurs)	451
3.5.	DLT-basierte Derivate und «Privacy Coins» (Exkurs)	452
3.6.	Liquiditätsgeber als Anbieter eines Wertrechtereisters (Exkurs)	453
a.	Registerwertrechte	453
b.	Wertrechtereister	454
c.	Anbiereigenschaft	456
3.7.	Dezentrale Handelsplattformen als Zentralverwahrer?	458
a.	Parallelen zu dezentralen Handelsplattformen	458
b.	Dezentrale Abrechnung und Abwicklung	459
c.	Kein Betreiber, keine Einrichtung	459
3.8.	Anbieter eines Wertrechtereisters als Effektenabwicklungssystem (Exkurs)	460
4.	Bankenrecht	461
4.1.	Einleitung	461
4.2.	Entgegennahme von Publikumseinlagen oder sammelverwahrten kryptobasierten Vermögenswerten	462
a.	Publikumseinlagen	462
i.	Im Allgemeinen	462
ii.	Virtuelle Währungen im Besonderen	464
b.	Sammelverwahrte kryptobasierte Vermögenswerte	465
c.	Individuell verwahrte kryptobasierte Vermögenswerte	468
4.3.	Aus- und Absonderbarkeit im Konkurs (Exkurs)	468
a.	Aussonderbarkeit nach Art. 242 SchKG	468
b.	Aussonderbarkeit nach Art. 242a SchKG	472
c.	Absonderbarkeit nach Art. 16 i.V.m. 37d BankG	474
d.	Fazit	474
4.4.	Keine Entgegennahme von Publikumseinlagen oder kryptobasierten Vermögenswerten durch dezentrale Handelsplattformen	475
5.	Finanzinstitutsrecht	479
5.1.	Einleitung	479
5.2.	Effektenhandel	479
a.	Im Allgemeinen	479
b.	Kein Effektenhandel durch dezentrale Handelsplattformen	481

c.	Kundenhändler	482
d.	Market Maker	482
e.	Initial Decentralized Exchange Offering (IDO)	486
6.	Finanzdienstleistungsrecht	488
6.1.	Einleitung	488
6.2.	Erbringen einer Finanzdienstleistung	490
a.	Im Allgemeinen	490
b.	Kein Erbringen einer Finanzdienstleistung durch dezentrale Handelsplattformen	490
c.	Nutzung einer dezentralen Handelsplattform	492
d.	Betrieb einer Handelsplattform als Finanzdienstleistung (Exkurs)	493
e.	Nutzung einer dezentralen Handelsplattform über einen Finanzdienstleister	494
f.	Bereitstellung von Liquidität über eine dezentrale Handelsplattform	495
g.	Vertragsrechtliche Bemerkungen (Exkurs)	499
h.	Softwareentwicklung	504
6.3.	Anbieten von Finanzinstrumenten	504
a.	Im Allgemeinen	504
b.	Bereitstellung von Liquidität über dezentrale Handelsplattformen	505
c.	Publikation von Informationen durch Frontend-Betreiber	507
7.	Zusammenfassung Kapitel V	509
VI.	Ansätze für die Regulierung dezentraler Handelsplattformen	515
1.	Herausforderungen für Aufsicht und Regulierung	515
1.1.	Herausforderungen	515
1.2.	Codebeispiel	518
1.3.	Fazit	518
2.	Unmöglichkeit eines Technologieverbots	520
2.1.	Vorbemerkungen	520
2.2.	Nutzung dezentraler Systeme	520
a.	Meinungs- und Informationsfreiheit	520
b.	Vertragsfreiheit und Privatautonomie	522
2.3.	Teilnahme an dezentralen Systemen	523
2.4.	Programmierung und Veröffentlichung von Software	524
2.5.	Fazit	526
3.	Anleger- und Funktionsschutz	527
3.1.	Anlegerschutz	527
3.2.	Funktions- und Systemschutz	529
3.3.	Implikationen für den Anleger- und Funktionsschutz	530
a.	Netzwerkbasierende Intermediation	530
b.	Traditionelle Finanzintermediäre	532
c.	Transparenz mit Vor- und Nachteilen	532
d.	Zivilrechtliche Haftung	533
4.	Marktorientierung in der Finanzmarktregulierung	535
4.1.	Einleitung	535
4.2.	Wettbewerb und Innovation	536
a.	Wettbewerb als «Regulator»	536

b.	Anlegerwohlfahrt	537
c.	Wettbewerb im FINMAG	539
4.3.	Marktorientierter Regulierungsansatz	542
a.	Begründung	542
b.	Inhalt und Umfang	542
c.	Vorschläge in Bezug auf dezentrale Handelsplattformen	543
i.	Übersicht der Regulierungsansätze	543
ii.	Anerkennung dezentraler Systeme als öffentlicher Koordinationsmechanismus	544
iii.	Anreize zur Kooperation	546
iv.	Offenlegungsregime auf der Grundlage von Verhaltenskodizes	548
v.	Investor Education	557
vi.	Öffnung dezentraler Systeme für traditionelle Finanzintermediäre	560
4.4.	Fazit	562
5.	Zusammenfassung Kapitel VI	564
VII.	Dezentralität als neues Rechtsprinzip	567
1.	Dezentralität als soziotechnisches Phänomen	567
1.1.	Einleitung	567
1.2.	Mittel zum Zweck	568
1.3.	Nutzen von Dezentralität	569
2.	Anerkennung von Dezentralität als Ordnungsprinzip	572
2.1.	Vorbemerkung	572
2.2.	Parallele zum Wettbewerb als Ordnungsprinzip	572
2.3.	Dezentralität im Verfassungsrecht	573
a.	Einleitung	573
b.	Wirtschaftsordnung	573
c.	Politische Ordnung	574
2.4.	Dezentralität im Zivilrecht	575
a.	Privatautonomie	575
b.	Konzernrecht	576
2.5.	Dezentralität im Wertpapier- und Finanzmarktrecht	577
a.	Einleitung	577
b.	Gründe für eine Anerkennung	577
c.	Anerkennung dezentraler Netzwerke	579
i.	Wertpapierrecht	579
ii.	Finanzmarktrecht	581
d.	Anerkennung dezentraler Applikationen und insb. dezentraler Handelsplattformen	582
2.6.	Steuerrecht	584
2.7.	Politischer und regulatorischer Kurswechsel?	585
3.	Konkretisierung von Dezentralität in Form eines Rechtsprinzips	590
3.1.	Rechtsprinzip	590
a.	Begriff und Normativität	590
b.	Konsequenzen eines solchen Rechtsprinzips	591
c.	Feststellung der Konkretisierungsbedürftigkeit	592

3.2.	Dezentralitätstest	593
a.	Vorschlag eines «Dezentralitätstests» in Lehre und Praxis	593
b.	Vertrauensminimierung	595
c.	Entmachtung bzw. Kontrollverteilung	597
i.	Einleitung	597
ii.	Machtbereiche	597
d.	Fazit	601
3.3.	Konkretisierung der Dezentralität am Beispiel eines dezentralen Netzwerks	603
a.	Vorbemerkung	603
b.	Vielzahl von Netzwerkteilnehmern	603
c.	Unabhängigkeit der Netzwerkteilnehmer	604
d.	Manipulationsresistenz von Daten	607
e.	Publizität von Code und Daten	609
f.	Belastbarkeit der kryptoökonomischen Anreize	610
g.	Fazit	611
4.	Dezentralitätstest für Handelsplattformen	612
4.1.	Vorbemerkungen	612
4.2.	Funktionaler Dezentralitätstest	613
a.	Hauptfunktionen	613
i.	Einleitung	613
ii.	Systemfunktionen	614
iii.	Technische Handelsfunktionen	615
iv.	Politökonomische Funktionen	616
b.	Nebenfunktionen	618
i.	Einleitung	618
ii.	Softwareentwicklung	618
iii.	Benutzeroberfläche	620
iv.	Immaterialgüterrechte	623
v.	Gebühren	625
4.3.	Notwendigkeit einer Gesamtbetrachtung der Funktionen	626
4.4.	Rechtsfolgen des Dezentralitätstests	628
a.	Vorbemerkungen	628
b.	Bei Bestehen des Dezentralitätstests	628
c.	Bei Nichtbestehen des Dezentralitätstests	629
d.	Abschliessende Bemerkungen	630
4.5.	Einstufung der unterschiedlichen Plattformkategorien	630
a.	Vorbemerkungen	630
b.	Custodial und Custodial OTC-Handelsplattformen	631
c.	Non-custodial P2O-Handelsplattformen	632
d.	Escrow-basierte P2P-Handelsplattformen	632
e.	Atomic Swap-basierte P2P-Handelsplattformen	633
f.	Smart Contract-basierte P2P-Handelsplattformen	634
g.	Smart Contract-basierte Liquiditätspools	635
h.	Smart Contract-basierte Aggregatoren	636
i.	Layer-2-Handelsplattformen	636
j.	On-chain-Handelsplattformen	637
k.	Hybride Handelsplattformen	638

5. Diskussion	639
6. Zusammenfassung Kapitel VII	644
VIII. <u>Schlussthesen</u>	647
1. <u>Dezentrale Systeme sind ein Phänomen, das zwischen Markt und Finanzmarktpolitik eingepfercht zu sein scheint</u>	647
2. <u>Die Wechselhaftigkeit von Intermediation und Disintermediation bestätigt sich auch für dezentrale Systeme</u>	649
3. <u>Dezentrale Systeme basieren auf eigenständigen Regelungs- und Handlungsstrukturen, weshalb sie mit der Rechtsordnung bis zu einem gewissen Grad in Konkurrenz stehen</u>	651
4. <u>Der von der Finanzmarktaufsicht verfolgte funktionale Ansatz ist grundsätzlich auch für DeFi angemessen, muss aber den anders gearteten Risiken dezentraler Handelsplattformen Rechnung tragen</u>	653
5. <u>Die grosse Eigenverantwortung der Nutzer macht den Einsatz von Intermediären in gewissen Situationen sinnvoll</u>	655
6. <u>Das Rechtsprinzip der Dezentralität kann heute als grundsätzlich anerkannt betrachtet werden; dessen langfristige Beständigkeit ist aber fraglich</u>	657
7. <u>Regulierung kann ein wichtiger Treiber der Dezentralisierung von Protokollen sein, was bei zurückhaltenden Eingriffen letztlich im Interesse der Nutzer ist</u>	659
<u>Curriculum Vitae</u>	662

Literaturverzeichnis

- Ox Core Team, Post-mortem: Ox v2.0 Exchange Vulnerability, 18. Juli 2019, <https://blog.oxproject.com/post-mortem-ox-v2-0-exchange-vulnerability-763015399578>
- Ox, Ox Legal Guide, Federal Anti-Money Laundering Regulation, undatiert, <https://0x.org/docs/guides/legal-guide#federal-anti-money-laundering-regulation>
- Ox, Core Concepts, Extending the Ox protocol, undatiert, <https://0x.org/docs/core-concepts#extending-the-0x-protocol>
- Ox, Core Concepts, Networked liquidity, undatiert, <https://0x.org/docs/core-concepts#networked-liquidity>
- Ox, Core Concepts, Off-chain relay, on-chain settlement, undatiert, <https://0x.org/docs/core-concepts#off-chain-relay-on-chain-settlement>
- Ox, Market-making on Ox, Fetching off-chain orders, undatiert, <https://0x.org/docs/guides/market-making-on-0x#fetching-off-chain-orders>
- Ox, ZRX Portal FAQ, How are liquidity rewards calculated?, undatiert, <https://0x.org/docs/guides/zrx-portal-faq#how-are-liquidity-rewards-calculated>
- 1inch, 1inch API, undatiert, <https://docs.1inch.io/api/>
- 21 Analytics, 21 Analytics Enables the First Automated Travel Rule Compliant Bitcoin Transaction, 21. August 2020, <https://www.21analytics.ch/blog/21-analytics-enables-the-first-automated-travel-rule-compliant-bitcoin-transaction-in-switzerland>
- 21 Analytics, Swiss Regulator Further Reduces Threshold for Buying Bitcoin KYC-less, 20. August 2021, <https://www.21analytics.ch/blog/swiss-regulator-further-reduces-threshold-for-buying-bitcoin-kyc-less>
- 21Shares, Digital Asset ETPs, undatiert, <https://21shares.com/de/product>
- van Aaken Anne, Normative Grundlagen der ökonomischen Theorie im öffentlichen Recht, in: van Aaken Anne/Schmid-Lübbert Stefanie (Hrsg.), Beiträge zur ökonomischen Theorie im Öffentlichen Recht, Wiesbaden 2003, 89–118
- Aave, Arc. An Introduction to Aave Arc, undatiert, <https://github.com/aave/protocol-v2/blob/feat/permissioned-market/aave-arc-whitepaper.pdf>
- Aave, Introducing Aave Arc, 18. November 2021, https://aave.mirror.xyz/JcA9DzQHK6o8YYMmxT43Vqq5HoHvjTrFnd_UprKWQ?s
- Aave, Protocol Whitepaper V1.0, Januar 2020, https://github.com/aave/aave-protocol/blob/master/docs/Aave_Protocol_Whitepaper_v1_0.pdf
- Abadi Joseph/Brunnermeier Markus, Blockchain Economics, NBER Working Paper 25407, Dezember 2019, <http://www.nber.org/papers/w25407>

- Abbühl Andri, Effektenqualität von Blockchain-Token. Überlegungen zur FINMA-Wegleitung und Prospektpflicht, iusNet BR-KR 23.12.2021
- Abegg Andreas/Bärtschi Harald/Dietrich Andreas (Hrsg.), Prinzipien des Finanzmarktrechts. Einführung in das Finanzmarktrecht mit Repetitionsfragen und Fällen samt Lösungen sowie Literaturübersicht, RWP 5, 3. Aufl., Zürich/Basel/Genf 2019 (Autor, in: Abegg/Bärtschi/Dietrich, § Rz.)
- Abegg Philipp, Rechtliche Risiken im grenzüberschreitenden Zahlungsverkehr, in: Emenegger Susan (Hrsg.), Cross-Border Banking, SBT 2009, Basel 2009, 105–129
- Abegglen Sandro, Der Bankkonzern in der Schnittmenge von Privat- und Aufsichtsrecht; zugleich zur Rechenschafts- und Ablieferungspflicht bei bankkonzerninternen Vergütungen, in: Kunz Peter V./Herren Dorothea/Cottier Thomas/Matteoti René (Hrsg.), Wirtschaftsrecht in Theorie und Praxis. Festschrift für Roland von Büren, Basel 2009, 657–690
- Abegglen Sandro/Andreotti Fabio, Best Execution gemäss FIDLEG. Eine privat- und aufsichtsrechtliche Betrachtung, GesKR 2020, 36–59
- Abegglen Sandro/Luterbacher Léonie, Das Verhältnis der FIDLEG-Verhaltensregeln zum Privatrecht, ZSR 2020 I, 223–252
- Abegglen Sandro/Wettstein Yannick, Zum Anbieten kollektiver Kapitalanlagen unter dem FIDLEG – und ausgewählte Aspekte der dabei einzuhaltenden Verhaltenspflichten, SZW 2018, 131–146
- Abramowicz Michael, Cryptocurrency-Based Law, Arizona Law Review 2016, 359–420
- Acharya Viral V./Anginer Deniz/Warburton A. Joseph, The End of Market Discipline? Investor Expectations of Implicit Government Guarantees, 1. Mai 2016, <https://ssrn.com/abstract=1961656>
- Acheson Noelle, Crypto Long & Short: How Bitcoin Development Is Evolving – And What's Behind It, 29. November 2020, <https://www.coindesk.com/markets/2020/11/29/crypto-long-short-how-bitcoin-development-is-evolving-and-whats-behind-it/>
- Achleitner Ann-Kristin, Handbuch Investment Banking, 3. Aufl., Wiesbaden 2002
- Ackermann Jürg-Beat/Zehnder Stephanie, Art. 305bis StGB – Geldwäscherei, in: Ackermann Jürg-Beat (Hrsg.), Kommentar Kriminelles Vermögen – Kriminelle Organisation. Einziehung, Kriminelle Organisation, Finanzierung des Terrorismus, Geldwäscherei, Bd. II, Zürich/Basel/Genf 2018
- Cochran Adam, 1. Oktober 2020, <https://twitter.com/AdamScochran/status/1311729888399896577>
- Back Adam, Hashcash – A Denial of Service Counter-Measure, 1. August 2002, www.hashcash.org/hashcash.pdf
- Adams Hayden, Uniswap Whitepaper, undatiert, <https://hackmd.io/@HaydenAdams/HJ9jLsfTz#%F0%9F%A6%84-Uniswap-Whitepaper>

-
- Adams Hayden/Zinsmeister Noah/Robinson Dan, Uniswap v2 Core, März 2020, <https://uniswap.org/whitepaper.pdf>
- Adams Hayden/Zinsmeister Noah/Salem Moody/Keefer River/Robinson Dan, Uniswap v3 Core, März 2021, <https://uniswap.org/whitepaper-v3.pdf>
- Admati Anat/Hellwig Martin, The Bankers' New Clothes. What's Wrong with Banking and What to Do about It, Princeton/Oxford 2017
- Adrian Reinhold/Heidorn Thomas, Der Bankbetrieb. Lehrbuch und Aufgaben, 15. Aufl., Wiesbaden 2000
- Aebi-Müller Regina E./Müller Christoph (Hrsg.), Berner Kommentar. Art. 1-18 OR mit allgemeiner Einleitung in das Schweizerische Obligationenrecht, Bern 2018 (Autor, in: BK OR, Art. N)
- Aghion Philippe/Bloom Nick/Blundell Richard/Griffith Rachel/Howitt Peter, Competition and Innovation: An Inverted-U Relationship, The Quarterly Journal of Economics 2005, 701-728
- Agrawal Neeraj, Making sense of Lightning network nodes and money transmission licensing, 4. Januar 2018, <https://www.coincenter.org/making-sense-of-lightning-network-nodes-and-money-transmission-licensing/>
- Ahn T. K./Ostrom Elinor, Social capital and collective action, in: Castiglione Dario/van Deth Jan W./Wolleb Guglielmo (Hrsg.), The Handbook of Social Capital, Oxford/New York 2008, 70-100
- AirSwap, FAQ, How does trading on AirSwap work?, undatiert, <https://support.airswap.io/en/articles/3778594-how-does-trading-on-airswap-work>
- Akentiiev Anthony, Parity Multisig Hacked. Again, Parity Multisig Hacked. Again, 8. November 2017, <https://medium.com/chain-cloud-company-blog/parity-multisig-hack-again-b46771eaa838>
- Akerlof George A., The Market for «Lemons»: Qualitative Uncertainty and the Market Mechanism, The Quarterly Journal of Economics 1970, 488-500
- Aktionariat, Brokerbot, undatiert, <https://aktionariat.com/brokerbot.html>
- Alchian Armen A., Property Rights, in: The New Palgrave Dictionary of Economics, 3. Aufl., London 2018, 10892-10897
- Alchian Armen A., Some Economics of Property Rights, Il Politico 1965, 816-829
- Alchian Armen A./Demsetz Harold, Production, Information Costs, and Economic Organization, The American Economic Review 1972, 777-795
- Alchian Armen A./Demsetz Harold, The Property Right Paradigm, The Journal of Economic History 1973, 16-27
- Alethena, Share-Dispenser-ServiceHunter, undatiert, <https://github.com/Alethena/Share-Dispenser-ServiceHunter>

- Ali Robleh D./Haldane Andrew G./Nahai-Williamson Paul, Towards a common financial language, Paper presented at the Securities Industry and Financial Markets Association (SIFMA) «Building a Global Legal Entity Identifier Framework» Symposium, New York, 14. März 2012
- Aliber Robert Z./Kindleberger Charles P., Maniacs, Panics, and Crashes. A History of Financial Crises, 7. Aufl., Hampshire/New York 2015
- Allen Darcy W.E./Berg Chris/Markey-Towler Brendan/Novak Mikayla/Potts Jason, Blockchain and the evolution of institutional technologies: Implications for innovation policy, Research Policy 2020, 1–8
- Allen Darcy W.E./Berg Chris/Novak Mikayla, Blockchain: an entangled political economy approach, Journal of Public Finance and Public Choice 2018, 105–125
- Allen Douglas W., What Are Transaction Costs?, in: Zerbe Richard O. (Hrsg.), Research in Law and Economics, Bd. 14, Greenwich 1991, 1–18
- Allen Franklin, The Market for Information and the Origin of Financial Intermediation, Journal of Financial Intermediation 1990, 1–30
- Allen Franklin/Gale Douglas, Financial Contagion, Journal of Political Economy 2000, 1–33
- Alloway Tracy/Weisenthal Joe, Benoît Cœuré on Central Bank Digital Currencies and the Future of Monetary Policy, 22. Oktober 2020, <https://www.bloomberg.com/news/articles/2020-10-22/beno-t-c-ur-on-central-bank-digital-currencies-and-the-future-of-monetary-policy>
- Alpar Paul/Alt Rainer/Bensberg Frank/Weimann Peter, Anwendungsorientierte Wirtschaftsinformatik. Strategische Planung, Entwicklung und Nutzung von Informationssystemen, 9. Aufl., Wiesbaden 2019
- Alt Rainer/Puschmann Thomas, Digitalisierung der Finanzindustrie. Grundlagen der Fintech-Revolution, Berlin Heidelberg 2016
- Altschuler Samantha, Should Centralized Exchange Regulations Apply to Cryptocurrency Protocols?, Stanford Journal of Blockchain Law & Policy 2022, 92–113
- Amico Jeff, Open Sourcing Our Token Delegate Program, 26. August 2021, <https://a16z.com/2021/08/26/open-sourcing-our-token-delegate-program/>
- Amler Hendrik/Eckey Lisa/Faust Sebastian/Kaiser Marcel/Sandner Philipp/Schlosser Benjamin, DeFi-ning DeFi: Challenges & Pathway, 14. Januar 2021, <https://arxiv.org/abs/2101.05589>
- Ammori Marvin, Decentralized Finance: What It is, Why It Matters, 15. Juni 2021, <https://future.a16z.com/cryptos-fourth-wave-defi-poised-for-breakthrough/>
- Ammous Saifedean, The Bitcoin Standard: The Decentralized Alternative to Central Banking, Hoboken 2018

- Amores-Sesar Ignacio/Cachin Christian/Mićić Jovana, Security Analysis of Ripple Consensus, in: Bramas Quentin/Oshman Rotem/Romano Paolo (Hrsg.), 24th International Conference on Principles of Distributed Systems (OPODIS 2020), LIPIcs 184, Saarbrücken/Wadern 2021, 10:1–10:16
- Ampleforth, Ampleforth «Geysers», undatiert, <https://www.ampleforth.org/dapps/>
- Amstutz Marc, Konzernorganisationsrecht 2.0, SZW 2016, 2–20
- Ancelle Juliette/Fischer Philipp, Regulation of Crowdfunding Activities in Switzerland: Where do we Stand?, Jusletter vom 22. Februar 2016
- Andreessen Marc, Why Bitcoin Matters, 21. Januar 2014, <https://dealbook.nytimes.com/2014/01/21/why-bitcoin-matters/>
- Andreoni James/Miller John H., Rational Cooperation in the Finitely Repeated Prisoner's Dilemma: Experimental Evidence, The Economic Journal 1993, 570–585
- Andreotti Fabio, Finanzmarktrechtliche Produktverbote: Anwendungsbereich und Grenzen aus rechtlicher und ökonomischer Sicht, 30. Juni 2014, <https://ssrn.com/abstract=3006035>
- Andreotti Fabio, § 11 Handel und Handelsplattformen, in: Zellweger-Gutknecht Corinne/Tschudi Dominik/MacCabe Kevin (Hrsg.), Handbuch Kryptowerte, Basel 2024 (im Erscheinen)
- Andreotti Fabio, Institutionelle Freiräume dank dezentraler Governance?, in: Kessler Olivier (Hrsg.), Liberalismus 2.0. Wie neue Technologien der Freiheit Auftrieb verleihen, Zürich 2021, 125–143
- Andreotti Fabio, Das Bitcoin Lightning Netzwerk – Einführung und rechtliche Einordnung von LNBTC und der Teilnahme am Netzwerk (Teil 1), iusNet BR-KR 22.12.2022
- Andreotti Fabio, Das Bitcoin Lightning Netzwerk – Einführung und rechtliche Einordnung von LNBTC und der Teilnahme am Netzwerk (Teil 2), iusNet BR-KR 22.12.2022
- Andreotti Fabio/Zimmermann Stephan/Prantl Florian, Custodial Staking. Eine Einordnung in das Schweizer Finanzmarktrecht, GesKR 2023, 333–354
- Androulaki Elli/Karame Ghassan O./Roeschlin Marc/Scherer Tobias/Capkun Srdjan, Evaluating User Privacy in Bitcoin, in: Sadeghi Ahmad-Reza (Hrsg.), Financial Cryptography and Data Security, LNCS 7859, Berlin/Heidelberg 2013, 34–51
- di Angelo Monika/Salzer Gernot, Tokens, Types, and Standards: Identification and Utilization in Ethereum, in: Xu Jie/Schulte Stefan/Ruppel Peter/Küpper Axel/Jadav Divyesh (Hrsg.), 2020 IEEE International Conference on Decentralized Applications and Infrastructures (DAPPS), Danvers/Piscataway 2020, 1–10
- Angeris Guillermo/Chitra Tarun, Improved Price Oracles: Constant Function Market Makers, AFT '20: Proceedings of the Second ACM Conference on Advances in Financial Technologies 2020, 80–91

- Angeris Guillermo/Kao Hsien-Tang/Chiang Rei/Noyes Charlie/Chitra Tarun, An Analysis of Uniswap markets, *Cryptoeconomic Systems* 2021, 1–30
- Ankenbrand Thomas/Bieri Denis, Architekturrahmen für Open Banking und Open Finance, 17. September 2020, <https://www.swissbanking.org/de/themen/digitalisierung/openbanking/blogparade/architekturrahmen-fuer-open-finance-banking>
- Anker-Sørensen Linn/Zetzsche Dirk A., From Centralized to Decentralized Finance: The Issue of «Fake-DeFi», 22. Dezember 2022, <https://ssrn.com/abstract=3978815>
- Antonopoulos Andreas M., Cargo Class Bitcoin with PayPal [PayPal Bitcoin isn't Bitcoin], 1. Dezember 2020, <https://youtu.be/C4OIUEaW5Jc>
- Antonopoulos Andreas M., *Mastering Bitcoin. Programming the Open Blockchain*, 2. Aufl., Sebastopol 2017
- Antonopoulos Andreas M., *The Internet of Money. A Collection of Talks by Andreas M. Antonopoulos*, Bd. 1, 2017, <https://theinternetofmoney.info/>
- Antonopoulos Andreas M./Wood Gavin, *Mastering Ethereum. Building Smart Contracts and DApps*, Sebastopol 2019
- Aquilina Matteo/Frost Jon/Schrimpf Andreas, Addressing the risks in crypto: laying out the options, *BIS Bulletin* Nr. 66, 12. Januar 2023
- Aragon Network, Whitepaper, 18. Juli 2019, <https://github.com/aragon/whitepaper>
- Aragon Wiki, undatiert, <https://wiki.aragon.org/>
- Aramonte Sirio/Huang Wenqian/Schrimpf Andreas, DeFi risks and the decentralisation illusion, *BIS Quarterly Review* Dezember 2021, 21–36
- Aref Magda/Fábián Luca/Weber Simon, Digitale Originale dank NFTs? Rechtliche Analyse einer (angeblichen) Revolution, *GesKR* 2021, 385–399
- Arias Leo, List of Ethereum Smart Contracts Post-Mortems, undatiert, <https://forum.openzeppelin.com/t/list-of-ethereum-smart-contracts-post-mortems/>
- Aristoteles, Politik, in: Ursula Wolf (Hrsg.), *Aristoteles, Politik*, rowohlt's enzyklopädie, 4. Aufl., Hamburg 2014
- Arluck Jacob, Amending Tezos, 29. November 2018, <https://medium.com/tezos/amending-tezos-b77949d97e1e>
- von Arnould Andreas, *Völkerrecht*, 3. Aufl., Heidelberg 2016
- Arner Douglas W./Avgouleas Emilios/Busch Danny/Schwarcz Steven L. (Hrsg.), *Systemic Risk in the Financial Sector. Ten Years after the Great Crash, Waterloo* 2019
- Arner Douglas W./Barberis János/Buckley Ross P., *The Evolution of FinTech: A New Post-Crisis Paradigm*, University of New South Wales Law Research Series 2016, Nr. 62, 19. Dezember 2019, <https://ssrn.com/abstract=2676553>

- Arner Douglas/Auer Raphael/Frost Jon, Stablecoins: risks, potential and regulation, BIS Working Papers Nr. 905, November 2020
- Arrow Kenneth J., Economic Welfare and the Allocation of Resources for Invention, in: National Bureau of Economic Research (Hrsg.), The Rate and Direction of Inventive Activity: Economic and Social Factors, Princeton 1962, 609–626
- Arrow Kenneth J., The Organization of Economic Activity: Issues Pertinent to the Choice of Market versus Nonmarket Allocation, in: Haveman Robert H./Margolis Julius (Hrsg.), Public Expenditures and Policy Analysis, Chicago 1970, 500–518
- Arrow Kenneth J., Uncertainty and the Welfare Economics of Medical Care, The American Economic Review 1963, 941–973
- Arrow Kenneth J./Forsythe Robert/Gorham Michael/Hahn Robert/Hanson Robin/Ledyard John O./Levmore Saul/Litan Robert/Milgrom Paul/Nelson Forrest D./Neumann George R./Ottaviani Marco /Schelling Thomas C./Shiller Robert J./Smith Vernon L./Snowberg Erik/Sunstein Cass R./Tetlock Paul C./Tetlock Philip E./Varians Hal R./Wolfers Justin/Zitzewitz Eric, The Promise of Prediction Markets, Science 2008, 877–878
- Arruñada Benito, Blockchain's Struggle to Deliver Impersonal Exchange, Minnesota Journal of Law, Science & Technology 2018, 55–105
- Arruñada Benito, Prospects of Blockchain in Contract and Property, European Property Law Journal 2020, 231–259
- Arslanian Henri/Fischer Fabrice, The Future of Finance. The Impact of FinTech, AI, and Crypto on Financial Services, Cham 2019
- Arter Oliver/Jörg Florian S., Informationspflichten beim Discount-Brokerage, AJP 2001, 52–68
- Arthur Terry/Booth Philipp, Does Britain Need a Financial Regulator? Statutory Regulation, Private Regulation and Financial Markets, London 2010
- Arthur W. Brian, Complexity and the Economy, in: W. Brian Arthur (Hrsg.), Complexity and the Economy, Oxford/New York 2015, 182–188
- Arthur W. Brian, Complexity Economics. A Different Framework for Economic Thought, in: W. Brian Arthur (Hrsg.), Complexity and the Economy, Oxford/New York 2015, 1–29
- ARTICLE 19, Blockchain and freedom of expression, London 2019, <https://www.article19.org/wp-content/uploads/2019/07/Blockchain-and-FOE-v4.pdf>
- Arzt Gunther, Das missglückte Strafgesetz – am Beispiel der Geldwäschegesetzgebung, in: Diederichsen Uwe/Dreier Ralf R. (Hrsg.), Das missglückte Gesetz. 8. Symposium der Kommission «Die Funktion des Gesetzes in Geschichte und Gegenwart», Göttingen 1997, 17–38
- Arzt Gunther, Steuerdelikte als Vortat – Verkommt der Kampf gegen Geldwäscherei zum Vorwand? Kritik aus der Wissenschaft, ST 2011, 268–274

- Assange Julian, Cypherpunks. Freedom and the Future of the Internet. With Jacob Appelbaum, Andy Müller-Maguhn and Jérémie Zimmermann, New York/London 2012
- Atik Jeffery/Gerro George, Hard Forks on the Bitcoin Blockchain: Reversible Exit, Continuing Voice, Stanford Journal of Blockchain Law & Policy 2018, 24–40
- Attack Jeremy, Financial innovations and crises: The view backwards from Northern Rock, in: Attack Jeremy/Neal Larry (Hrsg.), The Origins and Development of Financial Markets and Institutions. From the Seventeenth Century to the Present, Cambridge/New York 2009, 1–31
- Attah Elikem, Five most prolific 51% attacks in crypto: Verge, Ethereum Classic, Bitcoin Gold, Feathercoin, Vertcoin, 24. April 2019, <https://cryptoslate.com/prolific-51-attacks-crypto-verge-ethereum-classic-bitcoin-gold-feathercoin-vertcoin/>
- Atzei Nicola/Bartoletti Massimo/Cimoli Tiziana, A Survey of Attacks on Ethereum Smart Contracts (SoK), in: Maffei Matteo/Ryan Mark (Hrsg.): Principles of Security and Trust, LNCS 10204, Berlin/Heidelberg 2017, 164–186
- Auer Raphael, Beyond the doomsday economics of «proof-of-work» in cryptocurrencies, BIS Working Papers Nr. 765, Januar 2019
- Auer Raphael, Embedded supervision: how to build regulation into decentralised finance, BIS Working Papers Nr. 811, September 2019 (revised May 2022)
- Auer Raphael/Böhme Rainer, The technology of retail central bank digital currency, BIS Quarterly Review März 2020, 85–100
- Auer Raphael/Cornelli Giulio/Frost Jon, Rise of the central bank digital currencies: drivers, approaches and technologies, BIS Working Papers Nr. 880, August 2020
- Auer Raphael/Farag Marc/Lewrick Ulf/Orazem Lovrenc/Zoss Marcus, Banking in the shadow of Bitcoin? The institutional adoption of cryptocurrencies, BIS Working Papers Nr. 1013, Mai 2022
- Auer Raphael/Frost Jon/Vidal Pastor Jose Maria, Miners as intermediaries: extractable value and market manipulation in crypto and DeFi, BIS Bulletin Nr. 58, 16. Juni 2022
- Auer Raphael/Haslhofer Bernhard/Kitzler Stefan/Saggese Pietro/Victor Friedhelm, The Technology of Decentralized Finance (DeFi), BIS Working Papers Nr. 1066, 17. Januar 2023
- Augur, The Ultimate Guide to Decentralized Prediction Markets, 2018, <https://www.augur.net/blog/prediction-markets/>
- Aurora Labs, IDEX: A Real-Time and High-Throughput Ethereum Smart Contract Exchange, Version 0.7.6, 23. Januar 2019, <https://blog.idex.io/resources/idex-white-paper>
- Avan-Nomayo Osato, DeFi hacks and exploits total \$285M since 2019, Messari reports, 29. April 2021, <https://cointelegraph.com/news/defi-hacks-and-exploits-total-285m-since-2019-messari-reports>

- Avgouleas Emilios, Governance of Global Financial Markets. The Law, The Economics, The Politics, Cambridge/New York 2012
- Avgouleas Emilios/Kiayias Aggelos, The Promise of Blockchain Technology for Global Securities and Derivatives Markets: The New Financial Ecosystem and the 'Holy Grail' of Systemic Risk Containment, European Business Organization Law Review 2019, 81–110
- Awrey Dan, Complexity, Innovation, and the Regulation of Modern Financial Markets, Harvard Business Law Review 2012
- Axelrod Robert, The Complexity of Cooperation. Agent-based Models of Competition and Collaboration, Princeton 1997
- Axelrod Robert, The Evolution of Cooperation, New York 1984
- Azouvi Sarah/Hicks Alexander, SoK: Tools for Game Theoretic Models of Security for Cryptocurrencies, Cryptoeconomic Systems 2020, 1–44
- Bacharach Jeremy, La Communication 02/19 a-t-elle une base légale suffisante?, 2. September 2019, <https://cdbf.ch/1082/>
- Back Adam/Corallo Matt/Dashjr Luke/Friedenbach Mark/Maxwell Gregory/Miller Andrew/Poelstra Andrew/Timón Jorge/Wuille Pieter, Enabling Blockchain Innovations with Pegged Sidechains, 22. Oktober 2014, <https://www.blockstream.com/sidechains.pdf>
- Bacon Jean/David Michels Johan/Millard Christopher/Singh Jatinder, Blockchain Demystified: A Technical and Legal Introduction to Distributed and Centralised Ledgers, Richmond Journal of Law & Technology 2018, 1–106
- Badertscher Christian/Garay Juan/Maurer Ueli/Tschudi Daniel/Zikas Vassilis, But Why Does It Work? A Rational Protocol Design Treatment of Bitcoin, in: Nielsen Jesper Buus/Rijmen Vincent (Hrsg.), Advances in Cryptology – EUROCRYPT 2018, Cham 2018, LNCS 10821, 34–65
- Bagehot Walter, Lombard Street: A Description of the Money Market, Westport 1962
- Bahar Rashid/Nedwed Bianca, Grenzüberschreitendes Angebot von Finanzdienstleistungen und -produkten? Die Eidgenossenschaft schlägt zurück, SZW 2019, 618–638
- Bahar Rashid/Watter Rolf (Hrsg.), Basler Kommentar zum Finanzdienstleistungsgesetz/Finanzinstitutsgesetz, Basel 2023 (BSK FIDLEG/FINIG-Autor, Art. N)
- Bainbridge Stephen M., Dodd-Frank: Quack Federal Corporate Governance Round II, Minnesota Law Review 2011, 1779–1821
- Bainbridge Stephen M., Mandatory Disclosure: A Behavioral Analysis, University of Cincinnati Law Review 2000, 1023–1060
- Baisch Rainer, Basisinformationsblatt: Gute Produktinformation oder «Bett des Prokrustes»? , in: Grosz Mirina/Grünwald Seraina (Hrsg.), Recht und Wandel. Festschrift für Rolf H. Weber, Zürich/Basel/Genf 2016, 295–324

- Baisch Rainer/Baumann Simone/Weber Rolf H., «Shades of Grey» in Dark Pools, GesKR 2014, 183–198
- Baisch Rainer/Weber Rolf H., Prophylaxe durch Transparenz, in: Sethe Rolf/Thorsten Hens/von der Crone Hans Caspar/Weber Rolf H. (Hrsg.), Anlegerschutz im Finanzmarktrecht kontrovers diskutiert, SSFM 108, Zürich/Basel/Genf 2013, 169–211
- Balaji Arjun/Hasu, Grin and the Mythical Fair Launch. Grading Grin among a sea of cryptocurrency distribution models, 25. Januar 2019, <https://medium.com/@arjunblj/grin-and-the-mythical-fair-launch-395ca87a5e73>
- Balancer, Creating a Shared Pool, Shared Pool Creation, undatiert, <https://docs.balancer.finance/guides/creating-a-balancer-pool#shared-pool-creation>
- Balancer, FAQ, Basics, What is the Balancer Protocol?, undatiert, <https://docs.balancer.finance/getting-started/faq#what-is-the-balancer-protocol>
- Bancor Network, Introduction, undatiert, <https://docs.bancor.network/>
- Bancor, Bancor Help Center, FAQ, Service Restrictions, undatiert, <https://support.bancor.network/hc/en-us/articles/360030304352-Service-Restrictions>
- Bancor, Bancor Help Center, FAQ, Service Restrictions, undatiert, <https://support.bancor.network/hc/en-us/articles/360030304352-Service-Restrictions>
- Bandi-Lang Anna-Naomi/Mauchle Yves/Spoerlé Philip, Bucheffekten auf der Blockchain, GesKR 2021, 238–248
- Bankless, 66 – Crypto’s Existential Threat | MEV Panel: Phil Daian, Georgios Konstantopolus, Charlie Noyes, 24. Mai 2021, <http://podcast.banklessHQ.com/66-cryptos-existential-threat-mev-panel-phil-daian-georgios-konstantopolus-charlie-noyes>
- Banks Erik, The Palgrave Macmillan Dictionary of Finance, Investment and Banking, London/New York 2010
- Bar-Yam Yaneer, Dynamics of Complex Systems, Reading 1997
- Barabas Chelsea/Narula Neha/Zuckerman Ethan, Defending Internet Freedom through Decentralization: Back to the Future?, The Center for Civic Media & The Digital Currency Initiative MIT Media Lab, August 2017, https://dc.mit.edu/s/decentralized_web.pdf
- Barber Simon/Boyen Xavier/Shi Elaine/Uzun Ersin, Bitter to Better – How to Make Bitcoin a Better Currency, in: Keromytis Angelos D. (Hrsg.), Financial Cryptography and Data Security, LNCS 7397, Berlin/Heidelberg 2012, 399–414
- Barczentewicz Mikołaj, MEV on Ethereum: A Policy Analysis, International Center for Law & Economics (ICLE), 23. Januar 2023
- Barlow John Perry, A Declaration of the Independence of Cyberspace, in: Ludlow Peter (Hrsg.), Crypto Anarchy, Cyberstates, and Pirate Utopias, Cambridge/London 2001, 27–30

- Barnes Barry, *Understanding Agency. Social Theory and Responsible Action*, London 2000
- Barrett Brian, Why Facebook, Instagram, and WhatsApp All Went Down Today, 4. Oktober 2021, <https://www.wired.com/story/why-facebook-instagram-whatsapp-went-down-outage/>
- Barry Norman, *The Tradition of Spontaneous Order, Literature of Liberty* 1982, 7–58
- Bärtschi Harald, Finanzmarktregulierung im Fluss, SZW 2014, 459–491
- Bärtschi Harald, Vom papierlosen Wertpapier zum Robo-Verwaltungsrat: Gesellschaftsrecht im digitalen Wandel, in: Jung Peter/Krauskopf Frédéric/Cramer Conradin (Hrsg.), *Theorie und Praxis des Unternehmensrechts. Festschrift zu Ehren von Lukas Handschin*, Zürich/Basel/Genf 2020, 1–18
- Bärtschi Harald/Hirschi Yannick, Vertrauen im Kapitalmarkt, SZW 2017, 771–791
- Bärtschi Harald/Jacquemart Nicolas/Meyer Stephan D., Zahlung und Verzug bei virtuellen Währungen, in: Emmenegger Susan (Hrsg.), *Zahlungsverkehr*, SBT 2018, Basel 2018, 177–248
- Bärtschi Harald/Meisser Christian, Virtuelle Währungen aus finanzmarkt- und zivilrechtlicher Sicht, in: Weber Rolf H./Thouvenin Florent (Hrsg.), *Rechtliche Herausforderungen durch webbasierte und mobile Zahlungssysteme*, ZIK 61, Zürich/Basel/Genf 2015, 113–160
- Barzel Yoram, *A Theory of the State. Economic Rights, Legal Rights, and the Scope of the State*, Cambridge/New York 2002
- Bastiat Frédéric, La Loi, in: *Oeuvres complètes de Frédéric Bastiat*, Bd. 4, Paris 1854, 342–393
- Bauer Craig P., *Secret History. The Story of Cryptology*, Boca Raton 2013
- Bayern Shawn, Of Bitcoins, Independently Wealthy Software, and the Zero-Member LLC, *Northwestern University Law Review Online* 2014, 257–270
- Bayern Shawn/Burri Thomas/Grant Thomas Dale/Häusermann Daniel M./Möslein Florian/Williams Richard, Gesellschaftsrecht und autonome Systeme im Rechtsvergleich, AJP 2017, 192–203
- Bearle, Why IDEX is centralized and why should you care, 5. Mai 2018, <https://medium.com/@bearle/why-idex-is-centralized-and-why-should-you-care-193180fc5a87com/news/binance-dex-will-geoblock-users-from-29-countries-including-the-us>
- Bech Morten/Garratt Rodney, Central bank cryptocurrencies, *BIS Quarterly Review* September 2017, 55–70
- Bech Morten/Hancock Jenny/Rice Tara/Wadsworth Amber, On the future of securities settlement, *BIS Quarterly Review* März 2020, 67–83

- Beck Ulrich, Risikogesellschaft. Auf dem Weg in eine andere Moderne, Frankfurt a.M. 1986
- Becker Eva/Willke Helmut, «A Demonstrably Fragile Financial System» – Information and Knowledge Asymmetries in the Global Financial Crisis, in: Jansen Stephan A./Schröter Eckhard/Stehr Nico (Hrsg.), Fragile Stabilität – stabile Fragilität, Wiesbaden 2013, 219–242
- Becker Hermann (Hrsg.), Berner Kommentar. Einleitung, Art. 1–10 ZGB, Bern 1962 (Autor, in: BK ZGB, 1962, Art. N)
- Beeler Lukas, Bucheffekten. Übertragung, Stornierung und gutgläubiger Erwerb, SSHW 317, Diss. Zürich/St. Gallen 2013
- Behrens Alexander, COMP holders vote to change yield farming rules on Compound, 30. Juni 2020, <https://decrypt.co/34176/comp-holders-vote-change-yield-farming-rules-compound>
- Behrens Alexander, Uniswap Token Launch Has Set the Standard for DeFi, 17. September 2020, <https://decrypt.co/42208/uniswap-token-launch-has-set-the-standard-for-defi>
- Belcher Chris, [bitcoin-dev] Design for a CoinSwap implementation for massively improving Bitcoin privacy and fungibility, 25. Mai 2020, <https://lists.linuxfoundation.org/pipermail/bitcoin-dev/2020-May/017898.html>
- Belli Luca/Sappa Christiana, The Intermediary Conundrum. Cyber-Regulators, Cyber-Police or Both?, Journal of Intellectual Property, Information Technology and E-Commerce Law 2017, 183–198
- Ben-Ner Avner/Halldorsson Freyr, Trusting and trustworthiness: What are they, how to measure them, and what affects them, Journal of Economic Psychology 2010, 64–79
- Ben-Sasson Eli/Chiesa Alessandro/Garman Christina/Green Matthew/Miers Ian/Tromer Eran/Virza Madars, Zerocash: Decentralized Anonymout Payments from Bitcoin, 2014 IEEE Symposium on Security and Privacy 2014, 459–474
- Beneš Nadja, The Main Benefits of the DutchX Mechanism, 5. März 2018, <https://blog.gnosis.pm/the-main-benefits-of-the-dutchx-mechanism-6fc2ef6ee8b4>
- Benet Juan, IPFS – Content Addressed, Versioned, P2P File System (DRAFT 3), undatiert, <https://github.com/ipfs/papers/raw/master/ipfs-cap2pfs/ipfs-p2p-file-system.pdf>
- Benkler Yochai, Coase's Penguin, or, Linux and The Nature of the Firm, The Yale Law Journal 2002, 369–446
- Benkler Yochai, The Wealth of Networks. How Social Production Transforms Markets and Freedom, New Haven/London 2006

- Benkler Yochai/Nissenbaum Helen, Commons-based Peer Production and Virtue, *The Journal of Political Philosophy* 2006, 394–419
- Benos Evangelos/Garratt Rodney/Gurrola-Perez Pedro, *The Economics of Distributed Ledger Technology for Securities Settlement*, Ledger 2019, 121–156
- Benston George J./Smith Clifford W., Jr., A Transactions Cost Approach to the Theory of Financial Intermediation, *The Journal of Finance* 1976, 215–231
- Bentov Iddo/Breidenbach Lorenz/Daian Phil/Juels Ari/Li Yunqi/Zhao Xueyuan, The Cost of Decentralization in Ox and EtherDelta, 13. August 2017, <https://hackingdistributed.com/2017/08/13/cost-of-decent/>
- Benz Arthur, Einleitung: Governance – Modebegriff oder nützliches sozialwissenschaftliches Konzept?, in: Benz Arthur (Hrsg.), *Governance – Regieren in komplexen Regelsystemen. Eine Einführung*, Wiesbaden 2004, 11–28
- Berentsen Aleksander/Schär Fabian, *A Short Introduction to the World of Cryptocurrencies*, Federal Reserve Bank of St. Louis Review 2018, 1–16
- Berentsen Aleksander/Schär Fabian, *Bitcoin, Blockchain und Kryptoassets. Eine umfassende Einführung*, Basel 2017
- Berentsen Aleksander/Schär Fabian, The Case for Central Bank Electronic Money and the Non-case for Central Bank Cryptocurrencies, *Federal Reserve Bank of St. Louis Review* 2018, 97–106
- Béres Ferenc/Seres István A./Benczúr András A./Quntyne-Collins Mikerah, Blockchain is Watching You: Profiling and Deanonymizing Ethereum Users, 14. Oktober 2020, <https://arxiv.org/abs/2005.14051v2>
- Béres Ferenc/Seres István András/Benczúr András A., A Cryptoeconomic Traffic Analysis of Bitcoin's Lightning Network, *Cryptoeconomic Systems* 2020, 1–46
- Berg Alastair/Berg Chris, Exit, voice, and forking, *COSMOS + TAXIS* 2020, 76–89
- Berg Chris/Davidson Sinclair/Potts Jason, Blockchains as Constitutional Orders, in: Wagner Richard E. (Hrsg.), *James M. Buchanan. A Theorist of Political Economy and Social Philosophy*, Cham 2018, 383–397
- Berg Chris/Davidson Sinclair/Potts Jason, Proof of Work as Three-Sided Market, *frontiers in Blockchain* 2020, 1–5
- Berg Chris/Davidson Sinclair/Potts Jason, *Understanding the Blockchain Economy. An Introduction to Institutional Cryptoeconomics*, Cheltenham/Northampton 2019
- Berkovitz Dan M., Climate Change and Decentralized Finance: New Challenges for the CFTC, 8. Juni 2021, <https://www.cftc.gov/PressRoom/SpeechesTestimony/opa-berkovitz7>
- Berle Adolf A./Means Gardiner C., *The Modern Corporation and Private Property*, New York 1933

- Bernabe Jorge Bernal/Canovas Jose Luis/Hernandez-Ramos Jose L./Torres Moreno Rafael/Skarmeta Antonio, Privacy-Preserving Solutions for Blockchain: Review and Challenges, IEEE Access 2019, 164909–164940
- Bernanke Ben S., Deflation: Making Sure «It» Doesn't Happen Here, Remarks before the National Economists Club, Washington DC, 21. November 2002, <https://www.federalreserve.gov/boarddocs/speeches/2002/20021121/default.htm>
- Berners-Lee Tim, WWW: Past, Present, and Future, Computer 1996, 69–77
- Bernet Beat, Institutionelle Grundlagen der Finanzintermediation, München/Wien 2003
- Bernholz Peter, Monetary Regimes and Inflation, History, Economic and Political Relationships, Cheltenham/Northampton 2003
- Bernstein Peter L., Against the Gods. The Remarkable Story of Risk, New York 1998
- Bernstein William J., A Splendid Exchange. How Trade Shaped the World, New York 2008
- von Bertalanffy Ludwig, General System Theory. Foundation, Development, Applications, New York 1968
- Bertschinger Urs, Das Finanzmarktaufsichtsrecht vom vierten Quartal 2019 bis ins vierte Quartal 2020, SZW 2020, 702–725
- Bertschinger Urs, Zum neuen bankengesetzlichen Aussonderungsrecht (Art. 16 und 37b BankG). Parallelen und Unterschiede zu Art. 401 OR, AJP 1995, 426–434
- Biaggini Giovanni/Gächter Thomas/Kiener Regina (Hrsg.), Staatsrecht, 3. Aufl., Zürich/St. Gallen 2021 (Autor, in: Biaggini/Gächter/Kiener, Staatsrecht, § N)
- Bieri Noël/Uhlmann Kaspar, Technologieneutralität als Richtschnur im Umgang mit der Blockchain, Die Volkswirtschaft 5/2019, 9–11
- Bigart Andrew E./Boone Christopher L./Wilson D. E. (Ed), Jr., Cryptocurrency Addresses on OFAC Sanctions List, Lexology vom 27. März 2018
- Biryukov Alex/Khovratovich Dmitry/Pustogarov Ivan, Deanonymisation of Clients in Bitcoin P2P Network, in: Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security, New York 2014, 15–29
- Bisq, Dispute Resolution, undatiert, https://bisq.wiki/Dispute_resolution
- Bisq, Frequently asked questions, How is Bisq different from other decentralized exchanges?, undatiert, https://bisq.wiki/Frequently_asked_questions#How_is_Bisq_different_from_other_decentralized_exchanges.3F
- Bisq, Frequently asked questions, How is collusion between mediators, arbitrators, and traders prevented?, undatiert, https://bisq.wiki/Frequently_asked_questions#How_is_collusion_between_mediators.2C_arbitrators.2C_and_traders_prevented.3F

- Bisq, Frequently asked questions, Is Bisq safe?, undatiert, https://bisq.wiki/Frequently_asked_questions#Is_Bisq_safe.3F
- Bisq, Frequently asked questions, Why does Bisq require a security deposit in BTC?, undatiert, https://bisq.wiki/Frequently_asked_questions#Why_does_Bisq_require_a_security_deposit_in_BTC.3F
- Bisq, License, 24. April 2014, <https://github.com/bisq-network/bisq/blob/master/LI-CENSE>
- Bisq, The Bisq DAO, undatiert, <https://docs.bisq.network/user-dao-intro.html#the-bisq-dao>
- Bisq, undatiert, <https://github.com/bisq-network>
- Bitcoin Association Switzerland (BAS), Comments of Bitcoin Association Switzerland on the draft revised VASP Guidance, 20. April 2021, <https://www.bitcoinassociation.ch/bitcoin-association-switzerland/2021/6/23/0ltsle8cggntaf-bag86vwvwbztvudvh>
- Bitcoin Association Switzerland (BAS), Our Comment on GWV-FINMA adjustment for FinSA / FinIA, 9. April 2020, <https://www.bitcoinassociation.ch/bitcoin-association-switzerland/2020/4/9/our-comment-on-gwv-finma-adjustment-for-finsa-finia>
- Bitcoin Capital, 15 FiCAS Active Crypto ETP, undatiert, <https://bitcoincapital.com/product/>
- Bitcoin Core, Bitcoin Development, Bitcoin Core contributors, undatiert, <https://bitcoin.org/en/development#bitcoin-core-contributors>
- Bitcoin Wiki, Multi-signature, undatiert, <https://en.bitcoin.it/wiki/Multi-signature>
- Bitcoin Wiki, Privacy, Centralized mixers, undatiert, https://en.bitcoin.it/wiki/Privacy#Centralized_mixers
- Bitcoin Wiki, Privacy, CoinJoin, undatiert, <https://en.bitcoin.it/wiki/Privacy#CoinJoin>
- Bitcoin, BIPs, BIP 2, undatiert, <https://github.com/bitcoin/bips/blob/master/bip-0002.mediawiki>
- Bitfinex, Learn about Bitfinex Token Sales, undatiert, <https://support.bitfinex.com/hc/en-us/articles/900007030943-Learn-about-Bitfinex-Token-Sales>
- Bitkom, Decentralized Finance (DeFi) – A new Fintech Revolution? The Blockchain Trend explained, 2020
- BitMEX Research, The Schnorr Signature & Taproot Softfork Proposal, 8. Mai 2019, <https://blog.bitmex.com/the-schnorr-signature-taproot-softfork-proposal/>
- BitMEX, Trading on BitMEX, undatiert, <https://www.bitmex.com/app/tradingOverview#BitMEX-Contracts>

- Bitonic, DNB formally acknowledges complaints Bitonic and revokes wallet-verification requirement, 20. Mai 2021, <https://bitonic.nl/news/231/dnb-formally-acknowledge-complaints-bitonic-and-revokes-wallet-verification-requirement>
- BitShares, 5. Decentralized Exchange (DEX), 2019, https://how.bitshares.works/en/master/bts_holders/dex.html
- Bitwise Asset Management, Presentation to the U.S. Securities and Exchange Commission, 19. März 2019, 23, <https://www.sec.gov/comments/sr-nysearca-2019-01/srnysearca201901-5164833-183434.pdf>
- Bity SA, How do I buy cryptocurrencies without a Bity account ?, undatiert, <https://intercom.help/bity-help-center/en/articles/4615664-how-do-i-buy-cryptocurrencies-without-a-bity-account>
- Bity SA, Position de Bity SA sur la diminution du seuil de vérification des opérations de change proposée par la FINMA, 9. April 2020, <https://blog.bity.com/2020/04/09/position-de-bity-sa-sur-la-diminution-du-seuil-de-verification-des-operations-de-change-proposee-par-la-finma/>
- Black Julia, Decentrng Regulation: Understanding the Role of Regulation and Self-Regulation in a 'Post-Regulatory' World, Current Legal Problems 2001, 103-146
- Blair Tor, The True Enemy of Decentralization, 26. Februar 2018, <https://medium.com/@TorBair/the-true-enemy-of-decentralization-500065a26fb5>
- Blair William, Money and the democratisation of payments, Journal of International Banking Law and Regulation 2020, 173-181
- Blec Chris, Defi Watch, undatiert, <https://github.com/chrisblec/defiwatch>
- Blec Chris, The Trustlessness of DeFi's Top 10 Richest Products, 23. November 2020, <https://survivingdefi.substack.com/p/the-trustlessness-of-defis-top-10>
- Blocher Walter, The next big thing: Blockchain – Bitcoin – Smart Contracts, AnwBl 2016, 612-618
- Blockchain Association (BA), BA Responds to the Financial Action Task Force's «Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers», 28. Oktober 2021, <https://blockchainassoc.medium.com/ba-responds-to-the-financial-action-task-forces-updated-guidance-for-a-risk-based-approach-to-1e76476b11bd>
- Blockchain Association (BA), Comments on the Financial Action Task Force's «Draft Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers», 20. April 2021, <https://theblockchainassociation.org/wp-content/uploads/2021/04/BA-Response-to-FATF-Draft-Updated-Guidance-April-2021.pdf>
- Blockchain Association (BA), Self-Hosted Wallets and the Future of Free Societies. A Guide for Policymakers, November 2020

- Blockchain Association (BA), Understanding the SEC's Guidance on Digital Tokens: The Hinman Token Standard, 10. Januar 2019, <https://blockchainassoc.medium.com/understanding-the-secs-guidance-on-digital-tokens-the-hinman-token-standard-dd51c6105e2a>
- Blocknet, blocknetdx/block-dx, The Blocknet Protocol, undatiert, <https://github.com/blocknetdx/blocknet#the-blocknet-protocol>
- Böckli Peter, Schweizer Aktienrecht, 4. Aufl., Zürich/Basel/Genf 2009
- Böckli Peter, Schweizer Aktienrecht, 5. Aufl., Zürich/Basel/Genf 2022
- Bodie Zvi/Merton Robert C./Cleeton David L., Financial Economics, 2. Aufl., New Jersey 2009
- Bodó Balázs/Brekke Jaya Klara/Hoepman Jaap-Henk, Decentralisation in the blockchain space, Internet Policy Review 2021, 1–12
- Boehme-Neßler Volker, Die Macht der Algorithmen und die Ohnmacht des Rechts. Wie die Digitalisierung das Recht relativiert, NJW 2017, 3031–3037
- Boemle Max/Gsell Max/Jetzer Jean-Pierre/Nyffeler Paul/Thalmann Christian (Hrsg.), Geld-, Bank- und Finanzmarkt-Lexikon der Schweiz, Zürich 2002 (Autor, in: Boemle et al.)
- Bogatyy Ivan, Implementing Ethereum trading front-runs on the Bancor exchange in Python, 17. August 2017, <https://hackernoon.com/front-running-bancor-in-150-lines-of-python-with-ethereum-api-d5e2bfd0d798>
- Bogle John C., Individual Stockholder, R.I.P., 3. Oktober 2005, <https://www.wsj.com/articles/SB112829417598858002>
- Böhm Franz, Wettbewerb und Monopolkampf. Eine Untersuchung zur Frage des wirtschaftlichen Kampfrechts und zur Frage der rechtlichen Struktur der geltenden Wirtschaftsordnung, Berlin 1933
- Böhme Rainer/Christin Nicolas/Edelman Benjamin/Moore Tyler, Bitcoin: Economics, Technology, and Governance, Journal of Economic Perspectives 2015, 213–238
- Böhme Rainer/Pesch Paulina, Technische Grundlagen und datenschutzrechtliche Fragen der Blockchain-Technologie, DuD 2017, 473–481
- Boiron Marc, Twitter, 28. Oktober 2021, <https://twitter.com/boironattorney/status/1453725920489922569>
- Bokhenek Alexander/Kamakin Ivan/Hays Demelza, Redefine 2020: A Primer. Where decentralization meets finance, September 2020, <https://cointelegraph.com/consulting/byzantine-solutions/redefine-2020-a-primer-where-decentralization-meets-finance>
- Boldrin Michele/Levine David K., Against Intellectual Monopoly, Cambridge/New York 2008

- Boltz, Frequently Asked Questions, undatiert, <https://www.notion.so/Frequently-Asked-Questions-585328ae43944e2eba351050790d5eec>
- Bonneau Joseph/Meckler Izaak/Rao Vanishree/Shapiro Evan, Mina: Decentralized Cryptocurrency at Scale, März 2020, <https://minaprotocol.com/static/pdf/technicalWhitepaper.pdf>
- Bonneau Joseph/Miller Andrew/Clark Jeremy/Narayanan Arvind/Kroll Joshua A./Felten Edward W., SoK: Research Perspectives and Challenges for Bitcoin and Cryptocurrencies, Proceedings 2015 IEEE Symposium on Security and Privacy, 104–121
- Borge Maria/Kokoris-Kogias Eleftherios/Jovanovic Philipp/Gasser Linus/Gailly Nicolas/Ford Bryan, Proof-of-Personhood: Redemocratizing Permissionless Cryptocurrencies, in: 2017 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW) 2017, 23–26
- Borio Claudio, The financial cycle and macroeconomics: What have we learnt?, BIS Working Papers Nr. 395, Dezember 2012
- Borio Claudio/Claessens Stijn/Tarashev Nikola, Entity-based vs activity-based regulation: a framework and applications to traditional financial firms and big techs, BIS FSI Occasional Paper Nr. 19, August 2022
- Borio Claudio/Toniolo Gianni, One Hundred and Thirty Years of Central Bank Cooperation: A BIS Perspective, in: Borio Claudio/Toniolo Gianni/Clement Piet (Hrsg.), Past and Future of Central Bank Cooperation, Cambridge/New York 2008, 16–75
- Boškić Magdalena/Hepp Sebastian, zkKYC in Decentralized Finance (DeFi), GesKR 2023, 209–225
- Bösch René, Das FIDLEG-Prospektrecht ante portas – Guter Anlegerschutz?, SZW 2018, 451–461
- Bösch René, Das neue Schweizer Prospektrecht gemäss E-FIDLEG – eine Bestandesaufnahme und erste Würdigung, ZSR 2016 I, 81–103
- Bösch René, Neues Prospektrecht gemäss E-FIDLEG: Schnittstellen – Gereimtes und Ungereimtes – Verpasste Chancen, in: Weber Rolf H./Stoffel Walter A./Chenau Jean-Luc/Sethe Rolf (Hrsg.), Aktuelle Herausforderungen des Gesellschafts- und Finanzmarktrechts. Festschrift für Hans Caspar von der Crone zum 60. Geburtstag, Zürich/Basel/Genf 2017, 495–514
- Bösch René/Rayroux François/Winzeler Christoph/Stupp Eric (Hrsg.), Basler Kommentar zum Kollektivanlagengesetz (KAG), 2. Aufl., Basel 2016 (BSK KAG-Autor, Art. N)
- Bose Satyajit/Dong Guo/Simpson Anne, The Financial Ecosystem. The Role of Finance in Achieving Sustainability, Cham 2019
- Botsman Rachel, Who Can You Trust? How Technology Brought Us Together and Why It Might Drive Us Apart, New York 2017

- Bourveau Thomas/De George Emmanuel T./Ellahie Atif/Macciocchi Daniele, The Role of Disclosure and Information Intermediaries in an Unregulated Capital Market: Evidence from Initial Coin Offerings, *Journal of Accounting Research* 2021, 1–39
- Bowe Sean/Grigg Jack/Hopwood Daira, Recursive Proof Composition without a Trusted Setup, 17. Februar 2020, <https://eprint.iacr.org/2019/1021>
- Bowles Samuel/Gintis Herbert, Social Capital, Moral Sentiments, and Community Governance, in: Gintis Herbert/Bowles Samuel/Boyd Robert/Fehr Ernst (Hrsg.), *Moral Sentiments and Material Interests. The Foundations of Cooperation in Economic Life*, Cambridge/London 20005, 379–398
- Bracamonte Vanessa/Okada Hitoshi, The Issue of User Trust in Decentralized Applications Running on Blockchain Platforms, in: Cunningham Paul/Cunningham Miriam (Hrsg.), 2017 IEEE International Symposium on Technology and Society (IS-TAS) Proceedings, 1–4
- Braegelmann Tom/Kaulartz Markus, § 1 Einleitung, in: Braegelmann Tom/Kaulartz Markus (Hrsg.), *Rechtshandbuch Smart Contracts*, München 2019
- Branson Mark, Fintech and Blockchain: More than hype? A regulator's perspective, Keynote at the Swiss-UK Dialogue, 13. März 2018
- Branson Mark, Fintech und Negativzinsen: Chance und Herausforderung für den Finanzplatz Schweiz, Referat «Mittagsreihe des Europainstituts der Universität Zürich», 25. September 2016
- Branson Mark, Technologie und die Finanzbranche – die Chancen und Risiken, FINMA Jahresmedienkonferenz vom 27. März 2018
- Breidenbach Lorenz/Cachin Christian/Chan Benedict/Coventry Alex/Ellis Steve/Juels Ari//Koushanfar Farinaz/Miller Andrew/Magauran Brendan/Moroz Daniel/Nazarov Sergey/Topliceanu Alexandru/Tramèr Florian/Zhang Fan, Chainlink 2.0: Next Steps in the Evolution of Decentralized Oracle Networks, 15. April 2021, <https://chn.lk/whitepaper-v2>
- Breidenbach Lorenz/Daian Phil/Juels Ari/Gün Sirer Emin, An In-Depth Look at the Parity Multisig Bug, 22. Juli 2017, <https://hackingdistributed.com/2017/07/22/deep-dive-parity-bug/>
- Brekke Jaya Klara/Alsindi Wassim Zuhair, *Cryptoeconomis*, Internet Policy Review 2021, 1–8
- Brennan Geoffrey/Buchanan James M., The Reason of Rules. Constitutional Political Economy, in: Liberty Fund (Hrsg.), *The Collected Works of James M. Buchanan. The Reason of Rules. Constitutional Political Economy*, Bd. 10, Indianapolis 2000
- Brennan-Marquez Kiel, Extremely Broad Laws, *Arizona Law Review* 2019, 641–666
- Brescia Raymond H., Regulating the Sharing Economy: New and Old Insights into an Oversight Regime for the Peer-to- Peer Economy, *Nebraska Law Review* 2016, 87–145

- Breuer Wolfgang, Finanzintermediation im Kapitalmarktgleichgewicht, Diss. Köln, Wiesbaden 1993
- Brewer Eric, CAP Twelve years later: How the «Rules» have Changed, Computer 2012, 23–29
- Breyer Friedrich, Mikroökonomik. Eine Einführung, 7. Aufl., Berlin 2020
- Brito Jerry, The Case for Electronic Cash: Why Private Peer-to-Peer Payments are Essential to an Open Society, Coin Center Report, Februar 2019
- Brito Jerry/Castillo Andrea, Bitcoin: A Primer for Policymakers, Arlington 2016
- Brito Jerry/Van Valkenburgh Peter, The ideal regulatory environment for Bitcoin, 25. August 2020, <https://www.coincenter.org/the-ideal-regulatory-environment-for-bitcoin/>
- Broadbent Ben, Central banks and digital currencies, Bank of England Speech, 2. März 2016
- Brukham Jake, Are blockchain voters ‘dummies’? We can learn a lot about voting systems from the existing literature, 7. November 2019, <https://blog.coinfund.io/are-blockchain-voters-dummies-4a89a376de69>
- Brummer Chris, Disclosure, Dapps and DeFi, Stanford Journal of Blockchain Law & Policy 2022, 137–174
- Brummer Chris, Disruptive Technology and Securities Regulation, Fordham Law Review 2015, 977–1052
- Brummer Chris/Seira Rodrigo, Legal Wrappers and DAOs, 30. Mai 2022, <https://ssrn.com/abstract=4123737>
- Brummer Chris/Yadav Yesha, Fintech and the Innovation Trilemma, The Georgetown Law Journal 2019, 235–307
- Brunnermeier Markus K., Deciphering the Liquidity and Credit Crunch 2007–2008, Journal of Economic Perspectives 2009, 77–100
- Brunton Finn, Digital Cash. The Unknown History of the Anarchists, Utopians, and Technologists Who Created Cyptocurrency, Princeton/Oxford 2019
- Bryan Ford, Technologizing Democracy or Democratizing Technology? A Layered-Architecture Perspective on Potentials and Challenges, in: Bernhold Lucy/Landemore Hélène/Reich Rob (Hrsg.), Digital Technology and Democratic Theory, Chicago/London 2021, 274–308
- Buchanan James M., An Economic Theory of Clubs, Economica 1965, 1–14
- Buchanan James M., Politics without Romance. A Sketch of Positive Public Choice Theory and Its Normative Implications, in: Liberty Fund (Hrsg.), The Collected Works of James M. Buchanan. The Logical Foundations of Constitutional Liberty, Bd. 1, Indianapolis 1999, 45–59

- Buchanan James M., Rent Seeking and Profit Seeking, in: Liberty Fund (Hrsg.), The Collected Works of James M. Buchanan. The Logical Foundations of Constitutional Liberty, Bd. 1, Indianapolis 1999, 103–115
- Buchanan James M., The Domain of Constitutional Economics, Constitutional Political Economy 1990, 1–18
- Buchanan James M., The Paradox of «Being Governed», in: Liberty Fund (Hrsg.), The Collected Works of James M. Buchanan. The Limits of Liberty. Between Anarchy and Leviathan, Bd. 7, Indianapolis 2000, 116–135
- Buchanan James M./Tullock Gordon, The Calculus of Consent. Logical Foundations of Constitutional Democracy, in: Liberty Fund (Hrsg.), The Collected Works of James M. Buchanan, Bd. 3, Indianapolis 1999
- Buchanan James M./Yoon Yong J., Symmetric Tragedies: Commons and Anti-Commons, The Journal of Law and Economics 2000, 1–13
- Buchmann Johannes, Einführung in die Kryptographie, 6. Aufl., Berlin/Heidelberg 2016
- Buckley Ross P./Arner Douglas W./Zetsche Dirk A., FinTech. Finance, Technology and Regulation, Cambridge/New York 2024
- Budish Eric/Cramton Peter/Shim John, The High-Frequency Trading Arms Race: Frequent Batch Auctions as a Market Design Response, The Quarterly Journal of Economics 2015, 1547–1621
- Bühler Christoph B., Finanzmarktregulierung im Spannungsfeld von Recht und Politik, SJZ 2010, 469–478
- Bühler Christoph C., Regulierung im Bereich der Corporate Governance, Zürich/Basel/Genf 2009
- Bühler Simon, OTC-Handel mit nichtkotierten Aktien, ZStP 270, Diss. Zürich 2016
- Bull Andrew, Regulators Everywhere Should Follow Wyoming's DAO Law, 8. Juli 2021, <https://www.coindesk.com/markets/2021/07/08/regulators-everywhere-should-follow-wyomings-dao-law/>
- Burckhardt Christoph, Das Ende der Inhaberaktie?, ex ante 2/2018, 3–21, 9
- Burckhardt Walther, Methode und System des Rechts. Mit Beispielen, Zürich 1936
- Burghof Hans-Peter/Rudolph Bernd, Bankenaufsicht. Theorie und Praxis der Regulierung, Wiesbaden 1996
- Bürgi Benjamin/Kremer Michael, Die europäische Verordnung über Märkte für Kryptowerte (MiCAR) – Übersicht und potentielle Auswirkungen auf die Schweiz, iusNet BR-KR 25.08.2022
- Burke Jamie, Pathway to Decentralisation, Juli 2018, <https://outlierventures.io/research/pathway-to-decentralisation/>
- Burton David R., Alternatives to Crowdfunding, in: Dresner Steven (Hrsg.), Crowdfunding. A Guide to Raising Capital on the Internet, Hoboken 2014, 145–161

- Busch Alexander, El Salvador meint es ernst mit seinem Bitcoin-Experiment, 7. September 2021, <https://www.nzz.ch/wirtschaft/el-salvador-meint-es-ernst-mit-seinem-bitcoin-experiment-ld.1644094>
- Bustillos Maria, The Bitcoin Boom, 1. April 2013, <https://www.newyorker.com/tech/annals-of-technology/the-bitcoin-boom>
- Butcher Mike, Melonport dissolves in favor of its protocol, setting a new bar for the blockchain world, 11. Februar 2019, <https://techcrunch.com/2019/02/11/melonport-dissolves-in-favor-of-its-protocol-setting-a-new-bar-for-the-blockchain-world/>
- Buterin Vitalik, 26. Mai 2020, <https://medium.com/@VitalikButerin/i-feel-like-this-post-is-addressing-an-argument-that-isnt-the-actual-argument-that-mev-auction-b3c5e8fc1021>
- Buterin Vitalik, An Incomplete Guide to Rollups, 5. Januar 2021, <https://vitalik.ca/general/2021/01/05/rollup.html>
- Buterin Vitalik, Chain Interoperability, 9. September 2016, https://www.r3.com/wp-content/uploads/2018/04/Chain_Interoperability_R3.pdf
- Buterin Vitalik, Credible Neutrality As A Guiding Principle, 3. Januar 2020, <https://nakamoto.com/credible-neutrality/>
- Buterin Vitalik, DAOs, DACs, DAs and More: An Incomplete Terminology Guide, 6. Mai 2014, <https://blog.ethereum.org/2014/05/06/daos-dacs-das-and-more-an-incomplete-terminology-guide/>
- Buterin Vitalik, Hard Problems in Cryptocurrency: Five Years Later, 22. November 2019 <https://vitalik.ca/general/2019/11/22/progress.html>
- Buterin Vitalik, Improving front running resistance of $x*y=k$ market makers, März 2018, <https://ethresear.ch/t/improving-front-running-resistance-of-x-y-k-market-makers/1281>
- Buterin Vitalik, Introduction to Cryptoeconomics, Ethereum Foundation, 23. Februar 2017, <https://youtu.be/pKQdjaH1dRo>
- Buterin Vitalik, Launching the Ether Sale, 22. Juli 2014, <https://blog.ethereum.org/2014/07/22/launching-the-ether-sale/>
- Buterin Vitalik, Let's run on-chain decentralized exchanges the way we run prediction markets, 3. Oktober 2016, https://www.reddit.com/r/ethereum/comments/55m04x/lets_run_onchain_decentralized_exchanges_the_way/
- Buterin Vitalik, Moving beyond coin voting governance, 16. August 2021, <https://vitalik.ca/general/2021/08/16/voting3.html>
- Buterin Vitalik, Notes on Blockchain Governance, 17. Dezember 2017, <https://vitalik.ca/general/2017/12/17/voting.html>

- Buterin Vitalik, On Collusion, 3. April 2019, <https://vitalik.ca/general/2019/04/03/collusion.html>
- Buterin Vitalik, On Path Independence, 22. Juni 2017, <https://vitalik.ca/general/2017/06/22/marketmakers.html>
- Buterin Vitalik, On Public and Private Blockchains, 7. August 2015, <https://blog.ethereum.org/2015/08/07/on-public-and-private-blockchains/>
- Buterin Vitalik, On Settlement Finality, 9. Mai 2016, <https://blog.ethereum.org/2016/05/09/on-settlement-finality/>
- Buterin Vitalik, On-chain scaling to potentially ~500 tx/sec through mass tx validation, 22. September 2018, <https://ethresear.ch/t/on-chain-scaling-to-potentially-500-tx-sec-through-mass-tx-validation/3477>
- Buterin Vitalik, Parametrizing Casper: the decentralization/finality time/overhead tradeoff, 15. Januar 2017, <https://medium.com/@VitalikButerin/parametrizing-casper-the-decentralization-finality-time-overhead-tradeoff-3f2011672735>
- Buterin Vitalik, Quadratic Payments: A Primer, 7. Dezember 2019, <https://vitalik.ca/general/2019/12/07/quadratic.html>
- Buterin Vitalik, Scalable blockchains as data layers, 15. März 2019, <https://youtu.be/mOm47gBMfg8>
- Buterin Vitalik, The Meaning of Decentralization, 6. Februar 2017, <https://medium.com/@VitalikButerin/the-meaning-of-decentralization-a0c92b76a274>
- Buterin Vitalik, The Most Important Scarce Resource is Legitimacy, 23. März 2021, <https://vitalik.ca/general/2021/03/23/legitimacy.html>
- Buterin Vitalik, Twitter, 13. Oktober 2018, <https://twitter.com/VitalikButerin/status/1051160932699770882>
- Buterin Vitalik, Visions, Part 1: The Value of Blockchain Technology, 13. April 2015, <https://blog.ethereum.org/2015/04/13/visions-part-1-the-value-of-blockchain-technology>
- Buterin Vitalik, Why we need wide adoption of social recovery wallets, 11. Januar 2021, <https://vitalik.ca/general/2021/01/11/recovery.html>
- Buterin Vitalik/Hitzig Zoë/Weyl E. Glen, A Flexible Design for Funding Public Goods, Management Science 2019, 1–17
- Buterin Vitalik/Illum Jacob/Nadler Matthias/Schär Fabian/Soleimani Ameen, Blockchain Privacy and Regulatory Compliance: Towards a Practical Equilibrium, 6. September 2023, <https://ssrn.com/abstract=4563364>
- Butler Eamonn, Public Choice – A Primer, London 2012
- Butterfield Andrew/Ekembe Ngondi Gerard (Hrsg.), A Dictionary of Computer Science, 7. Aufl., Oxford/New York 2016

- Caldarelli Guido/Vespignani Alessandro, Preliminaries and Basic Definitions in Network Theory, in: Caldarelli Guido/Vespignani Alessandro (Hrsg.), Large Scale Structure and Dynamics of Complex Networks. From Information Technology to Finance and Natural Science, Singapur 2007, 5–16
- Calle George/Eidan Daniel, Central Bank Digital Currency: an innovation in payments, R3 White paper, April 2020
- Calusic Marko, Decentralized Exchanges im Lichte von Art. 73a ff. FinfraG, Bern 2023
- Cambridge Centre for Alternative Finance, 2nd Global Cryptoasset Benchmarking Study, Dezember 2018,
- Cambridge Centre for Alternative Finance, Distributed Ledger Technology Systems. A Conceptual Framework, August 2018
- Cambridge Centre for Alternative Finance, Global Cryptoasset Regulatory Landscape Study, April 2019
- Cambridge Centre for Alternative Finance, Legal and Regulatory Considerations for Digital Assets, 2020
- Camenisch Livia, Innovationsoffenheit als Verfassungsgrundsatz, SGRW 49, Diss. St. Gallen 2021
- Camp Jean/Lewis Ken, Code as speech: A discussion of Bernstein v. USDOJ, Karn v. US-DOS, and Junger v. Daley in light of the U.S. Supreme Court's recent shift to Federalism, Ethics and Information Technology 2001, 21–33
- Campbell Richmond, Background for the Uninitiated, in: Campbell Richmond/Sowden Lanning (Hrsg.), Paradoxes of Rationality and Cooperation: Prisoner's Dilemma and Newcomb's Problem, Vancouver 1985, 3–41
- Campbell Tim S./Kracaw William A., Information Production, Market Signalling, and the Theory of Financial Intermediation, The Journal of Finance 1980, 863–882
- Cantor Robin/Henry Stuart/Rayner Steve, Making Markets. An Interdisciplinary Perspective on Economic Exchange, Westport/London 1992
- Capie Forrest, Some historical perspective on financial regulation, in: Mayes David G./Wood Geoffrey E. (Hrsg.), The Structure of Financial Regulation, London/New York 2007, 69–85
- capital markets and technology association (CMTA), AML Standards for Digital Assets, Oktober 2018
- de Caria Riccardo, Definitions of Smart Contracts: Between Law and Code, in: DiMatteo Larry A./Cannarsa Michel/Poncibò Cristina (Hrsg.), The Cambridge Handbook of Smart Contracts, Blockchain Technology and Digital Platforms, Cambridge/New York 2020, 19–36

- Carlsten Miles/Kalodner Harry/Weinberg S. Matthew/Narayanan Arvind, On the Instability of Bitcoin Without the Block Reward, Proceedings of the 2016 ACM SIG-SAC Conference on Computer and Communications Security 2016, 154–167
- Carron Blaise/Botteron Valentin, Le droit des obligations face aux «contrats intelligents»: Blockchain, Smart Contracts et contrats de droit suisse, in: Carron Blaise/Müller Christoph (Hrsg.), 3e Journée des droits de la consommation et de la distribution. Blockchain et Smart Contracts – Défis juridiques, Basel 2018, 1–50
- Carter Nic/Jeng Linda, DeFi protocol risks: The paradox of cryptofinance, in: Coen Bill/Maurice Diane (Hrsg.), Regtech, Suptech and Beyond: Innovation and Technology in Financial Services, London 2021 (zitiert wird die vorveröffentlichte Version abrufbar unter <https://ssrn.com/abstract=3866699>)
- Casey Michael, 'DeFi' and 'TradFi' Must Work Together, IMF Finance & Development September 2022, 24–26
- Casey Michael J., Zcash's Halo Breakthrough Is a Big Deal – Not Just For Cryptocurrencies, 14. Oktober 2019, <https://www.coindesk.com/zcashs-halo-breakthrough-is-a-big-deal-not-just-for-cryptocurrencies>
- Casey Michael/Crane Jonah/Gensler Gary/Johnson Simon/Narula Neha, The Impact of Blockchain Technology on Finance: A Catalyst for Change, Geneva Reports on the World Economy 21, Genf 2018
- Castells Manuel, The Information Age. Economy, Society, and Culture. The Rise of the Network Society, Bd. I, 2. Aufl., Chichester 2010
- del Castillo Michael, Leaked «Tai Chi» Document Reveals Binance's Elaborate Scheme to Evade Bitcoin Regulators, 29. Oktober 2020, <https://www.forbes.com/sites/michaeldelcastillo/2020/10/29/leaked-tai-chi-document-reveals-binance-s-elaborate-scheme-to-evade-bitcoin-regulators/>
- del Castillo Michael, SEC Cyber Chief Puts A New Type Of Cryptocurrency Exchange On Notice, 9. November 2018, <https://www.forbes.com/sites/michaeldelcastillo/2018/11/09/new-sec-cyber-chief-puts-cryptocurrency-exchanges-on-notice/>
- Castor Amy, No Incentive? Algorand Blockchain Sparks Debate at Cryptography Event, 4. April 2017, <https://www.coindesk.com/markets/2017/04/04/no-incentive-algorand-blockchain-sparks-debate-at-cryptography-event/>
- Castro Miguel/Liskov Barbara, Practical Byzantine Fault Tolerance, Proceedings of the Third Symposium on Operating Systems Design and Implementation (OSDI) 1999, 173–186
- Catalini Christian/Boslego Jordan, Blockchain Technology and Organization Science: Decentralization Theatre or Novel Organizational Form?, MIT Working Paper 2019
- Catalini Christian/Gans Joshua A., Some Simple Economics of the Blockchain, Communications of the ACM 2020, 80–90

- Cato Institute/Blanchard III James U., An Interview with F. A. Hayek, 1984, <https://youtu.be/EYhEDxFwFRU?t=1160>
- CertiK, Exploiting a Smart Contract without Security Vulnerabilities: Analysis of True Seigniorage Dollar Attack Event, 17. März 2021, <https://www.certik.io/blog/announcements/exploitingasmartcontractwithoutsecurityvulnerabilitiesanalysisof-trueseignioragedollarattackevent>
- Chainalysis, The 2021 Crypto Crime Report. Everything you need to know about ransomware, darknet markets, and more, 16. Februar 2021
- Chainalysis, The KuCoin Hack: What We Know So Far and How the Hackers are Using DeFi Protocols to Launder Stolen Funds, 2. Oktober 2020, <https://blog.chainalysis.com/reports/kucoin-hack-2020-defi-uniswap>
- Champagne Phil, The Book of Satoshi. The Collected Writings of Bitcoin Creator Satoshi Nakamoto, 2014, <https://www.bookofsatoshi.com/>
- Chan Diana/Fontan Florence/Rosati Simonetta/Russo Daniela, The Securities Custody Industry, ECB Occasional Paper Series Nr. 68, August 2007
- Changelly, About, undatiert, <https://changelly.com/about>
- Changelly, Frequently Asked Questions, Transactions, undatiert, <https://changelly.com/faq>
- Changelly, How Changelly Suggests the Best Exchange Rates, 2016, <https://steemit.com/money/@changelly/how-changelly-suggests-the-best-exchange-rates>
- Chapman Anne, Barter as a Universal Mode of Exchange, L'Homme 1980, 33–83
- Chapparo Frank, Former SEC Commissioner says Ripple lawsuit will cause 'multi-billion dollar losses to innocent third parties', 23. Dezember 2020, <https://www.theblockcrypto.com/linked/89164/former-sec-commissioner-says-ripple-lawsuit-will-cause-multi-billion-dollar-losses-to-innocent-third-parties>
- Chaum David, Blind Signatures for Untraceable Payments, in: Chaum David/Rivest Ronald L./Sherman Alan T. (Hrsg.), Advances in Cryptology: Proceedings of Crypto 82, Boston 1983, 199–203
- Chaum David, Security without Identification: transaction systems to make big brother obsolete, Communications of the ACM 1985, 1030–1044
- Chaum David/Grothoff Christian/Moser Thomas, How to issue a central bank digital currency, SNB Working Papers 3/2021
- Chen Yan/Bellavitis Cristiano, Blockchain disruption and decentralized finance: The rise of decentralized business models, Journal of Business Venturing Insights 2020, 1–8
- Chervinsky Jake, 24. März 2021, <https://twitter.com/jchervinsky/status/1374738566530629632>

- Chipolina Scott, «We Need a Centralized Entity»: Binance CEO Changpeng Zhao. Changpeng Zhao, CEO of Binance, has admitted the crypto exchange needs a centralized entity to satisfy regulatory requirements, 16. September 2021, <https://decrypt.co/81066/we-need-centralized-entity-binance-ceo-changpeng-zhao>
- Chiu Jonathan/Koepl Thorsten V., Blockchain-Based Settlement for Asset Trading, *The Review of Financial Studies* 2019, 1716–1753
- Chod Jiri/Lyandres Evgeny, A Theory of ICOs: Diversification, Agency, and Information Asymmetry, *Management Science* 2021, 5969–5989
- Christensen Clayton M., *The Innovator's Dilemma*, New York 2000
- Cincinnati Josh, Zcash Governance: A Step Toward Decentralization, 4. Juni 2019, <https://www.zfnd.org/blog/multisig-governance/>
- CipherTrace, Cryptocurrency Crime and Anti-Money Laundering Report, Februar 2021, <https://ciphertrace.com/2020-year-end-cryptocurrency-%20crime-and-anti-money-laundering-report/>
- Claessens Stijn, Fragmentation in global financial markets: good or bad for financial stability?, BIS Working Papers Nr. 815, Oktober 2019
- Clayburgh Jesse/Zumwalt Matt/Benet Juan, Why is decentralized and distributed file storage critical for a better web?, 20. Juni 2017, <https://www.coincenter.org/why-is-decentralized-and-distributed-file-storage-critical-for-a-better-web/>
- Clayton Jay, Chairman's Testimony on Virtual Currencies: The Roles of the SEC and CFTC, 6. Februar 2018, <https://www.sec.gov/news/testimony/testimony-virtual-currencies-oversight-role-us-securities-and-exchange-commission>
- Clayton Jay, Statement on Cryptocurrencies and Initial Coin Offerings, 11. Dezember 2017, <https://www.sec.gov/news/public-statement/statement-clayton-2017-12-11>
- CleanApp, SEC v. EtherDelta {Big Picture}. Crypto for Regulators (CfR), Part 3 – Individual Liability, 14. November 2018, <https://medium.com/cryptolawreview/sec-v-etherdelta-big-picture-da9ba070efa2>
- Clement Reiner/Schreiber Dirk/Possauer Paul/Pakusch Christina, *Internet-Ökonomie. Grundlagen und Fallbeispiele der digitalen und vernetzten Wirtschaft*, 4. Aufl., Berlin 2019
- Clements Ryan, Emerging Canadian Crypto-Asset Jurisdictional Uncertainties and Regulatory Gaps, *Banking and Finance Law Review* 2021 (zitiert wird die vorveröffentlichte Version abrufbar unter <https://ssrn.com/abstract=3891809>)
- Cliff Dave/Northrop Linda, *The Global Financial Markets: An Ultra-Large-Scale Systems Perspective*, in: Calinescu Radu/Garlan David (Hrsg.), *Large-Scale Complex IT Systems. Development, Operation and Management*, Berlin/Heidelberg 2012, 29–70

- Coalition of Automated Legal Applications (coala), Model Law for Decentralized Autonomous Organizations (DAOs), 2021
- Coase Ronald H., The Firm, the Market, and the Law, Chicago/London 1988
- Coase Ronald H., The Nature of the Firm, *Economica* 1937, 386–405
- Coase Ronald H., The Problem of Social Cost, *Journal of Law and Economics* 1960, 1–44
- Coburn Zackary, EtherDelta: Off-chain Order Book with On-chain Settlement, 26. November 2017, https://youtu.be/2i7rR_2io1A
- Coelho-Prabhu Sid, A Beginner's Guide to Decentralized Finance (DeFi), 6. Januar 2020, <https://blog.coinbase.com/a-beginners-guide-to-decentralized-finance-defi-574c68ff43c4>
- Coffee John C., Jr., Gatekeepers: The Professions and Corporate Governance, Oxford/New York 2006
- Coggan Philip, Paper Promises. Debt, Money, and the New World Order, New York 2012
- Cohen Daniel, Our Modern Times. The New Nature of Capitalism in the Information Age, Cambridge/London 2003
- Cohen Lewis/Angelovska-Wilson Angela/Strong Greg, Decentralized Finance: Have digital assets and open blockchain networks found their «killer app»? , 2021, <https://www.globallegalinsights.com/practice-areas/blockchain-laws-and-regulations/11-decentralized-finance-have-digital-assets-and-open-blockchain-networks-found-their-killer-app/>
- Cohney Shaanan/Hoffman David/Sklaroff Jeremy/Wishnick David, Coin-Operated Capitalism, *Columbia Law Review* 2019, 591–676
- Coin Center, Comments to Her Majesty's Treasury on Transposition of the Fifth Money Laundering Directive, 7. Juni 2019, <https://www.coincenter.org/comment-to-her-majesty-s-treasury-on-transposition-of-the-fifth-money-laundering-directive/>
- Coin Center, Comments to the Financial Action Task Force on the March 2021 Draft updated Guidance for a risk-based approach to virtual assets and VASPs, 19. April 2021, <https://www.coincenter.org/comments-to-the-financial-action-task-force-on-the-march-2021-draft-updated-guidance-for-a-risk-based-approach-to-virtual-assets-and-vasps/>
- Coin Center, Comments to the Financial Crimes Enforcement Network on Requirements for Certain Transactions Involving Convertible Virtual Currency or Digital Assets, 22. Dezember 2020, <https://www.coincenter.org/app/uploads/2020/12/2020-12-22-comments-to-fincen.pdf>
- Coin Center, Comments to the Securities Exchange Commission on Amendments Regarding the Definition of 'Exchange' and Alternative Trading Systems, 14. April 2022, <https://www.coincenter.org/app/uploads/2022/04/SEC-Exchange-Rule-Comment.pdf>

- Coleman Jeff, State Channels, 6. November 2015, <https://www.jeffcoleman.ca/state-channels/>
- Commission Nationale de l'Informatique et des Libertés (CNIL), Blockchain et RGPD: quelles solutions pour un usage responsable en présence de données personnelles?, 24. September 2018
- Comolli Alexandra D./Korver Michele R., Surfing the First Wave of Cryptocurrency Money Laundering, Department of Justice Journal of Federal Law and Practice 2021, 183–235
- Condon Matt, Parity Wallet Hack 2: Electric Boogaloo, 8. November 2017, <https://hackernoon.com/parity-wallet-hack-2-electric-boogaloo-e493f2365303>
- Cong Lin William/He Zhiguo, Blockchain Disruption and Smart Contracts, The Review of Financial Studies 2019, 1754–1797
- Cong Lin William/He Zhiguo/Li Jiasun, Decentralized Mining in Centralized Pools, The Review of Financial Studies 2020, 1–40
- Cong Lin William/Li Xi/Tang Ke/Yang Yang, Crypto Wash Trading, März 2021, <https://ssrn.com/abstract=3530220>
- ConsenSys, Blockchain for Decentralized Finance (DeFi), undatiert, <https://consensys.net/blockchain-use-cases/decentralized-finance/>
- Contratto Franca, Crypto Markets: Regulators Worldwide Are Sharpening Their Knives, CapLaw-2023-38
- Contratto Franca, Das Anlegerleitbild im Wandel der Zeiten, in: Sethe Rolf/Hens Thorsten/von der Crone Hans Caspar/Weber Rolf H. (Hrsg.), Anlegerschutz im Finanzmarktrecht kontrovers diskutiert, SSFM 108, Zürich/Basel/Genf 2013, 47–83
- Contratto Franca, Hochfrequenzhandel und systemische Risiken, GesKR 2014, 143–160
- Contratto Franca, Technologie und Finanzmarktregulierung, Narrative von Interdependenz und Co-Evolution, in: Weber Rolf H./Stoffel Walter/Chenau Jean-Luc/Sethe Rolf (Hrsg.), Aktuelle Herausforderungen des Gesellschafts- und Finanzmarktrechts. Festschrift für Hans Caspar von der Crone zum 60. Geburtstag, Zürich 2017, 412–440
- Cooter Robert B., Jr./Ulen Thomas, Law and Economics, 6. Aufl., Harlow 2014
- Cornelius Kai, Vertragsabschluss durch autonome elektronische Agenten, MMR 2002, 353–358
- Cosimano Thomas F., Intermediation, Economica 1996, 131–143
- Costantini Renato, Effektenkommission heute, SJZ 2013, 25–34
- Courtois Nicolas T./Bahack Lear, On Subversive Miner Strategies and Block Withholding Attack in Bitcoin Digital Currency, 2. Dezember 2014, <https://arxiv.org/abs/1402.1718v5>
- Courvoisier Matthias, Prospektpflicht nach FIDLEG, SZW 2020, 307–322

- Cousaert Simon/Xu Jiahua/Matsui Toshiko, SoK: Yield Aggregators in DeFi, 14. September 2021, <https://arxiv.org/abs/2105.13891v3>
- Cowen Tylor, Law as a Public Good. The Economics of Anarchy, Economics and Philosophy 1992, 249–267
- Cox Joseph, Hackers Convinced Twitter Employee to Help Them Hijack Accounts, 16. Juli 2020, <https://www.vice.com/en/article/jgxd3d/twitter-insider-access-panel-account-hacks-biden-uber-bezos>
- Crain Brian Fabian, Solana – at Breakpoint. Anatoly Yakovenko, 17. November 2021, <https://epicenter.tv/episodes/418>
- Credit Suisse, Assessing Global Debt, 22. Januar 2019
- Crenshaw Caroline A., Digital Asset Securities – Common Goals and a Bridge to Better Outcomes, 12. Oktober 2021, <https://www.sec.gov/news/speech/crenshaw-sec-speaks-20211012>
- Crenshaw Caroline A., DeFi Risks, Regulations, and Opportunities, The International Journal of Blockchain Law November 2021, 4–11
- Crenshaw Caroline A., DeFi Risks, Statement Dissenting from Approval of Proposed Rule Changes to List and Trade Spot Bitcoin Exchange-Traded Products, 10. Januar 2024, <https://www.sec.gov/news/statement/crenshaw-statement-spot-bit-coin-011023>
- Croman Kyle/Decker Christian/Eyal Ittay/Efe Gencer Adem/Juels Ari/Kosba Ahmed/Miller Andrew/Saxena Prateek/Shi Elaine/Gün Sirer Emin/Song Dawn/Wattenhofer Roger, On Scaling Decentralized Blockchains (A Position Paper), in: Clark Jeremy/Meiklejohn Sarah/Ryan Peter Y.A./Wallach Dan/Brenner Michael/Rohloff Kurt (Hrsg.), Financial Cryptography and Data Security, LNCS 9604, Berlin/Heidelberg 2016, 106–125
- von der Crone Hans Caspar, Aktienrecht, 2. Aufl., Bern 2020
- von der Crone Hans Caspar/Baumgartner Fleur, Digitalisierung des Aktienrechts – Die Ausgabe von Aktien als Registerwertrechte, SZW 2020, 351–364
- von der Crone Hans Caspar/Beeler Lukas, Regelung systemrelevanter Banken aus wirtschaftsrechtlicher Sicht – Lösungsansätze zur Too-big-to-fail-Problematik in der Schweiz, ZSR 2011 I, 177–208
- von der Crone Hans Caspar/Beyeler Karin/Dédéyan Daniel, Stakeholder im Aktienrecht, ZSR 2003 I, 409–471
- von der Crone Hans Caspar/Bilek Eva, Aktienrechtliche Querbezüge zum geplanten Bucheffektengesetz (BEG), SZW 2008, 193–207
- von der Crone Hans Caspar/Derungs Merens, Aktien als digitalisierte Werte, SZW 2019, 2–18

- von der Crone Hans Caspar/Kessler Franz J./Angstmann Luca, Token in der Blockchain – privatrechtliche Aspekte der Distributed Ledger Technologie, SJZ 2018, 337–345
- von der Crone Hans Caspar/Monsch Martin/Meisser Luzius, Aktien-Token, GesKR 2019, 1–17
- von der Crone Hans Caspar/Projer Kaspar, Privatplatzierung, Crowdfunding, OTC-Handel – Eine rechtliche Analyse alternativer Wege, in: Gericke Dieter (Hrsg.), Private Equity V, EIZ 175, Zürich/Basel/Genf 2016, 19–76
- von der Crone Hans Caspar/Vetsch Johannes, Reputation and Regulation, in: Klewes Joachim/Wreschniok Robert (Hrsg.), Reputation Capital. Building and Maintaining Trust in the 21st Century, Berlin/Heidelberg 2009, 179–195
- Crypto Valley Association (CVA), The Travel Rule and its Impact on Cryptocurrency. A simple explanation of differences between FATF and the Swiss approach published by FINMA, 27. Januar 2021, <https://members.cryptovalley.swiss/news/387220>
- Crypto Valley Association Cybersecurity Working Group (CVA CWG), Privacy Techniques for Blockchains and DLTs, 30. Mai 2021, <https://members.cryptovalley.swiss/news/410146>
- Crypto Valley Association Regulatory Working Group (CVA RWG), CVA's answer to the consultation regarding the Federal Council Ordinance on the Adaptation of Federal Law to Developments in Distributed Ledger Technology (DLT), 2. Februar 2021
- Crypto Valley Association Regulatory Working Group (CVA RWG), Paper on Staking Services on Proof-of-Stake Protocols, 12. Dezember 2023
- Crypto Valley Association Regulatory Working Group (CVA RWG), The Custody of Crypto Assets in the Banking Act, 15. November 2021, <https://members.cryptovalley.swiss/news/561003>
- Crypto51, PoW 51% Attack Cost, undatiert, <https://www.crypto51.app/>
- CryptoDJ, Emergency update 0.17.2, 10. Juli 2020, <https://bitcoingold.org/emergency-update-0-17-2/>
- CryptoKitties, CryptoKitties: Collectible and Breedable Cats Empowered by Blockchain Technology, White Pa-Purr, Version 2.0, undatiert, https://drive.google.com/file/d/1soo-eAaJHzhw_XhFGMJp3VNcQoM43byS/view
- CryptoSec, Documented Timeline of Exchange Hacks, undatiert, <https://crypto-sec.info/exchange-hacks/>
- Curve Finance, Understanding Curve, undatiert, <https://resources.curve.fi/base-features/understanding-curve>
- Daft Richard L., Organization Theory and Design, 10. Aufl., Mason 2010
- Dai Foundation, Maker-OTC, undatiert, <https://github.com/daifoundation/maker-otc>
- Dai Wei, b-money, 1. November 1998, <http://nakamotoinstitute.org/b-money/>

- Daian Phil, Analysis of the DAO exploit, 18. Juni 2016, <https://hackingdistributed.com/2016/06/18/analysis-of-the-dao-exploit/>
- Daian Philip, MEV... wat do?, 15. April 2021, <https://pdaian.com/blog/mev-wat-do/>
- Daian Philip/Goldfeder Steven/Kell Tyler/Li Yunqi/Zhao Xueyuan/Bentov Iddo/Breidenbach Lorenz/Juels Ari, Flash Boys 2.0: Frontrunning in Decentralized Exchanges, Miner Extractable Value, and Consensus Instability, 2020 IEEE Symposium on Security and Privacy 2020, 910–927
- Dal Bó Ernesto, Regulatory Capture: A Review, Oxford Review of Economic Policy 2006, 203–225
- Dale Brady, Andre Cronje: DeFi Expressionist, 8. Dezember 2020, <https://www.coindesk.com/andre-cronje-most-influential-2020>
- Dalle Jean-Michel/Jullien Nicolas, 'Libre' software: turning fads into institutions?, Research Policy 2003, 1–11
- Dame-Boyle Alison, EFF at 25: Remembering the Case that Established Code as Speech, 16. April 2015, <https://www.eff.org/deeplinks/2015/04/remembering-case-established-code-speech>
- Daniel Treisman, The Architecture of Government. Rethinking Political Decentralization, Cambridge/New York 2007
- Dash, Governance, Understanding Dash Governance, undatiert, <https://docs.dash.org/en/stable/governance/understanding.html>
- Dash, PrivateSend and InstantSend, undatiert, <https://docs.dash.org/en/stable/wallets/dashcore/privatesend-instantsend.html>
- Dash, PrivateSend Legal Position, 2019, <https://media.dash.org/wp-content/uploads/Dash-PrivateSend-Legal-Position-EN.pdf>
- Davidson Sinclair/De Filippi Primavera/Potts Jason, Blockchains and the economic institutions of capitalism, Journal of Institutional Economics 2018, 639–658
- Davidson Sinclair/De Filippi Primavera/Potts Jason, Economics of Blockchain, 8. März 2016, <https://ssrn.com/abstract=2744751>
- Davies Glyn, A History of Money, Cardiff 2002
- Davis Evans Alicia, A Requiem for the Retail Investor?, Virginia Law Review 2009, 1105–1129
- De Filippi Primavera/Hassan Samer, Blockchain Technology as a Regulatory Technology: From Code is Law to Law is Code, First Monday, Dezember 2016
- De Filippi Primavera/Lavayssière Xavier, Blockchain Technology: Toward a Decentralized Governance of Digital Platforms?, in: Grear Anna/Bollier David (Hrsg.), The Great Awakening. New Modes of Life amidst Capitalist Ruins, Erde 2020, 185–222
- De Filippi Primavera/Loveluck Benjamin, The invisible politics of Bitcoin: governance crisis of a decentralised infrastructure, Internet Policy Review 2016, 1–28

- De Filippi Primavera/Vieira Miguel Said, The Commodification of Information Commons: The Case of Cloud Computing, The Columbia Science & Technology Law Review 2014, 102–143
- De Filippi Primavera/Wright Aaron, Blockchain and the Law. The Rule of Code, Cambridge/London 2018
- De Gregorio Giovanni, Blockchain and freedom of expression, in: Pollicino Oreste/De Gregorio Giovanni (Hrsg.), Blockchain and Public Law. Global Challenges in the Era of Decentralisation, Cheltenham/Northampton 2021, 123–140
- De Nikhilesh, CFTC Chairman Heath Tarbert Talks Ethereum, DeFi and the Next BitMEX, 14. Oktober 2020, <https://www.coindesk.com/policy/2020/10/14/cftc-chairman-heath-tarbert-talks-ethereum-defi-and-the-next-bitmex/>
- De Nikhilesh/Hochstein Marc, Tether's First Reserve Breakdown Shows Token 49% Backed by Unspecified Commercial Paper, 13. Mai 2021, <https://www.coindesk.com/tether-first-reserve-composition-report-usdt>
- Deaton John E., The Ethereum Free Pass, Fair Notice and the Fight Ahead, 22. September 2021, <https://www.crypto-law.us/the-ethereum-free-pass-fair-notice-and-the-fight-ahead/>
- Decker Christian, Privacy in Lightning, 27. Februar 2018, <https://snyke.net/post/privacy-in-lightning/>
- Decker Christian/Wattenhofer Roger, A Fast and Scalable Payment Network with Bitcoin Duplex Micropayment Channels, in: Pelc Andrzej/Schwarzmann Alexander A. (Hrsg.), Stabilization, Safety, and Security of Distributed Systems, LNCS 9212, Cham 2015, 3–18
- Decker Christian/Wattenhofer Roger, Bitcoin Transaction Malleability and MtGox, in: Kutyłowski Mirosław/Vaidya Jaideep (Hrsg.), Computer Security – ESORICS 2014, Part II, Cham 2014, 313–326
- Decred, DCRDEX, undatiert, <https://github.com/decred/dcrdex>
- Decred, DCRDEX, What is DEX?, undatiert, <https://github.com/decred/dcrdex#what-is-dex>
- Decred, decred/atomicswap, undatiert, <https://github.com/decred/atomicswap/>
- Decred, Introduction to Decred Governance, undatiert, <https://docs.decred.org/governance/overview/>
- Decred, Overview, What is Decred?, undatiert, <https://docs.decred.org/#what-is-decred>
- Decrypt Media, Edward Snowden Talks Privacy Coins at Ethereum 2021, 6. Mai 2021, <https://youtu.be/JRsvz6pRtZE?t=787>
- Deek Fadi P./McHugh James A. M., Open Source. Technology and Policy, Cambridge/New York 2007

- Deeter Ken, DeRisking DeFi: Guarded Launches, 27. Mai 2020, <https://medium.com/electric-capital/derisking-defi-guarded-launches-2600ce730e0a>
- DeFi For Good, DeFi Swiss Law Regulation 2021 Dr. Reto Luthiger MLL, 8. Juni 2021, <https://youtu.be/rA3yYWLJTJg>
- DeFi Pulse, What is Defi?, 3. September 2019, <https://defipulse.com/blog/what-is-defi/>
- DeFi Watch, About DeFi Watch, undatiert, <https://defiwatch.net/about/>
- Delgado-Segura Sergi/Bakshi Surya/Pérez-Solà Cristina/Litton James/Pachulski Andrew/Miller Andrew/Bhattacharjee Bobby, TxProbe: Discovering Bitcoin's Network Topology Using Orphan Transactions, in: Goldberg Ian/Moore Tyler (Hrsg.): Financial Cryptography and Data Security, LNCS 11598, Cham 2019, 550–566
- Dell'Erba Marco, Stablecoins in Cryptoeconomics: From Initial Coin Offerings to Central Bank Digital Currencies, New York University Journal of Legislation and Public Policy 2019, 1–47
- Dell'Erba Marco, Crypto-Trading Platforms as Exchanges, Michigan State Law Review 2024 (im Erscheinen) (zitiert wird die vorveröffentlichte Version abrufbar unter <https://ssrn.com/abstract=4405361>)
- Delphi Digital, Decentralized Finance (DeFi). Thematic Insights, März 2019, <https://www.delphidigital.io/reports/decentralized-finance/>
- Demeester Tuur, The Bitcoin Reformation. A Report by Adamant Research, 7. November 2019, <https://docsend.com/view/ijd8qrs>
- Demil Benoît/Lecocq Xavier, Neither Market nor Hierarchy nor Network: The Emergence of Bazaar Governance, Organization Studies 2006, 1447–1466
- Demsetz Harold, Toward a Theory of Property Rights, The American Economic Review 1967, 347–359
- DeNardis Laura, The Global War for Internet Governance, New Haven 2014
- Depository Trust & Clearing Corporation (DTCC), Embracing Disruption. Tapping the Potential of Distributed Ledgers to Improve the Post-Trade Landscape, Januar 2016
- DeversiFi, Frequently Asked Questions, What is the purpose of the Data Availability Committee?, undatiert, <https://support.deversifi.com/en/article/deversifi-what-is-the-purpose-of-the-data-availability-committee-mqslt3/>
- DeversiFi, StarkWare Settlement Layer, undatiert, <https://docs.deversifi.com/articles/StarkWareSettlementLayer>
- DeversiFi, What is DeversiFi, undatiert, <https://support.deversifi.com/en/article/de-versifi-what-is-deversifi-ra2kw7/>
- DeversiFi, Withdrawing Tokens From DeversiFi, undatiert, <https://support.deversifi.com/en/article/deversifi-withdrawing-tokens-1vo38bg/>

- Di Fabio Udo, Reformatorische Ethik zwischen Logik der Wirtschaft und Privatautonomie des Lebensalltags, in: Di Fabio Udo (Hrsg.), Reformation und die Ethik der Wirtschaft, Tübingen 2018, 65–88
- Di Fabio Udo, Risikoentscheidung im Rechtsstaat: Zum Wandel der Dogmatik im öffentlichen Recht, insbesondere am Beispiel der Arzneiüberwachung, Tübingen 1994
- Diamond Douglas W., Financial Intermediation and Delegated Monitoring, *The Review of Economic Studies* 1984, 393–414
- Diamond Douglas W./Dybvig Philip H., Bank Runs, Deposit Insurance, and Liquidity, *The Journal of Political Economy* 1983, 401–419
- Dickinson Andrew, Cryptocurrencies and the Conflict of Laws, in: Fox David/Green Sarah (Hrsg.), *Cryptocurrencies in Public and Private Law*, Oxford 2019
- Dictionary of Banking and Finance, 3. Aufl., London 2005
- Dietrich Diemo/Vollmer Uwe, *Finanzverträge und Finanzintermediation*, Wiesbaden 2005
- Diffie Whitfield/Hellman Martin E., New Directions in Cryptography, *IEEE Transactions on Information Theory* 1976, 644–654
- Dimitropoulos Georgios, Global Currencies and Domestic Regulation. Embedding through Enabling?, in: Hacker Philipp/Lianos Ioannis/Dimitropoulos Georgios/Eich Stefan (Hrsg.), *Regulating Blockchain. Techno-Social and Legal Challenges*, Oxford/New York 2019, 112–139
- Dingle Pamela/Buchner Daniel, ION – Booting up the network, 10. Juni 2020, <https://techcommunity.microsoft.com/t5/identity-standards-blog/ion-booting-up-the-network/ba-p/1441552>
- Dittmar Jeremiah/Seabold Skipper, New Media and Competition: Printing and Europe's Transformation after Gutenberg, *Journal of Political Economy* 2021/22 (im Erscheinen) (zitiert wird die vorveröffentlichte Version abrufbar unter <https://cep.lse.ac.uk/pubs/download/dp1600.pdf>)
- Dixon Chris, Why Decentralization Matters, 18. Februar 2018, <https://cdixon.org/2018/02/18/why-decentralization-matters>
- Dobrauz-Saldapenna Günther/Schrackmann Mark A., Economics of Smart Contracts: Efficiency and Legal Challenges, in: Kaili Eva/Psarrakis Dimitrios (Hrsg.), *Disintermediation Economics. The Impact of Blockchain on Markets and Policies*, Cham 2021, 33–46
- DODO, DODO V2 docs, Product Description, undatiert, <https://dodoex.github.io/docs/docs/#product-description>
- Donald David C., From Block Lords to Blockchain: How Securities Dealers Make Markets, *The Journal of Corporation Law* 2018, 29–64

- Donald David C., Heart of Darkness: The Problem at the Core of the U.S. Proxy System and its Solution, Virginia Law & Business Review 2011, 41–100
- Donald David C., Networked securities markets: from cross-listing to direct connection, in: Arner Douglas W./Wan Wai Yee/Godwin Andrew/Shen Wei/Gibson Evan (Hrsg.), Research Handbook on Asian Financial Law, Cheltenham/Northampton 2020, 86–100
- Donald David C./Miraz Mahdi H., Multilateral Transparency For Securities Markets Through DLT, Fordham Journal of Corporate & Financial Law 2019, 97–153
- Dooley John F., History of Cryptography and Cryptanalysis. Codes, Ciphers, and Their Algorithms, Cham 2018
- dOrgTech, dex-react, undatiert, <https://github.com/dOrgTech/dex-react>
- Douceur John R., The Sybil Attack, in: Druschel Peter/Kaashoek Frans/Rowstron Antony (Hrsg.), Peer-to-Peer Systems, IPTPS 2002, 251–260
- Douglas Simon/McFarlane Ben, Defining Property Rights, in: Penner James/Smith Henry E. (Hrsg.), Philosophical Foundations of Property Law, Oxford/New York 2013, 219–243
- Dowd Kevin, Measuring Market Risk, 2. Aufl., Chichester/Hoboken 2005
- Dowd Kevin, New Private Monies. A Bit-Part Player?, London 2014
- Dowd Mark/McDonald John/Schuh Justin, The Art of Software Security Assessment. Identifying and Preventing Software Vulnerabilities, Boston 2007
- Downs Anthony, An Economic Theory of Democracy, New York 1957
- Droll Thomas/Podlich Natalia/Wedow Michael, Out of Sight, out of mind? On the risk of sub-custodian structures, Journal of Banking & Finance 2016, 47–56
- Dunning_Krugerrands, 17. Juni 2018, https://www.reddit.com/r/ethtrader/comments/8rpv5m/index_is_not_actually_decentralized_more_like/
- Dürr David, Privatrecht als Recht des wirtschaftlichen Strukturwandels, in: Walder Hans Ulrich/Tobias Jaag/Dieter Zobl (Hrsg.), Aspekte des Wirtschaftsrechts. Festgabe zum Schweizerischen Juristentag 1994, Zürich 1994, 51–68
- DutchX, undatiert, <https://dutchx.readthedocs.io/en/latest/>
- DutchX, undatiert, <https://dutchx.readthedocs.io/en/latest/>
- dwdollar, New Exchange (Bitcoin Market), BitcoinTalk.org, 15. Januar 2010, <https://bitcointalk.org/index.php?topic=20.0>
- Dwork Cynthia/Naor Moni, Pricing via Processing or Combatting Junk Mail, in: Brickell Ernest F. (Hrsg.), Advances in Cryptology – CRYPTO' 92, Berlin/Heidelberg 1993, 139–147
- Dwyer Gerald P., Jr./Samartín Margarita, Why do banks promise to pay par on demand?, Journal of Financial Stability 2009, 147–169

- dYdX, General, undatiert, <https://docs.dydx.exchange/#general>
- Dyson Ben/Hodgson Graham, Digital Cash. Why Central Bank Should Start Issuing Electronic Money, Januar 2016
- Eagleton Catherine/Williams Jonathan, Money. A History, London 2006
- Earle Timothy C., Trust, Confidence, and the 2008 Global Financial Crisis, Risk Analysis 2009, 785–792
- Easterbrook Frank H./Fischel Daniel R., The Economic Structure of Corporate Law, Cambridge/London 1991
- Eckert Martin, Digitale Daten als Wirtschaftsgut: Besitz und Eigentum an digitalen Daten, SJZ 2016, 265–274
- Ecosystem Support, Guide to ESP, undatiert, <https://esp.ethereum.foundation/en/guide/>
- Editorial Board, A Bipartisan Cryptocurrency Crackup. Negotiators wrote a sloppy provision that could slow innovation, 10. August 2021, <https://www.wsj.com/articles/a-bipartisan-cryptocurrency-crackup-senate-infrastructure-bill-11628626924>
- EEK637, [Temperature Check] – Activate Uniswap Protocol Governance, 23. Februar 2023, <https://gov.uniswap.org/t/temperature-check-activate-uniswap-protocol-governance/22936>
- Eggen Mirjam, Chain of Contracts. Eine privatrechtliche Auseinandersetzung mit Distributed Ledgers, AJP 2017, 3–15
- Eggen Mirjam, Die schweizerische Prospektpflicht für Effekten – eine rechtsvergleichende Untersuchung der bestehenden Rechtslage, SZW 2010, 203–215
- Eggen Mirjam, Verträge über digitale Währungen. Eine privatrechtliche Qualifikation von Rechtsgeschäften in oder mit digitalen Währungen, Jusletter vom 4. Dezember 2017
- Eggen Mirjam, Was ist ein Token?, AJP 2018, 558–567
- Eggen Mirjam, Smart Contracts und allgemeine Geschäftsbedingungen, in: Emmenegger Susan/Hrubesch-Millauer Stephanie/Krauskopf Frédéric/Wolf Stephan (Hrsg.), Brücken bauen, Festschrift für Thomas Koller, Bern 2018, 155–175
- Eggen Mirjam/Schaefer Rupert, Regulierung grenzüberschreitender Tätigkeiten im Finanzmarktrecht, GesKR 2013, 368–385
- Eggen Mirjam/Sillaber Christian, DLT-Handelssysteme, Jusletter vom 11. Mai 2020
- Eggen Mirjam/Stengel Cornelia, Optionen zur rechtlichen Ausgestaltung von digitalem Zentralbankgeld (Wholesale CBDC), GesKR 2020, 200–2014
- Egle Carlo, Das schleichende Ende der Anonymität des Aktionärs. Unter besonderer Berücksichtigung der neuen Anti-Geldwäschereibestimmungen des GwG und der Art. 697i ff. OR, SSHW 343, Diss. Zürich/St. Gallen 2018

- Egorov Michael, StableSwap – efficient mechanism for Stablecoin liquidity, 10. November 2019, <https://curve.fi/files/stableswap-paper.pdf>
- Ehrenzeller Bernhard/Schindler Benjamin/Schweizer Rainer J./Vallender Klaus A. (Hrsg.), Die schweizerische Bundesverfassung. St. Galler Kommentar, 2 Bd., 3. Aufl., Zürich/St. Gallen 2014 (Autor, in: St. Galler Kommentar BV, Art. N)
- Ehrsam Fred, Blockchain Governance: Programming Our Future, 27. November 2017, <https://medium.com/@FEhrsam/blockchain-governance-programming-our-future-c3bfe30f2d74>
- Ehrsam Fred, Why Decentralized Exchange Protocols Matter, 27. September 2017, <https://medium.com/@FEhrsam/why-decentralized-exchange-protocols-matter-58fb5e08b320>
- Eich Stefan, Old Utopias, New Tax Havens. The Politics of Bitcoin in Historical Perspective, in: Hacker Philipp/Lianos Ioannis/Dimitropoulos Georgios/Eich Stefan (Hrsg.), Regulating Blockchain. Techno-Social and Legal Challenges, Oxford/New York 2019, 85–98
- Eichholz Liesl, The UNI Token: Is Uniswap Really Decentralized?, 24. September 2020, <https://insights.glassnode.com/uni-token-is-uniswap-really-decentralized/>
- Eifert Martin, Das Netzwerkdurchsetzungsgesetz und Plattformregulierung, in: Eifert Martin/Gostomzyk Tobias (Hrsg.), Netzwerkrecht. Die Zukunft des NetzDG und seine Folgen für die Netzwerkkommunikation, Baden-Baden 2018, 9–43
- Eisenhardt Kathleen M., Agency Theory: An Assessment and Review, Academy of Management Review 1989, 57–74
- Eisenhardt Kathleen M., Control: Organizational and Economic Approaches, Management Science 1985, 134–149
- Eisenstein Elizabeth L., The Printing Revolution in Early Modern Europe, 2. Aufl., Cambridge/New York 2005
- Ekelund Robert B., Jr./Hébert Robert F./Tollison Robert D., An Economic Analysis of the Protestant Reformation, Journal of Political Economy 2002, 646–671
- El Isa Mona, What will it take to scale DEX liquidity? Observations on market-making from GS to DeFi, 11. Mai 2020, <https://medium.com/enzymefinance/what-will-it-take-to-scale-dex-liquidity-b642b26f8ea3>
- Electric Coin Company, Halo: Recursive Proof Composition without a Trusted Setup, 10. September 2019, <https://electriccoin.co/blog/halo-recursive-proof-composition-without-a-trusted-setup/>
- Electronic Frontier Foundation (EFF), SEC's Action Against Decentralized Exchange Raises Constitutional Questions, 12. Februar 2019, <https://www.eff.org/deeplinks/2019/02/secs-action-against-decentralized-exchange-raises-constitutional-questions>

- Ellickson Robert C., Order without Law. How Neighbors Settle Disputes, Cambridge/London 1991
- Ellis Steve/Juels Ari/Nazarov Sergey, ChainLink. A Decentralized Oracle Network, 4. September 2017 (v1.0), <https://link.smartcontract.com/whitepaper>
- Emmenegger Susan/Döbeli Thirza, Kundenvertrauen in Banken, SZW 2017, 752–770
- Ender Tiffany/von der Crone Hans Caspar, Die Risiken des grenzüberschreitenden Dienstleistungsverkehrs aus dem Blickwinkel des schweizerischen Aufsichtsrechts. Verfügung der Eidgenössischen Finanzmarktaufsicht FINMA vom 11. Januar 2010, SZW 2010, 506–517
- Engert Andreas, Digitale Plattformen, AcP 2018, 304–376
- Enyi Jin/Dang Yen Le Ngoc, Regulating initial coin offerings («crypto-crowdfunding»), Butterworths Journal of International Banking and Finance Law 2017, 495–503
- Enz Benjamin V., Kryptowährungen im Lichte von Geldrecht und Konkursaussonderung, ZStP 293, Diss. Zürich 2019
- Enzyme, Enzyme Protocol v2, Governance Overview, undatiert, <https://docs.enzyme.finance/governance/overview>
- eosnewyork, eosuseragreement, EOS User Agreement, 14. März 2019, <https://github.com/eosnewyork/eosuseragreement>
- Epstein Richard A., Simple Rules for a Complex World, Cambridge/London 1995
- Ernst Wolfgang, Die Vertragsordnung – Rückblick und Ausblick, ZSR 2018 II, 5–86
- Errass Christoph, Technikregulierungen zur Gewährleistung von Sicherheit, Sicherheit & Recht 2016, 63–89
- Eskandari Shayan/Moosavi Seyedehmahsa/Clark Jeremy, SoK: Transparent Dishonesty: Front-Running Attacks on Blockchain, in: Bracciali Andrea/Clark Jeremy/Pintore Federico/Rønne Peter B./Sala Massimiliano (Hrsg.), Financial Cryptography and Data Security 2020, LNCS 11599, Cham 2020, 170–189
- Essebieer Jana/Auf der Maur Rolf, Fidleg als Chance für die Schweiz als Crowdfunding-Standort, Jusletter vom 28. September 2015
- Essebieer Jana/Bourgeois Janique, Open Banking – Der Zahlungsverkehr im Umbruch, EuZ 2018, 116–126
- Essebieer Jana/Wyss Dominic A., Von der Blockchain zu Smart Contracts, Jusletter vom 24. April 2017
- Essential, Why the Web 3.0 Matters and you should know about it, 30. Januar 2018, <https://medium.com/@essential/why-the-web-3-0-matters-and-you-should-know-about-it-a5851d63c949>
- Esser Hartmut, The two meanings of social capital, in: Castiglione Dario/van Deth Jan W./Wolleb Guglielmo (Hrsg.), The Handbook of Social Capital, Oxford/New York 2008, 22–49

- Ethereum Community, Ethereum Whitepaper, Token Systems, 9. Februar 2021, <https://ethereum.org/en/whitepaper/#token-systems>
- Ethereum Homestead, What is Ethereum?, 2016, <https://ethdocs.org/en/latest/introduction/what-is-ethereum.html>
- Ethereum Whitepaper, 9. Oktober 2020, <https://ethereum.org/en/whitepaper/>
- Ethereum Wiki, On sharding blockchains FAQs, undatiert, <https://eth.wiki/en/sharding/Sharding-FAQs>
- Ethereum, EIPs, undatiert, <https://github.com/ethereum/EIPs/blob/master/EIPS/eip-20.md>
- Ethereum, EIPs, undatiert, <https://github.com/ethereum/EIPs/blob/master/EIPS/eip-721.md>
- Ethereum, Ethereum Grants, undatiert, <https://ethereum.org/en/community/grants/>
- Ethereum, Ethereum Whitepaper, Computation And Turing-Completeness, 9. Februar 2021, <https://ethereum.org/en/whitepaper/#computation-and-turing-completeness>
- Ethereum, Ethereum Whitepaper, Scripting, 9. Februar 2021, <https://ethereum.org/en/whitepaper/#scripting>
- Ethereum, Ethereum Whitepaper. A Next-Generation Smart Contract and Decentralized Applications Platform, 29. Oktober 2021, <https://ethereum.org/en/whitepaper/>
- Ethereum, Introduction to Ethereum Improvement Proposals (EIPs), undatiert, <https://ethereum.org/en/eips/>
- Ethereum, Nodes and Clients, Clients, undatiert, <https://ethereum.org/en/developers/docs/nodes-and-clients/#clients>
- Ethereum, The ETH2 Upgrades, undatiert, <https://ethereum.org/en/eth2/>
- EthHub, Decentralized Finance, undatiert, <https://docs.ethhub.io/built-on-ethereum/open-finance/what-is-open-finance/>
- EthHub, Plasma, undatiert, <https://docs.ethhub.io/ethereum-roadmap/layer-2-scaling/plasma/>
- EthHub, What is the Ethereum Difficulty Bomb (Ice Age)?, undatiert, <https://docs.ethhub.io/questions-about-ethereum/what-is-the-difficulty-bomb/>
- EU Blockchain Observatory and Forum (EUBOF), Blockchain and Digital Identity. A Thematic Report, 2. Mai 2019
- EU Blockchain Observatory and Forum (EUBOF), Blockchain and the GDPR. A Thematic Report, 16. Oktober 2018

- EU Blockchain Observatory and Forum (EUBOF), Decentralised Finance (DeFi), 24. Mai 2022
- EU Blockchain Observatory and Forum (EUBOF), Governance of and with Blockchains. A Thematic Report, 20. Mai 2020
- Eucken Walter, Die Grundlagen der Nationalökonomie, 9. Aufl., Berlin/Heidelberg 1989
- Eucken Walter, Grundsätze der Wirtschaftspolitik, in: Eucken Edith/Hensel K. Paul (Hrsg.), Grundsätze der Wirtschaftspolitik, 7. Aufl., Tübingen 2004
- Euroclear/Oliver Wyman, Blockchain in Capital Markets. The Prize and the Journey, Februar 2016
- Euroclear/Slaughter and May, Blockchain Settlement. Regulation, innovation and application, November 2016
- Eyal Hertzog/Guy Benartzi/Galia Benartzi, Bancor Protocol. Continuous Liquidity for Cryptographic Tokens through their Smart Contracts, 18. März 2018, 4–6, https://storage.googleapis.com/website-bancor/2018/04/01ba8253-bancor_protocol_whitepaper_en.pdf
- Eyal Ittay/Gün Sirer Emin, How A Mining Monopoly Can Attack Bitcoin, 16. Juni 2014, <https://hackingdistributed.com/2014/06/16/how-a-mining-monopoly-can-attack-bitcoin/>
- Eyal Ittay/Gün Sirer Emin, It's Time For a Hard Bitcoin Fork, 13. Juni 2014, <https://hackingdistributed.com/2014/06/13/time-for-a-hard-bitcoin-fork/>
- Eyal Ittay/Gün Sirer Emin, Majority Is Not Enough: Bitcoin Mining Is Vulnerable, in: Christin Nicolas/Safavi-Naini Reihaneh (Hrsg.), Financial Cryptography and Data Security, LNCS 8437, Berlin/Heidelberg 2014, 436–454
- Fabozzi Frank J./Modigliani Franco/Jones Frank J., Foundations of Financial Markets and Institutions, Essex 2014
- Fairfield Joshua A.T., Smart Contracts, Bitcoin Bots, and Consumer Protection, Washington and Lee Law Review Online 2014, 35–50
- Fama Eugene F., Banking in the Theory of Finance, Journal of Monetary Economics 1980, 39–57
- Fanti Giulia/Bojja Venkatakrishnan Shaileshh/Bakshi Surya/Denby Bradley/Bhargava Shruti/Miller Andrew/Viswanath Pramod, Dandelion++: Lightweight Cryptocurrency Networking with Formal Anonymity Guarantees, Proceedings of the ACM on Measurement and Analysis of Computing Systems 2018, 29:1–29:34
- Fanti Giulia/Kogan Leonid/Oh Sewoong/Ruan Kathleen/Viswanath Pramod/Wang Gerui, Compounding of Wealth in Proof-of-Stake Cryptocurrencies, in: Goldberg Ian/Moore Tyler (Hrsg.), Financial Cryptography and Data Security, LNCS 11598, Cham 2019, 42–64

- Farrell Henry/Schneier Bruce, Tornado Cash Is Not Free Speech. It's a Golem, 13. Oktober 2022, <https://www.lawfaremedia.org/article/tornado-cash-not-free-speech-its-golem>
- Farrell Joseph/Klemperer Paul, Coordination and Lock-in: Competition with Switching Costs and Network Effects, in: Armstrong Mark/Porter Robert H. (Hrsg.), *Handbook of Industrial Organization*, 3. Bd., Amsterdam/Oxford 2007, 1967–2072
- Farrington Allen/Big AI, Only The Strong Survive. A Philosophical, Technical, and Economic Critique of Prospects in «Crypto» Beyond Bitcoin, 19. September 2021, <https://www.uncerto.com/only-the-strong-survive>
- Federrath Hannes, Geoblocking und die Möglichkeiten der Technik, ZUM 2015, 929–932
- Fehr Ernst/Fischbacher Urs, Why Social Preferences Matter – The Impact of Non-Selfish Motives on Competition, Cooperation and Incentives 2002, *The Economic Journal* 2002, C1–C33
- Fehr Ernst/Gächter Simon, Cooperation and Punishment in Public Good Experiments, *The American Economic Review* 2000, 980–994
- Fehr Ernst/Schmidt Klaus M., A Theory of Fairness, Competition and Co-operation, *Quarterly Journal of Economics* 1999, 817–868
- Fellmann Walter, Haftpflichtrecht im Zeichen der Digitalisierung, HAVE 2021, 105–111
- Felten Ed, Bitcoin Mining Now Dominated by One Pool, 16. Juni 2014, <https://freedom-to-tinker.com/2014/06/16/bitcoin-mining-now-dominated-by-one-pool/>
- Felten Ed, MEV auctions considered harmful, 26. Mai 2020, <https://medium.com/off-chainlabs/mev-auctions-considered-harmful-fa72f61a40ea>
- Ferguson Niall, *The Ascent of Money. A Financial History of the World*, New York/London 2008
- Ferreira Torres Christof/Camino Ramiro/State Radu, Frontrunner Jones and the Raiders of the Dark Forest: An Empirical Study of Frontrunning on the Ethereum Blockchain, 5. Februar 2021, <https://arxiv.org/abs/2102.03347>
- Fey Gerrit, *Banken zwischen Wettbewerb, Selbstkontrolle und staatlicher Regulierung. Eine ordnungsökonomische Analyse*, Stuttgart 2006
- Filecoin, What is Filecoin?, undatiert, <https://docs.filecoin.io/about-filecoin/what-is-filecoin/>
- Finck Michèle, *Blockchain Regulation and Governance in Europe*, Cambridge/New York 2019
- Finck Michèle, *Blockchains: Regulating the Unknown*, *German Law Journal* 2018, 665–692

- Finck Michèle, Digital Regulation: Designing a Supranational Legal Framework for the Platform Economy, LSE Law, Society and Economy Working Papers 15/2017, <https://ssrn.com/abstract=2990043>
- Findley Michael G./Nielson Daniel L./Sharman J. C., Global Shell Games. Experiments in Transnational Relations, Crime, and Terrorism, Cambridge/New York 2014
- Finestone Matthew, LRC Tokenomics v2, 27. Januar 2021, <https://medium.com/loopr-ing-protocol/lrc-tokenomics-v2-1e6fd99e9e9c>
- Fink Matthew P., The Rise of Mutual Funds. An Insider's View, Oxford/New York 2008
- Finney Hal, Re: Bitcoin Bank, 30. Dezember 2010, <https://bitcointalk.org/index.php?topic=2500.msg34211#msg34211>
- Finney Hal, RPOW – Reusable Proofs of Work, 15. August 2004, <https://nakamotoinstitute.org/rpow/>
- Fischer Damian A., Interessenkonflikte im Schweizer Privat- und Wirtschaftsrecht. Ein Beitrag zur dogmatischen Erfassung eines omnipräsenten Governance-Problems, Zürich/St. Gallen 2019
- Fischer Joel, Shareholder Value, Corporate Social Responsibility und Gegenvorschlag zur Konzernverantwortungsinitiative. Sieben goldene Regeln als Kompass für Verwaltungsrat und Management, GesKR 2021, 1-24
- Fischer Pius V., Rent-Seeking, Institutions and Reforms in Africa. Theory and Empirical Evidence for Tanzania, New York 2006
- Fisher Irving, 100% Money. Designed to keep checking banks 100% liquid; to prevent inflation and deflation; largely to cure or prevent depressions; and to wipe out much of the National Debt, New York 1936
- Flashbots Docs, welcome to flashbots, undatiert, <https://docs.flashbots.net/>
- Fligstein Neil, Markets as Politics: A Political-Cultural Approach to Market Institutions, American Sociological Review 1996, 656-673
- Floersch Karl, MEV Auction: Auctioning transaction ordering rights as a solution to Miner Extractable Value, Januar 2020, <https://ethresear.ch/t/mev-auction-auctioning-transaction-ordering-rights-as-a-solution-to-miner-extractable-value/6788>
- Flühmann Daniel/Hsu Peter Ch./Ender Tiffany, Regulation of Electronic Payment Service Providers in Switzerland. An Overview with a Focus on Retail Payment Services, GesKR 2017, 5-23
- Fögen Marie Theres, Die Enteignung der Wahrsager. Studien zum kaiserlichen Wissensmonopol in der Spätantike, 2. Aufl., Frankfurt a.M. 2016
- Foley Sean/Karlsen Jonathan R./Putniņš Tālis J., Sex, Drugs, and Bitcoin: How Much Illegal Activity Is Financed through Cryptocurrencies?, The Review of Financial Studies 2019, 1798-1853

- Forman Lawrence, 0x API's Smart Order Routing, 19. Mai 2020, <https://blog.0xproject.com/0x-apis-smart-order-routing-7af0195515e5>
- Forstmoser Peter/Meier-Hayoz Arthur/Nobel Peter, Schweizerisches Aktienrecht, Bern 1996
- Foss Nicolai J./Klein Peter G., Organizing Entrepreneurial Judgment. A New Approach to the Firm, Cambridge/New York 2012
- Foucault Michel, The History of Sexuality. An Introduction, Bd. 1, New York 1978
- Foucault Thierry/Pagano Marco/Röell Ailsa, Market Liquidity. Theory, Evidence, and Policy, Oxford/New York 2013
- Fox Merritt B./Glosten Lawrence R./Rauterberg Gabriel V., The New Stock Market: Sense and Nonsense, Duke Law Journal 2015, 191-277
- Foxley William, Everything You Ever Wanted to Know About the DeFi 'Flash Loan' Attack, 19. Februar 2020, <https://www.coindesk.com/everything-you-ever-wanted-to-know-about-the-defi-flash-loan-attack>
- Foxley William, OpenLaw Launches First 'Legal DAO' for Distributed VC Investments, 28. April 2020, <https://www.coindesk.com/tech/2020/04/28/openlaw-launches-first-legal-dao-for-distributed-vc-investments/>
- Foxley William, You Can Now Prove a Whole Blockchain With One Math Problem – Really, 14. September 2019, <https://www.coindesk.com/you-can-now-prove-a-whole-blockchain-with-one-math-problem-really>
- Frangella Emilio, Crypto Black Thursday: The Good, the Bad, and the Ugly, 19. März 2020, <https://medium.com/aave/crypto-black-thursday-the-good-the-bad-and-the-ugly-7f2acebf2b83>
- Franssen Maarten/Kroes Peter, Sociotechnical Systems, in: Olsen/Pedersen/Hendricks, A Companion to the Philosophy of Technology, Chichester 2009, 223-226
- Franz Böhm, Die Ordnung der Wirtschaft als geschichtliche Aufgabe und rechtsschöpfende Leistung, Stuttgart/Berlin 1937
- freeatnet, I forked EtherDelta: ForkDelta, 5. Januar 2018, https://www.reddit.com/r/EtherDelta/comments/7odsni/i_forked_etherdelta_forkdelta/
- frenchhoudini, EtherDelta is a decentralized exchange, 17. Juni 2017, https://www.reddit.com/r/EtherDelta/comments/6hrwnu/etherdelta_is_a_decentralized_exchange/
- frenchhoudini, How fees work, 17. Juni 2017, https://www.reddit.com/r/EtherDelta/comments/6hrvwl/how_fees_work/
- Frese Erich/Graumann Matthias/Talaulicar Till/Theuvsen Ludwig, Grundlagen der Organisation. Entscheidungsorientiertes Konzept der Organisationsgestaltung, 11. Aufl., Wiesbaden 2019

- Frey Bruno S., Not Just for the Money. An Economic Theory of Personal Motivation, Cheltenham/Brookfield 1997
- Frick Jürg/Aggteleky Tobias, Extraterritorial Application of CISA based on Doctrine of Effects (Auswirkungsprinzip)?, CapLaw-2015-59
- Friedman David D., Law as a Private Good. A Response to Tyler Cowen on the Economics of Anarchy, Economics and Philosophy 1994, 319–327
- Friedman Milton, A Program for Monetary Stability, in: Marshall D. Ketchum/Leon T. Kendall (Hrsg.), Readings in Financial Institutions, Boston 1965, 189–209
- Friedman Milton, Money Mischief. Episodes in Monetary History, San Diego/New York/London 1994
- Friedman Milton, The Optimum Quantity of Money, and Other Essays, London 1969
- Fritschi Mirjam Eva, Crowdfunding aus zivilrechtlicher Perspektive. Die Allgemeinen Geschäftsbedingungen Schweizer Plattformen und deren Einfluss auf die Rechtsbeziehungen der Beteiligten, Diss. Bern, Zürich/St. Gallen 2018
- Fröhlich-Bleuler Gianni, Urheber- und vertragsrechtliche Aspekte der Open Source Software, in: Jörg Florian S./Arter Oliver (Hrsg.), IT-Verträge, Bern 2007, 179–231
- Fromknecht Conner, Connecting Blockchains: Instant Cross-Chain Transactions On Lightning, 16. November 2017, <https://blog.lightning.engineering/announcement/2017/11/16/in-swap.html>
- Frost Jon, The economic forces driving fintech adoption across countries, BIS Working Paper Nr. 838, Februar 2020
- Furrer Andreas, Die Einbettung von Smart Contracts in das schweizerische Privatrecht, Anwaltsrevue 2018, 103–115
- Furrer Andreas/Glarner Andreas/Linder Thomas/Müller Luka, Die Rechtswirkung algorithmisch abgewickelter DLT-Transaktionen. Von der Notwendigkeit der funktionalen Kategorisierung eines Blockchain-Tokens und dessen Synchronisation mit der angestrebten Rechtswirkung, Jusletter vom 26. November 2018
- Furubotn Eirik G./Richter Rudolf, Institutions and Economic Theory. The Contribution of the New Institutional Economics, 2. Aufl., Ann Arbor 2005
- Fußwinkel Oliver/Kreiterling Christoph, Blockchain-Technologie – Gedanken zur Regulierung, BaFin Perspektiven 1/2018, 49–67
- Gächter Simon/Falk Armin, Reputation and Reciprocity: Consequences for the Labour Relation, The Scandinavian Journal of Economics 2002, 1–26
- Galloway Alexander R., Protocol. How Control Exists after Decentralization, Cambridge/London 2004
- van Gammeren Thomas Jan, Robo-Vermögensverwaltung und Robo-Advice, Bern 2020
- Gandal Neil/Hamrick JT/Moore Tyler/Oberman Tali, Price manipulation in the Bitcoin ecosystem, Journal of Monetary Economics 2018, 86–96

- Garcia Josh/Leung Jenny, Ketsal Open Standards. Data Points to Measure Blockchain Network Centralization, 21. Oktober 2020
- Gasiorkiewicz Lech/Monkiewicz Jan/Monkiewicz Marek, Technology-Driven Innovations in Financial Services: The Rise of Alternative Finance, Foundations of Management 2020, 137–150
- Gasser Urs/Schulz Wolfgang, Governance of Online Intermediaries: Observations from a Series of National Case Studies, The Berkman Center for Internet & Society Research Publication Series Nr. 2015-5, 18. Februar 2015
- Gauba Alexis/Koticha Zubin, The Need for an Incentive Scheme in Algorand, 27. März 2018, <https://medium.com/blockchain-at-berkeley/the-need-for-an-incentive-scheme-in-algorand-6fe9db45f2a7>
- Gauch Peter/Schlupe Walter R./Schmid Jörg/Emmenegger Susan, Schweizerisches Obligationenrecht Allgemeiner Teil (OR AT), Bd. 1, 11. Aufl., Zürich/Basel/Genf 2020
- GEB Docs, Governance Minimization Guide, undatiert, <https://docs.reflexer.finance/ungovernance/governance-minimization-guide>
- Gehrig Thomas, Intermediation in Search Markets, Journal of Economics & Management Strategy 1993, 97–120
- Geis George S., Traceable Shares and Corporate Law, Northwestern University Law Review 2018, 227–278
- Gensler Gary, Blockchain and Money, MIT Course, Fall 2018, Class 17, 13. November 2018, https://ocw.mit.edu/courses/sloan-school-of-management/15-s12-blockchain-and-money-fall-2018/lecture-slides/MIT15_S12F18_ses17.pdf
- Gensler Gary, Prepared Remarks At DC Fintech Week, 21. Oktober 2021, <https://www.sec.gov/news/speech/gensler-dc-fintech-2021-10-21>
- Gensler Gary, Prepared Remarks of Gary Gensler Before the American Bar Association Derivatives and Futures Law Committee Virtual Mid-Year Program, 21. Juli 2021, <https://www.sec.gov/news/speech/gensler-remarks-aba-derivatives-futures-law-committee-virtual-mid-year-program-072121>
- Gensler Gary, Remarks Before the Aspen Security Forum, 3. August 2021, <https://www.sec.gov/news/public-statement/gensler-aspen-security-forum-2021-08-03>
- Gerber Kaspar, Ausweitung der Covid-19-Zertifikatspflicht – Impfpflicht, Impfpflichtobligatorium oder schon Impfpflicht?, Jusletter Coronavirus-Blog, 15. September 2021, <https://jusletter.weblaw.ch/blog/gerber15092021.html>
- Gericke Dieter/Kuhn Daniel, Neue Meldepflichten bezüglich Aktionären, Gesellschaftern und wirtschaftlich Berechtigten – die «société anonyme» ist Geschichte, AJP 2015, 849–867

- Gericke Dieter/Olivier Baum, Corporate Governance: Wer ist der Governor?, SZW 2014, 345–361
- Gervais Arthur, Vorteile und Probleme von Blockchains, *digma* 2017, 128–131
- Gervais Arthur/Karame Ghassan O./Čapkun Vedran/Čapkun Srđjan, Is Bitcoin a Decentralized Currency?, *IEEE Security & Privacy* 2014, 54–60
- Gesser Uwe, Praxishandbuch Hochfrequenzhandel. Advanced: Produkte, Systeme, Regulierung, Bd. 2, Wiesbaden 2018
- Geva Benjamin, Cryptocurrencies and the Evolution of Banking, Money, and Payments, in: Brummer Chris (Hrsg.), *Cryptoassets. Legal, Regulatory, and Monetary Perspectives*, Oxford/New York 2019, 11–37
- Geva Benjamin, The Order to Pay Money in Medieval Continental Europe, in: Fox David/Ernst Wolfgang (Hrsg.), *Money in the Western Legal Tradition. Middle Ages to Bretton Woods*, Oxford/New York 2016, 409–440
- Giaglis George M./Klein Stefan/O’Keefe Robert M., The role of intermediaries in electronic marketplaces: developing a contingency model, *Information Systems Journal* 2002, 231–246
- Giancarlo J. Christopher, Keynote Address of CFTC Commissioner J. Christopher Giancarlo Before the Cato Institute, *Cryptocurrency: The Policy Challenges of a Decentralized Revolution. «If Allowed to Thrive, Blockchain May Finally Give Regulators Transparency»*, 12. April 2016, <https://www.cftc.gov/PressRoom/SpeechesTestimony/opagiancarlo-14>
- Giancarlo J. Christopher, Keynote Address of Commissioner J. Christopher Giancarlo before the Markit Group, 2016 Annual Customer Conference New York «Blockchain: A Regulatory Use Case», 10. Mai 2016, <https://www.cftc.gov/PressRoom/SpeechesTestimony/opagiancarlo-15>
- Gibson Adam, Payjoin, 15. Dezember 2018, <https://joinmarket.me/blog/blog/payjoin/>
- Giersch Herbert, Diskussionsbeitrag zu: Vertikale Kompetenzverteilung in Wirtschaftsgemeinschaften – Bestimmungsgründe und Probleme, in: Gerken Lüder (Hrsg.), *Europa zwischen Ordnungswettbewerb und Harmonisierung. Europäische Ordnungspolitik im Zeichen der Subsidiarität*, Berlin/Heidelberg 1995, 35–44
- Gigerenzer Gerd, *Bauchentscheidungen. Die Intelligenz des Unbewussten und die Macht der Intuition*, 13. Aufl., München 2008
- Gigi, Bitcoin Is Time, 14. Januar 2021, <https://dergigi.com/2021/01/14/bitcoin-is-time/>
- Gilder George, *Knowledge and Power. The Information Theory of Capitalism and how it is Revolutionizing our World*, Washington 2013
- Gilomen Hans-Jörg, *Wirtschaftsgeschichte des Mittelalters*, München 2014

- Gilson Ronald/Gordon Jeffrey N., The Agency Costs of Agency Capitalism: Activist Investors and the Revaluation of Governance Rights, Columbia Law Review 2013, 863–928
- Giovanoli Mario, Virtuelles Geld und globaler Finanzmarkt: Herausforderungen für den Juristen an der Schwelle des dritten Jahrtausends, SZW 1999, 125–137
- Gladstein Alex, Why Bitcoin Matters for Freedom, 19. Januar 2019, https://hrf.org/press_posts/why-bitcoin-matters-for-freedom/
- Glanzmann Lukas/Spoerlé Philip, Das neue Global Forum-Gesetz. Die geplante Enteignung von Inhaberaktionären und andere Unzulänglichkeiten, GesKR 2018, 87–108
- Glarner Andreas/Lindgren Alex, What have we learnt from the case of EtherDelta?, 10. Dezember 2018, https://www.mme.ch/fileadmin/files/documents/MME_Compact/2019/190307_What_have_we_learnt_from_the_case_of_EtherDelta.pdf
- Glarner Andreas/Meyer Stephan D., Smart Contracts in Escrow-Verhältnissen, Jusletter vom 4. Dezember 2017
- Glarner Andreas/Ganzoni Romedi/Hepp Sebastian, Erweiterter Geltungsbereich des Geldwäschereigesetzes im DLT-Bereich, AJP 2023, 1091–1103
- Glarner Andreas/Mognetti Anne-Lorinne, Tornado Cash – Sanctions – What are the impacts for non-US digital asset service providers?, 30. September 2022, <https://www.mme.ch/en/magazine/articles/tornado-cash-sanctions-what-are-the-impacts-for-non-us-digital-asset-service-providers>
- Glaser Florian, Pervasive Decentralisation of Digital Infrastructures: A Framework for Blockchain enabled System and Use Case Analysis, in: Bui Tung X./Sprague Ralph, Jr. (Hrsg.), Proceedings of the 50th Hawaii International Conference on System Sciences 2017, 1543–1552
- Gleeson Simon, The Legal Concept of Money, Oxford 2019
- Glosten Lawrence R., Is the Electronic Open Limit Order Book Inevitable?, The Journal of Finance 1994, 1127–1161
- Gnosis Auction, Benefits, undatiert, <https://ido-ux.dev.gnosisdev.com/#/docs#topAnchor>
- Gnosis Auction, How do Batch Auctions work?, undatiert, <https://ido-ux.dev.gnosisdev.com/#/docs/batch-auctions#topAnchor>
- Gnosis Protocol, Introduction to Gnosis Protocol, Benefits, undatiert, <https://docs.gnosis.io/protocol/docs/introduction1/#benefits>
- Gnosis Protocol, Introduction to Gnosis Protocol, Trades, undatiert, <https://docs.gnosis.io/protocol/docs/introduction1/#trades>
- Gnosis Protocol, Introduction to Gnosis Protocol, undatiert, <https://docs.gnosis.io/protocol/docs/introduction1/>

- Gnosis Safe, What is Gnosis Safe?, undatiert, <https://help.gnosis-safe.io/en/articles/3876456-what-is-gnosis-safe>
- Gnosis, dx-contracts, undatiert, <https://github.com/gnosis/dx-contracts>
- Gnosis, Experience & Challenges of Building a Fully Decentralized Trading Protocol, 10. März 2021, <https://medium.com/@gnosisPM/experience-challenges-of-building-a-fully-decentralized-trading-protocol-c6123a0e0336>
- Gnosis, Gnosis Whitepaper, 22. Dezember 2017, <https://github.com/gnosis/research/blob/master/gnosis-whitepaper.pdf>
- Gnosis, Gnosis Whitepaper, 22. Dezember 2017, <https://github.com/gnosis/research/blob/master/gnosis-whitepaper.pdf>
- Gobat Sébastien, Les monnaies virtuelles à l'épreuve de la LP. Questions choisies à l'exemple du bitcoin, AJP 2016, 1095–1105
- Goforth Carol R., Political Reality and Crypto Regulation, Chapman Law Review 2023, 599–643
- Gohari Ramin Silvan, Verweigerung von Geschäftsbeziehungen. Kartellrechtliche Analyse nach Schweizer, EU- und US-Recht, ASR 826, Diss. Bern 2017
- Gola Yashu, Bitcoin Cash: Single Mining Pool Controls 50% of Hashrate, 3. Januar 2019, <https://www.ccn.com/bitcoin-cash-single-mining-pool-controls-half-of-hashrate/>
- Goldenfeld Nigel/Kadanoff Leo P., Simple Lessons from Complexity, Science 1999, 87–89
- Gong Jian/Xu Wei, Cryptoeconomics. Igniting a New Era of Blockchain, Boca Raton 2020
- Good David, Individuals, Interpersonal Relations, and Trust, in: Gambetta Diego (Hrsg.), Trust. Making and Breaking Cooperative Relations, Oxford/Cambridge 1988, 31–48
- Goodenough Oliver R., Integrating Smart Contracts with the Legacy Legal System: A US Perspective, in: Cappelletti Benedetta/Carullo Gherardo (Hrsg.), Blockchain, Law and Governance, Cham 2021, 191–203
- Goodhart Charles, Central Banking, in: John Eatwell/Murray Milgate/Peter Newman (Hrsg.), The New Palgrave: Money, New York/London 1989, 88–92
- Goodhart Charles, The Evolution of Central Banks, Cambridge/London 1988
- Goodman L.M., Tezos – a self-amending crypto-ledger. White paper, 2. September 2014, <https://tezos.com/whitepaper.pdf>
- Gordon Clara-Ann/Lutz Tanja, Haftung für automatisierte Entscheidungen – Herausforderungen in der Praxis, SZW 2020, 53–61
- Gorham Michael/Singh Nidhi, Electronic Exchanges. The Global Transformation from Pits to Bits, Burlington/San Diego/London 2009

- Gorton Gary/Winton Andrew, Financial Intermediation, in: Constantinides George M./Haris Milton/Stulz René M. (Hrsg.), Handbook of the Economics of Finance. Corporate Finance, Bd. 1A, Amsterdam 2003, 431–552
- Graber Christoph K., GwG, 2. Aufl., Zürich/Basel/Genf 2003 (Graber, Kommentar GwG, Art. N)
- Graber Christoph K./Oberholzer Dominik, Das neue GwG, 3. Aufl., Zürich/Basel/Genf 2009 (Graber/Oberholzer, Kommentar GwG, Art. N)
- Graeber David, Debt. The First 5,000 Years, New York 2011
- Graham-Siegenthaler Barbara/Furrer Andreas, The Position of Blockchain Technology and Bitcoin in Swiss Law, Jusletter vom 8. Mai 2017
- Granovetter Mark, Economic Action and Social Structure: The Problem of Embeddedness, American Journal of Sociology 1985, 481–510
- Green Sarah, Cryptocurrencies: The Underlying Technology, in: Fox David/Green Sarah (Hrsg.), Cryptocurrencies in Public and Private Law, Oxford 2019
- Green Sarah/Snagg Ferdisha, Intermediated Securities and Distributed Ledger Technology, in: Gullifer Louise/Payne Jennifer (Hrsg.), Intermediation and Beyond, Oxford 2019, 337–358
- Greenwald Glenn, No Place to Hide. Edward Snowden, the NSA and the Surveillance State, London/New York 2014
- Greif Avner, Institutions and the Path to the Modern Economy. Lessons from Medieval Trade, Cambridge/New York 2006
- Greyscale, Grayscale Digital Large Cap Fund, undatiert, <https://grayscale.co/digital-large-cap/>
- Griffel Alain, Umweltrecht. In a Nutshell, 2. Aufl., Zürich/St. Gallen 2019
- Griffin John M./Shams Amin, Is Bitcoin Really Un-Tethered?, 28. Oktober 2019, <https://ssrn.com/abstract=3195066>
- Griffith Trey, sparkswap: Trade across blockchains without custody risk, 31. Juli 2018, <https://medium.com/sparkswap/sparkswap-trade-across-blockchains-without-custody-risk-a6bfe08013e>
- Grigg Ian, On the intersection of Ricardian and Smart Contracts, Februar 2015, https://iang.org/papers/intersection_ricardian_smart.html
- Grigg Ian, The Ricardian Contract, 6. Juli 2004, <https://nakamotoinstitute.org/the-ricardian-contract/>
- Grinberg Reuben, Bitcoin: An Innovative Alternative Digital Currency, Hastings Science & Technology Law Journal 2012, 159–208

- Gruber Michael/Palma Ulrich Ernst, § 48 Interessenwahrungspflicht und Vermeidung von Interessenkollisionen, in: Schäfer Frank A./Sethe Rolf/Lang Volker (Hrsg.), Handbuch der Vermögensverwaltung in Deutschland, Österreich, der Schweiz und Liechtenstein, 2. Aufl., München/Wien/Basel 2016
- Gruenstein Benjamin/Norris Evan/Barabander Daniel, Secret Notes And Anonymous Coins: Examining FinCEN's 2019 Guidance on Money Transmitters In The Context Of The Tornado Cash Indictment, Working Paper 1, The International Academy of Financial Crime Litigators, September 2023, <https://www.cravath.com/a/web/qyCBWVBLEMsqxPHtd9ykoc/87ntut/the-international-academy-of-financial-crime-litigators.pdf>
- Grünewald Seraina, Währungs- und geldwäschereirechtliche Fragen bei virtuellen Währungen, in: Weber Rolf H./Thouvenin Florent (Hrsg.), Rechtliche Herausforderungen durch webbasierte und mobile Zahlungssysteme, ZIK 61, Zürich/Basel/Genf 2015, 93–112
- Gudgeon Lewis/Moreno-Sanchez Pedro/Roos Stefanie/McCorry Patrick/Gervais Arthur, SoK: Layer-Two Blockchain Protocols, in: Bonneau Joseph/Heninger Nadia (Hrsg.), Financial Cryptography and Data Security 2020, LNCS 12059, Cham 2020, 201–226
- Gudgeon Lewis/Perez Daniel/Harz Dominik/Livshits Benjamin/Gervais Arthur, The Decentralized Financial Crisis, in: Proceedings Crypto Valley Conference on Blockchain Technology (CVCBT) 2020, 1–15
- Gudgeon Lewis/Werner Sam/Perez Daniel/Knotenbelt William J., DeFi Protocols for Loanable Funds: Interest Rates, Liquidity and Market Efficiency, in: 2nd ACM Conference on Advances in Financial Technologies (AFT '20), New York 2020, 92–112
- Guhl Theo/Koller Alfred, Das Schweizerische Obligationenrecht, Zürich/Basel/Genf 2000
- Guillaume Florence, L'effet disruptif des smart contracts et des DAOs sur le droit international privé, in: Richa Alexandre/Canapa Damiano (Hrsg.), Droit et économie numérique, CEDIDAC 73, Bern 2021, 35–59
- Gullifer Louise/Payne Jennifer, Corporate Finance Law. Principles and Policy, 3. Aufl., Oxford/New York 2020
- Gün Sirer Emin, Thoughts on the DAO Attack, 17. Juni 2016, <https://hackingdistributed.com/2016/06/17/thoughts-on-the-dao-hack/>
- Gün Sirer Emin/Daian Phil, Bancor Is Flawed, 19. Juni 2017, <https://hackingdistributed.com/2017/06/19/bancor-is-flawed/>
- Günther Elmar/Riethmüller Tobias, Einführung in das Crowdfunding. Formen, Anwendungsbereiche, Erfolgsfaktoren, rechtlicher Rahmen, Wiesbaden 2020

- Güring Philipp/Grigg Ian, Bitcoin & Gresham's Law – the economic inevitability of Collapse, Oktober/Dezember 2011, <http://iang.org/papers/BitcoinBreachesGreshamsLaw.pdf>
- Guseva Yuliya, The SEC, Digital Assets, and Game Theory, The Journal of Corporation Law 2021, 629–687
- gwp/InCore, Travel Rule Report, November 2020, <https://members.cryptovalley.swiss/news/387220>
- Gyr Eleonor, Smart Contracts and Contract Law, Jusletter IT vom 30. Juni 2022
- Gyr Eleonor, Blockchain und Smart Contracts. Die vertragsrechtlichen Implikationen einer neuen Technologie, Diss. Bern 2019
- Gyr Eleonor, Dezentrale Autonome Organisation DAO, Jusletter vom 4. Dezember 2017
- Hablützel Colin, Proof-of-Ownership and Crypto Adoption With Bitcoin Suisse, 11. Oktober 2020, <https://www.bitcoinsuisse.com/research/specials/proof-of-ownership-crypto-adoption-bitcoin-suisse>
- Hacker Philipp, Corporate Governance for Complex Cryptocurrencies? A Framework for Stability and Decision Making in Blockchain-Based Organizations, in: Hacker Philipp/Lianos Ioannis/Dimitropoulos Georgios/Eich Stefan (Hrsg.), Regulating Blockchain. Techno-Social and Legal Challenges, Oxford/New York 2019, 140–166
- Hacklin Fredrik/Raurich Vincent/Marxt Christian, Implications of Technological Convergence on Innovation Trajectories: The Case of ICT Industry, International Journal of Innovation and Technology Management 2005, 313–330
- Haene Philipp, Das Effektenabwicklungssystem SECOM, Mai 2009
- Haene Philipp/Sturm Andy, Was sich hinter den Kulissen der Finanzmärkte abspielt: Ein Überblick über die Schweizer Finanzmarktinфраstruktur, Mai 2009
- Häfelin Ulrich/Müller Georg/Uhlmann Felix, Allgemeines Verwaltungsrecht, 8. Aufl., Zürich/Genf/Basel 2020
- Halaburda Hanna/Haeringer Guillaume/Gans Joshua/Gandal Neil, The Microeconomics of Cryptocurrencies, Journal of Economic Literature 2022, 971–1013
- Haldane Andrew G., Rethinking the financial network, in: Jansen Stephan A./Schröter Eckhard/Steher Nico (Hrsg.), Fragile Stabilität – stabile Fragilität, Wiesbaden 2013, 243–278
- Haldane Andrew G., Systemic risk in banking ecosystems, Nature 2011, 351–355
- Haldane Andrew G./Madouros Vasileios, The Dog and the Frisbee, in: Federal Reserve Bank of Kansas (Hrsg.), Proceedings – Economic Policy Symposium – Jackson Hole 2012, 109–159
- von Hall Peter, Vorhandelstransparenzpflichten für Systematische Internalisierer, GesKR 2015, 497–505

- Haller Walter/Kölz Alfred/Gächter Thomas, Allgemeines Staatsrecht. Eine juristische Einführung in die Allgemeine Staatslehre, 6. Aufl., Zürich/Basel/Genf 2020
- Hamburger Philip, Is Administrative Law Unlawful?, Chicago/London 2014
- Hamwi Omar, Dash Complies with the Financial Action Task Force (FATF) Guidelines Including the 'Travel Rule', 23. Oktober 2019, <https://blog.dash.org/dash-complies-with-the-financial-action-task-force-fatf-guidelines-including-the-travel-rule-a4c658efc89d>
- Han Runchao/Lin Haoyu/Yu Jiangshan, On the optionality and fairness of Atomic Swaps, in: AFT '19 – Proceedings of the 1st ACM Conference on Advances in Financial Technologies, New York 2019, 62–75
- Handschin Lukas (Hrsg.), Zürcher Kommentar. Die Aktiengesellschaft. Allgemeine Bestimmungen, Art. 620–659b OR, 2. Aufl., Zürich/Basel/Genf 2016 (Autor, in: ZK OR, Art. N)
- Hanke Steve H./Sekerke Matt, Crypto's Legal White Space: Fact or Fiction?, 1. Oktober 2021, <https://www.nationalreview.com/2021/10/cryptos-legal-white-space-fact-or-fiction/>
- Hanson Robin, Logarithmic markets coring rules for modular combinatorial information aggregation, The Journal of Prediction Markets 2007, 3–15
- Hanson Robin, Shall We Vote on Values, But Bet on Beliefs?, The Journal of Political Philosophy 2013, 151–178
- Haque Raina S./Seira Silva-Herzog Rodrigo/Plummer Brent A./Rosario Nelson M., Blockchain Development and Fiduciary Duty, Stanford Journal of Blockchain Law & Policy 2019, 139–188
- Harari Yuval Noah, Sapiens. A Brief History of Humankind, London 2014
- Hardin Garrett, The Tragedy of the Commons, Science 1968, 1243–1248
- Hari Olivier, La revendication et la distraction d'office d'actifs dans une procédure d'insolvabilité: application des principes aux monnaies cryptographiques, GesKR 2017, 453–468
- Harper Colin, Bitcoin Independence Day: How This Watershed Day Defines Community Consensus, 1. August 2019, <https://bitcoinmagazine.com/culture/bitcoin-independence-day-how-this-watershed-day-defines-community-consensus>
- Harper Colin, Sparkswap, World's First Lightning Atomic Swap Exchange, Now in Beta, 8. April 2019, <https://bitcoinmagazine.com/technical/sparkswap-worlds-first-lightning-atomic-swap-exchange-now-in-beta>
- Hart Keith, Heads or Tails? Two Sides of the Coin, Man 1986, 637–656
- Hart Oliver, Incomplete Contracts and Control, The American Economic Review 2017, 1731–1752

- HarvardLawBFI, Governance Proposal 005 – DeFi Education Fund, 12. Juni 2021, <https://gov.uniswap.org/t/governance-proposal-005-defi-education-fund/12963>
- Harvey Campbell R., Cryptofinance, 14. Januar 2016, <https://ssrn.com/abstract=2438299>
- Harvey Campbell R./Ramachandran Ashwin/Santoro Joey, DeFi and the Future of Finance, Hoboken 2021
- Hassan Samer/De Filippi Primavera, The Expansion of Algorithmic Governance: From Code is Law to Law is Code, Field Actions Science Reports 2017, 88–90
- Hastenspflug Wolfgang, Das Securitizationsphänomen, Wiesbaden 1991
- Häusermann Daniel M., Konzernorganisationsrecht heute, SZW 2023, 559–570
- Hauser-Spühler Gabriela, Innovation vs. Regulation. Compliance im Digital-Finance-Bereich, LMP 6, Zürich/Basel/Genf 2017
- Hauser-Spühler Gabriela/Meisser Luzius, Eigenschaften der Kryptowährung Bitcoin, digma 2018, 6–12
- Hausheer Heinz (Hrsg.), Berner Kommentar. Die Erfüllung der Obligation, Art. 68–96 OR, 2. Aufl., Bern 2005 (Autor, in: BK OR, Art. N)
- Hausheer Heinz/Walter Hans Peter (Hrsg.), Berner Kommentar. Einleitung und Personenrecht, Art. 1–10 ZGB, Bern 2012 (Autor, in: BK ZGB, 2012, Art. N)
- Hautsch Nikolaus/Schaumburg Julia/Schienze Melanie, Financial Network Systemic Risk Contributions, Review of Finance 2015, 685–738
- Haux Dario Henri, Die digitale Allmende. Zur Frage des nachhaltigen Umgangs mit Kultur im digitalen Lebensraum, RNT 3, Diss. Zürich/St. Gallen 2021
- Haveno, Why a new Platform?, undatiert, <https://github.com/haveno-dex/haveno#why-a-new-platform>
- Hayden Adams, 24. Juli 2021, Twitter, <https://twitter.com/haydenzadams/status/1418962001989185538>
- von Hayek Friedrich August, Denationalisation of Money – The Argument Refined. An Analysis of the Theory and Practice of Concurrent Currencies, London 1990
- von Hayek Friedrich August, Der Wettbewerb als Entdeckungsverfahren, in: Streit Manfred E. (Hrsg.), Gesammelte Schriften in deutscher Sprache, Abt. A Bd. 4: Rechtsordnung und Handlungsordnung. Aufsätze zur Ordnungsökonomik, Tübingen 2003, 249–265
- von Hayek Friedrich August, Law, Legislation and Liberty. A new statement of the liberal principles of justice and political economy. The Mirage of Social Justice, Bd. 2, London 1998
- von Hayek Friedrich August, Law, Legislation and Liberty. A new statement of the liberal principles of justice and political economy. Rules and Order, Bd. 1, London 1998

- von Hayek Friedrich August, Prices and Production, New York 1935
- von Hayek Friedrich August, The Fatal Conceit. The Errors of Socialism, in: Bartley William W., III (Hrsg.), The Collected Works of Friedrich August Hayek, Bd. 1, London 1992
- von Hayek Friedrich August, The Meaning of Competition, in: von Hayek Friedrich August (Hrsg.), Individualism and Economic Order, Chicago/London 1948, 92–106
- von Hayek Friedrich August, The Use of Knowledge in Society, The American Economic Review 1945, 519–530
- Hays Demelza/Yorke Ben/Rosenberg Helen, DeFi Adoption 2020: A Definitive Guide to Entering the Industry, 2020, <https://cointelegraph.com/news/cointelegraph-consulting-releases-defi-guide-to-increase-wider-adoption>
- He Ping/Tang Dunzhe/Wang Jingwen, Staking Pool Centralization in Proof-of-Stake Blockchain Network, 28. November 2020, <https://ssrn.com/abstract=3609817>
- Heimbach Lioba/Wang Ye/Wattenhofer Roger, Behavior of Liquidity Providers in Decentralized Exchanges, 11. Oktober 2021, <https://arxiv.org/abs/2105.13822>
- Heinemann Andreas, § 9 Wettbewerbsrechtlicher Konsumentenschutz, in: Heiss Helmut/Loacker Leander D. (Hrsg.), Grundfragen des Konsumentenschutzes, Zürich/Basel/Genf 2020
- Heller Michael A., The Tragedy of the Anticommons: Property in the Transition from Marx to Markets, Harvard Law Review 1998, 621–688
- Helmy Karim, Measuring Bitcoin's Decentralization, 15. September 2020, <https://coin-metrics.io/measuring-bitcoins-decentralization/>
- Henderson Blake, Growing DeFi with the help of professional market makers. The new Request for Quote system by 0x, 26. August 2020, <https://blog.0xproject.com/growing-defi-with-the-help-of-professional-market-makers-0xs-new-request-for-quote-system-8d5fb08594bf>
- Henderson M. Todd/Raskin Max, A Regulatory Classification of Digital Assets: Toward an Operational Howey Test for Cryptocurrencies, ICOs, and Other Digital Assets, Columbia Business Law Review 2019, 443–493
- Herdegen Matthias, Principles of International Economic Law, 2. Aufl., Oxford/New York 2016
- Herlihy Maurice, Atomic Cross-Chain Swaps, Proceedings of the 2018 ACM Symposium on Principles of Distributed Computing 2018, 245–254
- Hertig Gérard/Meier-Schatz Christian J./Roth Robert/Roth Urs/Zobl Dieter (Hrsg.), Kommentar zum Bundesgesetz über die Börsen und den Effektenhandel, Zürich/Basel/Genf 2000 (Autor, in: Hertig et al., Kommentar BEHG, Art. N)
- Hertig Randall Maya, Freedom of Expression in the Internet, SRIEL 2016, 235–253

- Hess Charlotte/Ostrom Elinor, Introduction: An Overview of the Knowledge Commons, in: Hess Charlotte/Ostrom Elinor (Hrsg.), Understanding Knowledge as a Commons. From Theory to Practice, Cambridge/London 2007, 7–10
- Hess Eric W., Bridging Policy and Practice: A Pragmatic Approach to Decentralized Finance, Risk, and Regulation, Penn State Law Review 2024 (im Erscheinen) (zitiert wird die vorveröffentlichte Version abrufbar unter <https://ssrn.com/abstract=4571106>)
- Hess Martin, Die zentrale Gegenpartei im Effektenhandel – rechtliche Aspekte des Clearing, AJP 2004, 687–703
- Hess Martin, Euro-Zahlungen gemäss den SEPA-Rulebooks, insbesondere die Haftung der Banken, in: Emmenegger Susan (Hrsg.), Cross-Border Banking, SBT 2009, Basel 2009, 47–104
- Hess Martin, Stablecoins, AJP 2023, 938–949
- Hess Martin/Friedrich Alain, Das neue Bucheffektengesetz (BEG). Hinweise auf Grundlagen und praktische Auswirkungen, GesKR 2008, 98–118
- Hess Martin/Lienhard Stephanie, Übertragung von Vermögenswerten auf der Blockchain, Jusletter vom 4. Dezember 2017
- Hess Martin/Lienhard Stephanie, Unautorisierte Zahlungen mit virtuellen Währungen?, in: Emmenegger Susan (Hrsg.), Zahlungsverkehr, SBT 2018, Basel 2018, 155–176
- Hess Martin/Spielmann Patrick, Cryptocurrencies, Blockchain, Handelsplätze & Co. – Digitalisierte Werte unter Schweizer Recht, in: Reutter Thomas U./Werlen Thomas (Hrsg.), Kapitalmarkt – Recht und Transaktionen XII, Zürich/Basel/Genf 2017, 145–202
- Hess Nico, Geltungsbereich der bewilligungspflichtigen Tätigkeiten im Bankenrecht de lege lata und de lege ferenda, SSFM 142, Diss. Zürich 2023
- Hesse Hermann, Das Glasperlenspiel. Den Morgenlandfahrern, Frankfurt a.M. 1971
- Hettich Peter, «Wirksamer Wettbewerb». Theoretisches Konzept und Praxis, SGPHW 70, Diss. St. Gallen 2003
- Hettich Peter, Finanzierungsquellen für KMU im Zeitalter von Crowdfunding, GesKR 2013, 386–397
- Hettich Peter, Kooperative Risikoversorge – Regulierte Selbstregulierung im Recht der operationellen und technischen Risiken, Zürich/Basel/Genf 2014
- Higgins Stan, The Bitfinex Bitcoin Hack: What We Know (And Don't Know), 3. August 2016, <https://www.coindesk.com/bitfinex-bitcoin-hack-know-dont-know>
- Hinman William, Digital Asset Transactions: When Howey Met Gary (Plastic), 14. Juni 2018, <https://www.sec.gov/news/speech/speech-hinman-061418>
- von Hippel Eric, Democratizing Innovation, Cambridge/London 2005

- Hirschman Albert O., Exit, Voice, and Loyalty. Responses to Decline in Firms, Organizations, and the States, Cambridge/London 1970
- Hirshleifer Jack, From Weakest-Link to Best-Shot: The Voluntary Provision of Public Goods, Public Choice 1983, 371–386
- Hobbes Thomas, Leviathan, in: John C. A. Gaskin (Hrsg.), Oxford's World Classics, Oxford/New York 1998
- Hodder Sasha/Yakobi Rafael, Bitcoin Fungibility, Mixing and the Legal Limits on Maintaining Privacy, 17. März 2020, <https://bitcoinmagazine.com/culture/bitcoin-fungibility-mixing-and-the-legal-limits-on-maintaining-privacy>
- Hodgson Geoffrey M., Markets, in: The New Palgrave Dictionary of Economics, 3. Aufl., London 2018, 8298–8307
- Hodgson Geoffrey M., Opportunism is not the only reason why firms exist: why an explanatory emphasis on opportunism may mislead management strategy, Industrial and Corporate Change 2004, 401–418
- Hodgson Geoffrey M., What are Institutions?, Journal of Economic Issues 2006, 1–25
- Hodl Hodl, FAQ, Are you holding my funds?, undatiert, https://hodlhodl.com/pages/faq#are_you_holding_my_funds
- Hodl Hodl, Help Topics, How does Hodl Hodl ensure security, Multisig escrow, undatiert, https://hodlhodl.com/pages/help#title_security
- Hodl Hodl, Help Topics, How does Hodl Hodl ensure security, Reputation system, undatiert, https://hodlhodl.com/pages/help#title_security
- Hodl Hodl, Terms and Conditions, Definitions, 20. Oktober 2020, https://accounts.hodlhodl.com/pages/terms_of_service
- Hofert Eduard, Regulierung der Blockchains. Hoheitliche Steuerung der Netzwerke im Zahlungskontext, Tübingen 2018
- Höffe Otfried/Forschner Maximilian/Schöpf Alfred/Vossenkuhl Wilhelm, Lexikon der Ethik, 5. Aufl., München 1997
- Hoffmann David, Ethereum: The Digital Finance Stack, 25. Juli 2019, <https://medium.com/pov-crypto/ethereum-the-digital-finance-stack-4ba988c6c14b>
- Hoffmann-Riem Wolfgang, Innovation und Recht – Recht und Innovation. Recht im Ensemble seiner Kontexte, Tübingen 2016
- Hoffmann-Riem Wolfgang, Innovationsoffenheit und Innovationsverantwortung durch Recht. Aufgaben rechtswissenschaftlicher Innovationsforschung, AÖR 2006, 255–277
- Hofstetter Karl, Die Gleichbehandlung der Aktionäre in börsennotierten Gesellschaften, SZW 1996, 222–233
- Holler Manfred J./Illing Gerhard/Napel Stefan, Einführung in die Spieltheorie, 8. Aufl., Berlin 2019

- Honegger Lorenz/Mordrelle Eflamm, Die Krypto-Branche hat Angst vor einem «Lehman-Moment»: So beurteilen Experten die Risiken des Falls FTX für Anleger und den Finanzplatz, 11. November 2022, <https://www.nzz.ch/finanzen/die-krypto-branche-hat-angst-vor-einem-lehman-moment-jetzt-wird-der-ruf-nach-scha-erferer-regulierung-noch-lauter-ld.1711637>
- Honsell Heinrich, Römisches Recht, 8. Aufl., Berlin/Heidelberg 2015
- Honsell Heinrich/Vogt Nedim Peter/Watter Rolf (Hrsg.), Basler Kommentar zum Wertpapierrecht. Art. 965-1186 OR. Bucheffektengesetz. Haager Wertpapier-Übereinkommen. Art. 108a-108d IPRG, Basel 2012 (BSK Wertpapierrecht-Autor, Art. N)
- Watter Rolf/Vogt Hans-Ueli (Hrsg.), Basler Kommentar zum Obligationenrecht II. Art. 530-964 OR, inkl. Schlussbestimmungen, 6. Aufl., Basel 2023 (BSK OR II-Autor, Art. N)
- Hopt Klaus J., Der Kapitalanlegerschutz im Recht der Banken. Gesellschafts-, bank- und börsenrechtliche Anforderungen an das Beratungs- und Verwaltungsverhalten der Kreditinstitute, München 1975
- Hopt Klaus J., Interessenwahrung und Interessenkonflikte im Aktien-, Bank- und Berufsrecht. Zur Dogmatik des modernen Geschäftsbesorgungsrechts, ZGR 2004, 1-52
- Hospes Jan/Hötzendorfer Walter/Tschohl Christof/Kastelitz Markus, Kryptowährungen im Finanzmarktrecht und grundrechtliche Grenzen von Verboten, in: Schweighofer Erich/Kummer Franz/Saarenpää Ahti/Hötzendorfer Walter (Hrsg.), Verantwortungsbewusste Digitalisierung, IRIS 2020, Bern, 569-576.
- Howard Tom, Decentralized exchanges aren't ready for derivatives, 20. November 2021D, <https://cointelegraph.com/news/decentralized-exchanges-aren-t-ready-for-derivatives>
- Hsu Peter Ch./Flühmann Daniel (Hrsg.), Basler Kommentar Geldwäschereigesetz, Basel 2021 (BSK GwG-Autor, Art. N)
- Huberman Gur/Leshno Jacob D./Moallemi Ciamac, Monopoly without a Monopolist: An Economic Analysis of the Bitcoin Payment System, The Review of Economic Studies 2021, 1-30
- Huerta de Soto Jesús, Money, Bank Credit, and Economic Cycles, 3. Aufl., Auburn 2012
- Hug Dario, La protection du consommateur face aux nouvelles technologies de la conclusion et de l'exécution des contrats, in: Carron Blaise/Müller Christoph (Hrsg.), 3e Journée des droits de la consommation et de la distribution. Blockchain et Smart Contracts – Défis juridiques, Basel 2018, 115-167
- Hughes Eric, A Cypherpunk's Manifesto, in: Ludlow Peter (Hrsg.), Crypto Anarchy, Cyberstates, and Pirate Utopias, Cambridge/London 2001, 81-83

- Hügler Wolfgang Johannes, Finanzsysteme, wirtschaftliches Wachstum und die Rolle des Staates: Ein funktionaler Ansatz unter Berücksichtigung der Reform Erfahrung lateinamerikanischer Länder, Diss. Köln 2001
- Huguenin Claire, Obligationenrecht. Allgemeiner und Besonderer Teil, 3. Auf., Zürich/Basel/Genf 2019
- Hui Mary, Hong Kongers are using blockchain archives to fight government censorship, 26. Mai 2021, <https://qz.com/2008673/hong-kongers-use-blockchain-to-fight-government-censorship/>
- Hülsmann Jörg Guido, The Ethics of Money Production, Auburn 2008
- Human Rights Foundation, The Bitcoin Development Fund, undatiert, <https://hrf.org/devfund>
- Humbel Claude, Decentralized Finance. A new frontier of global financial markets regulation, GesKR 2022, 9–25
- Humbel Claude, Die Regelung der Vor- und Nachhandelstransparenz in der Europäischen Union und der Schweiz, ZStP 299, Diss. Zürich 2019,
- Humbel Claude, Organisierte Handelssysteme in der Schweiz – Quo vadis?, GesKR 2021, 25–41
- Humbel Claude/Eckert Fabrice, Decentralized Exchanges: Grundlagen, Risiken und ausgewählte aufsichtsrechtliche Aspekte, SZW 2023, 10–23
- Humphrey Caroline, Barter and Economic Disintegration, Man 1985, 48–72
- Hürlimann-Kaup Bettina, Aussonderung von Bitcoins im Konkurs des Verwahrers?, AJP 2018, 1447–1449
- Hürlimann-Kaup Bettina, Zahlung mit Bitcoins: Zahlung mit Sachen?, in: Emmenegger Susan (Hrsg.), Zahlungsverkehr, SBT 2018, Basel 2018, 139–154
- Hutzler Doris, Art. 10 GwG Vermögenssperre, in: Ackermann Jürg-Beat (Hrsg.), Kommentar Kriminelles Vermögen – Kriminelle Organisation. Einziehung, Kriminelle Organisation, Finanzierung des Terrorismus, Geldwäscherei, Bd. II, Zürich/Basel/Genf 2018
- Iannarone Nicole G., Computer as Confidant: Digital Investment Advice and the Fiduciary Standard, Chicago-Kent Law Review 2018, 141–163
- Ibanez Luis-Daniel/Simperl Elena/Gandon Fabien/Henry Story, Redecentralizing the Web with Distributed Ledgers, IEEE Intelligent Systems, Institute of Electrical and Electronics Engineers 2017, 92–95
- IDEX Blog, A Complete List of Cryptocurrency Exchange Hacks [Updated], 16. Juli 2020, <https://blog.idx.io/all-posts/a-complete-list-of-cryptocurrency-exchange-hacks-updated>

- IDEX, History of DEXs: Phase 3. Off-chain Execution, On-chain Settlement, 12. November 2020, <https://blog.index.io/all-posts/phase-3-off-chain-execution-on-chain-settlement>
- IDEX, IDEX 2.0: The Next Generation of Non-Custodial Trading, 31. Oktober 2019, <https://blog.index.io/resources/index-20-whitepaper>
- IDEX, Terms of Service and Privacy, 3. Identity Verification, undatiert, <https://exchange.index.io/legal>
- IDEX, Terms of Service and Privacy, 7. Restricted Jurisdictions, undatiert, <https://exchange.index.io/legal>
- Iffland Jacques/Läser Alessandra, Tokenisierung von Effekten. Ein neuer Weg an den Kapitalmarkt, GesKR 2018, 415–423
- Iffland Jacques/Ben Hattar Ariel, Central Securities Depositories in the Age of Tokenized Securities, CapLaw-2020-05
- Inderst Roman, Retail Finance: Thoughts on Reshaping Regulation and Consumer Protection after the Financial Crisis, EBOR 2009, 455–464
- Ingham Geoffrey, The Nature of Money, Cambridge/Malden 2004
- International Organization for Standardization (ISO), Information technology – Open Systems Interconnection – Basic Reference Model: The Basic Model, ISO/IEC 7498-1:1994(E), 2. Aufl., Genf 1994
- IPFS, What is IPFS?, undatiert, <https://docs.ipfs.io/concepts/what-is-ipfs/>
- Isler Michael, Datenschutz auf der Blockchain, Jusletter vom 4. Dezember 2017
- Isler Vanessa/Eckert Fabrice, 10 Fragen und Antworten zum FIDLEG, GesKR 2021, 42–56
- Ito Joichi/Narula Neha/Ali Robleh, The Blockchain Will Do to the Financial System What the Internet Did to Media, Harvard Business Review, 8. März 2017, <https://hbr.org/2017/03/the-blockchain-will-do-to-banks-and-law-firms-what-the-internet-did-to-media>
- Jaag Tobias/Rüssli Markus, Staats- und Verwaltungsrecht des Kantons Zürich, 5. Aufl., Zürich/Basel/Genf 2019
- Jaccard Gabriel Olivier Benjamin, Smart Contracts and the Role of Law, Jusletter IT vom 23. November 2017
- Jaccard Gabriel, Le dépôt de cryptoactifs dans la Loi sur les Banques, Jusletter vom 25. Oktober 2021
- Jaccard Gabriel/Tharin Adrien, GDPR & Blockchain: the Swiss take, Jusletter IT vom 4. Dezember 2018
- Jaccard Michel/Toral Mehmet, Smart contracts – de la théorie à la pratique, in: Richa Alexandre/Canapa Damiano (Hrsg.), Droit et économie numérique, CEDIDAC 73, Bern 2021, 1–34

- Jackson Eric M., The PayPal Wars. Battles with eBay, the Media, the Mafia, and the Rest of Planet Earth, Los Angeles 2004
- Jacob Adolf-Friedrich/Klein Sebastian, Investment Banking. Bankpolitik, Methoden und Konzepte, Wiesbaden 1996
- Jacobides Michael G./Cennamo Carmelo/Gawer Annabelle, Towards a theory of eco-systems, Strategic Management Journal 2018, 1–22
- Jacquemart Nicolas, Offene Blockchainsysteme und die Schutzziele des schweizerischen Finanzmarktrechts: unter Berücksichtigung möglicher Ansatzpunkte einer Regulierung, Diss. Zürich 2020
- Jacquemart Nicolas/Meyer Stephan D., Der Bitcoin-/Bitcoin-Cash-Hardfork. Die auftragsrechtliche Ablieferungspflicht bei Kryptowährungs-Dienstleistungen im Lichte der bundesgerichtlichen Rechtsprechung, GesKR 2017, 469–485
- Jacquemart Nicolas/Meyer Stephan D., Globalisierte Digitalisierung – Die Bedeutung des Rechts im Zeitalter von Blockchains, in: Krauskopf Patrick L./Babey Fabio (Hrsg.), Internationales Wirtschaftsrecht. Recht im Wandel zwischen Globalisierung und Re-Nationalisierung, Basel 2017, 5–15
- Jaeger Raphael/Hautle Thomas, Bankenkonskurs und Einlagensicherung in der Schweiz, AJP 2009, 395–404
- Jagannathan Ravi, On Frequent Batch Auctions for Stocks, Journal of Financial Econometrics 2020, 1–17
- jakub, What is a Vampire Attack? SushiSwap Saga Explained, 12. September 2020, <https://finematics.com/vampire-attack-sushiswap-explained/>
- Janczuk-Gorywoda Agnieszka, Blockchain and Payments. A Tale about Re-Intermediation, in: Hacker Philipp/Lianos Ioannis/Dimitropoulos Georgios/Eich Stefan (Hrsg.), Regulating Blockchain. Techno-Social and Legal Challenges, Oxford/New York 2019, 259–274
- Jang Jehyuk/Lee Heung-No, Profitable Double-Spending Attacks, Applied Sciences 2020, Nr. 10, 1–23
- Jarass Hans, Probleme der extraterritorialen Geltung verwaltungsrechtlicher Gesetze am Beispiel des neuen Geldwäschegesetzes, RIW 2017, 642–650
- Jensen Michael C./Meckling William H., Theory of the Firm: Managerial Behavior, Agency Costs and Ownership Structure, Journal of Financial Economics 1976, 305–360
- Jentzsch Christoph, Decentralized Autonomous Organization To Automate Governance, Final Draft – Under Review, undatiert, <https://download.slock.it/public/DAO/WhitePaper.pdf>
- Johnstone Syren, Secondary Markets in Digital Assets: Rethinking Regulatory Policy in Centralized and Decentralized Environments, Stanford Journal of Blockchain, Law & Policy 2020, 146–188

- Joint Working Group on interVASP Messaging Standards (JWG), interVASP Messaging Standards, IVMS101, Issue 1 FINAL, Mai 2020
- Jones Gareth R., Organizational Theory, Design, and Change, 7. Aufl., Harlow, 2013
- Jordan Thomas J., Braucht die Schweizerische Nationalbank Eigenkapital?, Referat vor der Statistisch-Volkswirtschaftlichen Gesellschaft Basel, 28. September 2011
- Judge Kathryn, Fragmentation Nodes: A Study in Financial Innovation, Complexity, and Systemic Risk, Stanford Law Review 2012, 657–726
- Judge Kathryn, Intermediary Influence, The University of Chicago Law Review 2015, 573–642
- Juels Ari/Breidenbach Lorenz/Tramèr Florian, Fair Sequencing Services: Enabling a Provably Fair DeFi Ecosystem, 11. September 2020, <https://blog.chain.link/chain-link-fair-sequencing-services-enabling-a-provably-fair-defi-ecosystem/>
- Juels Ari/Eyal Ittay/Kelkar Mahimna, Miners, Front-Running-as-a-Service Is Theft, 7. April 2021, <https://www.coindesk.com/miners-front-running-service-theft>
- Juliano Antonio, dYdX Launches BTC Perpetual Contract Market, 20. April 2020, <https://medium.com/dydxderivatives/dydx-launches-btc-perpetual-contract-market-68f59b193f7e>
- Juliano Antonio, dYdX: A Standard for Decentralized Margin Trading and Derivatives, 6. August 2018, <https://whitepaper.dydx.exchange/>
- Jülicher Tim/Röttgen Charlotte, Bots im Kontext von Wirtschaftsrecht und Cybercrime, InTeR 2018, 15–19
- Jullien Bruno/Zantman Wilfried Sand-, The Economics of Platforms: A Theory Guide for Competition Policy, Information Economics and Policy 2020, 1–19
- Jutzi Thomas, Grenzüberschreitende Vermögensverwaltung, Jusletter vom 29. November 2021
- Jutzi Thomas/Abbühl Andri, Fintech und DLT. Privat- und finanzmarktrechtliche Grundlagen in der Schweiz, Bern 2023
- Jutzi Thomas/Schären Simon, Erfassung bewilligungspflichtiger Gruppensachverhalte in der Finanzmarktaufsicht, GesKR 2012, 411–419
- Jutzi Thomas/Schären Simon, Europäisches Finanzmarktrecht im Umbruch. Neuausrichtung der Drittstaatenordnung?, GesKR 2019, 408–423
- Kaal Wulf A., Decentralization – Past, Present, and Future, University of St. Thomas (Minnesota) Legal Studies Research Paper Nr. 19–23, 5. Dezember 2019, <https://ssrn.com/abstract=3411897>
- Kaiser Nathan, DLT-Regulierung und Kryptowelt: Eine Bestandesaufnahme und kritische Würdigung der heutigen Dynamik, in: Gericke Dieter (Hrsg.), A wonderful world: Neue Möglichkeiten, neues Recht, neue Herausforderungen, Europa Institut (EIZ), 8. Tagung zu Private Equity, Zürich 2022, 203–224

- Kahn Alfred E., *The Economics of Regulation: Principles and Institutions*, Bd. 1: Economic Principles, New York/London 1970
- Kahn David, *The Codebreakers. The Story of Secret Writing*, New York 1967
- Kahneman Daniel/Slovic Paul/Tversky Amos (Hrsg.), *Judgment under uncertainty: Heuristics and biases*, Cambridge/New York 1982
- Kaiser Carolin, *Privacy and Identity Issues in Financial Transactions. The Proportionality of the European Anti-Money Laundering Legislation*, Ede 2018
- Kaiser Dirk, *Finanzintermediation durch Banken und Versicherungen, Die theoretischen Grundlagen der Bankassurance*, Wiesbaden 2006
- Kaissar Nir, *Investors Need More Than Regulators for Protection*. In a world of Bitcoin and NFTs, knowledge will be more important than government rules, 7. September 2021, <https://www.bloomberg.com/opinion/articles/2021-09-07/personal-finance-investors-need-more-than-regulators-for-protection>
- Kaplan David M., *Technology and Globalization*, in: Berg Olsen Jan Kyrre/Pedersen Stig Andur/Hendricks Vincent F. (Hrsg.), *A Companion to the Philosophy of Technology*, Malden/Oxford/Chichester 2009, 325–328
- Kappos George/Yousaf Haaron/Maller Mary/Meiklejohn Sarah, *An Empirical Analysis of Anonymity in Zcash*, in: 2018 Proceedings of the 27th USENIX Conference on Security Symposium, Berkeley 2018, 463–477
- Kappos George/Yousaf Haaron/Piotrowska Ania M./Kanjalkar Sanket/Delgado-Sergu Sergi/ Miller Andrew/Meiklejohn Sarah, *An Empirical Analysis of Privacy in the Lightning Network*, in: Borisov Nikita/Diaz Claudia (Hrsg.), *Financial Cryptography and Data Security 2021*, Teil 1, LNCS 12674, Berlin/Heidelberg 2021, 167–187
- Karamé Ghassan O./Androulaki Elli/Roeschlin Marc/Gervais Arthur/Čapkun Srdjan, *Misbehavior in Bitcoin: A Study of Double-Spending and Accountability*, *ACM Transactions on Information and System Security* 2015, 2:1–2:32
- Kau Marcel, *Der Staat und der Einzelne als Völkerrechtssubjekte*, in: Graf Vitzthum Wolfgang/Proelß Alexander, *Völkerrecht*, 7. Aufl., Berlin/Boston 2016
- Kaufmann Christine, *Multistakeholder Participation in Cyberspace*, *SRIEL* 2016, 217–234
- Kaulartz Markus, *Die Blockchain-Technologie. Hintergründe zur Distributed Ledger Technology und zu Blockchains*, *CR* 2016, 474–480
- Kaulartz Markus/Heckmann Jörn, *Smart Contracts – Anwendungen der Blockchain-Technologie*, *CR* 2016, 618–624
- Kelkar Mahimna/Zhang Fan/Goldfeder Steven/Juels Ari, *Order-Fairness for Byzantine Consensus*, in: Micciancio Daniele/Ristenpart Thomas (Hrsg.), *Advances in Cryptology – CRYPTO 2020*, Bd. 3, LNCS 12172, Cham 2020, 451–480
- Kelsen Hans, *Reine Rechtslehre. Einleitung in die rechtswissenschaftliche Problematik, Studienausgabe der 1. Auflage 1934*, in: Jestaedt Matthias (Hrsg.), *Tübingen* 2008

- Kerkemeyer Andreas, Blockchain-Transaktionen im Internationalen Recht, ZHR 2020, 793–829
- Kerkemeyer Andreas, Herausforderungen des Blockchain-Netzwerks für das Kapitalmarktrecht, ZGR 2020, 654–687
- Kerya Alex, GHash.IO is open for discussion, 16. Juni 2014, <https://web.archive.org/web/20140625201650/https://blog.cex.io/ghash-io-51-percent/>
- Keynes John Maynard, A Treatise on Money. The Pure Theory of Money, Bd. 1, London 1914
- Keynes John Maynard, The General Theory of Employment, Interest and Money, in: Robinson Austin/Moggridge Donald (Hrsg.), The Collected Writings of John Maynard Keynes, Bd. VII, Cambridge/New York 2013
- Khwaja Asim Ijaz/Mian Atif, Rent Seeking and Corruption in Financial Markets, Annual Review of Economics 2011, 579–600
- Kidd Jeremy, Fintech: Antidote to Rent-Seeking?, Chicago-Kent Law Review 2018, 165–192
- Kielholz Walter B., Trend zur Disintermediation im Finanzsektor, 5. Juli 2007, https://www.nzz.ch/trend_zur_disintermediation_im_financektor-1.516707
- Kieninger Eva-Maria, Wettbewerb der Privatrechtsordnungen im Europäischen Binnenmarkt. Studien zur Privatrechtskoordinierung in der Europäischen Union auf den Gebieten des Gesellschafts- und Vertragsrechts, Tübingen 2002
- Kiepuszewski Bartek, OasisDEX – past, present, future and its role in the DeFi ecosystem, 27. September 2019, <https://youtu.be/mwkl7beq0m8>
- Kilgus Sabine, Effektivität von Regulierung im Finanzmarktrecht, Zürich/St. Gallen 2007
- Kim Geun-Hyung, How Will Blockchain Technology Affect the Future of the Internet?, in: Park James J./Fong Simon James/Pan Yi/Sung Yunsick (Hrsg.), Advances in Computer Science and Ubiquitous Computing. CSA-CUTE 2019, Singapur 2021, 289–294
- King Mervyn, The End of Alchemy. Money, Banking and the Future of the Global Economy, London 2017
- Kinsella N. Stephan, Against Intellectual Property, Auburn 2008
- Kirchgässner Gebhard, Homo Oeconomicus, 4. Aufl., Tübingen 2013
- Kirilenko Andrei/Kyle Albert S./Samadi Mehrdad/Tuzan Tugkan, The Flash Crash: High-Frequency Trading in an Electronic Market, The Journal of Finance 2017, 967–998
- Kirzner Israel M., Competition and Entrepreneurship, in: Boettke Peter J./Sautet Frédéric (Hrsg.), The Collected Works of Israel M. Kirzner, Indianapolis 2013

- Kirzner Israel M., The Perils of Regulation: A Market-Process Approach, in: Kirzner Israel M. (Hrsg.), *Discovery and the Capitalist Process*, Chicago/London 1985
- Kisagun Can, Secret Markets: Front Running Prevention for Automated Market Makers, 8. Oktober 2020, <https://scrt.network/blog/secret-markets-front-running-prevention/>
- Kivlighan Isa, Aave Admin Key Handover, 28. Oktober 2020, <https://medium.com/aave/aave-admin-key-handover-3e09e603d348>
- Klebeck Ulf/Dobrauz-Saldapenna Günther, Einleitung, in: Klebeck Ulf/Dobrauz-Saldapenna Günther (Hrsg.), *Rechtshandbuch Digitale Finanzdienstleistungen. FinTechs, Mobile Payment, Crowdfunding, Blockchain, Kryptowährungen, ICOs, Robo-Advice*, München 2018, 1–32
- Klein Benjamin, The Competitive Supply of Money, *Journal of Money, Credit and Banking* 1974, 423–453
- Kleine Matthias, Das OSI-Referenzmodell, undatiert, <https://www.selflinux.de/selflinux/html/osi.html>
- Kleiner Beat, *Internationales Devisen-Schuldrecht. Fremdwährungs-, Euro- und Rechnungseinheitsschulden*, Zürich 1985
- Kley Andreas, Menschenwürde als Rechtsprinzip? Überlegungen zur Rolle der Menschenwürde als Argument in rechtlichen und politischen Verfahren, in: Schwinges Christoph Rainer (Hrsg.), *Veröffentlichungen der Gesellschaft für Universitäts- und Wissenschaftsgeschichte*, Bd. 10, Basel 2008, 259–289
- Klöhn Lars, *Kapitalmarkt, Spekulation und Behavioral Finance. Eine interdisziplinäre und vergleichende Analyse zum Fluch und Segen der Spekulation und ihrer Regulierung durch Recht und Markt*, Berlin 2006
- Klöhn Lars, Wertpapierhandelsrecht diesseits und jenseits des Informationsparadigmas, *ZHR* 2013, 349–387
- Knapp Georg Friedrich, *The State Theory of Money*, London 1924
- Knight Frank H., *Risk, Uncertainty and Profit*, New York 1964
- Knobloch Stefan, Weitgehende Abschaffung der Inhaberaktien und weitere Neuerungen durch das Global-Forum-Gesetz, in: Müller Matthias P.A./Forrer Lucas/Zuur Floris (Hrsg.), *Das Aktienrecht im Wandel. Zum 50. Geburtstag von Hans-Ueli Vogt*, Zürich/St. Gallen 2020, 345–365
- Knorr Cetina Karin/Preda Alex, Introduction, in: Knorr Cetina Karin/Preda Alex (Hrsg.), *The Sociology of Financial Markets*, Oxford/New York 2005, 1–14
- Koenig Beat Gino, *Das Kassa- und Termingeschäft im Interbankendevisenhandel. Eine rechtliche Analyse*, Zürich 1989

- Kogens Ronald/Luchsinger Gähwiler Catrina, Token als Erklärungsträger für Forderungs- und Mitgliedschaftsrechte. Rivalisierende, unkörperliche Gegenstände als Novität – eine zivilrechtliche Einordnung, Jusletter vom 17. Dezember 2018
- Kogens Ronald/Montanari Mark, Möglichkeiten zur rechtsgeschäftlichen Begründung von Sicherungsrechten an Kryptowährungen als unkörperliche Gegenstände sui generis unter geltendem Recht, SZW 2021, 461–469
- de Koker Louis, The FATF's customer identification framework: fit for purpose?, Journal of Money Laundering Control 2014, 281–295
- Kokorin Ilya, The anatomy of crypto failures and investor protection under MiCAR, Capital Markets Law Journal 2023, 1–26
- Kolev Stefan, Neoliberale Leitideen zum Staat. Die Rolle des Staates in der Wirtschaftspolitik im Werk von Walter Eucken, Friedrich August von Hayek, Ludwig von Mises und Wilhelm Röpke, Diss. Hamburg 2011, <http://hdl.handle.net/10419/54194>
- Kollmann Hanns-Peter, Autonome und intelligente Wertpapierhandelssystem. Analyse, Regulierung und Haftung, Tübingen 2019
- Komodo Team, Community Update on AtomicDEX & KYC/AML, 21. Oktober 2020, <https://komodoplatfrom.com/en/blog/community-update-on-atomicdex-kyc-aml/>
- Komodo Team, Standby: The Regulation is Coming, 9. Oktober 2020, <https://komodo-platform.com/en/blog/standby-the-regulation-is-coming/>
- Komodo, AtomicDEX and Atomic Swaps, Additional Details, Dealing with Confirmations, 2020, <https://developers.komodoplatfrom.com/basic-docs/start-here/core-technology-discussions/atomicdex.html#additional-details>
- Komodo, AtomicDEX and Atomic Swaps, Atomic Swaps, 2020, <https://developers.komodoplatfrom.com/basic-docs/start-here/core-technology-discussions/atomicdex.html#atomic-swaps>
- Komodo, AtomicDEX and Atomic Swaps, Order Matching with Full-Relay and Non-Relay Nodes, 2020, <https://developers.komodoplatfrom.com/basic-docs/start-here/core-technology-discussions/atomicdex.html#the-decentralized-order-book>
- Komodo, Introduction to AtomicDEX, Why is AtomicDEX Special?, 2020, <https://docs.komodoplatfrom.com/basic-docs/atomicdex/atomicdex-tutorials/introduction-to-atomicdex.html#why-is-atomicdex-special>
- Komodo, Komodo's Atomic-Swap Powered, Decentralized Exchange: Barterdex, 2019, <https://docs.komodoplatfrom.com/whitepaper/chapter6.html>
- Köndgen Johannes, Effizienzorientierung im Kapitalmarktrecht?, in: Fleischer Holger/Zimmer Daniel (Hrsg.), Effizienz als Regelungsziel im Handels- und Wirtschaftsrecht, Frankfurt a.M. 2008, 100–139

- König Elke, Nach 5 Jahren Finanzkrise: Hat der Wettbewerb als Ordnungsprinzip auf den Finanzmärkten ausgedient?, in: Körber Torsten (Hrsg.), Wettbewerbsbeschränkungen auf staatlich gelenkten Märkten. Referate der 4. Göttinger Kartellrechtsgespräche vom 13. Juni 2014 anlässlich des 80. Geburtstags von Prof. Dr. Dr. h.c. Ulrich Immenga, Baden-Baden 2015, 103–106
- Konstantopoulos Georgios/Buterin Vitalik, Ethereum Reorgs After The Merge, 20. Juli 2021, <https://www.paradigm.xyz/2021/07/ethereum-reorgs-after-the-merge/>
- Koopman Christopher/Mitchell Matthew/Thierer Adam, The Sharing Economy and Consumer Protection Regulation: The Case for Policy Change, The Journal of Business, Entrepreneurship & the Law 2015, 529–545
- Koops Bert-Jaap/Kosta Eleni, Looking for some light through the lens of «cryptowar» history: Policy options for law enforcement authorities against «going dark», Computer Law & Security Review 2018, 890–900
- Köppelmann Martin, DutchX – fully decentralized auction based exchange, Juli 2018, <https://ethresear.ch/t/dutchx-fully-decentralized-auction-based-exchange/2443>
- Koppl Roger, From Crisis to Confidence. Macroeconomics after the Crash, London 2014
- Kose M. Ayhan/Nagle Peter/Ohnsorge Franziska/Sugawara Naotaka, Global Waves of Debt. Causes and Consequences, Washington 2020
- Kraakman Reinier H., Gatekeepers: The Anatomy of a Third-Party Enforcement Strategy, Journal of Law, Economics, & Organization 1986, 53–104
- Kraakman Reinier, Agency Problems and Legal Strategies, in: Kraakman Reinier/Armour John/Davies Paul/Enriques Luca/Hansmann Henry/Hertig Gerard/Hopt Klaus/Kanda Hideki/Pargendler Mariana/Ringe Wolf-Georg/Rock Edward (Hrsg.), The Anatomy of Corporate Law. A Comparative and Functional Approach, 3. Aufl., Oxford/New York 2017, 29–47
- Kramer Stefan/Meier Urs, Tokenisierung von Finanzinstrumenten. Gemäss dem Entwurf des Bundesgesetzes zur Verbesserung der Rahmenbedingungen für Blockchain/DLT, GesKR 2020, 60–77
- Kramer Stefan/Oser David/Meier Urs, Tokenisierung von Finanzinstrumenten de lege ferenda. Unter besonderer Berücksichtigung von nicht kotierten Aktien, Jusletter vom 6. Mai 2019
- Kramer Stefan/Wyss Dominic, Verwahrung von digitalen Aktiven, in: Weber Rolf H./Kuhn Hans (Hrsg.), Entwicklungen im Schweizer Blockchain-Recht, Basel 2021
- Kreutler Kei, Announcing Gnosis Protocol, 15. April 2020, <https://blog.gnosis.pm/announcing-the-gnosis-protocol-89b3d7794da7>
- Kroll Joshua A./Davey Ian C./Felten Edward W., The Economics of Bitcoin Mining, or Bitcoin in the Presence of Adversaries, The Twelfth Workshop on the Economics of Information Security (WEIS 2013), Washington, DC 2013

- Kronke Herbert/Haubold Jens, Börsen- und Kapitalmarktrecht, in: Kronke Herbert/Melis Werner/Kuhn Hans (Hrsg.), Handbuch Internationales Wirtschaftsrecht, 3. Aufl., Köln/Zürich 2017
- Krueger Anne O., The Political Economy of the Rent-Seeking Society, The American Economic Review 1974, 291–303
- Kübler Friedrich, Effizienz als Rechtsprinzip. Überlegungen zum rechtspraktischen Gebrauch ökonomischer Argumente, in: Baur Jürgen F./Hopt Klaus J./Mailänder K. Peter (Hrsg.), Festschrift für Ernst Steindorff zum 70. Geburtstag am 13. März 1990, Berlin/New York 1990, 687–704
- Kuhn Hans, Digitale Aktiven im schweizerischen Privatrecht, in: Weber Rolf H./Kuhn Hans (Hrsg.), Entwicklungen im Schweizer Blockchain-Recht, Basel 2021
- Kuhn Hans, Kollisionsrechtliche Aspekte der Derivateregulierung, SZW 2014, 362–382
- Kuhn Hans, Primärmarktregulierung, in: Weber Rolf H./Kuhn Hans (Hrsg.), Entwicklungen im Schweizer Blockchain-Recht, Basel 2021
- Kuhn Hans, Taxonomie, in: Weber Rolf H./Kuhn Hans (Hrsg.), Entwicklungen im Schweizer Blockchain-Recht, Basel 2021
- Kuhn Hans/Stengel Cornelia/Meisser Luzius/Weber Rolf H., Wertrechte als Rechtsrahmen für die Token-Wirtschaft, Jusletter IT vom 23. Mai 2019
- Kuhn Hans/Weber Rolf H., Einleitung, in: Weber Rolf H./Kuhn Hans (Hrsg.), Entwicklungen im Schweizer Blockchain-Recht, Basel 2021
- Kuhn Hans/Weber Rolf H., Zur Umsetzung des Basler Krypto-Standards in der Schweiz. Wie verhält sich nationale Finanzmarktpolitik zu internationalen Standards?, Jusletter IT vom 15. Februar 2024
- Kuhn Thomas S., The Structure of Scientific Revolutions, 3. Aufl., Chicago/London 1996
- Kunz Michael, Der Fluch der bösen Tat. Anmerkungen zum neuen DLT-Bundesgesetz, Jusletter vom 14. Dezember 2020
- Kunz Michael, Technologieneutralität – falsch verstanden. Anmerkungen zur FINMA-Aufsichtsmitteilung 2/2019, Jusletter vom 18. November 2019
- Kunz Peter V., Crowdfunding, Jusletter vom 25. August 2014
- Kunz Peter V., FINMA-Regulierung(en): Macht des Faktischen versus Rechtsstaatlichkeit, Jusletter vom 7. Mai 2018
- Kunz Peter V., Investmentgesellschaften – ein Testfall für das Geldwäschereigesetz (GwG)?, ZBJV 2006, 249–264
- Kunz Peter V., Sondermethodik zur wirtschaftsrechtlichen Rechtsanwendung?, recht 2017, 141–156
- Kunz Peter V./Jutzi Thomas/Schären Simon, Geldwäschereigesetz (GwG), Bern 2017 (SHK GwG-Autor, Art. N)

- Kuster Hans, Wer ist Finanzintermediär nach dem Geldwäschereigesetz?, SZW 1999, 233–243
- Kwon Yujin/Liu Jian/Kim Minjeong/Song Dawn/Kim Yongdae, Impossibility of Full Decentralization in Permissionless Blockchains, Proceedings of the 1st ACM Conference on Advances in Financial Technologies 2019, 110–123
- Kyber Network, Kyber Fed Price Reserve (FPR): On-Chain Market Making for Professionals, 9. Juni 2020, <https://blog.kyber.network/kyber-fed-price-reserve-fpr-on-chain-market-making-for-professionals-7fea29ceac6c>
- Kyber Network, Kyber: An On-Chain Liquidity Protocol, v.01, 22. April 2019, https://files.kyber.network/Kyber_Protocol_22_April_v0.1.pdf
- Kyber Network/BitGo Inc/Republic Protocol, Wrapped Tokens. A multi-institutional framework for tokenizing any asset, Whitepaper v.02, 24. Januar 2019, <https://wbtc.network/assets/wrapped-tokens-whitepaper.pdf>
- Laffont Jean-Jacques, The New Economics of Regulation Ten Years Later, *Econometrica* 1994, 507–537
- Laffont Jean-Jacques/Tirole Jean, The Politics of Government Decision-Making: A Theory of Regulatory Capture, *The Quarterly Journal of Economics* 1991, 1089–1127
- Lai Tony, Blockchain, Law and Governance: General Conclusion, in: Cappiello Benedetta/Carullo Gherardo (Hrsg.), *Blockchain, Law and Governance*, Cham 2021, 289–304
- Lamont Owen A., Short Sale Constraints and Overpricing, in: Fabozzi Frank J. (Hrsg.), *Short Selling. Strategies, Risks, and Rewards*, Hoboken 2004, 179–204
- Lamport Leslie, Paxos Made Simple, *ACM SIGACT News* 2001, Nr. 4, 51–58
- Lamport Leslie, The Part-Time Parliament, *ACM Transactions on Computer Systems* 1998, 133–169
- Lamport Leslie/Shostak Robert/Pease Marshall, The Byzantine Generals Problem, *ACM Transactions on Programming Languages and System* 1982, 382–401
- Landes William M./Posner Richard A., *The Economic Structure of Intellectual Property Law*, Cambridge/London 2003
- Langenbucher Katja, Digitales Finanzwesen. Vom Bargeld zu virtuellen Währungen, *AcP* 2018, 385–429
- Latimer Paul/Maume Philipp, Promoting Information in the Marketplace for Financial Services. *Financial Market Regulation and International Standards*, Cham 2015
- Laurie Ben, Decentralised Currencies Are Probably Impossible. But Let's at Least Make Them Efficient, 5. Juli 2011, <https://www.links.org/files/decentralised-currencies.pdf>

- Lavoie Don/Baetjer Howard/Tulloch William, High-tech Hayekians, in: Birner Jack/Garrouste Pierre (Hrsg.), Markets, Information and Communication. Austrian perspectives on the Internet economy, London/New York 2004, 91-125
- Le Goues Claire/Forrest Stephanie/Weimer Westley, The Case for Software Evolution, in: Proceedings of the FSE/SDP workshop on Future of software engineering research, New York 2010, 205-210
- Lee Barton E./Moroz Daniel J./Parkes David C., The Political Economy of Blockchain Governance, 8. Februar 2020, <https://ssrn.com/abstract=3537314>
- Lee Jei Young, A decentralized token economy: How blockchain and cryptocurrency can revolutionize business, Business Horizons 2019, 773-784
- Lee Joseph, Crypto-Finance, Law and Regulation. Governing an Emerging Ecosystem, Abingdon/New York 2022
- Lee Timothy B., Entangling the Web, 3. August 2006, <https://www.nytimes.com/2006/08/03/opinion/03lee.html>
- Leeson Peter T., Government, clubs, and constitutions, Journal of Economic Behavior & Organization 2011, 301-308
- Lehmann Matthias, Who Owns Bitcoin? Private Law Facing the Blockchain, Minnesota Journal of Law, Science & Technology 2019, 93-136
- Lehmann Matthias, Global Rules for a Global Market Place? Regulation and Supervision of Fintech Providers, Boston University International Law Journal 2020, 118-256
- Leimgruber Dominik/Flückiger Björn-Gunnar, Schweizer Fintech-Regulierung – Ein Überblick, Jusletter vom 6. November 2017
- Leiner Barry M./Cerf Vinton G./Clark David D./Kahn Robert E./Kleinrock Leonard/Lynch Daniel C./Postel Jon/Roberts Larry G./Wolff Stephen, Brief History of the Internet, 1997
- Leins-Zurmuehle Sarah, Ideation, Conceptualization, Realization – Discovering the Creative Scope in Software Engineering from the Perspective of Copyright and Patent Law, Diss. Zürich 2021
- Leising Matthew, MetaMask's Blockchain Mobile App Opens Doors For Next-Level Web, 2. September 2020, <https://www.bloomberg.com/news/articles/2020-09-02/metamask-s-blockchain-mobile-app-opens-doors-for-next-level-web>
- Leising Matthew, Out of the Ether. The Amazing Story of Ethereum and the \$55 Million Heist That Almost Destroyed It All, Hoboken 2021
- Leland Heyne E./Pyle David H., Informational Asymmetries, Financial Structure, and Financial Intermediation, The Journal of Finance 1977, 371-387

- Lelieveldt Simon, Dutch judge slaps DNB (Dutch central bank) on the wrist in court case of crypto-pioneer Bitonic on wallet-verification!, 11. April 2021, <https://finhstams-terdam.medium.com/dutch-judge-slaps-dnb-dutch-central-bank-on-the-wrist-in-court-case-of-crypto-pioneer-bitonic-on-b9ca5d9c145>
- Leonhard Robert Donald, Decentralized Finance on the Ethereum Blockchain, 25. März 2019, <https://ssrn.com/abstract=3359732>
- Lerner Abba P., Money as a Creature of the State, The American Economic Review 1947, 312–317
- Lerner Josh/Tirole Jean, Some Simple Economics of Open Source, The Journal of Industrial Economics 2002, 197–234
- Lerner Sergio Demian, P2PtradeX: P2P Trading between cryptocurrencies, 5. Juli 2012, <https://bitcointalk.org/index.php?topic=91843>
- Lessig Lawrence, Code and other laws of cyberspace, New York 1999
- Lessig Lawrence, Code, Version 2.0, New York 2006
- Lessig Lawrence, The Future of Ideas. The Fate of Commons in a Connected World, New York 2001
- Lesuisse Itamar, Argent: The most secure wallet, 6. Mai 2021, <https://www.argent.xyz/blog/a-new-era-for-crypto-security/>
- Lettieri Nicola, Law in Turing's Cathedral. Notes on the Algorithmic Turn of the Legal Universe, in: Barfield Woodrow (Hrsg.), The Cambridge Handbook of The Law of Algorithms, Cambridge/New York 2021, 691–721
- Levi Michael/Reuter Peter/Halliday Terence, Can the AML system be evaluated without better data?, Crime, Law and Social Change 2018, 307–328
- Levi Stuart/Drylewski Alex/Michael Daniel, Drawing lines in a borderless world: applying Morrison to crypto, 6. Juni 2023, <https://www.reuters.com/legal/legalindustry/drawing-lines-borderless-world-applying-morrison-crypto-2023-06-06/>
- Levine Michael E./Forrence Jennifer L., Regulatory Capture, Public Interest, and the Public Agenda: Toward a Synthesis, Journal of Law, Economics, & Organization 1990, 167–198
- Levy Steven, crypto. How the code rebels beat the government – saving privacy in the digital age, New York/London 2001
- Lewis Michael, Flash Boys. A Wallstreet Revolt, New York/London 2014
- Lewis Paul, The Ostroms and Hayek as Theorists of Complex Adaptive Systems: Commonality and Complementarity, in: Aligica Paul Dragos/Lewis Paul/Storr Virgil H. (Hrsg.), The Austrian and Bloomington Schools of Political Economy, Bingley 2017, 35–66
- Lewis Sarah Jamie, Twitter, 14. August 2018, <https://twitter.com/SarahJamieLewis/status/1029213719694209024> (Lewis, Authority, Twitter)

- Lewis Sarah Jamie, Twitter, 14. August 2018, <https://twitter.com/SarahJamieLewis/status/1029219421628203008> (Lewis, Holistic concept, Twitter)
- Lewis Sarah Jamie, Twitter, 14. August 2018, <https://twitter.com/SarahJamieLewis/status/1029216215342804993> (Lewis, Sybil, Twitter)
- Li Tian, Why we are forking 0x, 14. Dezember 2018, <https://medium.com/hydro-protocol/why-we-are-forking-0x-97dc48ee0426>
- Lianos Ioannis, Blockchain Competition. Gaining Competitive Advantage in the Digital Economy – Competition Law Implications, in: Hacker Philipp/Lianos Ioannis/Dimitropoulos Georgios/Eich Stefan (Hrsg.), Regulating Blockchain. Techno-Social and Legal Challenges, Oxford/New York 2019, 329–410
- LibSubmarine, Defeat Front-Running on Ethereum, undatiert, m.w.H., <https://libsubmarine.org/>
- Liebau Daniel/Krapels Nicholas J., An Exploratory Essay on Minimum Disclosure Requirements for Cryptocurrency and Utility Token Issuers, Cryptoeconomic Systems 2021, 1–20
- Liebenberg Lauren, The Electronic Financial Markets of the Future, and survival strategies of the broker-dealers, New York 2002
- Lin Lindsay X., Deconstructing Decentralized Exchanges, Stanford Journal of Blockchain Law & Policy 2019, 58–77
- Lin Tom C.W., Infinite Financial Intermediation, Wake Forest Law Review 2015, 643–669
- Lipton Alexander/Cohen Lewis, DeFi: a path forward, International Financial Law Review vom 9. September 2021, <https://www.iflr.com/article/b1thnhzpsrjqf/defi-a-pathway-forward>
- Levi Stuart D./Lipton Alex B., An Introduction to Smart Contracts and Their Potential and Inherent Limitations, Harvard Law School Forum on Corporate Governance 2018, 26. Mai 2018, <https://corpgov.law.harvard.edu/2018/05/26/an-introduction-to-smart-contracts-and-their-potential-and-inherent-limitations/>
- Liu Bowen/Sun Siwei/Szalachowski Pawel, SMACS: Smart Contract Access Control Service, in: 2020 50th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), Piscataway 2020, 221–232
- LocalBitcoins, About, undatiert, <https://localbitcoins.com/about>
- LocalBitcoins, Escrow – Your Best Friend on LocalBitcoins, 4. November 2020, <https://blog.localbitcoins.com/escrow-your-best-friend-on-localbitcoins-660882bad779>
- LocalBitcoins, FIN-FSA registers LocalBitcoins as a Virtual Currency Provider, 11. November 2019, <https://localbitcoins.com/blog/fin-fsa-registers-localbitcoins/>
- LocalBitcoins, Frequently Asked Questions, How am I protected from being scammed?, undatiert, <https://localbitcoins.com/faq>

- LocalBitcoins, Frequently Asked Questions, How does the feedback system work?, undatiert, <https://localbitcoins.com/faq>
- LocalBitcoins, LocalBitcoins' Guide to Account Verification, undatiert, <https://localbitcoins.com/guides/verification-guide>
- Locke John, Second Treatise of Government, in: Goldie Mark (Hrsg.), Oxford's World Classics, Oxford/New York 2016
- Lohmann Melinda F., Ein zukunftssträchtiger Haftungsrahmen für Künstliche Intelligenz, HAVE 2021, 111–120
- Long Caitlin, The Real Story Of The Repo Market Meltdown, And What It Means For Bitcoin, 25. September 2019, <https://www.forbes.com/sites/caitlinlong/2019/09/25/the-real-story-of-the-repo-market-meltdown-and-what-it-means-for-bitcoin/>
- Loopring, Guide: How to use the L2 Loopring Exchange, 2. März 2021, <https://loopring.org/#/post/guide-how-to-use-the-l2-loopring-exchange>
- Loopring, Loopring 3, undatiert, https://github.com/Loopring/protocols/blob/master/packages/loopring_v3/DESIGN.md
- Lopez Robert S., The Commercial Revolution of the Middle Ages. 950–1350, Cambridge/New York 1976
- Lu Alan, Building a Decentralized Exchange in Ethereum, 6. März 2017, <https://blog.gnosis.pm/building-a-decentralized-exchange-in-ethereum-eea4e7452d6e>
- Luckner Stefan/Schröder Jan/Slamka Christian/Franke Markus/Geyer-Schulz Andreas/Skiera Bernd/Spann Martin/Weinhardt Christof, Prediction Markets. Fundamentals, Designs, and Applications, Wiesbaden 2012
- Luhmann Niklas, Die Wirtschaft der Gesellschaft, 2. Aufl., Frankfurt a.M. 1996
- Luhmann Niklas, Funktionen und Folgen formaler Organisation, 2. Aufl., Berlin 1972
- Luhmann Niklas, Rechtssoziologie, 3. Aufl., Opladen 1987
- Luhmann Niklas, Soziale Systeme. Grundriss einer allgemeinen Theorie, 4. Aufl., Frankfurt a.M. 1991
- Lumineau Fabrice/Wang Wenqian/Schilke Oliver, Blockchain Governance – A New Way of Organizing Collaborations?, Organization Science 2021, 500–521
- Luther William J./Stein Smith Sean, Is Bitcoin a decentralized payment mechanism?, Journal of Institutional Economics 2020, 433–444
- Luthiger Reto, Geldwäschereibekämpfung bei Investmentgesellschaften. Die Anteilsbeziehung im GwG, Diss. St. Gallen/Zürich 2017
- Luthiger Reto, The New Swiss DLT Law – Curse Or Blessing?, IFC Review vom 14. Juli 2021, <https://www.ifcreview.com/articles/2021/july/the-new-swiss-dlt-law-curse-or-blessing/>

- Luthiger Reto/Kuhn Hans, Aufsichtsrechtliche Rahmenbedingungen, in: Weber Rolf H./Kuhn Hans (Hrsg.), *Entwicklungen im Schweizer Blockchain-Recht*, Basel 2021
- Lyons Daniel A., Public Use, Public Choice and the Urban Growth Machine: Competing Political Economies of Takings Law, *University of Michigan Journal of Law Reform* 2009, 265–322
- Ma June/Gans Joshua S./Tourky Rabee, Market Structure in Bitcoin Mining, Rotman School of Management Working Paper Nr. 3103104, 28. Juni 2019, <https://ssrn.com/abstract=3103104>
- MacCabe Kevin, *Die Abbildung von Vermögenswerten durch Anlage-Tokens*, BstRA 135, Diss. Basel 2019
- MacDonald Trent J., Spontaneous order in the formation of non-territorial political jurisdictions, Working Paper, 1. Mai 2015, <https://ssrn.com/abstract=2661250>
- MacDonald Trent J./Allen Darcy W.E./Potts Jason, Blockchains and the Boundaries of Self-Organized Economies: Predictions for the Future of Banking, in: Tasca Paolo/Aste Tomaso/Pelizzon Lorian/Perony Nicolas (Hrsg.), *Banking Beyond Banks and Money. A Guide to Banking Services in the Twenty-First Century*, Cham 2016, 279–296
- MacKinnon Rebecca/Hickok Elonnai/Bar Allon/Lim Hai-in, *Fostering Freedom Online: The Role of Internet Intermediaries*, UNESCO und Internet Society Bericht 2014
- MacMillan Douglas/Torbati Yeganeh, Robinhood and Citadel's relationship comes into focus as Washington vows to examine stock-market moves, 29. Januar 2021, <https://www.washingtonpost.com/business/2021/01/29/robinhood-citadel-gamstop-reddit/>
- MacNeil Iain G., *An Introduction to the Law on Financial Investment*, 2. Aufl., Oxford/Portland 2012
- Mägerle Jürg/Oleschak Robert, *Das Zahlungssystem Swiss Interbank Clearing (SIC)*, November 2019
- Mahlmann Matthias, *Rechtsphilosophie und Rechtstheorie*, 2. Aufl., Baden-Baden 2012
- Mainelli Michael/Milne Alistair, The Impact and Potential of Blockchain on the Securities Transaction Lifecycle, SWIFT Institute Working Paper Nr. 2015-007, 9. Mai 2016
- Maire Sonja/Gerszt Arie, DLT-Vorlage des Bundesrates: Zivil- und finanzmarktrechtliche Aspekte, in: Reutter Thomas U./Werlen Thomas (Hrsg.), *Kapitalmarkt – Recht und Transaktionen XV*, Zürich 2020, 121–150
- Maizar Karim/Kühne Armin, Crowdinvesting – Ein neues Kapitel im Kapitalmarkt?, in: Reutter Thomas U./Werlen Thomas (Hrsg.), *Kapitalmarkttransaktionen X*, Zürich/Genf/Basel 2016, 87–130

- MakerDAO Blog, What Are Blockchain Bridges, and Why are they Important for DeFi?, 19. März 2021, <https://blog.makerdao.com/what-are-blockchain-bridges-and-why-are-they-important-for-defi/>
- MakerDAO, Governance, undatiert, <https://community-development.makerdao.com/en/learn/governance>
- MakerDAO, Oracles, undatiert, <https://makerdao.world/en/learn/Oracles>
- MakerDAO, Recent Market Activity and Next Steps, 12. März 2020, <https://blog.makerdao.com/recent-market-activity-and-next-steps/>
- MakerDAO, The Maker Protocol: MakerDAO's Multi-Collateral Dai (MCD) System, undatiert, <https://makerdao.com/en/whitepaper/>
- Makridakis Spyros/Christodoulou Klitos, Blockchain: Current Challenges and Future Prospects/Applications, Future Internet 2019, 1–16
- Malinova Katya/Park Andreas, Market Design with Blockchain Technology, 26. Juli 2017, <https://ssrn.com/abstract=2785626>
- Malinvaud Edmond, Decentralization, in: Eatwell John/Milgate Murray/Newman Peter (Hrsg.), The New Palgrave: Allocation, Information and Markets, London/Basingstoke 1989, 71–76
- Malone Thomas W./Yates Joanne/Benjamin Robert I., Electronic Markets and Electronic Hierarchies, Communications of the ACM 1987, 484–497
- Malwa Shaurya, 70% of Ethereum Nodes Are Hosted on Centralized Services, 8. Oktober 2020, <https://decrypt.co/44321/70-of-ethereum-nodes-are-hosted-on-centralized-services>
- Manahov Viktor, Front-Running Scalping Strategies and Market Manipulation: Why Does High-Frequency Trading Need Stricter Regulation?, The Financial Review 2016, 363–402
- Mancini-Griffoli Tommaso/Soledad Martinez Peria Maria/Agur Itai/Ari Anil/Kiff John/Popescu Adina/Rochon Céline, Casting Light on Central Bank Digital Currency, in: Brummer Chris (Hrsg.), Cryptoassets. Legal, Regulatory, and Monetary Perspectives, Oxford/New York 2019, 307–337
- Mancini-Griffoli Tommaso/Soledad Martinez Peria Maria/Agur Itai/Ari Anil/Kiff John/Popescu Adina/Rochon Céline, Casting Light on Central Bank Digital Currency, IMF Staff Discussion Note, November 2018
- Mankiw N. Gregory, Principles of Microeconomics, 8. Aufl., Boston 2018
- Mann Maximilian, Die Decentralized Autonomous Organization – ein neuer Gesellschaftstyp? Gesellschaftsrechtliche und kollisionsrechtliche Implikationen, NZG 2017, 1014–1020
- Mansell Robin, The public's interest in intermediaries, info 2015, 8–18

- Mapperson Joshua, How many DeFi projects still have 'God Mode' admin keys? More than you think, 25. September 2020, <https://cointelegraph.com/news/how-many-defi-projects-still-have-god-mode-admin-keys-more-than-you-think>
- Marathon Digital Holdings, Marathon Digital Holdings Becomes the First North American Enterprise Miner to Produce Fully AML and OFAC Compliant Bitcoin, 5. Mai 2021, <https://ir.marathondh.com/news-events/press-releases/detail/1239/marathon-digital-holdings-becomes-the-first-north-american>
- MariaDB, Business Source License 1.1, <https://mariadb.com/bsl1/>
- Mariani Stefano, Coordination of Complex Sociotechnical Systems. Self-organisation of Knowledge in MoK, Cham 2016
- Markowitz Harry, Portfolio Selection, The Journal of Finance 1952, 77–91
- Martin Christopher Catherine, The Bridging Model: Exploring the Roles of Trust and Enforcement in Banking, Bitcoin, and the Blockchain, Nevada Law Journal 2015, 139–180
- Martinazzi Stefano/Flori Andrea, The evolving topology of the Lightning Network: Centralization, efficiency, robustness, synchronization, and anonymity, PloS ONE 2020, 1–18
- Martinelli Fernando/Mushegian Nikolai, A non-custodial portfolio manager, liquidity provider, and price sensor, 19. September 2019, <https://balancer.finance/whitepaper>
- Martiny Dieter, Die Anknüpfung an den Markt, in: Basedow Jürgen/Hopt Klaus J./Kötz Hein (Hrsg.), Festschrift für Ulrich Drobnig zum siebzigsten Geburtstag, Tübingen 1998, 389–408
- Marx Karl, Das Kapital. Kritik der politischen Ökonomie, Bd. 1, 39. Aufl., Berlin 2008
- Matic, FAQ, Polygon Multisigs, undatiert, <https://docs.matic.network/docs/faq/com-mit-chain-multisigs>
- Matonis Jon, WikiLeaks Bypasses Financial Blockade With Bitcoin, 20. August 2012, <https://www.forbes.com/sites/jonmatonis/2012/08/20/wikileaks-bypasses-financial-blockade-with-bitcoin/?sh=5e29d59d7202>
- Matthews Philip W., The Bankers' Clearing House, What it is and what it does, London 1921
- Mattli Walter, Darkness by Design. The Hidden Power in Global Capital Markets, Princeton/Oxford 2019
- Mauchle Yves, Die regulatorische Antwort auf FinTech: Evolution oder Revolution? Eine Verortung aktueller Entwicklungen, SZW 2017, 810–830
- Mauchle Yves, Tokenisierung unter dem revidierten Schweizer Recht – ein einfacher und kostengünstiger Weg zu einem liquiden Markt?, iusNet BR-KR 28.10.2021

- Mauchle Yves, Tokens als Effekten. Anknüpfung, Fungibilität und Abgrenzung mit funktionalem Vergleich zum US-Recht, GesKR 2022, 183–194
- Maurenbrecher Benedikt, Von der Investment Services Directive zur Markets in Financial Instruments Directive – ein Überblick aus Schweizer Sicht, AJP 2005, 19–38
- Maurenbrecher Benedikt/Leisinger Benjamin, Decentralized Finance (Teil 1), SJZ 2022, 647–657
- Maurenbrecher Benedikt/Leisinger Benjamin, Decentralized Finance (Teil 2), SJZ 2022, 704–718
- Maurenbrecher Benedikt/Meier Urs, Insolvenzrechtlicher Schutz der Nutzer virtueller Währungen, Jusletter vom 4. Dezember 2017
- Mavroudis Vasilios/Melton Hayden, Libra: Fair Order-Matching for Electronic Financial Exchanges, in: AFT '19 – Conference on Advances in Financial Technologies, New York 2019, 156–168
- Maxwell Gregory, [bitcoin-dev] Taproot: Privacy preserving switchable scripting, 23. Januar 2018, <https://lists.linuxfoundation.org/pipermail/bitcoin-dev/2018-January/015614.html>
- Maxwell Gregory, CoinJoin: Bitcoin privacy for the real world, 22. August 2013, <https://bitcointalk.org/index.php?topic=279249.0>
- Maxwell Gregory/Poelstra Andrew/Seurin Yannick/Wuille Pieter, Simple Schnorr multi-signatures with applications to Bitcoin, Designs, Codes and Cryptography 2019, 2139–2164
- May Peter J., Social Regulation, in: Salomon Lester M. (Hrsg.), The Tools of Government. A Guide to the New Governance, Oxford/New York 2002, 156–185
- May Robert M./Levin Simon A./Sugihara George, Ecology for bankers, Nature 2008, 893–895
- May Timothy C., Crypto Anarchy and Virtual Communities, in: Ludlow Peter (Hrsg.), Crypto Anarchy, Cyberstates, and Pirate Utopias, Cambridge/London 2001, 65–79
- May Timothy C., The Crypto Anarchist Manifesto, in: Ludlow Peter (Hrsg.), Crypto Anarchy, Cyberstates, and Pirate Utopias, Cambridge/London 2001, 61–64
- Mayer Thomas, Die Neue Ordnung des Geldes, 2. Aufl., München 2015
- McCall James, Part 3 Beyond the Wall – Does SEC regulation accomplish goals?, 29. September 2021, <https://lexdao.substack.com/p/part-3-beyond-the-wall-does-sec-regulation?>
- McChesney Fred S., Money for Nothing. Politicians, Rent Extraction, and Political Extortion, Cambridge/London 1997
- McConaghy Trent, The DCS Triangle. Decentralized, Consistent, Scalable. Pick any two., 10. Juli 2016, <https://blog.bigchaindb.com/the-dcs-triangle-5ce0e9e0f1dc>

- McLeod Chris, Who's along for the ride? Chris McLeod digs into the IP rights interests in the world's volatile digital currencies, CITMA Review März/April 2019, 16–20
- McMillan Jonathan, The End of Banking. Money, Credit, and the Digital Revolution, Zürich 2014
- Medina Eden, Rethinking algorithmic regulation, Kybernetes 2015, 1005–1019
- Mehrling Perry, The inherent hierarchy of money, in: Taylor Lance/Rezai Armon/Michl Thomas (Hrsg.), Social Fairness and Economics. Economic essays in the spirit of Duncan Foley, London/New York 2013, 394–404
- Meier Julia/Schuppli Benedikt, The DAO Hack and the Living Law of the Blockchain, in: Dal Molin-Kränzlin Alexandra/Schneuwly Anne Mirjam/Stojanovic Jasna (Hrsg.), Digitalisierung – Gesellschaft – Recht, APARIUZ Bd. 20, Zürich/St. Gallen 2019, 27–43
- Meier-Hayoz Arthur (Hrsg.), Berner Kommentar. Inhalt des Vertrages, Art. 19–22 OR, Bern 1991 (Autor, in: BK OR, Art. N)
- Meier-Hayoz Arthur, Abschied vom Wertpapier? ZBJV 1986, 385–401
- Meier-Hayoz Arthur/Forstmoser Peter, Schweizerisches Gesellschaftsrecht. Mit neuem Aktien- und Handelsregisterrecht, 13. Aufl., Bern 2023
- Meier-Hayoz Arthur/von der Crone Hans Caspar, Wertpapierrecht, 3. Aufl., Bern 2018
- Meier-Schatz Christian J., Über Entwicklung, Begriff und Aufgaben des Wirtschaftsrechts, ZSR 1982 I, 267–312
- Meier-Schatz Christian J., Wirtschaftsrecht und Unternehmenspublizität, Zürich 1989
- Meiklejohn Sarah/Orlandi Claudio, Privacy-Enhancing Overlays in Bitcoin, in: Brenner Michael/ Christin Nicolas/Johnson Benjamin/Rohloff Kurt (Hrsg.), Financial Cryptography and Data Security, LNCS 8976, Berlin/Heidelberg 2015, 127–141
- Meiklejohn Sarah/Pomarole Marjori/Jordan Grant/Levchenko Kirill/McCoy Damon/Voelker Geoffrey M./Savage Stefan, A fistful of bitcoins: characterizing payments among men with no names, IMC '13: Proceedings of the 2013 Internet Measurement Conference, 127–140
- Meirich David, Regulatorische Einordnung von Decentralized Finance, SSFM 144, Diss. Zürich 2023
- Meisser Christian/Meisser Luzius/Kogens Ronald, Verfügungsmacht und Verfügungsrecht an Bitcoins im Konkurs, Jusletter IT vom 24. Mai 2018
- Ménard Claude/Shirley Mary M., Introduction, in: Ménard Claude/Shirley Mary M. (Hrsg.), Handbook of New Institutional Economics, Dordrecht 2005
- Menger Carl, Grundsätze der Volkswirtschaftslehre, Wien 1871
- Menger Carl, On the Origin of Money, The Economic Journal 1892, 239–255
- Merkle Ralph C., Secure Communications Over Insecure Channels, Communications of the ACM 1978, 294–299

- Merkli Thomas, Internationales Verwaltungsrecht: Das Territorialitätsprinzip und seine Ausnahmen, in: XIII. Treffen der obersten Verwaltungsgerichtshöfe Österreichs, Deutschlands, des Fürstentums Liechtenstein und der Schweiz, Vaduz 2002, https://www.bger.ch/files/live/sites/bger/files/pdf/de/territorialitaetsprinzip_und_seine_ausnahmen.pdf
- Mersch Yves, Virtual currencies ante portas, Speech at the 39th meeting of the Governor's Club Bodrum, Turkey, 14. Mai 2018, <https://www.ecb.europa.eu/press/key/date/2018/html/ecb.sp180514.en.html>
- Mersinger Summer K., Dissenting Statement of Commissioner Summer K. Mersinger Regarding Enforcement Actions Against: 1) Opyn, Inc.; 2) Deridex, Inc.; and 3) ZeroEx, Inc., 7. September 2023, <https://www.cftc.gov/PressRoom/Speeches-Testimony/mersingerstatement090723>
- Mertens Peter/Bodendorf Freimut/König Wolfgang/Schumann Matthias/Hess Thomas/Buxmann Peter, Grundzüge der Wirtschaftsinformatik, 12. Aufl., Berlin 2017
- Merton Robert C., A Functional Perspective of Financial Intermediation, Financial Management 1995, 23–41
- Mesa, FAQ, What advantages do ring trades bring?, undatiert, <https://mesa.eth.link/#/faq>
- Messari Research, DEX v. EX – Unqualified Opinions #21, 24. Oktober 2018, <https://messari.substack.com/p/dex-v-ex-unqualified-opinions-21>
- Messari, Crypto Exchange Real Spot Volume, undatiert, <https://messari.io/exchanges>
- Messari, Messari Methodology: What Constitutes a DeFi Token, 18. August 2020, <https://messari.io/article/messari-methodology-what-constitutes-a-defi-token>
- Messias Johnnatan/Alzayat Mohamed/Chandrasekaran Balakrishnan/Gummadi Krishna P./Loiseau Patrick/Mislove Alain, Selfish & Opaque Transaction Ordering in the Bitcoin Blockchain: The Case for Chain Neutrality, IMC 2021 – ACM Internet Measurement Conference 2021, 1–16
- Metz Cade, The Bitcoin Schism Shows the Genius of Open Source, 19. August 2015, <https://www.wired.com/2015/08/bitcoin-schism-shows-genius-open-source/>
- MEV-Explore v0, Frequently Asked Questions (FAQ), What is MEV?, undatiert, <https://explore.flashbots.net/faq>
- MEV-Explore v0, Frequently Asked Questions (FAQ), Why MEV as Maximal Extractable Value instead of Miner Extractable Value?, undatiert, <https://explore.flashbots.net/faq>
- Meyer Stephan D., Dezentrale autonome Organisationen (DAOs) und das Gesellschaftsrecht der Zukunft. Selbstdurchsetzende Programme als Exekutivorgane globaler Peer-to-Peer-Gesellschaften, AJP 2023, 319–338
- Meyer Stephan D., Rechte an und aus Blockchain-basierten Crypto Tokens, ZStP 313, Diss. Zürich 2022

- Meyer Stephan D./Schuppli Benedikt, «Smart Contracts» und deren Einordnung in das schweizerische Vertragsrecht, recht 2017, 204–224
- Mian Atif/Sufi Amir, House of Debt. How They (and You) Caused the Great Recession, and How We Can Prevent It from Happening Again, Chicago/London 2014
- michael1011, Submarine Swaps, 19. Februar 2019, <https://medium.com/boltzHQ/submarine-swaps-c509ce0fb1db>
- Michaels Dave/Kiernan Paul, Crypto's 'DeFi' Projects Aren't Immune to Regulation, SEC's Gensler Says, 19. August 2021, <https://www.wsj.com/articles/cryptos-defi-projects-arent-immune-to-regulation-secs-gensler-says-11629365401>
- Micheler Eva, Custody Chains and Asset Values: Why Crypto-Securities Are Worth Contemplating, Cambridge Law Journal 2015, 505–533
- Micheler Eva/von der Heyde Luke, Holding, clearing and settling securities through blockchain/distributed ledger technology: creating an efficient system by empowering investors, Butterworths Journal of International Banking and Financial Law 2016, 652–656
- Michie Ranald C., The Global Securities Market. A History, Oxford/New York 2006
- Michie Ranald C., The London Stock Exchange. A History, Oxford/New York 1999
- Michie Ranald, Financial Capitalism, in: Neal Larry/Williamson Jeffrey G. (Hrsg.), The Cambridge History of Capitalism. The Spread of Capitalism from 1848 to the Present, Bd. 2, Cambridge/New York 2014, 230–263
- MicroStrategy, MicroStrategy Announces Over \$1B in Total Bitcoin Purchases in 2020, 21. Dezember 2020, <https://ir.microstrategy.com/news-releases/news-release-details/microstrategy-announces-over-1b-total-bitcoin-purchases-2020>
- MicroStrategy, MicroStrategy Completes \$650 Million Offering of 0.750% Convertible Senior Notes Due 2025, 11. Dezember 2020, <https://ir.microstrategy.com/news-releases/news-release-details/microstrategy-completes-650-million-offering-0750-convertible>
- Miers Ian/Garman Christina/Green Matthew/Rubin Aviel D., Zerocoin: Anonymous Distributed E-Cash from Bitcoin, 2013 IEEE Symposium on Security and Privacy 2013, 397–411
- Mik Eliza, Smart contracts: terminology, technical limitations and real world complexity, Law, Innovation and Technology 2017, 1–32
- Milgrom Paul/Roberts John, Economics, Organization and Management, Englewood Cliffs 1992
- Mill John Stuart, On Liberty, in: Bromwich David/Kateb George (Hrsg.), On Liberty, New Haven/London 2003

- Miller Andrew, Permissioned and Permissionless Blockchains, in: Shetty Sachin S./Kamhoua Charles A./Njilla Laurent L. (Hrsg.), *Blockchains for Distributed Systems Security*, Hoboken 2019, 193–203
- Miller Mark S./Drexler K. Eric, Markets and Computation: Agoric Open Systems, in: Huberman Bernardo A. (Hrsg.), *The Ecology of Computation*, New York 1988, 133–176
- Miller Steve, Decentralized Exchanges, 13. November 2018, <https://messari.io/re-source/decentralized-exchanges>
- Millon Marcia H./Thakor Anjan V., Moral Hazard and Information Sharing: A Model of Financial Information Gathering, *The Journal of Finance* 1985, 1403–1422
- Mills David/Wang Kathy/Malone Brendan/Ravi Anjana/Marquardt Jeff/Chen Clinton/Badev Anton/Brezinski Timothy/Fahy Linda/Liao Kimberley/Kargenian Vanessa/Ellithorpe Max/Ng Wendy/Baird Maria, Distributed ledger technology in payments, clearing, and settlement, Federal Reserve System, Finance and Economics Discussion Series 2016–095
- Milne Alistair, Central Securities Depositories and Securities Clearing and Settlement: Business Practice and Public Policy Concerns, in: Diehl Martin/Alexandrova-Kabadjova Biliana/Heuver Richard/Martínez-Jaramillo Serafín (Hrsg.), *Analyzing the Economics of Financial Market Infrastructures*, Hershey 2016, 334–358
- Mina Foundation, 22kB-Sized Blockchain – A Technical Reference, 12. März 2021, <https://minaprotocol.com/blog/22kb-sized-blockchain-a-technical-reference>
- Minsky Hyman P., *Stabilizing an Unstable Economy*, New York 2008
- Miraz Mahdi H./Donald David C., Atomic Cross-chain Swaps: Development, Trajectory and Potential of Non-monetary Digital Token Swap Facilities, *Annals of Emerging Technologies in Computing* 2019, 42–50
- Miraz Mahdi H./Donald David C., Lapps: Technological, Legal and Market Potentials of Blockchain Lightning Network Applications, ICISDM 2019: Proceedings of the 2019 3rd International Conference on Information System and Data Mining 2019, 185–189
- von Mises Ludwig, *Bureaucracy*, New Haven 1944
- von Mises Ludwig, *Human Action. A Treatise on Economics*, Auburn 1998
- von Mises Ludwig, *Theorie des Geldes und der Umlaufmittel*, 2. Aufl., Berlin 2005
- Mishkin Frederic S./Eakins Stanley G., *Financial Markets and Institutions*, 9. Aufl., Harlow/London 2018
- MME, Conceptual Framework for Legal and Risk Assessment of Crypto Tokens. Classification of decentralized blockchain-based assets, «Block 2» Version, 1. Mai 2018
- MME, Stellungnahme zur Vernehmlassung zu den DLT-Gesetzesänderungen, 27. Juni 2019, https://www.mme.ch/fileadmin/files/documents/Publikationen/2019/190630_MME_Stellungnahme_Vernehmlassung_DLT_Gesetzesänderungen.pdf

- Mockchain.io, Mockchain, 12. August 2019, <https://mockchain.io/>
- Moin Amani/Sekniqi Kevin /Sirer Emin Gun, SoK: A Classification Framework for Stablecoin Designs, in: Bonneau Joseph/Heninger Nadia (Hrsg.), Financial Cryptography and Data Security 2020, LNCS 12059, Cham 2020, 174–197
- Möllers Thomas M. J., Effizienz als Massstab des Kapitalmarktrechts: Die Verwendung empirischer und ökonomischer Argumente zur Begründung zivil-, straf- und öffentlich-rechtlicher Sanktionen, AcP 2008, 1–36
- Möllers Thomas M. J./Kernchen Eva, Information Overload am Kapitalmarkt. Plädoyer zur Einführung eines Kurzfinanzberichts auf empirischer, psychologischer und rechtsvergleichender Basis, ZGR 2011, 1–26
- Molo Giovanni/Drzalic Jana, Können Kryptowährungen compliant sein?, AJP 2019, 40–57
- Moloney Niamh, EU Securities and Financial Markets Regulation, 4. Aufl., Oxford/New York 2023
- Monsch Martin, Hochfrequenzhandel. Eine rechtsökonomische Analyse des Phänomens sowie eine rechtsdogmatische Betrachtung des schweizerischen Aufsichtsrechts unter funktionaler Berücksichtigung des europäischen Rechts, SSFM 126, Diss. Zürich/Basel/Genf 2018
- Montoya Christian, How one hacker stole thousands of dollars worth of cryptocurrency with a classic code injection..., 25. September 2017, <https://hackernoon.com/how-one-hacker-stole-thousands-of-dollars-worth-of-cryptocurrency-with-a-classic-code-injection-a3aba5d2bff0>
- Mooney Charles W., Jr., Beyond Intermediation: A New (Fintech) Model for Securities Holding Infrastructures, University of Pennsylvania Journal of Business Law 2020, 386–456
- Mooney Charles W., Jr., Beyond Negotiability: A New Model for Transfer and Pledge of Interests in Securities Controlled by Intermediaries, Cardozo Law Review 1990, 305–427
- Mooney Charles W., Jr., Global Standards for Securities Holding Infrastructures: A Soft Law/Fintech Model for Reform, Michigan Journal of International Law 2019, 531–547
- Mooney Charles W., Jr., The Truth About Shortfall of Intermediated Securities – perspectives under the Geneva Securities Convention, United States Law, and the Future European Legislation, in: Conac Pierre-Henri/Segna Ulrich/Thévenoz Luc (Hrsg.), Intermediated Securities: The Impact of the Geneva Securities Convention and the Future European Legislation, Cambridge/New York 2013, 160–192
- Moore Tyler/Christin Nicolas, Beware the Middleman: Empirical Analysis of Bitcoin-Exchange Risk, in: Sadeghi Ahmad-Reza (Hrsg.), Financial Cryptography and Data Security, LNCS 7859, Berlin/Heidelberg 2013, 25–33

- Morell Michael/Kirshner Josh/Schoenberger Thomas, An Analysis of Bitcoin's Use in Illicit Finance, 6. April 2021, https://cryptoforinnovation.org/resources/Analysis_of_Bitcoin_in_Illicit_Finance.pdf
- Morgan Nicholas, Lido Dominance Prompts Warnings About Liquid Staking Derivatives, 4. September 2023, <https://decrypt.co/154804/lido-lsd-liquid-staking-decentralization>
- Möri Barbara Anita, Blockchain und Datenschutz. Technische Möglichkeiten und rechtliche Herausforderungen anhand eines Use Cases, Jusletter IT vom 23. Mai 2019
- Morris David Z., DeFi Is Like Nothing Regulators Have Seen Before. How Should They Tackle It?, 19. Oktober 2021, <https://www.coindesk.com/policy/2021/10/19/defi-is-like-nothing-regulators-have-seen-before-how-should-they-tackle-it/>
- Morris David Z., Gary Gensler Isn't Buying your Decentralization Theater. The SEC chief has a point: DeFi is often not as decentralized as its proponents like to claim, 19. August 2021, <https://www.coindesk.com/markets/2021/08/19/gary-gensler-isnt-buying-your-decentralization-theater/>
- Morris David Z., The Node: Europe's Hidden Agenda on Crypto Wallets, 23. Juli 2021, <https://www.coindesk.com/europe-anonymous-crypto-wallets>
- Morscher Lukas/Staub Lukas, Tokenisierung von Effekten für Private Equity and Private Debt, in: Gericke Dieter (Hrsg.), Venture Capital Reinvented: Markt, Recht, Steuern, 7. Tagung Private Equity Tagungsband 2020, EIZ 207, Zürich 2021, 193–224
- Möser Malte/Böhme Rainer, Trends, Tips, Tolls: A Longitudinal Study of Bitcoin Transaction Fees, in: Brenner Michael/Christin Nicolas/Johnson Benjamin/Rohloff Kurt (Hrsg.), Financial Cryptography and Data Security, LNCS 8976, Berlin/Heidelberg 2015, 19–33
- Möser Malte/Böhme Rainer/Breuker Dominic, An Inquiry into Money Laundering Tools in the Bitcoin Ecosystem, 2013 APWG eCrime Researchers Summit 2014, 76–89
- Möslein Florian, Finanzinnovation und Rechtsordnung: Eine Einführung, in: Möslein Florian (Hrsg.), Finanzinnovation und Rechtsordnung. Gestaltung, unternehmerischer Einsatz und Marktregulierung, Zürich/Basel/Genf 2014, 1–44
- Möslein Florian, Smart Contracts im Zivil- und Handelsrecht, ZHR 2019, 254–293
- Mow Samson, Tether Lands on the Liquid Network, 29. Juli 2019, <https://blockstream.com/2019/07/29/en-tether-lands-on-the-liquid-network/>
- Mt Pelerin Group SA, bridge-v2, undatiert, <https://github.com/MtPelerin/bridge-v2/blob/master/contracts/exchange/Exchange.sol>
- Mt Pelerin Group SA, Mt Pelerin. Bringing the Entire Bank on Chain for Better, Fairer Banking, White Paper, version 2.2, undatiert, <https://www.mtpelerin.com/docs/mt-pelerin-white-paper.pdf>

- Mueller Bernhard, Is Tether a Black Swan?, 19. Juni 2021, <https://muellerberndt.medium.com/is-tether-a-black-swan-51095720b01c>
- Müller Christoph, Die Smart Contracts aus Sicht des Schweizerischen Obligationenrechts, ZBJV 2019, 330–352
- Müller Georg, Privateigentum heute. Vom Sinn des Eigentums und seiner privatrechtlichen Gewährleistung, ZSR 1981 II, 1–116
- Müller Georg/Uhlmann Felix, Elemente einer Rechtssetzungslehre, 3. Aufl., Zürich/Basel/Genf 2013
- Müller Lucien, «Eigenverantwortung» am Beispiel der privaten Internetnutzung, in: Gschwend Lukas/Hettich Peter/Müller-Chen Markus/Schindler Benjamin/Wildhaber Isabelle (Hrsg.), Recht im digitalen Zeitalter. Festgabe Schweizerischer Juristentag 2015 in St. Gallen, Zürich/St. Gallen 2015, 541–570
- Müller Lukas/Ong Malik, Aktuelles zum Recht der Kryptowährungen, AJP 2020, 198–212
- Müller Lukas/Reutlinger Milena/Kaiser Philippe J. A., Entwicklungen in der Regulierung von virtuellen Währungen in der Schweiz und der Europäischen Union, EuZ 2018, 80–102
- Müller Lukas/Seiler Reto, Smart Contracts aus Sicht des Vertragsrechts. Funktionsweise, Anwendungsfälle und Leistungsstörungen, AJP 2019, 317–328
- Müller Matthias P. A., Blockchain und Gesellschaftsrecht: ein Streifzug durch Möglichkeiten und Hürden, Expert Focus 2019, 485–489
- Murdoch Steven J., Quantifying and Measuring Anonymity, in: Garcia-Alfaro Joaquin/Lioudakis Georgios/Cuppens-Boulahia Nora/Foley Simon/Fitzgerald William M. (Hrsg.), Data Privacy Management and Spontaneous Security, LNCS 8247, Berlin/Heidelberg 2014, 3–13
- Murray Alex/Kuban Scott/Josefy Matt/Anderson Jon, Contracting in the Smart Era: The Implications of Blockchain and Decentralized Autonomous Organizations for Contracting and Corporate Governance, Academy of Management Perspectives 2019, 1–53
- Muzzy Everett/Anderson Mally, Measuring Blockchain Decentralization. An approach to quantifying decentralization of the Ethereum network over time, undatiert, <https://consensys.net/research/measuring-blockchain-decentralization/>
- Nabilou Hossein, Bitcoin Governance as a Decentralized Financial Market Structure, Stanford Journal of Blockchain Law & Policy 2021, 26–51
- Nabilou Hossein, How to regulate Bitcoin? Decentralized regulation for a decentralized cryptocurrency, International Journal of Law and Information Technology 2019, 266–291
- Nadler Matthias/Schär Fabian, Decentralized Finance, Centralized Ownership? An Iterative Mapping Process to Measure Protocol Token Distribution, 16. Dezember 2020, <https://arxiv.org/abs/2012.09306>

- Nadler Matthias/Schär Fabian, Tornado Cash and Blockchain Privacy: A Primer for Economists and Policymakers, Federal Reserve Bank of St. Louis Review 2023, 122–136
- Nagel Thomas, Der persönliche und sachliche Geltungsbereich des schweizerischen Geldwäschereigesetzes (GwG). Mit rechtsvergleichenden Hinweisen zu internationalen Standards, dem Recht der Europäischen Union und dem deutschen Recht, SSFM 132, Diss. Zürich/Basel/Genf 2020
- Nagel Thomas, Soll das Aufbewahren von Vermögenswerten künftig dem Geldwäschereigesetz unterstellt werden?, GesKR 2020, 113–122
- Nagel Thomas, Dienstleistungen für den Zahlungsverkehr unter dem Geldwäschereigesetz, GesKR 2023, 72–87
- Nakamoto Satoshi, Bitcoin: A Peer-to-Peer Electronic Cash System, 31. Oktober 2008, <https://bitcoin.org/bitcoin.pdf>
- Nakamoto Satoshi, Re: Repost: How anonymous are bitcoins? 25. November 2009, <https://bitcointalk.org/index.php?topic=8.msg34#msg34>
- Nakamoto Satoshi, Re: Scalability and transaction rate, 29. Juli 2010, <https://bitcointalk.org/index.php?topic=532.msg6306#msg6306>
- Nansen, Eth2 Deposit Contract, undatiert, <https://pro.nansen.ai/eth2-deposit-contract>
- Narayanan Arvind, What Happened to the Crypto Dream?, Part 1, IEEE Security & Privacy 2013 II, 75–76
- Narayanan Arvind, What Happened to the Crypto Dream?, Part 2, IEEE Security & Privacy 2013 II, 68–71
- Narayanan Arvind/Bonneau Joseph/Felten Edward/Miller Andrew/Goldfeder Steven, Bitcoin and Cryptocurrency Technologies. A Comprehensive Introduction, Princeton/Oxford 2016
- Narayanan Arvind/Clark Jeremy, Bitcoin's Academic Pedigree. The concept of cryptocurrencies is built from forgotten ideas in research literature, acmqueue 2017, 1–30
- National Institute of Standards and Technology (NIST), Guide to General Server Security, Juli 2008
- National Taxpayers Union, Interview with Milton Friedman on Anti-Trust and Tech, 1999, <https://youtu.be/mlwxdyLnMXM?t=872>
- Nayak Malathi, Ripple Says SEC 'Picking' Crypto Winners and Losers in XRP Fight, 5. März 2021, <https://www.bloomberg.com/news/articles/2021-03-05/ripple-says-sec-picking-crypto-winners-and-losers-in-xrp-fight>
- Nef Robert, Lob des Non-Zentralismus, 2. Aufl., Sankt Augustin 2006
- Nelson Danny, Binance Blockade of Wasabi Wallet Could Point to a Crypto Crack-Up, 26. Dezember 2019, <https://www.coindesk.com/policy/2019/12/26/binance-blockade-of-wasabi-wallet-could-point-to-a-crypto-crack-up/>

- Nesbitt Mark, Deep Chain Reorganization Detected on Ethereum Classic (ETC), 7. Januar 2019, <https://blog.coinbase.com/ethereum-classic-etc-is-currently-being-51-attacked-33be13ce32de>
- Newton Casey, Twitter officially kills off key features in third-party apps, The Verge, 16. August 2018, <https://www.theverge.com/2018/8/16/17699626/twitter-third-party-apps-streaming-api-deprecation>
- Neyer Gene/Geva Benjamin, Blockchain and Payment Systems: What are the Benefits and Costs?, Journal of Payments Strategy and Systems 2017, 215–225
- Nguyen Andrew/Luu Loi/Ng Ming, Dynamic Automated Market Making, Februar 2021, <https://files.kyber.network/DMM-Feb21.pdf>
- Nicholls Christopher C., Open Banking and the Rise of FinTech: Innovative Finance and Functional Regulation, Banking & Finance Law Review 2019, 121–151
- Nick Jonas/Poelstra Andrew/Sanders Gregory, Liquid: A Bitcoin Sidechain, Whitepaper, 22. Mai 2020, <https://blockstream.com/assets/downloads/pdf/liquid-whitepaper.pdf>
- Niepert Dirk, Reserves for All? Central Bank Digital Currency, Deposits, and Their (Non-)Equivalence, International Journal of Central Banking 2020, 211–238
- Nikolić Ivica/Kolluri Aashish/Sergey Ilya/Saxena Prateek/Hobor Aquinas, Finding The Greedy, Prodigal, and Suicidal Contracts at Scale, in: 2018 Annual Computer Security Applications Conference (ACSAC '18), New York 2018, 653–663
- Nilsson Kim, The missing MtGox bitcoins, 19. April 2015, <https://blog.wizsec.jp/2015/04/the-missing-mtgox-bitcoins.html>
- Nobel Peter, Die Nationalbank als Lender of Last Resort – ein leeres Versprechen oder Notrecht?, in: Walder Hans Ulrich/Jaag Tobias/Zobl Dieter (Hrsg.), Aspekte des Wirtschaftsrechts. Festgabe zum Schweizerischen Juristentag 1994, Zürich 1994, 497–510
- Nobel Peter, Die wirtschaftliche Betrachtungsweise im Recht, SJZ 2017, 457–469
- Nobel Peter, Finanzmarktrecht: Neue Architektur – Neuer Wein?, BJM 2015, 129–153
- Nobel Peter, Risikobegriff in der Ökonomie und im Recht, SZW 2016, 551–557
- Nobel Peter, Schweizerisches Finanzmarktrecht, 4. Aufl., Bern 2019
- Nobel Peter, Ursachen der Finanzkrise und seitherige Regulierungsentwicklung, SZW 2018, 588–597
- Nobel Peter, Was heisst Überregulierung?, SZW 2014, 589–599
- Nobel Peter/Zimmermann Heinz, Entwicklung und Struktur von Effektenmärkten, SZW 2011, 511–532

- Nobel Peter/Zimmermann Heinz, Finanzinnovationen in Rechtswissenschaft und Finanzmarkttheorie, in: Möslin Florian (Hrsg.), Finanzinnovation und Rechtsordnung. Gestaltung, unternehmerischer Einsatz und Marktregulierung, Zürich/Basel/Genf 2014, 45–97
- Noether Shen/Mackenzie Adam/the Monero Research Lab, Ring Confidential Transactions, Ledger 2016, 1–18
- Nolan Tier, Alt chains and atomic transfers, 2. Mai 2013, <https://bitcointalk.org/index.php?topic=193281>
- Noone Greg, The case against bitcoin: Why governments are cracking down on crypto, 13. Mai 2021, <https://techmonitor.ai/policy/digital-economy/case-against-bitcoin-governments-plan-cryptocurrency-ban>
- Nooteboom Bart/Six Frédérique, Introduction, in: Nooteboom Bart/Six Frédérique (Hrsg.), The Trust Process in Organizations. Empirical Studies of the Determinants and the Process of Trust Development, Cheltenham/Northampton 2003, 1–15
- North Douglass C., A Transaction Cost Theory of Politics, Journal of Theoretical Politics 1990, 355–367
- North Douglass C., Institutions, Institutional Change and Economic Performance, Cambridge/New York 1990
- North Douglass C., Transaction Costs, Institutions, and Economic History, Zeitschrift für die gesamte Staatswissenschaft 1984, 7–17
- North Douglass C./Weingast Barry R., Constitutions and Commitment: The Evolution of Institutions Governing Public Choice in Seventeenth-Century England, The Journal of Economic History 1989, 803–832
- Nougayrède Delphine, Towards a Global Financial Register? The Case for End Investor Transparency in Central Securities Depositories, Journal of Financial Regulation 2018, 276–313
- Nouy Danièle, Gaming the rules or ruling the game? – How to deal with regulatory arbitrage, 33rd SUERF Colloquium, Helsinki, 15. September 2017, <https://www.banking-supervision.europa.eu/press/speeches/date/2017/html/ssm.sp170915.en.html>
- Nyman Linus/Mikkonen Tommi/Lindman Juho/Fougère Martin, Forking: the Invisible Hand of Sustainability in Open Source Software, in: Hammouda Imed/Lundell Björn (Hrsg.), Proceedings of SOS 2011: Towards Sustainable Open Source, Tampere 2011, 1–5
- O’Neal Stephen, EOS Proves Yet Again That Decentralization Is Not Its Priority, 15. November 2018, m.w.H., <https://cointelegraph.com/news/eos-proves-yet-again-that-decentralization-is-not-its-priority>

- O'Neal Stephen, Stellar's Blockchain Briefly Goes Offline, Confirming the Project Lacks Decentralization, 20. Mai 2019, <https://cointelegraph.com/news/stellars-blockchain-briefly-goes-offline-confirming-the-project-lacks-decentralization>
- OasisDEX, Introduction to the OasisDEX Protocol, High Level Overview, undatiert, <https://oasisdex.com/docs/guides/introduction#high-level-overview>
- OasisDEX, OasisDEX Market Taker Guide, Fill or Kill orders, undatiert, <https://oasisdex.com/docs/guides/market-taker#fill-or-kill-orders>
- Obadia Alex, Flashbots: Frontrunning the MEV Crisis, 23. November 2020, <https://medium.com/flashbots/frontrunning-the-mev-crisis-40629a613752>
- Obrecht Matthias, Einblicke in die DLT-Praxis der FINMA, Europa Institut (EIZ), Seminar Blockchain-Recht, Die neue DLT-Gesetzgebung in der Praxis, 29. August 2023
- ten Oever Niels/Moriarty Kathleen, The Tao of IETF. A Novice's Guide to the Internet Engineering Task Force, 2019, <https://www.ietf.org/about/participate/tao/>
- Offchain Labs, Arbitrum One Outage Report, 14. September 2021, <https://medium.com/offchainlabs/arbitrum-one-outage-report-d365b24d49c>
- Ogus Anthony, Regulation. Legal Form and Economic Theory, Oxford/Portland 2004
- Okamoto Tatsuaki/Ohta Kazuo, Universal Electronic Cash, in: Feigenbaum Joan (Hrsg.), Advances in Cryptology – CRYPTO '91, LNCS 576, Berlin/Heidelberg 1992, 324–337
- Oleschak Robert, Die Zentrale Gegenpartei SIX x-clear, Januar 2009
- Oliveira Luis/Zavolokina Liudmila/Bauer Ingrid/Schwabe Gerhard, To Token or not to Token: Tools for Understanding Blockchain Tokens, in: International Conference of Information Systems (ICIS 2018), San Francisco 2018, 1–17
- Oliver Hart, Firms, Contracts, and Financial Structure, Oxford/New York 1995
- Olivier Kessler/Beat Kappeler (Hrsg.), Null-Risiko-Gesellschaft. Zwischen Sicherheitswahn und Kurzsichtigkeit, Zürich 2021
- Olson Mancur, The Logic of Collective Action. Public Goods and the Theory of Groups, Cambridge/London 2002
- Olstrom Elinor, Governing the Commons. The evolution of institutions for collective action, Cambridge/New York 1990
- Omarova Saule T., Technology v Technocracy: Fintech as a Regulatory Challenge, Journal of Financial Regulation 2020, 75–124
- Omarova Saule T., The People's Ledger: How to Democratize Money and Finance the Economy, Vanderbilt Law Review 2021, 1231–1300
- Omlor Sebastian, Kryptowährungen im Geldrecht, ZHR 2019, 294–345
- Open Assets, open-assets-protocol, undatiert, <https://github.com/OpenAssets/open-assets-protocol/blob/master/specification.mediawiki>

- Open Source Initiative, Licenses & Standards, undatiert, <https://opensource.org/licenses>
- OpenDEX, OpenDEX Features, undatiert, <https://opendex.network/#opendex-features>
- OpenZeppelin, Contracts 4.x, Access Control, Ownership and Ownable, undatiert, <https://docs.openzeppelin.com/contracts/4.x/access-control#ownership-and-ownable>
- OpenZeppelin, Contracts 4.x, Access Control, Role-Based Access Control, undatiert, <https://docs.openzeppelin.com/contracts/4.x/access-control#role-based-access-control>
- OpenZeppelin, Contracts 4.x, Access Control, undatiert, <https://docs.openzeppelin.com/contracts/4.x/access-control>
- OpenZeppelin, Contracts 4.x, Governance, Timelock, undatiert, <https://docs.openzeppelin.com/contracts/4.x/api/governance#timelock>
- Optimism, Optimistic Sequencing, What happens if the sequencer goes offline?, undatiert, <https://community.optimism.io/docs/protocol/sequencing.html#what-happens-if-the-sequencer-goes-offline>
- Orwell George, Nineteen Eighty-Four, New York/London/Toronto 1992
- Oshiro Brent, Exploring the 0x DeFi Ecosystem. Our universe is bigger and more liquid than ever, 17. Februar 2021, <https://blog.0xproject.com/exploring-the-0x-defi-ecosystem-3afe70379be0>
- Osterloh Margit/Weibel Antoinette, Investition Vertrauen. Prozesse der Vertrauensentwicklung in Organisationen, Wiesbaden 2006
- Ostrom Elinor, Beyond Markets and States: Polycentric Governance of Complex Economic Systems, The American Economic Review 2010, 641–672
- Ostrom Elinor, Collective Action and the Evolution of Social Norms, The Journal of Economic Perspectives 2000, 137–158
- Ostrom Elinor/Walker James/Gardner Roy, Covenants With and Without a Sword: Self-Governance is Possible, The American Political Science Review 1992, 404–417
- Othman Abraham, Automated Market Making: Theory and Practice, Diss. 2012, <http://reports-archive.adm.cs.cmu.edu/anon/2012/CMU-CS-12-123.pdf>
- Ötsch Walter Otto/Pühringer Stephan/Hirte Katrin, Netzwerke des Marktes. Ordoliberalismus als Politische Ökonomie, Wiesbaden 2018
- Oved Michael/Mosites Don, Swap: A Peer-to-Peer Protocol for Trading Ethereum Tokens, 21. Juni 2017, <https://www.airswap.io/pdfs/SwapWhitepaper.pdf>
- Özsu M. Tamer/Valduriez Patrick, Principles of Distributed Database Systems, 3. Aufl., New York 2011

- Özsu M. Tamer/Valduriez Patrick, Principles of Distributed Database Systems, 4. Aufl., Cham 2020
- Pacces Alessio M., Financial intermediation in the securities markets. Law and economics of conduct of business regulation, International Review of Law and Economics 2000, 479–510
- Paech Philipp, Securities, intermediation and the blockchain: an inevitable choice between liquidity and legal certainty?, Uniform Law Review 2016, 612–639
- Paech Philipp, The Governance of Blockchain Financial Networks, The Modern Law Review 2017, 1073–1110
- Palley Stephen D., The SEC Meets Decentralization Theater with Safe Harbors for Token Sales, 10. Februar 2020, <https://www.andersonkill.com/Publications/The-SEC-meets-decentralization-theater-with-safe-harbors-for-token-sales>
- Panisi Federico/Buckley Ross P./Arner Douglas, Blockchain and Public Companies: A Revolution in Share Ownership Transparency, Proxy Voting and Corporate Governance?, Stanford Journal of Blockchain Law & Policy 2019, 189–220
- Parity, A Postmortem on the Parity Multi-Sig Library Self-Destruct, 15. November 2017, <https://www.parity.io/a-postmortem-on-the-parity-multi-sig-library-self-destruct/>
- du Pasquier Shelby R./Fischer Philipp, Cross-border financial services in and from Switzerland. Regulatory frameworks and practical considerations, GesKR 2010, 436–461
- Patt Yale N./Patel Sanjay J., introduction to computing systems. from bits to gates to C and beyond, New York 2005
- Paul Milgrom R./North Douglass C./Weingast Barry R., The Role of Institutions in the Revival of Trade: The Law Merchant, Private Judges and the Champagne Fairs, Economics and Politics 1990, 1–23
- Paumgarten Nick, The Prophets of Cryptocurrency Survey The Boom and Bust, 15. Oktober 2018, <https://www.newyorker.com/magazine/2018/10/22/the-prophets-of-cryptocurrency-survey-the-boom-and-bust>
- Payne Jennifer, The Role of Gatekeepers, in: Moloney Niamh/Ferran Eilís/Payne Jennifer (Hrsg.), The Oxford Handbook of Financial Regulation, Oxford/New York 2015, 254–280
- PayPal, undatiert, <https://www.paypal.com/us/smarthelp/article/cryptocurrency-on-paypal-faqs-|paypal-us-faq4398>
- Pearson Jordan, ‘THIS IS NOT A DRILL.’ A Hacker Allegedly Stole \$32 Million in Ethereum, 19. Juli 2017, https://www.vice.com/en_us/article/zmvkke/this-is-not-a-drill-a-hacker-allegedly-stole-dollar32-million-in-ethereum

- Peaster William M., «Paradigm Shift» First Security Token Arrives on Ethereum's Uniswap DEX, 6. November 2019, <https://blockonomi.com/first-security-token-on-uniswap-dex/>
- PeckShield, bZx Hack Full Disclosure (With Detailed Profit Analysis), 18. Februar 2020, <https://medium.com/@peckshield/bzx-hack-full-disclosure-with-detailed-profit-analysis-e6b1fa9b18fc>
- Peirce Hester M., Atomic Trading, 22. Februar 2021, <https://www.sec.gov/news/speech/peirce-atomic-trading-2021-02-22>
- Peirce Hester M., Lawless in Austin, 8. Oktober 2021, <https://www.sec.gov/news/speech/peirce-2021-10-08>
- Peirce Hester M., Remarks at Meeting of Investor Advisory Committee, 9. September 2021, <https://www.sec.gov/news/public-statement/peirce-iac-090921>
- Peirce Hester M., Renegade Pandas: Opportunities for Cross Border Cooperation in Regulation of Digital Assets, 30. Juli 2019, <https://www.sec.gov/news/speech/speech-peirce-073019>
- Peirce Hester M., Running on Empty: A Proposal to Fill the Gap Between Regulation and Decentralization, 6. Februar 2020, <https://www.sec.gov/news/speech/peirce-remarks-blockress-2020-02-06>
- Peirce Hester M., CommissionerPeirce, SafeHarbor 2.0, undatiert, <https://github.com/CommissionerPeirce/SafeHarbor2.0>
- Peirce Hester M., Twitter, 6. August 2021, <https://twitter.com/hesterpeirce/status/1423637816492318722>
- Peirce Hester M., Dissenting Statement on the Proposal to Amend Regulation ATS, 26. Januar 2022, <https://www.sec.gov/news/statement/peirce-ats-20220126>
- Peirce Hester M./Uyeda Mark T., On Today's Episode of As the Crypto World Turns: Statement on ShapeShift AG, 5. März 2024, <https://www.sec.gov/news/statement/peirce-uyeda-statement-a-crypto-world-turns-03-06-24>
- Pelker C. Alden/Brown Christopher B./Tucker Richard M., Using Blockchain Analysis From Investigation to Trial, Department of Justice Journal of Federal Law and Practice 2021, 59–100
- Peltzman Sam, Toward a More General Theory of Regulation, The Journal of Law & Economics 1976, 211–240
- Perez Carlota, Technological Revolutions and Financial Capital. The Dynamics of Bubbles and Golden Ages, Cheltenham/Northampton 2002
- Perez Carlota, Technological revolutions and techno-economic paradigms, Cambridge Journal of Economics 2010, 185–202

- Pesch Paulina/Böhme Rainer, Datenschutz trotz öffentlicher Blockchain? Chancen und Risiken bei der Verfolgung und Prävention Bitcoin-bezogener Straftaten, DuD 2017, 93–98
- Peters Gareth W./Panayi Efstathios, Understanding Modern Banking Ledgers Through Blockchain Technologies: Future of Transaction Processing and Smart Contracts on the Internet of Money, in: Tasca Paolo/Aste Tomaso/Pelizzon Lorian/Perony Nicolas (Hrsg.), Banking Beyond Banks and Money. A Guide to Banking Services in the Twenty-First Century, Cham 2016, 239–278
- Peterson Jack/Krug Joseph/Zoltu Micah/Williams Austin K./Alexander Stephanie, Augur: a Decentralized Oracle and Prediction Market Platform (v2.0), 1. November 2019, <https://www.augur.net/whitepaper.pdf>
- Picot Arnold/Reichwald Ralf/Wigand Rolf T./Möslein Kathrin M./Neuburger Rahild/Neyer Anne-Katrin, Die grenzenlose Unternehmung. Information, Organisation & Führung, 6. Aufl., Wiesbaden 2020
- Pigou Arthur C., The Economics of Welfare, London 1920
- Pilkington Marc, Blockchain technology: principles and applications, in: Olleros F. Xavier/Zhegu Majlinda (Hrsg.), Research Handbook on Digital Transformations, Cheltenham/Northampton 2016, 225–253
- Piller François, Virtuelle Währungen – Reale Rechtsprobleme?, AJP 2017, 1426–1438
- Pinna Andrea/Ruttenberg Wiebe, Distiributed ledger technologies in securities post-trading. Revolution or evolution?, European Central Bank Occasional Paper Series Nr. 172, April 2016
- Plattner Matthias, Datenschutzrechtliche Herausforderungen der Distributed-Ledger-Technologie, Zürich/Basel/Genf 2021
- Plenio Martin/Senn Myriam (Hrsg.), Kommentar zum Nationalbankgesetz (NBG) und Bundesgesetz über die Währung und die Zahlungsmittel (WZG), Zürich/St. Gallen 2021 (Autor, in: Kommentar NBG/WZG, Art. N)
- Pmcgoohan, Miners Frontrunning, 11. August 2014, https://www.reddit.com/r/ethereum/comments/2d84yv/miners_frontrunning/
- Pmcgoohan, Why Ethereum's Miner Extractable Value Problem Is Way Worse Than You Think, 10. Mai 2021, <https://www.coindesk.com/ethereum-mev-frontrunning-solutions>
- Poelstra Andrew, Mimblewimble, 6. Oktober 2016, <https://download.wpsoftware.net/bitcoin/wizardry/mimblewimble.pdf>
- Pol Ronald F., Anti-money laundering: The world's least effective policy experiment? Together, we can fix it, Policy Design and Practice 2020, 73–94
- Pol Ronald F., Uncomfortable truths? ML = BS and AML = BS2, Journal of Financial Crime 2018, 294–308

- Polanyi Michael, *The Logic of Liberty. Reflections and Rejoinders*, Abingdon 1998
- Poldena Tomas/Schlauri Simon/Schweizer Samuel, *Rechtliche Voraussetzungen der Nutzung von Open-Source-Software in der öffentlichen Verwaltung, insbesondere des Kantons Bern*, Berlin 2017
- Polkadex, *Polkadex Orderbook*, Introduction, undatiert, <https://docs.polkadex.trade/orderbookIntroduction/>
- Polleit Thorsten/von Prollius Michael, *Geldreform. Vom schlechten Staatsgeld zum guten Marktgeld*, 2. Aufl., Grevenbroich 2011
- Poon Joseph/Buterin Vitalik, *Plasma: Scalable Autonomous Smart Contracts*, Working Draft, 11. August 2017, <https://www.plasma.io/plasma-deprecated.pdf>
- Poon Joseph/Dryja Thaddeus, *The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments*, Draft Version 0.5.9.2, 14. Januar 2016
- Popescu Andrei-Dragoș, *Decentralized Finance (DeFi) – The Lego of Finance*, in: Vlăduțescu Ștefan/Bunăiașu Claudiu Marian/Negrea Xenia (Hrsg.), *Social Sciences and Education Research Review* 2020, 321–349
- Popper Karl, *The Necessity of Peace*, in: Popper Karl (Hrsg.), *All Life is Problem Solving*, London/New York 1999, 139–144
- Popper Nathaniel, *Digital Gold. Bitcoin and the Inside Story of the Misfits and Millionaires Trying to Reinvent Money*, New York 2016
- Porter Michael E., *Competitive Advantage. Creating and Sustaining Superior Performance*, New York 1998
- Portmann Matthias, *Best execution im Spannungsfeld neuer Finanzmarktphänomene*, SSFM 113, Diss. Zürich/Basel/Genf 2013
- Poskriakov Fedor, *Conservation et négoce de cryptoactifs – aspects choisis du droit des marchés financiers*, in: Richa Alexandre/Canapa Damiano (Hrsg.), *Droit et économie numérique*, CEDIDAC 73, Bern 2021, 83–130
- Poskriakov Fedor, *Crowdlending – swiss regulatory regime – Quo vadis?*, Jusletter vom 13. März 2017
- Poskriakov Fedor/Chiriaeva Maria/Cavin Christophe, *Cryptocurrency compliance and risks: A European KYC/AML perspective*, 2021, <https://www.globallegalinsights.com/practice-areas/blockchain-laws-and-regulations/10-cryptocurrency-compliance-and-risks-a-european-kyc-aml-perspective>
- Post Kollen, *Marathon says its mining pool will stop censoring transactions following bitcoin community outcry*, 2. Juni 2021, <https://www.theblockcrypto.com/linked/106865/marathon-ofac-bitcoin-mining-pool-taproot>
- Powell Walter W., *Neither Market Nor Hierarchy: Network Forms of Organization*, *Research in Organizational Behavior* 1999, 295–336

- Powers Benjamin, Zcash Announces 'Halo Arc' and Timeline for Protocol Privacy Update, 12. April 2021, <https://www.coindesk.com/zcash-halo-arc-timeline-protocol-privacy-update>
- Prantl Florian, Aufsichtsrechtliche Erfassung von «Robo Advice» in der Schweiz – Verhaltensregeln des Finanzdienstleistungsgesetzes beim digitalen und automatisierten Anlagegeschäft, Bern 2020
- Price Rob, Why You Shouldn't Be Worried About A Bitcoin Ban. Although they may seem threatening, bans on Bitcoin have never worked and will continue to be circumvented by the network, 5. Mai 2021, <https://bitcoinmagazine.com/culture/why-governments-cant-ban-bitcoin>
- Proctor Charles, Mann on the Legal Aspect of Money, 7. Aufl., Oxford 2012
- Project Serum, Fees, undatiert, <https://projectserum.com/staking-voting>
- Project Serum, undatiert, <https://github.com/project-serum>
- Prosi Gerhard, Europäische Integration durch Wettbewerb? Eine politisch-ökonomische Analyse, in: Radnitzky Gerard/Bouillon Hardy (Hrsg.), Ordnungstheorie und Ordnungspolitik, Berlin/Heidelberg/New York 1991, 119–135
- Protocol Labs, Filecoin: A Decentralized Storage Network, 19. Juli 2017, <https://filecoin.io/filecoin.pdf>
- Pulver Urs/Schott Bertrand G., Das Insolvenzrecht für Banken und Effektenhändler – Überblick über die Sonderregelung und ausgewählte Fragen, in: Sprecher Thomas (Hrsg.), Sanierung und Insolvenz von Unternehmen, EIZ 112, Zürich/Basel/Genf 2011, 237–291
- Puschmann Thomas/Weber Rolf H., Neuerfindung des Finanzsektors?, SZW 2017, 79–94
- Qin Kaihua/Zhou Liyi/Gervais Arthur, Quantifying Blockchain Extractable Value: How dark is the forest?, 10. Dezember 2021, <https://arxiv.org/abs/2101.05511>
- Quintenz Brian D., Remarks at the 38th Annual GITEX Technology Week Conference, 16. Oktober 2018, <https://www.cftc.gov/PressRoom/SpeechesTestimony/opaquintenz16>
- Quisquater Jean-Jacques/Giullou Louis/Berson Tom, How to Explain Zero-Knowledge Protocols to Your Children, in: Brassard Gilles (Hrsg.), Advances in Cryptology – CRYPTO '89, LNCS 435, Berlin/Heidelberg 1990, 628–631
- Qureshi Haseeb, A hacker stole \$31M of Ether – how it happened, and what it means for Ethereum, 20. Juli 2017, <https://www.freecodecamp.org/news/a-hacker-stole-31m-of-ether-how-it-happened-and-what-it-means-for-ethereum-9e5dc29e33ce/>
- Qureshi Haseeb, Flash Loans: Why Flash Attacks will be the New Normal, 27. Februar 2020, <https://medium.com/dragonfly-research/flash-loans-why-flash-attacks-will-be-the-new-normal-5144e23ac75a>

- Qureshi Haseeb, Unbundling Uniswap: The Future of On-Chain Market Making, 20. August 2020, <https://medium.com/dragonfly-research/unbundling-uniswap-the-future-of-on-chain-market-making-1c7d6948d570>
- Qureshi Haseeb, What explains the rise of AMMs?, 22. Juli 2020, <https://medium.com/dragonfly-research/what-explains-the-rise-of-amms-7d008aflc399>
- Qureshi Haseeb, Why Decentralization Isn't as Important as You Think, 31. März 2020, <https://haseebq.com/why-decentralization-isnt-as-important-as-you-think/>
- Qureshi Haseeb/Lee Leland, Ethereum is now unforkable, thanks to DeFi, 31. Oktober 2019, <https://haseebq.com/ethereum-is-now-unforkable-thanks-to-defi/>
- Rafa, Liquidations -> Batch vs Dutch auctions, 29. Juni 2020, <https://forum.maker-dao.com/t/liquidations-batch-vs-dutch-auctions/2960>
- Ragnedda Massimo/Destefanis Giuseppe, Blockchain: a disruptive Technology, in: Ragnedda Massimo/Destefanis Giuseppe (Hrsg.), Blockchain and Web 3.0. Social, Economic, and Technological Challenges, London/New York 2020, 1–11
- Rahm Erhard/Saake Gunter/Sattler Kai-Uwe, Verteiltes und Paralleles Datenmanagement. Von verteilten Datenbanken zu Big Data und Cloud, Berlin/Heidelberg 2015
- Rai Rahul, The Past, Present, and Future of Decentralized Exchanges, 17. März 2021, <https://medium.com/gamma-point-capital/the-past-present-and-future-of-decentralized-exchanges-95dc1cfb6412>
- Rajan Raghuram G./Zingales Luigi, The great reversals: the politics of financial development in the twentieth century, Journal of Financial Economics 2003, 5–50
- Ramakrishnan Ram T. S./Thakor Anjan V., Information Reliability and a Theory of Financial Intermediation, The Review of Economic Studies 1984, 415–432
- Rammert Werner, Distributed agency and advanced technology. Or: how to analyze constellations of collective inter-agency, in: Passoth Jan-Hendrik/Peuker Birgit/Schillmeier Michael (Hrsg.), Agency without Actors? New approaches to collective action, London/New York 2012, 89–112
- Ramos Simona/Ellul Joshua, The MEV Saga: Can Regulation Illuminate the Dark Forest?, 2. Mai 2023, <https://arxiv.org/abs/2305.03718>
- Raskin Max, The Law and Legality of Smart Contracts, Georgetown Law Technology Review 2017, 305–341
- Raymond Eric S., The Cathedral and the Bazaar. Musings on Linux and Open Source by an Accidental Revolutionary, Sebastopol 2001
- Raymond Mark/DeNardis Laura, Multistakeholderism: anatomy of an inchoate global institution, International Theory 2015, 572–616
- Raz Joseph, The Authority of Law. Essays on Law and Morality, Oxford/New York 1979
- ReasonTV, Cypherpunks Write Code, Oktober 2020, <https://www.youtube.com/playlist?list=PLBuns9Evn1w-T2RwqMhUnTZbTTe-M-g42>

- Rehm Christian/Werlen Thomas, Paradigmenwechsel in der Primärkapitalmarktregulierung, in: Reutter Thomas U./Werlen Thomas (Hrsg.), Kapitalmarkttransaktionen IX, EIZ 152, Zürich/Basel/Genf 2014, 55–87
- Reichmuth Patricia/von der Crone Hans Caspar, Crowdlending als bewilligungspflichtige Entgegennahme von Publikumseinlagen. Bundesgerichtsurteil 2C_352/2016 vom 9. Dezember 2016, SZW 2017, 253–268
- Reid Fergal/Harrigan Martin, An Analysis of Anonymity in the Bitcoin System, in: 2011 IEEE International Conference on Privacy, Security, Risk and Trust and IEEE International Conference on Social Computing, Danvers/Piscataway 2011, 1318–1326
- Reidenberg Joel R., Lex Informatica: The Formulation of Information Policy Rules through Technology, Texas Law Review 1998, 553–593
- Reinhart Carmen M./Rogoff Kenneth S., This Time is Different. Eight Centuries of Financial Folly, Princeton/Oxford 2009
- Reiser Nina, Anlegerschutz durch Trennung?, SZW 2017, 452–467
- Reiser Nina, Ist der Bankbegriff im Lichte aktueller technologischer Entwicklungen noch zeitgemäss?, AJP 2018, 811–824
- Reiser Nina/Wyss Lukas, Vollgeld-Initiative und Alternativkonzepte, SZW 2018, 164–178
- Reisman George, Capitalism. A Treatise on Economics, Ottawa 1998
- Remund Cédric/Wyss Dominic, Insider Trading im digitalen Zeitalter: Neue Herausforderungen und Risiken, SZW 2023, 24–43
- Ren, A privacy preserving virtual machine powering zero-knowledge financial applications, Litepaper v1.2, 2019, <https://renproject.io/litepaper.pdf>
- Ren, Home, undatiert, <https://github.com/renproject/ren/wiki>
- Rennig Christopher, Finanztechnologische Innovationen im Bankenaufsichtsrecht, Tübingen 2022
- RenProject, Ren, Darknodes, 21. Oktober 2020, <https://github.com/renproject/ren/wiki#darknodes>
- Rettig Lane, The key ingredients to a better blockchain, Part II: Decentralization. Our understanding of what makes a blockchain successful is becoming clear. What will it take to succeed?, 15. September 2019, <https://www.etherean.org/blockchain/2019/09/15/key-ingredients-better-blockchain-part-ii-decentralization.html>
- Rettig Rebecca/Mosier Michael/Gilman Katja, Genuine DeFi as Critical Infrastructure: A Conceptual Framework for Combating Illicit Finance Activity in Decentralized Finance, 29. Januar 2024, <https://ssrn.com/abstract=4607332>
- Revolut, undatiert, <https://www.revolut.com/go-from-cash-to-crypto-instantly>
- Reyes Carla L., If Rockefeller Were a Coder, The George Washington Law Review 2019, 373–429

- Reyes Carla L., Moving Beyond Bitcoin to an Endogenous Theory of Decentralized Ledger Technology Regulation: An Initial Proposal, *Villanova Law Review* 2016, 191–234
- Reymond Michel José, Mises au point sur la notion de Non Fungible Token, Jusletter vom 31. Mai 2021
- Rhinow René/Schmid Gerhard/Biaggini Giovanni/Uhlmann Felix, *Öffentliches Wirtschaftsrecht*, 2. Aufl., Basel 2011
- Ribstein Larry E., Fencing Fiduciary Duties, *Boston University Law Review* 2010, 899–920
- Ribstein Larry, Bubble Laws, *Houston Law Review* 2003, 77–97
- Richards Neil, Apple's «Code = Speech» Mistake, 1. März 2016, <https://www.technologyreview.com/2016/03/01/161811/apples-code-speech-mistake/>
- Richter Klaus/Rost Jan-Michael, *Komplexe Systeme*, Frankfurt a.M. 2002
- Ricketts Martin, *The Economics of Business Enterprise. An Introduction to Economic Organization and the Theory of the Firm*, 3. Aufl., Cheltenham/Northampton 2002
- Rieglinig David, OpenVASP: An Open Protocol to Implement FATF's Travel Rule for Virtual Assets, 14. November 2019
- Rifkin Jeremy, *The Zero Marginal Cost Society. The Internet of Things, the Collaborative Commons, and the Eclipse of Capitalism*, New York 2014
- Riker William H., *The Theory of Political Coalitions*, New Haven/London 1962
- Rimle Alois, *Recht des schweizerischen Finanzmarktes. Ein Grundriss für die Praxis*, Zürich 2004
- Riordan Jaani, *The Liability of Internet Intermediaries*, Oxford 2016
- Ripperger Tanja, *Ökonomik des Vertrauens. Analyse eines Organisationsprinzips*, 2. Aufl., Tübingen 2003
- Rivest Ron L./Shamir Adi/Adleman Leonard, A Method for Obtaining Digital Signatures and Public- Key Cryptosystems, *Communications of the ACM* 1978, 120–126
- Rizzo Pete, Ghash.io: We Will Never Launch a 51% Attack Against Bitcoin, <https://www.coindesk.com/ghash-io-never-launch-51-attack>
- Rizzo Pete, The Last Days of Satoshi: What Happened When Bitcoin's Creator Disappeared, 26. April 2021, <https://bitcoinmagazine.com/technical/what-happened-when-bitcoin-creator-satoshi-nakamoto-disappeared>
- Roberts Austin, Security in Decentralized Exchanges, 26. Dezember 2017, <https://blog.openrelay.xyz/dex-sec/>
- Robinhood, undatiert, <https://robinhood.com/us/en/about/crypto/>
- Robinson Dan/Konstantopoulos Georgios, Ethereum is a Dark Forest, 28. August 2020, <https://medium.com/@danrobinson/ethereum-is-a-dark-forest-ecc5f0505dff>

- Robinson Tom, KuCoin thief sells out millions in crypto tokens on decentralized exchanges – but Elliptic can still trace them, 29. September 2020, <https://www.elliptic.co/blog/kucoin-thief-sells-out-millions-in-crypto-tokens-on-decentralized-exchanges>
- Rochet Jean-Charles/Tirole Jean, Platform Competition in Two-Sided Markets, Journal of the European Economic Association 2003, 990–1029
- Rogoff Kenneth, Dealing with Monetary Paralysis at the Zero Bound, Journal of Economic Perspectives 2017, 47–66
- Rohr Andreas, Bin ich Finanzintermediär? Ein Handbuch zur Auslegung von Art. 2 Abs. 3 GwG, Bern 2004
- Rohr Jonathan/Wright Aaron, Blockchain-Based Token Sales, Initial Coin Offerings, and the Democratization of Public Capital Markets, Hastings Law Journal 2019, 463–524
- Romano Roberta, The Need for Competition in International Securities Regulation, Theoretical Inquiries in Law 2001, 387–562
- Romano Roberta, The Sarbanes-Oxley Act and the Making of Quack Corporate Governance, The Yale Law Journal 2005, 1521–1611
- Romiti Matteo/Victor Friedhelm/Moreno-Sanchez Pedro/Nordholt Peter Sebastian/Haslhofer Bernhard/Maffei Matteo, Cross-Layer De-anonymization Methods in the Lightning Protocol, in: Borisov Nikita/Diaz Claudia (Hrsg.), Financial Cryptography and Data Security 2021, Teil 1, LNCS 12674, Berlin/Heidelberg 2021, 187–204
- Ron Dorit/Shamir Adi, Quantitative Analysis of the Full Bitcoin Transaction Graph, in: Sadeghi Ahmad-Reza (Hrsg.), Financial Cryptography and Data Security, LNCS 7859, Berlin/Heidelberg 2013, 6–24
- Ronning Anthony, Current State of Lightning Network Privacy, 10. Mai 2021, <https://abytesjourney.com/lightning-privacy/>
- Rosenberg Nathan, Uncertainty and Technological Change, in: Landau Ralph/Taylor Timothy/Wright Gavin (Hrsg.), The Mosaic of Economic Growth, Stanford 1996, 334–356
- Rosenfeld Meni, Analysis of hashrate-based double-spending, 12. Februar 2014, <https://arxiv.org/abs/1402.2009v1>
- Rosenfeld Meni, Overview of Colored Coins, 4. Dezember 2012, <https://bitcoil.co.il/BitcoinX.pdf>
- Rosenthal David, Das neue Datenschutzgesetz, Jusletter vom 16. November 2020
- Ross Stephen A., The Economic Theory of Agency: The Principal's Problem, The American Economic Review 1973, 134–139
- Roşu Ioanid/Saleh Fahad, Evolution of Shares in a Proof-of-Stake Cryptocurrency, Management Science 2020, 1–12

- Rothbard Murray N., *Man, Economy, and State. A Treatise on Economic Principles. With Power and Market. Government and the Economy*, 2. Aufl., Auburn 2009
- Rothbard Murray N., *The Mystery of Banking*, 2. Aufl., Auburn 2008
- Roughgarden Tim, *Algorithmic game theory*, Communications of the ACM 2010, 78–86
- Roukny Tarik/Bersini Hugues/Pirotte Hugues/Caldarelli Guido/Battiston Stefano, *Default Cascades in Complex Networks: Topology and Systemic Risk*, Scientific Reports 2013, 1–8
- Roy Avik, *Bitcoin and the U.S. Fiscal Reckoning*, National Affairs 2021, Nr. 49, 71–86
- Rubinstein Ariel/Wolinsky Asher, *Middlemen*, The Quarterly Journal of Economics 1987, 581–593
- Rubinstein-Salzedo Simon, *Cryptography*, Cham 2018
- Ruffner Markus, *Die ökonomischen Grundlagen eines Rechts der Publikumsgesellschaft. Ein Beitrag zur Theorie der Corporate Governance*, Zürich 2000
- Russo Camila, *The Infinite Machine. How an Army of Crypto-Hackers Is Building the Next Internet with Ethereum*, New York 2020
- Ryan-Collins Josh/Greenham Tony/Werner Richard/Jackson Andrew, *Where Does Money Come From? A Guide to the UK Monetary and Banking System*, London 2012
- Rysman Marc, *The Economics of Two-Sided Markets*, Journal of Perspectives 2009, 125–143
- de R. Barondes Royce, *The Bespeaks Caution Doctrine: Revisiting The Application of Federal Securities Law To Opinions and Estimates*, The Journal of Corporation Law 1994, 243–284
- van Saberhagen Nicolas, *CryptoNote v 2.0*, 17. Oktober 2013, <https://cryptonote.org/whitepaper.pdf>
- Sai Ashish Rajendra/Buckley Jim/Fitzgerald Brian/Le Gear Andrew, *Taxonomy of centralization in public blockchain systems: A systematic literature review*, Information Processing and Management 2021, 1–35
- Salami Iwa, *Financial Crime Update*, Butterworths Journal of International Banking and Financial Law 2020, 496–499
- Salanié Bernard, *The Economics of Contracts. A Primer*, 2. Aufl., Cambridge/London 2005
- Salin Phillip, *Costs and Computers*, Release 1.0, 25. November 1991
- Salin Phillip, *Freedom of Speech in Software*, 15. Juli 1991, <http://www.philsalin.com/patents.html>
- Salter Alexander W./Luther William J., *Synthesizing State and Spontaneous Order Theories of Money*, Advances in Austrian Economics 2014, 161–178

- Samczsun, Escaping the Dark Forest, 24. September 2020, <https://samczsun.com/escaping-the-dark-forest/>
- Samczsun, Taking undercollateralized loans for fun and for profit. Price manipulation, now with 100% more blockchain, 30. September 2019, <https://samczsun.com/taking-undercollateralized-loans-for-fun-and-for-profit/>
- Sams Robert, Bitcoin Blockchain for Distributed Clearing: A Critical Assessment, The Capco Institute Journal of Financial Transformation 2015, 39–46
- Samuelson Paul A./Nordhaus William D., Microeconomics, 19. Aufl., New York 2010,
- San Miguel Maxi/Johnson Jeffrey H./Kertesz Janos/Kaski Kimmo/Díaz-Guilera Albert/MacKay Robert S./Loreto Vittorio/Érdi Peter/Helbing Dirk, Challenges in complex systems science, The European Physical Journal Special Topics 2012, 245–271
- Sandler Todd, Buchanan clubs, Constitutional Political Economy 2013, 265–284
- Santori Marco, What is Money Transmission and Why Does it Matter?, 7. April 2015, <https://www.coincenter.org/education/policy-and-regulation/money-transmission/>
- Savary Fiona, Regulierung dominanter Internetplattformen. Eigenheiten, Herausforderungen und Lösungsansätze im Licht von Ökonomie, Innovation und Recht, SGRW 32, Diss. Zürich/St. Gallen 2017
- Say Jean-Baptiste, A Treatise on Political Economy, or the Production, Distribution and Consumption of Wealth, New York 1971
- Schaefer Rupert, Alte Regeln, neue Technologien: Der strategische Ansatz der FINMA im Fintech-Bereich, Veranstaltung «Zehn Jahre Finanzmarktaufsicht» der Universität Zürich, 7. November 2019
- Schaller Alexandra, Continuous Linked Settlement: History and Implications, Diss. Zürich 2007
- Schaller Jean-Marc, Finanzanalysten-Recht. Die Berufstätigkeit der Finanzanalysten im Rahmen des Privat-, Straf- und Aufsichtsrechts, SSB 79, Diss. Zürich 2004
- Schär Fabian, Decentralized Finance: On Blockchain- and Smart Contract-Based Financial Markets, Federal Reserve Bank of St. Louis Review 2021, 153–174
- Schär Fabian, DeFi Is Transparent, Unless You Look Closely, 13. April 2021, <https://www.coindesk.com/defi-is-transparent-unless-you-look-closely>
- Schär Fabian, DeFi's Promise and Pitfalls, IMF Finance & Development, September 2022, 33–35
- Schären Simon/Dobrauz-Saldapenna Günther/Liebi Martin, Organisierte Handelssysteme im neuen FinfraG – Versuch einer regulatorischen Kategorisierung, SZW 2016, 194–201

- Schärli Kilian/Meisser Luzius/Luthiger Reto, Finanzmarktrechtliche Einordnung des Stakings von Kryptowährungen, Jusletter IT vom 30. September 2021
- Schelling Thomas C., *The Strategy of Conflict*, Cambridge/London 1960
- Schenker Urs, Konzerne im Börsenrecht, in: Kunz Peter V./Arter Oliver/Jörg Florian S. (Hrsg.), *Entwicklungen im Gesellschaftsrecht VIII*, Bern 2013, 163–201
- Schickler Jack, 'We Are All F****d': The Developers of Tornado Cash and the Future of Crypto, 5. Dezember 2022, <https://www.coindesk.com/consensus-magazine/2022/12/05/alexey-pertsev-most-influential-2022/>
- Schiener Dominik, Liquid Democracy: True Democracy for the 21st Century, 23. November 2015, <https://medium.com/organizer-sandbox/liquid-democracy-true-democracy-for-the-21st-century-7c66f5e53b6f>
- Schilling de Carvalho Pedro, Retaining Influence in Post-Brexit International Financial Regulation: Lessons from the UK's FinTech Framework, *Journal of Financial Regulation* 2022, 104–131
- Schlegel Stefan/Schuppli Benedikt, Die Rolle des Staates als Transaktionskostenfunktion – wie verändert die Digitalisierung den Wirkungsbereich des öffentlichen Rechts? Skizze einer Forschungsagenda jenseits von technologischem Determinismus und der Sehnsucht nach dem Primat der Politik, *ex ante* 2/2019, 3–16
- Schleiffer Patrick/Schärli Patrick, Ausnahmen von der Prospektpflicht unter dem künftigen Finanzdienstleistungsgesetz, *GesKR* 2018, 1–9
- Schleiffer Patrick/Schärli Patrick, Grenzüberschreitende Erbringung von Finanzdienstleistungen, *GesKR* 2020, 24–35
- Schlupe Walter R., Über Funktionalität im Wirtschaftsrecht, in: Walder Hans Ulrich/Jaag Tobias/Zobl Dieter (Hrsg.), *Aspekte des Wirtschaftsrecht. Festgabe zum Schweizerischen Juristentag 1994*, Zürich 1994, 139–180
- Schlupe Walter R., Was ist Wirtschaftsrecht?, in: Jagmetti Riccardo L./Schlupe Walter R. (Hrsg.), *Festschrift für Walter Hug zum 70. Geburtstag*, Bern 1968, 25–95
- Schmid Jean-Daniel/Schmid Alexander, Bitcoin – eine Einführung in die Funktionsweise sowie eine Auslegeordnung und erste Analyse möglicher rechtlicher Fragestellungen, Jusletter vom 4. Juni 2012
- Schmid Jörg, Informationspflichten des Finanzdienstleisters bei «Execution-only-Geschäften», in: Emmenegger Susan (Hrsg.), *Bankvertragsrecht*, SBT 2017, Basel 2017, 221–242
- Schmoeckel Mathias, *Rechtsgeschichte der Wirtschaft. Seit dem 19. Jahrhundert*, Tübingen 2008
- Schneiberg Marc/Bartley Tim, Regulating or redesigning finance? Market architectures, normal accidents, and dilemmas of regulatory reform, in: Lounsbury Michael/Hirsch Paul M. (Hrsg.), *Markets on Trial: The Economic Sociology of the U.S. Financial Crisis, Part A*, Bingley 2011, 281–307

- Schneider Aaron, Decentralization: Conceptualization and Measurement, *Studies in Comparative International Development* 2003, 32–56
- Schneider Friedrich, Restricting or abolishing cash: an effective instrument for fighting the shadow economy, crime and terrorism?, in: Deutsche Bundesbank (Hrsg.), *War on Cash? Is there a Future for Cash?*, International Cash Conference 2017, Frankfurt a.M. 2017, 44–91
- Schneider Nathan, Decentralization: an incomplete ambition, *Journal of Cultural Economy* 2019, 265–285
- Schneuwly Andreas, Crowdfunding aus rechtlicher Sicht, *AJP* 2014, 1610–1626
- Schnyder Anton K., *Wirtschaftskollisionsrecht. Sonderanknüpfung und extraterritoriale Anwendung wirtschaftsrechtlicher Normen unter besonderer Berücksichtigung von Marktrecht*, Zürich 1990
- Schönknecht Florian, Der Einlagebegriff nach Bankengesetz, *GesKR* 2016, 300–319
- Schott Markus, Der «Wettbewerb der Systeme». Überlegungen zu einem *obiter dictum* des Bundesgerichts im Fall Glarner Sach (BGE 138 I 378), in: Belser Eva Maria/Waldmann Bernhard (Hrsg.), *Mehr oder weniger Staat? Festschrift für Peter Hänni zum 65. Geburtstag*, Bern 2015, 387–396
- Schotter Andrew, *The economic theory of social institutions*, Cambridge/New York 1981
- Schrepel Thibault, Collusion by Blockchain and Smart Contracts, *Harvard Journal of Law & Technology* 2019, 117–166
- Schueffel Patrick, Taming the Beast: A Scientific Definition of Fintech, *Journal of Innovation Management* 2016, 32–54
- Schuler Katrin/Cloots Ann Sofie/Schär, Fabian, On Defi and On-Chain CeFi: How (Not) to Regulate Decentralized Finance, *Journal of Financial Regulation* 2024, 1–30
- Schumpeter Joseph A., *Business Cycles. A Theoretical, Historical, and Statistical Analysis of the Capitalist Process*, Bd. 1, New York/London 1939
- Schumpeter Joseph A., *Capitalism, Socialism and Democracy*, London/New York 2003
- Schumpeter Joseph A., *Theorie der wirtschaftlichen Entwicklung*, 7. Aufl., Berlin 1987
- Schuster Rolf/Färber Johannes/Eberl Markus, *Digital Cash. Zahlungssysteme im Internet*, Berlin/Heidelberg 1997
- Schwarcz Steven L., Rethinking the Disclosure Paradigm in a World of Complexity, *University of Illinois Law Review* 2004, 1–38
- Schwarcz Steven L., Protecting Financial Markets: Lessons from the Subprime Mortgage Meltdown, *Minnesota Law Review* 2008, 373–406
- Schwarcz Steven L., Regulating Complexity in Financial Markets, *Washington University Law Review* 2009, 211–268

- Schwarcz Steven L., Securitization and Post-Crisis Financial Regulation, Cornell Law Review 2016, 115–139
- Schwarcz Steven L./Benjamin Joanna, Intermediary Risk in the Indirect Holding System for Securities, Duke Journal of Comparative & International Law 2002, 309–330
- Schwartz Robert A./Francioni Reto, Equity Markets in Action. The Fundamentals of Liquidity, Market Structure & Trading, Hoboken 2004
- Schweitzer Frank/Fagiolo Giorgio/Sornette Didier/Vega-Redondo Fernando/Vespignani Alessandro/White Douglas R., Economic Networks: The New Challenges, Science 2009, 422–425
- Schwenzer Ingeborg/Fountoulakis Christiana, Schweizerisches Obligationenrecht. Allgemeiner Teil, 8. Aufl., Bern 2020
- Schwinger Robert A., Can there be law without people?, New York Law Journal, 24. Januar 2023, <https://www.law.com/newyorklawjournal/2023/01/23/can-there-be-law-without-people/>
- Scott Michael, Delphi. A History of the Center of the Ancient World, Princeton/Woodstock 2014
- Secret Network, General Overview, undatiert, <https://build.scrt.network/overview.html>
- Seidel Marc-David L., Questioning Centralized Organizations in a Time of Distributed Trust, Journal of Management Inquiry 2017, 1–5
- Seiler Benedikt/Seiler Daniel, Sind Kryptowährungen wie Bitcoin (BTC), Ethereum (ETH) und Ripple (XRP) als Sachen im Sinne des ZGB zu behandeln?, sui-generis 2018
- Seiler Hansjörg, Recht und technische Risiken. Grundzüge des technischen Sicherheitsrechts, Zürich 1997
- Seira Rodrigo/amyaxizhang/Robinson Dan, Base Layer Neutrality. Sanctions and Censorship Implications for Blockchain Infrastructure, 8. September 2022, <https://www.paradigm.xyz/2022/09/base-layer-neutrality>
- Senn Myriam, Decentralisation of Economic Law – An Oxymoron?, Journal of Corporate Law Studies 2005, 427–464
- Senn Myriam, Non-State Regulatory Regimes. Understanding Institutional Transformation, Berlin/Heidelberg 2011
- Senn Myriam, Transnationalität im Recht als Herausforderung, ZSR 2015 I, 493–512
- SerHack/Monero Community, Mastering Monero. The future of private transactions, 2019
- Serum Academy, Serum DEX List, undatiert, <https://serum-academy.com/en/dex-list/>

- Serum Foundation, Serum – White Paper, Juli 2020, <https://projectserum.com/serum-white-paper.pdf>
- Serum, A technical introduction to the Serum DEX, undatiert, https://docs.google.com/document/d/1isGJES4jzQutl0GtQGutqrBUqeHxl_xJNXdtOv4Sdl
- Sester Peter, Vertragsschluss und Verbraucherschutz beim Einsatz von Software-Agenten, Informatik Spektrum 2004, 311–322
- Sethe Rolf, § 8 Konsumentenschutz beim Vermögensaufbau, in: Heiss Helmut/Loacker Leander D. (Hrsg.), Grundfragen des Konsumentenschutzes, Zürich/Basel/Genf 2020
- Sethe Rolf, Anlegerschutz im Recht der Vermögensverwaltung, Köln 2005
- Sethe Rolf, Das Drittstaatenregime von MiFIR und MiFID II, SZW 2014, 615–631
- Sethe Rolf, Einlagensicherung und Systemstabilität – Einige Gedanken zur Reform des Schweizer Einlegerschutzes, SZW 2012, 507–522
- Sethe Rolf, FIDLEG und das Vertragsrecht: Kundensegmentierung im Spannungsverhältnis von Aufsichtsrecht und Privatrecht, in: Emmenegger Susan (Hrsg.), Bankvertragsrecht, SBT 2017, Basel 2017, 215–220
- Sethe Rolf, Ist die neue Finanzmarktregulierung funktionsfähig?, SZW 2018, 605–618
- Sethe Rolf, MiFIR/MiFID II – Drittstaatenzugang für die Schweiz und Äquivalenz von FINIG/FIDLEG, in: Gericke Dieter (Hrsg.), Private Equity VI. PE 6.0: Neue Mitspieler, neue Technologien, neue Themen, neues Recht, EIZ 190, Zürich/Basel/Genf 2018, 135–169
- Sethe Rolf, Treuepflichten der Banken bei der Vermögensanlage, AcP 2012, 80–156
- Sethe Rolf, Wettbewerb als Regelungsziel der europäischen Finanzmarktgesetzgebung, in: Notter Markus/Weber Rolf H./Heinemann Andreas/Baumgartner Tobias (Hrsg.), Europäische Idee und Integration – mittendrin und nicht dabei? Liber Amicorum für Andreas Kellerhals, Zürich/Basel/Genf 2018, 375–385
- Sethe Rolf/Bösch René/Favre Olivier/Kramer Stefan/Schott Ansgar (Hrsg.), Kommentar zum Finanzdienstleistungsgesetz FIDLEG, Zürich/Basel/Genf 2021 (SK FIDLEG-Autor, Art. N)
- Sethe Rolf/Fahrländer Lukas, Frontrunning durch Vermögensverwalter als Insiderdelikt, in: Jositsch Daniel/Schwarzenegger Christian/Wohlers Wolfgang (Hrsg.), Festschrift für Andreas Donatsch, Zürich 2017, 449–511
- Sethe Rolf/Fahrländer Lukas, Licht und Schatten der geplanten Reform der Einlagensicherung, SZW 2019, 639–653
- Sethe Rolf/Favre Olivier/Hess Martin/Kramer Stefan/Schott Ansgar (Hrsg.), Kommentar zum Finanzmarktinfrastrukturgesetz FinfraG, Zürich/Basel/Genf 2017 (SK FinfraG-Autor, Art. N)

- Sethe Rolf/Lehmann Matthias, § 15 Internationales Bank- und Finanzdienstleistungsrecht, in: Tietje Christian/Nowrot Karsten (Hrsg.), Internationales Wirtschaftsrecht, 3. Aufl., Berlin/Boston 2022
- Sethe Rolf/Seiler Moritz, Dokumentation und Rechenschaft im geplanten FIDLEG, in: Waldburger Robert/Sester Peter/Peter Christoph/Baer Charlotte M. (Hrsg.), Law & Economics. Festschrift für Peter Nobel zum 70. Geburtstag, Bern 2015, 431–455
- Seward James K., Corporate Financial Policy and the Theory of Financial Intermediation, The Journal of Finance 1990, 351–377
- Shafik Minouche, A New Heart for a Changing Payments System, Bank of England Speech, 27. Januar 2016
- ShapeShift, What is ShapeShift?, undatiert, <https://shapeshift.com/faq>
- Shapiro Andrew L., The Control Revolution. How the Internet is Putting Individuals in Charge and Changing the World We Know, New York 1999
- Shapiro Carl/Varian Hal R., Information Rules. A Strategic Guide to the Network Economy, Boston 1999
- Shapiro Evan, Building a Private Gateway between the Real World and Crypto: Three Use Cases, 23. März 2021, <https://minaprotocol.com/blog/building-a-private-gateway-between-the-real-world-and-crypto-three-use-cases>
- Shapiro Gabriel, An open letter to SEC Commissioner Peirce on token safe harbors, 14. Februar 2020, <https://www.theblockcrypto.com/post/55985/an-open-letter-to-sec-commissioner-peirce-on-token-safe-harbors>
- Shapiro Gabriel, Defining Decentralization for Law, 16. April 2020, <https://lex-node.medium.com/defining-decentralization-for-law-58ca54e18b2a>
- Shapiro Gabriel, In Defense of Szabo's Law, For a (Mostly) Non-Legal Crypto System. A Lawyer's Response to Vlad Zamfir's «Against Szabo's Law, For A New Crypto Legal System», 26. Januar 2019, <https://medium.com/coinmonks/in-defense-of-szabos-law-for-a-mostly-non-legal-crypto-system-8f1ce2b364a6>
- Shapiro Gabriel, Twitter, 10. Oktober 2021, https://twitter.com/lex_node/status/1447183100312698882 (Shapiro, DAO 2, Twitter)
- Shapiro Gabriel, Twitter, 26. Mai 2020, https://twitter.com/lex_node/status/1265316170975997953 (Shapiro, DAO 1, Twitter)
- Shapiro Gabriel, Twitter, 30. September 2021, https://twitter.com/lex_node/status/1443687325343563782 (Shapiro, Paradox, Twitter)
- Sharman Jason C., The Money Laundry: Regulating Criminal Finance in the Global Economy, Ithaca 2011
- Shcherbak Sergii, How Should Bitcoin Be Regulated?, European Journal of Legal Studies 2014, 41–83

- Shen Maria, Electric Capital Developer Report (2020), 10. Dezember 2020, <https://medium.com/electric-capital/electric-capital-developer-report-2020-9417165c6444>
- Shen Muyao, Binance's CZ Views 'CeDeFi' as a Complement, Not a Competitor, to DeFi, 14. Oktober 2020, <https://www.coindesk.com/binance-smart-chain-cz-defi>
- Sheng Tony, Let's ditch «decentralized», 3. September 2018, <https://tonysheng.substack.com/p/decentralized-definition>
- Sheng Tony/Sparango Ben, Trust Spectrum, 24. März 2020, <https://multicoin.capital/2020/03/24/trust-spectrum/>
- Shevchenko Andrey, For Some Reason, Wash Trading Happens on Decentralized Exchanges Too, 25. Juli 2020, <https://cointelegraph.com/news/for-some-reason-wash-trading-happens-on-decentralized-exchanges-too>
- Shiller Robert J., Capitalism and Financial Innovation, Financial Analysts Journal 2013, 21-25
- Shiller Robert J., Finance and the Good Society, Princeton/Oxford 2012
- Shiller Robert J., From Efficient Markets Theory to Behavioral Finance, Journal of Economic Perspectives 2003, 83-114
- Shin Laura, Can Bitcoin Be Secured Only by Transaction Fees? Two Researchers Sound Off, 14. September 2021, <https://unchainedpodcast.com/can-bitcoin-be-secured-only-by-transaction-fees-two-researchers-sound-off/>
- Shin Laura, Everything You Need to Know About the Looming Battle Over Privacy in Crypto, 17. November 2020, <https://unchainedpodcast.com/everything-you-need-to-know-about-the-looming-battle-over-privacy-in-crypto/>
- Shin Laura, How This DOJ Strike Force Hunts Down Cryptocurrency Criminals, 20. Oktober 2020, <https://unchainedpodcast.com/how-this-doj-strike-force-hunts-down-cryptocurrency-criminals/>
- Shin Laura, PayPal Would Need These Two Things In Order to Issue a Stablecoin, 16. November 2021, <https://unchainedpodcast.com/paypal-would-need-these-two-things-in-order-to-issue-a-stablecoin/>
- Shin Laura, People Expected a Big SEC Enforcement Action This Week. What Happened?, 1. Oktober 2021, <https://unchainedpodcast.com/people-expected-a-big-sec-enforcement-action-this-week-what-happened/>
- Shin Laura, Solana's Outage Lasted 17 Hours. What Does This Mean for Decentralization?, 17. September 2021, <https://unchainedpodcast.com/solanas-outage-lasted-17-hours-what-does-this-mean-for-decentralization/>
- Shleifer Andrei, Inefficient Markets. An Introduction to Behavioral Finance, Oxford/New York 2004
- Siegel Marc, Bekämpfung der Terrorismusfinanzierung – die Rolle der Finanzmarktaufsicht, Die Volkswirtschaft 11/2005, 26-28

- Silfversten Erik/Favaro Marina/Slapakova Linda/Ishikawa Sascha/Liu James/Salas Adrian, Exploring the use of Zcash cryptocurrency for illicit or criminal purposes, RAND Europe, Santa Monica/Cambridge 2020
- Sillitoe Paul, Why Spheres of Exchange?, *Ethnology* 2006, 1–23
- silto, Black Thursday Response Thread, Summary of the Situation, 12. März 2020, <https://forum.makerdao.com/t/black-thursday-response-thread/1433>
- Simmchen Christoph, Blockchain (R)Evolution. Verwendungsmöglichkeiten und Risiken, MMR 2017, 162–165
- Simon Herbert A., A Behavioral Model of Rational Choice, *The Quarterly Journal of Economics* 1955, 99–118
- Simon Herbert A., The Architecture of Complexity, *Proceedings of the American Philosophical Society* 1962, 467–482
- Simone Baumann, Crowdfunding im Finanzmarktrecht, SSFM 117, Diss. Zürich/Basel/Genf 2014
- Simons Institute, Blockchain Intermediation, 21. November 2019, <https://youtu.be/jwZcWoinVU>
- Sinclair Sebastian, Uniswap's First Governance Vote Ends in Ironic Failure, 20. Oktober 2020, <https://www.coindesk.com/tech/2020/10/20/uniswaps-first-governance-vote-ends-in-ironic-failure/>
- Singer Andrew, Cleaning Up Crypto Exchange Wash Trading Will Take Global Regulation, 29. Juli 2020, <https://cointelegraph.com/news/cleaning-up-crypto-exchange-wash-trading-will-take-global-regulation>
- Singer Andrew, FUD or regulatory change? Rumor clouds swirl around crypto exchanges, 9. November 2020, <https://cointelegraph.com/news/fud-or-regulatory-change-rumor-clouds-swirl-around-crypto-exchanges>
- Singh Manmohan, The Economics of Collateral-Chains, *Banque Stratégie* 2012, 16–17
- Singh Manmohan, Velocity of Pledged Collateral: Analysis and Implications, IMF Working Paper November 2011
- Singh Manmohan/Aitken James, The (sizable) Role of Rehypothecation in the Shadow Banking System, IMF Working Paper Juli 2010
- Singh Spandana, Blockchain Is Helping to Circumvent Censorship in China, 18. August 2018, <https://slate.com/technology/2018/07/blockchain-is-helping-to-circumvent-censorship-in-china.html>
- SIX Group Ltd, Annual Report 2022, März 2023
- Sixt Elfriede, Schwarmökonomie und Crowdfunding. Webbasierte Finanzierungssysteme im Rahmen realwirtschaftlicher Bedingungen, Wiesbaden 2014
- Skoglund Jimmy/Chen Wei, Financial Risk Management. Applications in Market, Credit, Asset and Liability Management and Firmwide Risk, Hoboken 2015

- Slepak Greg/Petrova Anya, The DCS Theorem, 4. Oktober 2017, <https://arxiv.org/abs/1801.04335>
- Smith Adam, An Inquiry into the Nature and Causes of the Wealth of Nations, Bd. 1, London 1776, in: Campbell Roy Harold/Skinner Andrew S. (Hrsg.), The Glasgow edition of the works and correspondence of Adam Smith, Bd. 1, Oxford 1979
- Smith Adam, An Inquiry into the Nature and Causes of the Wealth of Nations, Bd. 2, London 1776, in: Campbell Roy Harold/Skinner Andrew S. (Hrsg.), The Glasgow edition of the works and correspondence of Adam Smith, Bd. 2, Oxford 1979
- Smith Benjamin, An Exchange Protocol for the Decentralized Web, 23. September 2019, <https://github.com/gnosis/dex-research/blob/master/dFusion/dfusion.v1.pdf>
- Smith Vernon L., An Experimental Study of Competitive Market Behavior, The Journal of Political Economy 1962, 111-137
- Smith Vernon L., Experimental Methods in the Political Economy of Exchange, in: Smith Vernon L. (Hrsg.), Bargaining and Market Behavior. Essays in Experimental Economics, Cambridge/New York 2000, 240-256
- Smullen John/Hand Nicholas (Hrsg.), A Dictionary of Finance and Banking, 3. Aufl., Oxford/New York 2005
- Snider Myles/Samani Kyle/Jain Tushar, Delegated Proof of Stake: Features & Tradeoffs, 2. März 2018, <https://multicoin.capital/2018/03/02/delegated-proof-stake-features-tradeoffs/>
- Snowden Edward, Permanent Record, London 2019
- Soleimani Ameen, What You Should Know Before Putting Half a Million DAI in Compound, 4. September 2019, <https://ameensol.medium.com/what-you-should-know-before-putting-half-a-million-dai-in-compound-fafdb2645f77>
- Sombart Werner, Der Moderne Kapitalismus. Die Genesis des Kapitalismus, Bd. 1, Leipzig 1902
- Song Jimmy, Understanding Segwit Block Size, 3. Juli 2017, <https://medium.com/@jimmysong/understanding-segwit-block-size-fd901b87c9d4>
- Sopov Vladislav, KYC/AML and Hidden Centralization: A libp2p-based Atomic Swaps Exchange Protocol, 5. Juli 2019, <https://medium.com/hackernoon/kyc-aml-and-hidden-centralization-a-libp2p-based-atomic-swaps-exchange-protocol-93eec9a876ba>
- Sornette Didier, Why Stock Markets Crash. Critical Events in Complex Financial Systems, Princeton/Oxford 2003
- Spacek Dirk, Online-Crowdfunding, sic! 2013, 277-292
- Specogna Rhea, Codebasiertes Regelsystem. Grenzen und Möglichkeiten privater Streiterledigung, PIRR 1, Diss. Zürich 2023

- Spence Michael, Job Market Signaling, The Quarterly Journal of Economics 1973, 355–374
- Spillmann Till/Giger Andrea, Ein modernes Prospektrecht für die Schweiz. Prospektspflicht, Prospektinhalt und Prospektprüfung gemäss dem neuen Finanzdienstleistungsgesetz, GesKR 2019, 182–205
- Spillmann Till/Meyer Richard, FIDLEG – Prospektregelung, in: Reutter Thomas U./Werlen Thomas (Hrsg.), Kapitalmarkttransaktionen X, EIZ 163, Zürich/Basel/Genf 2016, 7–50
- Spindler Gerald/Thorun Christian, Die Rolle der Ko-Regulierung in der Informationsgesellschaft. Handlungsempfehlung für eine digitale Ordnungspolitik, MMR-Beilage 2016, 1–28
- Spremann Klaus/Gantenbein Pascal, Finanzmärkte. Grundlagen, Instrumente, Zusammenhänge, 2. Aufl., Konstanz/München 2013
- Square, Square, Inc. Invests \$50 Million in Bitcoin, 8. Oktober 2020, <https://squareup.com/us/en/press/2020-bitcoin-investment>
- Srinivasan Balaji S., Quantifying Decentralization. We must be able to measure blockchain decentralization before we can improve it, 28. Juli 2017, <https://news.earn.com/quantifying-decentralization-e39db233c28e>
- Srinivasan Balaji S., Yes, You May Need a Blockchain. While scaling challenges abound, it's clear public blockchains offer something quite different to traditional databases, 14. Mai 2019, <https://www.coindesk.com/markets/2019/05/14/yes-you-may-need-a-blockchain/>
- Stallman Richard M., Free Software, Free Society: Selected Essays of Richard M. Stallman, 3. Aufl., Boston 2015
- Stampfli Ludwig, Das DLT-Gesetz: Anforderungen an eine Blockchain nach Art. 973d Abs. 2 OR, Bern 2022
- Stark Josh, Making Sense of Layer 2 (Devcon 4), Ethereum Foundation, 11. Dezember 2018, <https://www.youtube.com/watch?v=RghzB4C9aSg>
- StarkEx Docs V2, Data Availability Modes, undatiert, <https://docs.starkware.co/starkex-docs-v2/starkex-deep-dive/data-availability-modes>
- Staub Christian, Das schweizerische Bankenaufsichtsrecht und die Kreditkrise, GesKR 2009, 499–513
- Staub Lukas, Kann die FinTech-Bewilligung mit den Vorschlägen des Bundesrates die in sie gesetzten Erwartungen künftig erfüllen?, iusNet BR-KR 27.04.2023
- Stay Ronald J., Cryptic Controversy: U.S. Government Restrictions on Cryptography Exports and the Plight of Philip Zimmermann, Georgia State University Law Review 1997, 581–604
- Steiner Florian Louis, Zur Revision des Bucheffektengesetzes, GesKR 2016, 335–347

- Stengel Cornelia, Blockchain/Distributed Ledger Technology – Eine zivilrechtliche Betrachtung, in: Reutter Thomas U./Werlen Thomas (Hrsg.), Innovation und Disruption: Sanierungen, Exits, LIBOR-Ablösung und Blockchain, Kapitalmarkt – Recht und Transaktionen XVI, EIZ 210, Zürich 2021, 135–155
- Stengel Cornelia/Aus der Au Roman, Blockchain: Eine Technologie für effektiven Datenschutz?, sic! 2018, 439–452
- Stengel Cornelia/Bianchi Luca, Geldwäscherei und Terrorismusfinanzierung, in: Weber Rolf H./Kuhn Hans (Hrsg.), Entwicklungen im Schweizer Blockchain-Recht, Basel 2021
- Stengel Cornelia/Weber Thomas, Digitale und mobile Zahlungssysteme. Technologie, Verträge und Regulation von Kreditkarten, Wallets und E-Geld, Zürich/Basel/Genf 2016
- Stengel Cornelia/Wirthensohn Gino/Stäubli Luca, Regulierung von künstlicher Intelligenz für FinTech-Anwendungen, SZW 2021, 395–418
- Stigler George J., Competition, in: Sills David L. (Hrsg.) International Encyclopedia of the Social Sciences, Bd. 3, New York 1968, 181–186
- Stigler George J., Public Regulation of the Securities Markets, The Journal of Business 1964, 117–142
- Stigler George J., The Theory of Economic Regulation, The Bell Journal of Economics and Management Science 1971, 3–21
- Stigler George J., The Theory of Price, 4. Aufl., New York/London 1987
- Stiglitz Joseph E., Government Failure vs. Market Failure: Principles of Regulation, in: Balleisen Edward J./Moss David A. (Hrsg.), Government and Markets: Toward a New Theory of Regulation, Cambridge/New York 2009, 13–53
- Stiglitz Joseph E., Principal and Agent, in: Eatwell John/Milgate Murray/Newman Peter (Hrsg.), The New Palgrave: Allocation, Information and Markets, London/Basingstoke 1989, 241–253
- Stillhart Georg, Theorie der Finanzintermediation und Regulierung von Banken, Diss. Bern 2002
- Stokes Luke, The EOS User Agreement is Live!, 12. April 2019, <https://steemit.com/eos/@lukestokes/the-eos-user-agreement-is-live>
- Stoll Hans R., Future of Securities Markets: Competition or Consolidation?, Financial Analysts Journal 2008, 15–26
- Stowasser Joseph M./Petschenig Michael/Skutsch Franz (Hrsg.), STOWASSER. Lateinisch-deutsches Schulwörterbuch, München 2006
- Strasser Othmar, Zur Rolle der Banken bei der Rechtsdurchsetzung, SJZ 2011, 21–30

- strategy&/PricewaterhouseCoopers/Crypto Valley Association, 6th ICO / STO Report. A Strategic Perspective, Spring 2020 Edition, <https://www.pwc.ch/en/insights/fs/6th-ico-sto-report.html>
- Straub Wolfgang, Softwareschutz. Urheberrecht, Patentrecht, Open Source, Zürich/St. Gallen 2011
- Stringham Edward Peter, Private Governance. Creating Order in Economic and Social Life, Oxford/New York 2015
- Stroponiati Katerina/Abugov Ilya/Varelas Yiannis/Stroponiatis Kostas/Jurgeleviciene Modesta/Savanth Raghunatha Rao Yashoda, Decentralized governance in DeFi: Examples and pitfalls, 29. Oktober 2020, <https://dappradar.com/blog/decentralized-governance-in-defi-examples-and-pitfalls>
- Sundararajan Arun, The Sharing Economy. The End of Employment and the Rise of Crowd-Based Capitalism, Cambridge/London 2016
- Sunstein Cass R., Infotopia: How Many Minds Produce Knowledge, Oxford/New York 2006
- Sunstein Cass R., Laws of Fear. Beyond the Precautionary Principle, Cambridge/New York 2005
- Surden Harry, Computable Contracts, University of California Davis Law Review 2012, 629–700
- Surya Aruna, An Overview of the Bisq Network, 25. Februar 2019, <https://bisq.network/blog/an-overview-of-the-bisq-network/>
- Swanson Tim, Consensus-as-a-service: a brief report on the emergence of permissioned, distributed ledger systems, 6. April 2015, <https://www.ofnumbers.com/wp-content/uploads/2015/04/Permissioned-distributed-ledgers.pdf>
- Swanson Tim, Great Chain of Numbers: A Guide to Smart Contracts, Smart Property and Trustless Asset Management, 2014
- Swanson Tim, Settlement Risks Involving Public Blockchains, 24. März 2016, <https://www.ofnumbers.com/2016/03/24/settlement-risks-involving-public-blockchains/>
- Swarm Markets, FAQ, undatiert, <https://docs.swarm.markets/getting-started/faq>
- Swartz Lana, What was Bitcoin, what will it be? The techno-economic imaginaries of a new money technology, Cultural Studies 2018, 623–650
- Swiss Blockchain Federation (SBF), Circular 2019/01 Tokenized Equity. Guidelines for Issuers of Equity and Related Tokens, 14. November 2019
- Swiss Blockchain Federation (SBF), Circular 2020/01 Secondary Markets for Security Tokens, 12. Oktober 2021
- Swiss Blockchain Federation (SBF), Circular 2021/01 Ledger-based Securities, 12. Oktober 2021

- Swiss Blockchain Federation (SBF), Comments of Swiss Blockchain Federation on the draft revised VASP Guidance, 19. April 2021, http://blockchainfederation.ch/wp-content/uploads/2021/05/Letter_FATF.pdf
- Swiss Blockchain Federation (SBF), Zirkular 2023/01, Staking, 5. September 2023
- Swiss Blockchain Federation (SBF), Zirkular 2023/01, Staking, April 2024 (im Erscheinen)
- Swiss Finance + Technology Association (SFTA), Vernehmlassung: Bundesgesetz zur Anpassung des Bundesrechts an Entwicklungen der Technik verteilter elektronischer Register, 13. Juni 2019
- Swiss Fintech Innovations (SFTI), Future of Financial Institutions. View 2030, Discussion Paper, 2020
- Swiss LegalTech Association (SLTA), Data, Blockchain and Smart Contracts, Proposal for a robust and forward-looking Swiss ecosystem, Regulatory Task Force Report, 27. April 2018
- SwissBanking, Kommentar zur Vereinbarung über die Standesregeln zur Sorgfaltpflicht der Banken (VSB 20), 2020
- SwissBanking, Open Banking. Eine Auslegeordnung für den Schweizer Finanzplatz, 9. Juli 2020
- SwissBanking/Swiss Fintech Innovations (SFTI), Open Finance in der Schweiz, Hintergrund zum Rollenverständnis am Finanzplatz Schweiz, 4. März 2021
- Swissquote, undatiert, <https://de.swissquote.com/crypto-assets>
- Switchero TradeHub, Introduction, undatiert, <https://guide.switchero.com/>
- sxysun, Short Note on {Monarch, Moloch, Mafia} Extractable Value, 6. November 2022, <https://hackmd.io/@sxysun/short-note-ext>
- Synthetic Community, Layer 2, undatiert, <https://syntheticcommunity/docs/layer-2>
- Synthetic Community, Project Overview, undatiert, <https://syntheticcommunity/docs/intro-overview>
- Synthetic Community, Staking Overview, undatiert, <https://syntheticcommunity/docs/staking-snx-overview>
- Synthetic, Litepaper, Synthetic.Exchange, Version 1.4, März 2020, <https://docs.synthetic.io/litepaper/#syntheticexchange>
- Synthetic, Litepaper, System Architecture, Version 1.4, März 2020, <https://docs.synthetic.io/litepaper/#system-architecture>
- Szabo Nick, Bit Gold, 29. Dezember 2005, <http://nakamotoinstitute.org/bit-gold/>
- Szabo Nick, Formalizing and Securing Relationships on Public Networks, 1997, <https://nakamotoinstitute.org/formalizing-securing-relationships/>

- Szabo Nick, Money, blockchains, and social scalability, 9. Februar 2017, <https://unenumerated.blogspot.com/2017/02/money-blockchains-and-social-scalability.html>
- Szabo Nick, Smart Contracts, 1994, <https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html>
- Szabo Nick, Smart Contracts: Building Blocks for Digital Markets, 1996, http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html
- Szabo Nick, Trusted Third Parties are Security Holes, 2001, <https://nakamotoinstitute.org/trusted-third-parties/>
- Szabo Nick, Wet code and dry, 24. August 2008, <https://unenumerated.blogspot.com/2006/11/wet-code-and-dry.html>
- Tadelis Steven, Game Theory. An Introduction, Princeton/Oxford 2013
- Takanashi Yuta/Matsuo Shin'ichiro/Burger Eric/Sullivan Clare/Miller James/Sato Hirotoshi, Call for Multi-Stakeholder Communication to Establish a Governance Mechanism for the Emerging Blockchain-Based Financial Ecosystem. Part 2 of 2, Stanford Journal of Blockchain Law & Policy 2020, 117-145
- Takanashi Yuta/Matsuo Shin'ichiro/Burger Eric/Sullivan Clare/Miller James/Sato Hirotoshi, Call for Multi-Stakeholder Communication to Establish a Governance Mechanism for the Emerging Blockchain-Based Financial Ecosystem, Stanford Journal of Blockchain Law & Policy 2020, 1-20
- Taleb Nassim Nicholas, Antifragile. Things That Gain From Disorder, London/New York 2013
- Taleb Nassim Nicholas, The Black Swan. The Impact of the Highly Improbable, New York 2007
- Tapscott Don/Tapscott Alex, How Blockchain Will Change Organizations, MIT Sloan Management Review 2017, 10-13
- Taube Tamara, Entstehung, Bedeutung und Umfang der Sorgfaltspflichten der Schweizer Banken bei der Geldwäschereiprävention im Bankenalltag, SGSF 9, Diss. Zürich/St. Gallen 2013
- Taylor Matt, How Matcha finds the best prices for DeFi traders, 28. Juli 2020, <https://matcha.xyz/blog/how-matcha-finds-the-best-prices>
- tBTC, tBTC Security Model, 18. April 2020, <https://tbtc.network/developers/tbtc-security-model/>
- Team Gemini, You're One Step Closer to Financial Freedom With Shielded ZEC Withdrawals, 29. September 2020, <https://www.gemini.com/blog/youre-one-step-closer-to-financial-freedom-with-shielded-zec-withdrawals>

- Telos Blockchain Network Operating Agreement (TBNOA), undatiert, <https://tb-noa.org/details.html?docid=6>
- Telos Foundation, Telos Governance Explained – The Operating Agreement, 5. Oktober 2018, <https://medium.com/telos-foundation/telos-governance-explained-the-operating-agreement-e3d1eea137b>
- Ter-Sahakyan Gohar, Economic and Legal Risks of Private Investors in Cross-Border Securities Investment Processes. EU, Swiss and Russian regulatory perspectives, Diss. Zürich, 2020
- Tesla, Tesla Inc., Form 10-K, Annual Report Pursuant to Section 13 or 15(d) of the Securities Exchange Act of 1934, 8. Februar 2021, https://ir.tesla.com/flysystem/s3/sec/000156459021004599/tsla-10k_20201231-gen.pdf
- tether, Legal, Terms of Service, 12. Mai 2020, <https://tether.to/legal/>
- tether, Tether: Fiat currencies on the Bitcoin blockchain, Juni 2016, <https://tether.to/wp-content/uploads/2016/06/TetherWhitePaper.pdf>
- Teubner Gunther, «Verbund», «Verband» oder «Verkehr»? , ZHR 1990, 295–324
- Teubner Gunther, Digitale Rechtssubjekte? Zum privatrechtlichen Status autonomer Softwareagenten, AcP 2018, 155–205
- Teubner Gunther, Unitas Multiplex. Das Konzernrecht in der neuen Dezentralität der Unternehmensgruppe, ZGR 1991, 189–217
- Teubner Gunther/Willke Helmut, Kontext und Autonomie: Gesellschaftliche Selbststeuerung durch reflexives Recht, Zeitschrift für Rechtssoziologie, 1984, 4–35
- Thaler Richard H./Sunstein Cass R., Nudge. Improving Decisions About Health, Wealth, and Happiness, New Haven/London 2008
- The Attacker, An Open Letter, 18. Juni 2016, <https://pastebin.com/CcGUBgDG>
- The Blocknet Protocol, The Evolution of the Decentralized Exchange: A Brief History, 13. Mai 2019, <https://theblocknetchannel.medium.com/the-evolution-of-the-decentralized-exchange-a-brief-history-888ee0ce1803>
- The Blocknet Protocol, Understanding a Decentralized Exchange, 6. Februar 2018, <https://theblocknetchannel.medium.com/understanding-a-decentralized-exchange-eee9e1043f45>
- The Defiant, DeFi Transparency x The Defiant & DeFiWatch, 4. August 2021, <https://youtu.be/kOK5u93JnRQ>
- The Defiant, Uniswap Website Geo-Ban Can't Stop DeFi, 9. Dezember 2019, <https://newsletter.thedefiant.io/p/uniswap-website-geo-ban-cant-stop-370>
- The Economist, The trust machine. The technology behind bitcoin could transform how the economy works, 31. Oktober 2015, <https://www.economist.com/leaders/2015/10/31/the-trust-machine>
- The Stablecoin Index, undatiert, <https://stablecoinindex.com/projects>

- Thelesklaf Daniel/Wyss Ralph/van Thiel Mark/Ordolli Stiliano, GwG Kommentar. Schweizerisches Geldwäschereigesetz mit weiteren Erlassen, 3. Aufl., Zürich 2019 (OFK GwG-Autor, Art. N)
- Thévenoz Luc, Intermediated Securities, Legal Risk, and the International Harmonisation of Commercial Law, *Stanford Journal of Law, Business and Finance* 2008, 384–452
- Thévenoz Luc/Werro Franz (Hrsg.), *Commentaire romand Code des obligations I. Art. 1-529 CO*, 3. Aufl., Basel 2021 (CR CO I-Autor, Art. N)
- Thierer Adam, *Permissionless Innovation. The Continuing Case for Comprehensive Technological Freedom*, Arlington 2016
- Thompson Nicholas/Barrett Brian, How Twitter Survived Its Biggest Hack – and Plans to Stop the Next One, 24. September 2020, <https://www.wired.com/story/inside-twitter-hack-election-plan/>
- THORChain, Continuous Liquidity Pools, undatiert, <https://docs.thorchain.org/how-it-works/continuous-liquidity-pools>
- THORChain, Introduction, undatiert, <https://docs.thorchain.org/>
- THORChain, Technology, undatiert, <https://docs.thorchain.org/technology>
- thorchain.org, THORChain TSS: Leader-less Threshold Signature Protocol, 10. Juli 2020, <https://github.com/thorchain/Resources/raw/master/Whitepapers/THORChain-TSS-Paper-June2020.pdf>
- THORSwap, What is THORSwap, FAQ, undatiert, <https://thorswap.finance/faq/>
- Thouvenin Florent/Stiller Burkhard/Hettich Peter/Bocek Thomas/Reutimann Kento, Keine Netzsperrern im Urheberrecht, sic! 2017, 701–722
- Thür Hanspeter, Die Privatsphäre im Zeitalter von Big Data, *Jusletter IT* vom 21. Mai 2015
- Thurman Andrew, DeFi lending platform Aave reveals ‘permissioned pool’ for institutions, 12. Mai 2021, <https://cointelegraph.com/news/defi-lending-platform-aave-reveals-private-pool-for-institutions>
- Tien Lee, Publishing Software as a Speech Act, *Berkeley Technology Law Journal* 2000, 629–712
- Tietje Christian/Lehmann Matthias, The Role and Prospects of International Law in Financial Regulation and Supervision, in: Cottier Thomas/Jackson John H./Lastra Rosa M. (Hrsg.), *International Law in Financial Regulation and Monetary Affairs*, Oxford 2012, 133–150
- Tobin James, Financial Intermediaries, in: Eatwell John/Milgate Murray/Newman Peter (Hrsg.), *The New Palgrave: Money*, New York/London 1989, 157–174
- Tobler Simone, MiCAR – Höhenflug oder unsanfte Landung für Schweizer Krypto-Anbieter?, *EuZ* 04/2023, E1–E45

de Tocqueville Alexis, De la démocratie en Amérique, 12. Aufl., Paris 2012

TokenTrade: Marketplace for Ethereum ERC20 Tokens, undatiert, <https://www.reddit.com/r/tokentrade/>

Tornado Cash, Introducing Private Transactions On Ethereum NOW!, 6. August 2019, <https://tornado-cash.medium.com/introducing-private-transactions-on-ethereum-now-42ee915babe0>

Torpey Kyle, Exploring The Centralization Risks Of Bitcoin's Lightning Network, 5. Mai 2016, <https://bitcoinmagazine.com/articles/exploring-the-centralization-risks-of-bitcoin-s-lightning-network-1462460852>

Townsend Robert M., Distributed Ledgers. Design and Regulation of Financial Infrastructure and Payment Systems, Cambridge/London 2020

Tran Ki Chong, What is WBTC?, 6. April 2020, <https://decrypt.co/resources/what-is-wbtc-explained-bitcoin-ethereum-defi>

Tränkle Stefan, Blockchain/Distributed Ledger Technology – Eine finanzmarktrechtliche Betrachtung, in: Reutter Thomas U./Werlen Thomas (Hrsg.), Innovation und Disruption: Sanierungen, Exits, LIBOR-Ablösung und Blockchain, Kapitalmarkt – Recht und Transaktionen XVI, EIZ 210, Zürich 2021, 157–167

Trautman Lawrence, Virtual Currencies; Bitcoin & What Now After Liberty Reserve, Silk Road, and Mt. Gox?, Richmond Journal of Law and Technology 2014, 1–108

TRM, FATF Provides Final Guidance, 28. Oktober 2021, <https://www.trmlabs.com/post/fatf-provides-final-guidance>

Troncoso Carmela/Isaakidis Marios/Danezis George/Halpin Harry, Systematizing Decentralization and Privacy: Lessons from 15 Years of Research and Deployments, Proceedings on Privacy Enhancing Technologies 2017, 307–329

Trüeb Hans Rudolf, Smart Contracts, in: Grolimund Pascal/Koller Alfred/Loacker Leander D./Portmann Wolfgang (Hrsg.), Festschrift für Anton K. Schnyder zum 65. Geburtstag, Zürich/Basel/Genf 2018, 723–734

Tschannen Pierre/Zimmerli Ulrich/Müller Markus, Allgemeines Verwaltungsrecht, 4. Aufl., Bern 2014

Tschentscher Axel, Grundprinzipien des Rechts. Einführung in die Rechtswissenschaft mit Beispielen aus dem schweizerischen Recht, Bern/Stuttgart/Wien 2003

Tual Stephan, A Primer to Decentralized Autonomous Organizations (DAOs), 3. März 2016, <https://blog.slock.it/a-primer-to-the-decentralized-autonomous-organization-dao-69fb125bd3cd>

Tullock Gordon, The Welfare Costs of Tariffs, Monopolies, and Theft, Western Economic Journal 1967, 224–232

Tullock Gordon/Seldon Arthur/Brady Gordon L., Government Failure. A Primer in Public Choice, Washington 2002

- Turing Alan M., On Computable Numbers, with an Application to the Entscheidungsproblem, Proceedings of the London Mathematical Society 1936, 230–265
- Turner Adair, Between Debt and Devil. Money, Credit, and Fixing Global Finance, Princeton/Oxford 2016
- Tversky Amos/Kahneman Daniel, The Framing of Decisions and the Psychology of Choice, Science 1981, 453–458
- Tyrell Marcel/Böhme Rainer, Der Finanzsektor und die Resonanzkatastrophe, in: Janzen Stephan A./Schröter Eckhard/Steher Nico (Hrsg.), Fragile Stabilität – stabile Fragilität, Wiesbaden 2013, 279–302
- Uhlmann Felix/Stojanovic Jasna, Vertrauen im Finanzmarktrecht aus öffentlich-rechtlicher Sicht, SZW 2017, 732–742
- ul Hassan Fakhar/Ali Anwaar/Rahouti Mohamed/Latif Siddique/Kanhere Salil/Singh Jatinder/Al-Fuqaha Ala/Janjua Umar/Noor Mian Adnan/Qadir Junaid/Crowcroft Jon, Blockchain and the Future of the Internet: A Comprehensive Review, 13. November 2020, <https://arxiv.org/abs/1904.00733>
- UMA, UMA Initial Uniswap Listing, 22. April 2020, <https://medium.com/uma-project/umas-initial-uniswap-listing-afa7b6f6a330>
- Uniform Law Commission (ULC), Uniform Regulation of Virtual-Currency Businesses Act. With Prefatory Note and Comments, 9. Oktober 2017, <https://www.uniform-laws.org/committees/community-home?Community-Key=e104aaa8-c10f-45a7-a34a-0423c2106778>
- Uniswap, Ecosystem Participants, undatiert, <https://uniswap.org/docs/v2/protocol-overview/ecosystem-participants/>
- Uniswap, How Uniswap works, undatiert, <https://uniswap.org/docs/v2/protocol-overview/how-uniswap-works/>
- Uniswap, Introducing Sybil, 15. Dezember 2020, <https://uniswap.org/blog/sybil/>
- Uniswap, Introducing UNI, 16. September 2020, <https://uniswap.org/blog/uni/>
- Uniswap, Introducing Uniswap V3, 23. März 2021, <https://uniswap.org/blog/uniswap-v3/>
- Uniswap, Introducing Uniswap V3, License, 23. März 2021, <https://uniswap.org/blog/uniswap-v3/#license>
- Uniswap, Token access on app.uniswap.org, 23. Juli 2021, <https://uniswap.org/blog/token-access-app/>
- Uniswap, Twitter, 13. August 2019, <https://twitter.com/uniswap/status/1161348524799221760>
- Uniswap, Uniswap Interface, undatiert, <https://github.com/Uniswap/uniswap-interface/releases/>

- Uniswap, Uniswap on Arbitrum (Alpha launch)!, 31. August 2021, <https://uniswap.org/blog/uniswap-arbitrum-alpha/>
- Uniswap, Uniswap on Optimism (Alpha launch)!, 13. Juli 2021, <https://uniswap.org/blog/uniswap-optimism-alpha/>
- Van Doeren Peter, GameStop, Payments for Order Flow, and High Frequency Trading, 1. Februar 2021, <https://www.cato.org/blog/gamestop-payments-order-flow-high-frequency-trading>
- Van Loo Rory, Making Innovation More Competitive: The Case of Fintech, UCLA Law Review 2018, 232–279
- Van Valkenburgh Peter, Broad, Ambiguous, or Delegated: Constitutional Infirmities of the Bank Secrecy Act, Coin Center Report, November 2023, <https://www.coincenter.org/broad-ambiguous-or-delegated-constitutional-infirmities-of-the-bank-secrecy-act/>
- Van Valkenburgh Peter, Electronic Cash, Decentralized Exchange, and the Constitution, Coin Center Report, März 2019, <https://www.coincenter.org/electronic-cash-decentralized-exchange-and-the-constitution/>
- Van Valkenburgh Peter, FinCEN's new cryptocurrency guidance matches Coin Center recommendations, 9. Mai 2019, <https://www.coincenter.org/fincens-new-cryptocurrency-guidance-matches-coin-center-recommendations/>
- Van Valkenburgh Peter, Framework for Securities Regulation of Cryptocurrencies, Version 2.0., August 2018, <https://www.coincenter.org/framework-for-securities-regulation-of-cryptocurrencies/>
- Van Valkenburgh Peter, New Tornado Cash indictments seem to run counter to FinCEN guidance. Our initial thoughts on a case that could potentially criminalize the publication of software code, 23. August 2023, <https://www.coincenter.org/new-tornado-cash-indictments-seem-to-run-counter-to-fincen-guidance/>
- Van Valkenburgh Peter, The Bank Secrecy Act, Cryptocurrencies, and New Tokens: What is Known and What Remains Ambiguous, Coin Center Report, Mai 2017, <https://www.coincenter.org/app/uploads/2020/05/report-bsa-crypto-to-ken1.pdf>
- Van Valkenburgh Peter, The differences between Bitcoin and Libra should matter to policymakers. The two have different design goals, work in different ways, and raise different regulatory questions, 8. Juli 2019, <https://www.coincenter.org/the-differences-between-bitcoin-and-libra-should-matter-to-policymakers/>
- Van Valkenburgh Peter, The long-awaited FATF crypto guidance is not as bad as it could have been, but still flawed. Here's the good, bad, and ugly, 28. Oktober 2021, <https://www.coincenter.org/the-long-awaited-fatf-crypto-guidance-is-not-as-bad-as-it-could-have-been-but-still-flawed/>

- Van Valkenburgh Peter, The Need for a Federal Alternative to State Money Transmission Licensing, Coin Center Report, Januar 2018, <https://coincenter.org/entry/federal-alternative-to-state-money-transmission>
- Van Valkenburgh Peter, The Uniform Law Commission Has Given States a Clear Path to Approach Bitcoin, 27. Juli 2017, <https://www.coincenter.org/the-uniform-law-commission-has-given-states-a-clear-path-to-approach-bitcoin/>
- Van Valkenburgh Peter, The Unintended(?) Consequences of the STABLE Act, 3. Dezember 2020, <https://www.coincenter.org/the-unintended-consequences-of-the-stable-act/>
- Van Valkenburgh Peter, The upcoming FATF interpretive note is not doomsday for cryptocurrency, 20. Juni 2019, <https://www.coincenter.org/the-upcoming-fatf-interpretive-note-is-not-doomsday-for-cryptocurrency/>
- Van Valkenburgh Peter, There's no such thing as a decentralized exchange, 3. Oktober 2020, <https://www.theblockcrypto.com/post/79768/theres-no-such-thing-as-a-decentralized-exchange>
- Van Valkenburgh Peter, Tornado Cash is no «golem.» It's a tool for privacy and free speech. A rebuttal of a recent article in Lawfare by Henry Farrell and Bruce Schneier, 26. Oktober 2022, <https://www.coincenter.org/tornado-cash-is-no-golem-its-a-tool-for-privacy-and-free-speech/>
- Van Valkenburgh Peter, What could «decentralization» mean in the context of the law? How Bitcoin's inception helps us understand good policy for securities regulation. 15. Juni 2018, <https://www.coincenter.org/what-could-decentralization-mean-in-the-context-of-the-law/>
- Vatiero Massimiliano, Smart contracts, transaction costs and adaptation, 25. Februar 2020, <https://ssrn.com/abstract=3259958>
- Velde François R., Was John Law's System a bubble? The Mississippi Bubble revisited, in: Attack Jeremy/Neal Larry (Hrsg.), The Origins and Development of Financial Markets and Institutions. From the Seventeenth Century to the Present, Cambridge/ New York 2009, 99–120
- Vergne Jean-Philippe (JP), Web3 as Decentralization Theater? A Framework for Envisioning Decentralization Strategically, 2023, <https://cryptocarnival.wtf/vergne>
- Victor Friedhelm, Address Clustering Heuristics for Ethereum, in: Bonneau Joseph/Heninger Nadia (Hrsg.), Financial Cryptography and Data Security 2020, LNCS 12059, Cham 2020, 617–633
- Victor Friedhelm/Weintraud Andrea Marie, Detecting and Quantifying Wash Trading on Decentralized Cryptocurrency Exchanges, in: Leskovec Jure/Grobelnik Marko/Najork Marc (Hrsg.), Proceedings of the Web Conference 2021, New York 2021, 23–32

- Villiger Mark E., Handbuch der Europäischen Menschenrechtskonvention (EMRK) mit besonderer Berücksichtigung der Rechtsprechung des Europäischen Gerichtshofs für Menschenrechte in Schweizer Fällen, 3. Aufl., Zürich/Genf/Basel 2020
- Vivek, How to Attack and Defend Quadratic Funding, 11. März 2021, <https://gitcoin.co/blog/how-to-attack-and-defend-quadratic-funding/>
- Voell Zack/Pan David, OKEEx Suspends Withdrawals, Says Key Holder Not Available Due to Cooperation With Investigation, 16. Oktober 2020, <https://www.coindesk.com/okex-suspends-withdrawals>
- Vogel Alexander/Heiz Christoph/Luthiger Reto, FIDLEG/FINIG Kommentar. Bundesgesetz über die Finanzdienstleistungen und Bundesgesetz über die Finanzinstitute und weiteren Erlassen, Zürich 2020 (OFK FIDLEG/FINIG-Vogel/Heiz/Luthiger, Art. N)
- Vogel Alexander/Heiz Christoph/Luthiger Reto, FinfraG/BEG Kommentar. Finanzmarktinfrastukturgesetz und Bucheffektengesetz mit HWPÜ und weiteren Erlassen, Zürich 2019 (OFK FinfraG/BEG-Vogel/Heiz/Luthiger, Art. N)
- Voltaire, La Bégueule, 1772, [https://fr.wikisource.org/wiki/Contes_en_vers_\(Voltaire\)/La_B%C3%A9gueule](https://fr.wikisource.org/wiki/Contes_en_vers_(Voltaire)/La_B%C3%A9gueule)
- Vontobel, Tracker Certificates on Crypto Currencies, undatiert, <https://derinet.vontobel.com/CH/EN/cryptoworld>
- Voorhees Erik, Introducing ShapeShift Membership, 4. September 2018, <https://web.archive.org/web/20180904213955/https://info.shapeshift.io/blog/2018/09/04/introducing-shapeshift-membership/>
- Voorhees Erik, Looting of the Fox: The Story of Sabotage at ShapeShift, 19. April 2016, <https://news.bitcoin.com/looting-fox-sabotage-shapeshift/>
- Voorhees Erik, No More KYC with ShapeShift, 6. Januar 2021, <https://erikvoorhees.medium.com/no-more-kyc-with-shapeshift-6d95a3e63ddf>
- Voorhees Erik, ShapeShift Decentralizes, 14. Juli 2021, <https://erikvoorhees.medium.com/shapeshift-is-decentralizing-639bb4c82fc8>
- Vorick David, Announcing Homescreen: Decentralized Frontends for Web3, 17. September 2021, <https://blog.sia.tech/announcing-homescreen-decentralized-frontends-for-web3-113a3564530d>
- Voshmgir Shermin, § 2 Smart Contracts, Blockchains und automatisch ausführbare Protokolle, in: Braegelmann Tom/Kaulartz Markus (Hrsg.), Rechtshandbuch Smart Contracts, München 2019
- Voshmgir Shermin, Disrupting governance with blockchains and smart contracts, Strategic Change 2017, 499–509
- Voshmgir Shermin/Zargham Michael, Foundations of Cryptoeconomic Systems, Working Paper Series 1/2020, WU Vienna University of Economics and Business, 2020, <https://epub.wu.ac.at/7782/>

- Waespi Oliver, Organisationshaftung. Risiko und Unsorgfalt bei der Geschäftsherrenhaftung, ASR 700, Diss. Bern 2005
- Wagner Alexander F./Weber Rolf H., Corporate Governance auf der Blockchain, SZW 2017, 59–70
- Wagner R. Polk, Information Wants to Be Free: Intellectual Property and the Mythologies of Control, Columbia Law Review 2003, 995–1034
- Walch Angela, Blockchain Emergencies & Open-Source Software Governance: Is «Rough Consensus» a Suicide Pact?, in: Proceedings of the 2021 Spring Conference: The Impact of Blockchain on the Practice of Law, New York University Journal of Law & Business 2021, 699–704
- Walch Angela, Deconstructing «Decentralization». Exploring the Core Claim of Crypto Systems, in: Brummer Chris (Hrsg.), Cryptoassets. Legal, Regulatory, and Monetary Perspectives, Oxford/New York 2019, 39–68
- Walch Angela, In Code(rs) We Trust: Software Developers as Fiduciaries in Public Blockchains, in: Hacker Philipp/Lianos Ioannis/Dimitropoulos Georgios/Eich Stefan (Hrsg.), Regulating Blockchain. Techno-Social and Legal Challenges, Oxford/New York 2019, 58–81
- Walch Angela, The Bitcoin Blockchain as Financial Market Infrastructure: A Consideration of Operational Risk, New York University Journal of Legislation & Public Policy 2015, 837–893
- Walden Jesse, Progressive Decentralization: A Playbook for Building Crypto Applications, 9. Januar 2020, <https://a16z.com/2020/01/09/progressive-decentralization-crypto-product-management/>
- Waldmann Bernhard/Belser Eva Maria/Epiney Astrid (Hrsg.), Basler Kommentar zur Bundesverfassung, Basel 2015 (BSK BV-Autor, Art. N)
- Wales Justin S./Ovelmen Richard J., Bitcoin is Speech: Notes Toward Developing the Conceptual Contours of Its Protection Under the First Amendment, University of Miami Law Review 2019, 204–275
- Walker George, Financial Markets and Exchanges, in: Blair Michael/Walker George/Wiley Stuart (Hrsg.), Financial Markets and Exchanges Law, 2. Aufl., Oxford 2012, N 1.01–1.156
- Walker George, Financial Technology Law – A New Beginning and a New Future, The International Lawyer 2017, 137–216
- Wall Eric/Malm Gustaf, Using Blockchain Technology and Smart Contracts to Create a Distributed Securities Depository, Master's Thesis, Lund 2016
- Wall Larry D., Fractional Reserve Cryptocurrency Banks, April 2019, <https://www.frbatlanta.org/cenfig/publications/notesfromthevault/04-fractional-reserve-cryptocurrency-banks-2019-04-25>

- Wang Dabao/Wu Siwei/Lin Ziling/Wu Lei/Yuan Xingliang/Zhou Yajin/Wang Haoyu/ Ren Kui, Towards A First Step to Understand Flash Loan and Its Applications in DeFi Ecosystem, in: 2021 Proceedings of the Ninth International Workshop on Security in Blockchain and Cloud Computing, New York 2021, 23–28
- Wang Daniel, Withdraw from Loopring 3.1 – the First-Ever Experiment of Shutting Down a zkRollup, 7. Februar 2021, <https://medium.com/loopring-protocol/withdraw-from-loopring-3-1-the-first-ever-experiment-of-shutting-down-a-zkrollup-24e6f333ca57>
- Wang Daniel/Zhou Jay/Wang Alex/Finestone Matthew, Loopring: A Decentralized Token Exchange Protocol, 8. September 2018, https://loopring.org/resources/en_whitepaper.pdf
- Wang Loong, How RenVM Actually Works. Bringing Bitcoin, Bitcoin Cash, and Zcash to Ethereum, 9. Januar 2020, <https://medium.com/renproject/how-renvm-actually-works-c2f76a2630c4>
- Wang Qin/Li Rujia/Wang Qi/Chen Shiping, Non-Fungible Token (NFT): Overview, Evaluation, Opportunities and Challenges, 25. Oktober 2021, <https://arxiv.org/abs/2105.07447>
- Wang Ye/Zuest Patrick/Yao Yaxing/Lu Zhicong/Wattenhofer Roger, Impact and User Perception of Sandwich Attacks in the DeFi Ecosystem, in: Proceedings of the 2022 CHI Conference on Human Factors in Computing Systems, 2022, 1–15
- Ward Allen M./Heichelheim Fritz M./Yeo Cedric A., A History of the Roman People, 6. Aufl., London/New York 2016
- Warren Will, Compliant peer-to-peer trading. Towards the next wave of DEX adoption, 19. April 2018, <https://blog.0xproject.com/compliant-peer-to-peer-trading-4dab8e5c3162>
- Warren Will, Decentralized Exchange, 10. Oktober 2018, <https://www.coincenter.org/education/key-concepts/decentralized-exchange/>
- Warren Will, Front-running, Griefing and the Perils of Virtual Settlement (Part 1), 22. Dezember 2017, <https://medium.com/0x-project/front-running-griefing-and-the-perils-of-virtual-settlement-part-1-8554ab283e97>
- Warren Will, Front-running, Griefing and the Perils of Virtual Settlement (Part 2), 9. Februar 2018, <https://medium.com/0x-project/front-running-griefing-and-the-perils-of-virtual-settlement-part-2-921b00109e21>
- Warren Will, The difference between App Coins and Protocol Tokens, 2. Februar 2017, <https://blog.0xproject.com/the-difference-between-app-coins-and-protocol-tokens-7281a428348c>
- Warren Will/Bandeali Amir, 0x: An open protocol for decentralized exchange on the Ethereum blockchain, 21. Februar 2017, https://0x.org/pdfs/0x_white_paper.pdf

- wasabi docs, coinjoin, undatiert, <https://docs.wasabiwallet.io/using-wasabi/Coin-Join.html>
- Wattenhofer Roger, The Science of the Blockchain, 2016
- Watter Rolf, Handel in Wertschriften auf einer Netto-Basis, in: Walder Hans Ulrich/Jaag Tobias/Zobl Dieter (Hrsg.), Aspekte des Wirtschaftsrechts. Festgabe zum Schweizerischen Juristentag 1994, Zürich 1994, 181–194
- Watter Rolf, Investorenschutz im Kapitalmarktrecht, AJP 1997, 269–282
- Watter Rolf/Bahar Rashid (Hrsg.), Finanzmarktaufsichtsgesetz. Finanzmarktinfrastukturgesetz, 3. Aufl., Basel 2019 (BSK FINMAG/FinfraG-Autor, Art. N)
- Watter Rolf/Spillmann Till, Corporate Social Responsibility – Leitplanken für den Verwaltungsrat Schweizerischer Aktiengesellschaften, GesKR 2006, 94–116
- Watter Rolf/Vogt Nedim Peter (Hrsg.), Basler Kommentar zum Börsengesetz und Finanzmarktaufsichtsgesetz. Art. 161, 161bis, 305bis, 305ter Strafgesetzbuch, 2. Aufl., Basel 2011 (BSK BEHG/FINMAG-Autor, Art. N)
- Watter Rolf/Vogt Nedim Peter/Bauer Thomas/Winzeler Christoph (Hrsg.), Basler Kommentar zum Bankengesetz, 2. Aufl., Basel 2013 (BSK BankG-Autor, Art. N)
- WBTC, Order Book, undatiert, <https://wbtc.network/dashboard/order-book>
- Wearn Alex, Pragmatic Decentralization: How IDEX Will Approach Industry Regulations, 1. November 2018, <https://blog.idex.io/all-posts/pragmatic-decentralization-how-idex-will-approach-industry-regulations>
- Weber Max, Grundriss der Sozialökonomik. III. Abteilung: Wirtschaft und Gesellschaft, Tübingen 1922
- Weber Rolf H., Ausgabe von und Handel mit (digitalen) Wertrechten, in: Arpagaus Reto/Stadler Ralph/Werlen Thomas (Hrsg.), Das Schweizerische Bankgeschäft, Zürich/Basel/Genf 2021
- Weber Rolf H., Blockchain als rechtliche Herausforderung, Jusletter IT vom 18. Mai 2017
- Weber Rolf H., Börsenrecht. Börsengesetz (BEHG) mit weiteren Erlassen, 2. Aufl., Zürich 2013 (OFK BEHG-Weber, Art. N)
- Weber Rolf H., Braucht die digitale Welt ein neues Haftungsrecht, Jusletter IT vom 21. September 2017
- Weber Rolf H., Cybergovernance revisited, Jusletter IT vom 30. September 2021
- Weber Rolf H., DLT-Handelsplattformen, Spannungsfeld von Technologie und Recht, ITSL 10, Zürich 2022
- Weber Rolf H., E-Commerce und Recht. Rechtliche Rahmenbedingungen elektronischer Geschäftsformen, 2. Aufl., Zürich/Basel/Genf 2010
- Weber Rolf H., Elements of a Legal Framework for Cyberspace, SRIEL 2016, 195–215

- Weber Rolf H., Führen die neuen Technologien zur Disruption der Finanzmarktregulierung?, SZW 2018, 684–695
- Weber Rolf H., Global Financial Architecture and Decentralized CBDC Regimes, in: Gortsos Christos V./Sethe Rolf, Central Bank Digital Currencies. Proceedings of a Colloquium, Zürich 2023, 13–31
- Weber Rolf H., Haftungsfragen beim Handel von digitalen Vermögenswerten, SJZ 2021, 679–687
- Weber Rolf H., Handel mit digitalen Aktiven, in: Weber Rolf H./Kuhn Hans (Hrsg.), Entwicklungen im Schweizer Blockchain-Recht, Basel 2021
- Weber Rolf H., Internet Governance at the Point of No Return, Zürich 2021
- Weber Rolf H., Legal foundations of multistakeholder decision-making, ZSR 2016 I, 247–267
- Weber Rolf H., Leistungsstörungen und Rechtsdurchsetzung bei Smart Contracts, Jusletter vom 4. Dezember 2017
- Weber Rolf H., Multilayered Governance in International Financial Regulation and Supervision, Journal of International Economic Law 2010, 683–704
- Weber Rolf H., Open Finance und Decentralized Finance – Entwicklungen in einem disruptiven Finanzmarktumfeld, SZW 2022, 3–13
- Weber Rolf H., Rahmen und Wege globaler Rechtsentwicklungen, SJZ 2016, 293–301
- Weber Rolf H., Rose is a rose is a rose is a rose – what about code and law?, Computer Law & Security Review 2018, 701–706
- Weber Rolf H., Shaping Internet Governance: Regulatory Challenges, Zürich/Basel/Genf 2009
- Weber Rolf H., Sicherheit und Resilienz in DLT-Finanzmarktinfrastrukturen, Jusletter vom 13. Juni 2022
- Weber Rolf H., Smart Contracts: Vertrags- und verfügungsrechtlicher Regelungsbedarf, sic! 2018, 291–301
- Weber Rolf H., State Interventions and Competition Distortion in Financial Markets, SZW 2009, 428–438
- Weber Rolf H., The Interplay of Blockchain Technologies and Data Protection, Jusletter IT vom 30. September 2020
- Weber Rolf H., The Role of Law in Constituting Financial Markets, Journal of International Banking Law and Regulation 2017, 253–260
- Weber Rolf H., Wettbewerb zwischen internationalen Standards, SZW 2015, 579–585
- Weber Rolf H., Zivilrechtliche Aspekte von Geschäftsabwicklungen auf DLT-Handelsplattformen, SZW 2021, 450–460

- Weber Rolf H./Baisch Rainer, Crowdinvesting mittels Initial Coin Offering – Regulierungsaufgaben im Token-Universum, SZW 2019, 135–154
- Weber Rolf H./Baisch Rainer, DLT-basierte Finanzprodukte, SZW 2021, 683–697
- Weber Rolf H./Baisch Rainer, FinTech – eligible safeguards to foster the regulatory framework, Journal of International Banking Law and Regulation 2018, 335–350
- Weber Rolf H./Baisch Rainer, Regulierung von Robo-Advice, AJP 2016, 1065–1078
- Weber Rolf H./Baumann Simone, FinTech – Schweizer Finanzmarktregulierung im Lichte disruptiver Technologien. Regulierungsansätze für neue Finanzdienstleistungstechnologien, Jusletter vom 21. September 2015
- Weber Rolf H./Iacangelo Salvatore, Rechtsfragen bei der Übertragung von Token, Jusletter IT vom 24. Mai 2018
- Weber Rolf H./Yildiz Okan, Alternative Dispute Resolution auf DLT-Handelsplattformen. Tauglichkeit der Online Dispute Resolution und der On-Chain Arbitration für DLT-Handelsplattformen, Jusletter vom 14. Juni 2021
- Weber Steven, The Success of Open Source, Cambridge/London 2004
- Weingärtner Tim/Fasser Fabian/Reis Sá da Costa Pedro/Farkas Walter, Deciphering DeFi: A Comprehensive Analysis and Visualization of Risks in Decentralized Finance, Journal of Risk and Financial Management 2023, 1–25
- Weisenthal Joe/Alloway Tracy, Hayden Adams Explains Uniswap and the Rise of DeFi, 6. Mai 2021, <https://www.bloomberg.com/news/articles/2021-05-06/hayden-adams-explains-uniswap-and-the-rise-of-defi>
- Wendell Holmes Oliver, Jr., The Common Law, Boston 1881
- Werbach Kevin, The Blockchain and the New Architecture of Trust, Cambridge/London 2018
- Werbach Kevin/Cornell Nicolas, Contracts Ex Machina, Duke Law Journal 2017, 313–382
- Werlen Thomas, Konzeptionelle Grundlagen des schweizerischen Kapitalmarktrechts, SSB 23, Diss. Zürich
- Werlen Thomas/Hertner Jonas, Crowdfunding nach Schweizer Art. Rückbesinnung auf die Prinzipien der Kapitalmarktregulierung, in: Gschwend Lukas/Hettich Peter/Müller-Chen Markus/Schindler Benjamin/Wildhaber Isabelle (Hrsg.), Recht im digitalen Zeitalter. Festgabe Schweizerischer Juristentag 2015 in St. Gallen, Zürich/St. Gallen 2015, 315–330
- Werlen Thomas/Weber Simon, Switzerland's Quest for a Safe Haven for Crypto Products, CapLaw-2023-39
- Werner Sam M./Perez Daniel/Gudgeon Lewis/Klages-Mundt Arianah/Harz Dominik/Knotenbelt William J., SoK: Decentralized Finance (DeFi), 30. April 2021, <https://arxiv.org/abs/2101.08778>

- Wesseling Mara, The European Fight against Terrorism Financing. Professional Fields and New Governing Practices, Amsterdam 2013
- Wharton Blockchain and Digital Asset Project, DeFi Beyond the Hype. The Emerging World of Decentralized Finance, Mai 2021
- Wheeler Tom, From Gutenberg to Google. The History of Our Future, Washington 2019
- Wherlock Alexander/Haeberli Daniel, Use of liquidity pools on DEX and the application of Swiss regulations to liquidity tokens, International Financial Law Review Winter 2021, <https://www.iflr.com/article/2a647e1ubbp4gem6zftvk/use-of-liquidity-pools-on-dex-and-the-application-of-swiss-regulations-to-liquidity-tokens>
- White Hat Group, A Modified Version of a Common Multisig Had A Vulnerability – The WHG Took Action & Will Return the Funds, 19. Juli 2017, https://www.reddit.com/r/ethereum/comments/6obofq/a_modified_version_of_a_common_multisig_had_a/
- White Kyle, Do Lawmakers Use AML as an Excuse to Centralize Crypto and Blockchain?, 13. November 2019, <https://cointelegraph.com/news/do-lawmakers-use-aml-as-an-excuse-to-centralize-crypto-and-blockchain>
- Whitehouse-Levine Miller, Twitter, 28. Oktober 2021, <https://twitter.com/millercwl/status/1453712314939674629>
- whiterabbit, Black Thursday for MakerDAO: \$8.32 million was liquidated for 0 DAI, 14. März 2020, https://medium.com/@whiterabbit_hq/black-thursday-for-makerdao-8-32-million-was-liquidated-for-0-dai-36b83cac56b6
- Whitworth Brian, Social-Technical Systems, in: Ghaoui Claude (Hrsg.), Encyclopedia of Human Computer Interaction, Hershey/London 2006, 533–541
- Wiatrowski Aleksander, Blockchain Technology – a Threat or a Solution for Data Protection?, Jusletter IT vom 22. Februar 2018
- Wicki Jodok, Market Making und Kurspflege kotierter eigener Aktien durch Effektenhändler, Diss. Zürich 2001
- Widmer Lühlinger Corinne/Oser David (Hrsg.), Basler Kommentar zum Obligationenrecht I. Art. 1-529 OR, 7. Aufl., Basel 2019 (BSK OR I-Autor, Art. N)
- Wieczner Jen, Gary Gensler on Crypto, SPACs, and Robinhood, 13. September 2021, <https://nymag.com/intelligencer/2021/09/gary-gensler-sec-chair-crypto-spacs-robinhood.html>
- Wielsch Dan, Die Ordnungen der Netzwerke. AGB – Code – Community Standards, in: Eifert Martin/Gostomzyk Tobias (Hrsg.), Netzwerkrecht. Die Zukunft des NetzDG und seine Folgen für die Netzwerkkommunikation, Baden-Baden 2018, 61–94
- Wiener Norbert, Cybernetics; or, Control and Communication in the Animal and the Machine, Cambridge/London 2019

- Wiener Norbert, The Human Use of Human Beings, Cybernetics and Society, London 1989
- Wierichs Günter/Smets Stefan, Gabler Kompakt-Lexikon Bank und Börse. 2.000 Begriffe nachschlagen, verstehen, anwenden, 5. Aufl., Wiesbaden 2010
- Wikipedia, Everyday: the First 5000 Days, undatiert, https://en.wikipedia.org/wiki/Everydays:_the_First_5000_Days
- Wilcox Zooko, Final text of ZIP 1014, 15. Februar 2020, <https://forum.zcashcommunity.com/t/final-text-of-zip-1014/36002>
- Wilcox Zooko, Funding, Incentives, and Governance, 1. Februar 2016, <https://electriccoin.co/blog/funding/>
- Wilcox Zooko, What is Zcash?, 6. Dezember 2016, <https://www.coincenter.org/what-is-zcash/>
- Wildi Marianne, Open Banking, in: Emmenegger Susan (Hrsg.), Zahlungsverkehr, SBT 2018, Basel 2018, 1–12
- Wilhelm Alex, Popular Bitcoin Mining Pool Promises To Restrict Its Compute Power To Prevent Feared '51%' Fiasco, 16. Juli 2014, <https://techcrunch.com/2014/07/16/popular-bitcoin-mining-pool-promises-to-restrict-its-compute-power-to-prevent-feared-51-fiasco/>
- Williamson Oliver E., Calculativeness, trust and economic organization, Journal of Law and Economics 1993, 453–486
- Williamson Oliver E., Credible Commitments: Using Hostages to Support Exchange, The American Economic Review 1983, 519–540
- Williamson Oliver E., Markets and Hierarchies. Analysis and Antitrust Implications, New York/London 1975
- Williamson Oliver E., Opportunism and its Critics, Managerial and Decision Economics 1993, 97–107
- Williamson Oliver E., The Economic Institutions of Capitalism. Firms, Markets, Relational Contracting, New York 1985
- Williamson Oliver E., The Economics of Organization: The Transaction Cost Approach, The American Journal of Sociology, 1981, 548–577
- Williamson Oliver E., The Mechanisms of Governance, New York/Oxford 1996
- Williamson Oliver E., The modern corporation: origins, evolution, attributes, Journal of Economic Literature 1981, 1537–1568
- Williamson Stephen D., Financial Intermediation, Business Failures, and Real Business Cycles, Journal of Political Economy 1987, 1196–1216

- Willke Helmut, Transparency after the Financial Crisis. Democracy, Transparency, and the Veil of Ignorance, in: Jansen Stephan A./Schröter Eckhard/Stehr Nico (Hrsg.), Transparenz. Multidisziplinäre Durchsichten durch Phänomene und Theorien des Undurchsichtigen, Wiesbaden 2010, 56–81
- Winer Eric, Gemini Is Now the World's First Licensed Zcash Exchange!, 14. Mai 2018, <https://www.gemini.com/blog/gemini-is-now-the-worlds-first-licensed-zcash-exchange>
- Winjum James O., Accounting and the Rise of Capitalism: An Accountant's View, Journal of Accounting Research 1971, 333–350
- Wintermute Molly, Hegic: On-chain Options Trading Protocol on Ethereum Powered by Hedge Contracts and Liquidity Pools, 20. Februar 2020, <https://ipfs.io/ipfs/QmWy8x6vEunH4gD2gWT4Bt4bBwWX2KAEUov46tCLvMRcME>
- van Wirdum Aaron, A Primer on Bitcoin Governance, or Why Developers Aren't in Charge of the Protocol, 7. September 2016, <https://bitcoinmagazine.com/culture/a-primer-on-bitcoin-governance-or-why-developers-aren-t-in-charge-of-the-protocol-1473270427>
- van Wirdum Aaron, Bitcoin as a Privacycoin: This Tech is Making Bitcoin More Private, 3. September 2018, <https://bitcoinmagazine.com/technical/bitcoin-privacycoin-tech-making-bitcoin-more-private>
- van Wirdum Aaron, The Long Road to SegWit: How Bitcoin's Biggest Protocol Upgrade Became Reality, 23. August 2017, <https://bitcoinmagazine.com/technical/the-long-road-to-segwit-how-bitcoins-biggest-protocol-upgrade-became-reality>
- Wittreck Fabian, Money in Medieval Philosophy, in: Fox David/Ernst Wolfgang (Hrsg.), Money in the Western Legal Tradition. Middle Ages to Bretton Woods, Oxford/New York 2016, 53–70
- Wolff Max, Introducing Marble. A Smart Contract Bank, 16. Juli 2018, <https://medium.com/marbleorg/introducing-marble-a-smart-contract-bank-c9c438a12890>
- Wolfson Rachel, DeFi and Eth2 are whole new convos for regulators, says SEC's Hester Peirce, 4. Dezember 2020, <https://cointelegraph.com/news/defi-and-eth-2-0-are-whole-new-convos-for-regulators-says-sec-s-hester-peirce>
- Wood Gavin, Allegality. Systems that can't care, 2014, <https://youtu.be/Zh9BYTSrGU?si=LmuRdkPqnoz14ewh>
- Wood Gavin, Ethereum: A Secure Decentralised Generalised Transaction Ledger. Yellow Paper, Berlin Version 888949c, 15. Oktober 2021, <https://ethereum.github.io/yellowpaper/paper.pdf>
- Wood Gavin, Less-techy: What is Web 3.0?, 23. April 2014, <http://gavwood.com/web3lt.html>

- World Economic Forum (WEF), Decentralized Finance (DeFi) Policy-Maker Toolkit. White Paper, Juni 2021
- World Economic Forum (WEF), Rethinking Financial Innovation. Reducing Negative Outcomes While Retaining The Benefits, 2012
- Wörsdörfer Manuel, Die normativen und wirtschaftsethischen Grundlagen des Ordoliberalismus, Diss. Frankfurt a.M. 2011
- Wright Aaron, The Growth & Regulatory Challenges of Decentralized Finance, in: Proceedings of the 2021 Spring Conference: The Impact of Blockchain on the Practice of Law, New York University Journal of Law & Business 2021, 686–693
- Wright Aaron/De Filippi Primavera, Decentralized Blockchain Technology and the Rise of Lex Cryptographia, 25. Juli 2017, <https://ssrn.com/abstract=2580664>
- Wu Huixin/Wang Feng, A Survey of Noninteractive Zero Knowledge Proof System and Its Applications, The Scientific World Journal 2014, 1–7
- Wu Jing/Savoie Michel, Peer-to-Peer Network Architecture, in: Bidgoli Hossein (Hrsg.), Handbook of Computer Networks. Distributed Networks, Network Planning, Control, Management, and New Trends and Applications, Bd. 3, Hoboken 2008, 131–151
- Wu Ke/Wheatley Spencer/Sornette Didier, Classification of cryptocurrency coins and tokens by the dynamics of their market capitalizations, Royal Society Open Science 2018, 1–20
- Wu Tim, Will Artificial Intelligence Eat the Law? The Rise of Hybrid Social-Ordering Systems, Columbia Law Review 2019, 2001–2028
- Wüst Karl/Gervais Arthur, Do you need a Blockchain?, in: 2018 Crypto Valley Conference on Blockchain Technology 2018, 45–54
- Wyss David/Zulauf Urs, Fiktiver Sitz oder faktische Zweigniederlassung? Der räumliche Geltungsbereich schweizerischer Finanzmarktaufsichtsgesetze und ihre Durchsetzung durch die Eidg. Bankenkommission gegenüber ausländischen Banken und Effektenhändlern, in: Spühler Karl (Hrsg.) Internationales Zivilprozess- und Verfahrensrecht, EIZ 37, Zürich 2001, 117–152
- Wyss Dominic, Gegenstand und Übertragung von DLT-Wertrechten. Gemäss den vorgesehenen Gesetzesanpassungen im Zusammenhang mit verteilten elektronischen Registern, Jusletter vom 1. Juli 2019
- Wyss Martin, Gold, Glanz und Schein in der Gesetzgebung, ZBl 2018, 3–25
- Xu Jiahua/Ackerer Damien/Dubovitskaya Alevtina, A Game-Theoretic Analysis of Cross-Chain Atomic Swaps with HTLCs, 20. April 2021, <https://arxiv.org/abs/2011.11325>
- Xu Jiahua/Vavryk Nazariy/Paruch Krzysztof/Cousaert Simon, SoK: Decentralized Exchanges (DEX) with Automated Market Maker (AMM) protocols, 14. März 2023, <https://arxiv.org/abs/2103.12732>

- Yaga Dylan/Mell Peter/Roby Nik/Scarfone Karen, Blockchain Technology Overview, NISTIR 8202, Oktober 2018
- Yakovenko Anatoly, Solana: A new architecture for a high performance blockchain v0.8.13, undatiert, <https://solana.com/solana-whitepaper.pdf>
- Yakubowski Max, Is Bitcoin Protected as Speech Under the 1st Amendment? Experts Answer, 26. August 2019, <https://cointelegraph.com/news/is-bitcoin-protected-as-speech-under-the-1st-amendment-experts-answer>
- Yamey Basil S., Scientific Bookkeeping and the Rise of Capitalism, The Economic History Review 1949, 99–113
- Yansen Guillermina, Blockchain and data market. The case of Wibson from a critical perspective, in: Ragnedda Massimo/Destefanis Giuseppe (Hrsg.), Blockchain and Web 3.0. Social, Economic, and Technological Challenges, London/New York 2020, 159–173
- Yavaş Abdullah, Search and Trading in Intermediated Markets, Journal of Economics & Management Strategy 1996, 195–216
- Yearn Finance, Disclaimer, undatiert, <https://beta.yearn.finance/disclaimer>
- Yermack David, Corporate Governance and Blockchains, Review of Finance 2017, 7–31
- Yeung Ching-man Au/Liccardi Ilaria/Lu Kanghao/Seneviratne Oshani/Berners-Lee Tim, Decentralization: The Future of Online Social Networking, W3C Workshop on the Future of Social Networking, 2008, <http://www.w3.org/2008/09/msnws/papers/decentralization.pdf>
- Yeung Karen, Algorithmic regulation: A critical interrogation, Regulation & Governance 2018, 505–523
- Yocom-Piatt Jake, A New Kind of DEX, 5. Juni 2018, <https://blog.decred.org/2018/06/05/A-New-Kind-of-DEX>
- Yocom-Piatt Jake, On-Chain Atomic Swaps, 20. September 2017, <https://blog.decred.org/2017/09/20/On-Chain-Atomic-Swaps/>
- Zachariadis Markos/Ozcan Pinar, The API Economy and Digital Transformation in Financial Services: The case of Open Banking, SWIFT Institute Working Paper Nr. 2016-001, 15. Juni 2017
- Zakhary Victor/Agrawal Divyakant/El Abbadi Amr, Atomic Commitment Across Blockchains, Proceedings of the VLDB Endowment 2020, 1319–1331
- Zamani Efraxia D./Giaglis George M., With a little help from the miners: distributed ledger technology and market disintermediation, Industrial Management & Data Systems 2018, 637–652
- Zamfir Vlad, Against on-chain governance, 1. Dezember 2017, https://medium.com/@Vlad_Zamfir/against-on-chain-governance-a4ceacd040ca

- Zamfir Vlad, Against Szabo's Law, For a New Crypto Legal System, 26. Januar 2019, <https://medium.com/cryptolawreview/against-szabos-law-for-a-new-crypto-legal-system-d00d0f3d3827>
- Zamfir Vlad, What is Cryptoeconomics?, 1. Februar 2015, <https://youtu.be/9lw3s7iGUXQ>
- Zcash, How It Works, undatiert, <https://z.cash/technology/>
- Zcash, Parameter Generation, undatiert <https://z.cash/technology/paramgen/>
- Zcash, What are zk-SNARKs?, undatiert, <https://z.cash/technology/zksnarks/>
- Zech Herbert, Entscheidungen digitaler autonomer Systeme: Empfehlen sich Regelungen zu Verantwortung und Haftung?, in: Verhandlungen des 73. Deutschen Juristentages, Bd. I Gutachten, München 2020, A 1-A 112
- Zech Herbert, Zivilrechtliche Haftung für den Einsatz von Robotern – Zuweisung von Automatisierungs- und Autonomierisiken, in: Gless Sabine/Seelmann Kurt (Hrsg.), Intelligente Agenten und das Recht, Baden-Baden 2016, 163–204
- Zellweger-Gutknecht Corinne, Developing the Right Regulatory Regime for Cryptocurrencies and Other Value Data, in: Fox David/Green Sarah (Hrsg.), Cryptocurrencies in Public and Private Law, Oxford 2019
- Zellweger-Gutknecht Corinne, Vernehmlassung «Änderung des Bankengesetzes» vom 25. Mai 2023, 20. Juni 2023, https://ius.unibas.ch/fileadmin/user_upload/ius/09_Upload_Personenprofile/01_Professuren/Zellweger-Gutknecht_Corinne/Vernehmlassung_Bankengesetz_Zellweger-Gutknecht_oU.pdf
- Zellweger-Gutknecht Corinne/Monnerat Lucien, § 1 Internationaler Kontext: Schweizerisches Registerwertrecht, in: Omlor Sebastian/Möslein Florian/Grundmann Stefan (Hrsg.), Elektronische Wertpapiere, Tübingen 2021
- Zellweger-Gutknecht Corinne/Seiler Benedikt, § 19 Switzerland, in: Maume Philipp/Maute Lena/Fromberger Mathias (Hrsg.), The Law of Crypto Assets, München/Baden-Baden/Oxford, 475–491
- Zellweger-Gutknecht Corinne/Weber Rolf H., Digital Money – Taxonomy and Regulatory Approaches, EuZ 06/2022, G1–G34
- Zellweger-Gutknecht Corinne/Weber Rolf H., Private Zahlungsmittel und Zahlungssysteme, Jusletter vom 11. Januar 2021
- Zetzsche Dirk A./Arner Douglas W./Buckley Ross P., Decentralized Finance, Journal of Financial Regulation 2020, 172–203
- Zetzsche Dirk A./Birdthistle William A./Arner Douglas W./Buckley Ross P., Digital Finance Platforms: Toward a New Regulatory Paradigm, University of Pennsylvania Journal of Business Law 2020, 273–339

- Zetzsche Dirk/Buckley Ross P./Arner Douglas W., The Distributed Liability of Distributed Ledgers: Legal Risks of Blockchain, University of Illinois Law Review 2018, 1361–1407
- Zetzsche Dirk/Buckley Ross P./Arner Douglas W./van Eck Maurits C., Remaining regulatory challenges in digital finance and crypto-assets after MiCA, Study requested by the European Parliament's Committee on Economic and Monetary Affairs (ECON), Mai 2023
- Zhang Jeffery Y., The Rise of Market Concentration and Rent Seeking in the Financial Sector, Harvard, John. M. Olin Center for Law, Economics, and Business, Fellows' Discussion Paper Series, Discussion Paper Nr. 72, 25. April 2017, http://www.law.harvard.edu/programs/olin_center/fellows_papers/pdf/Zhang_72.pdf
- Zhao Wolfie/Biggs John, Binance Customer Data Has Leaked: What We Know and What We Don't, 7. August 2019, <https://www.coindesk.com/binance-kyc-issue>
- Zhou Liyi/Qin Kaihua/Ferreira Torres Christof/Le Duc V/Gervais Arthur, High-Frequency Trading on Decentralized On-Chain Exchanges, in: 2021 IEEE Symposium on Security and Privacy (SP), San Francisco 2021, 428–445
- Zhou Liyi/Qin Kaihua/Gervais Arthur, A2MM: Mitigating Frontrunning, Transaction Reordering and Consensus Instability in Decentralized Exchanges, 18. Juni 2021, <https://arxiv.org/abs/2106.07371>
- Zimmermann Heinz, Effektenhandel im technologischen und regulatorischen Umbruch, in: Strebel-Aerni Brigitte (Hrsg.), Finanzmärkte im Banne von Big Data, Zürich/Genf/Basel 2012, 95–136
- Zimmermann Philipp R., PGP Source Code and Internals, Cambridge/London 1995
- Zinaman Evan, Where the Rubber Meets the Road. A MEV-Aware, Functionalist Review of OFAC Risk «on the Base Layer», 3. Mai 2023, <https://zzzin.substack.com/p/where-the-rubber-meets-the-road>
- Zinsmeister Noah, Overview of Uniswap, undatiert, <https://github.com/Uniswap/universe>
- Zittrain Jonathan L., The Future of the Internet – And How to Stop It, New Haven/London 2008
- zkSync, Decentralization, 24. September 2021, <https://zksync.io/faq/decentralization.html>
- Zmudzinski Adrian, Binance DEX Website Will Geoblock Users From 29 Countries, Including the US, 2. Juni 2019, <https://cointelegraph>
- Zobl Dieter, Der Vermögensverwaltungsauftrag der Banken unter besonderer Berücksichtigung von Interessenkonflikten, in: Forstmoser Peter/Tercier Pierre/Zäch Roger (Hrsg.), Innominatverträge, Festgabe zum 60. Geburtstag von Walter R. Schluep, Zürich 1988, 319–336

- Zobl Dieter, Internationale Übertragung und Verwahrung von Wertpapieren (aus schweizerischer Sicht), SZW 2001, 105–121
- Zobl Dieter/Hess Martin/Schott Ansgar (Hrsg.), Kommentar zum Bucheffektengesetz (BEG) sowie zum HWPÜ und den relevanten Bestimmungen im OR und IPRG, Zürich/Basel/Genf 2013 (Autor, in: Kommentar BEG, Art. N)
- Zobl Dieter/Kramer Stefan, Schweizerisches Kapitalmarktrecht, Zürich 2004
- Zobl Dieter/Lambert Claude, Zur Entmaterialisierung der Wertpapiere, SZW 1991, 117–139
- Zobl Dieter/Schwob Renate/Weber Rolf H./Winzeler Christoph/Kaufmann Christine/Kramer Stefan (Hrsg.), Kommentar zum Bundesgesetz über die Banken und Sparkassen, Zürich/Basel/Genf 2015 (Autor, in: Zobl et al., Kommentar BankG, Art. N)
- Zobl Martin/Lysakowski Michael, E-Persönlichkeit für Algorithmen?, digma 2019, 42–47
- Zogg Samuel, Bitcoin als Rechtsobjekt – eine zivilrechtliche Einordnung, recht 2019, 95–120
- Zogg Samuel, Das Aussonderungsrecht nach Art. 401 OR – eine Neuordnung, AJP 2020, 979–1007
- Zogg Samuel, Zwangsvollstreckungsrechtliche Behandlung von Kryptowährungen, recht 1/2020, 1–23
- Zollinger Dave, Die Geldabflussvorschriften der GwV-FINMA und andere Sonderbarkeiten, ContraLegem 2018, 116–119
- Zoltu Micah, How to turn \$20M into \$340M in 15 seconds, 9. Dezember 2019, <https://medium.com/coinmonks/how-to-turn-20m-into-340m-in-15-seconds-48d161a42311>
- Zuberbühler Daniel, Finanzmarktregulierung und kein Ende?, in: Héritier Lachat Anne/Hirsch Laurent (Hrsg.), De Lege Ferenda. Réflexions sur le droit désirable en l'honneur du Professeur Alain Hirsch, Genf 2004, 281–295
- Zulauf Urs/Gava Roy, FINMA's Enforcement in Court, SZW 2019, 99–113
- Züst Anna, Zulassung von genomeditierten Nutzpflanzen in der Schweiz. Regulierungsoptionen unter Berücksichtigung der Zulassungssysteme in der Europäischen Union und den Vereinigten Staaten von Amerika, SRLR 17, Zürich/St. Gallen 2021
- Zysset Pascal/Nagel Thomas, Der räumliche Geltungsbereich des Geldwäschereigesetzes, GesKR 2018, 140–155

Materialienverzeichnis

- Article 29 Data Protection Working Party, Opinion 14/2011 on data protection issues related to the prevention of money laundering and terrorist financing, 13. Juni 2011
- Aufsichtskommission VSB, Praxis der Aufsichtskommission zur Sorgfaltspflicht der Banken 2005-2010
- BaFin, Merkblatt. Zweites Hinweisschreiben zu Prospekt- und Erlaubnispflichten im Zusammenhang mit der Ausgabe sogenannter Krypto-Token, 16. August 2019
- Bank for International Settlements (BIS), CBDC. Central bank digital currencies: foundational principles and core features, Report Nr. 1, 2020
- Bank for International Settlements (BIS), Delivery versus Payment in Securities Settlement Systems. Report prepared by the Committee on Payment and Settlement Systems of the central banks of the Group of Ten countries, Basel 1992
- Bank for International Settlements (BIS), Real-Time Gross Settlement Systems. Report prepared by the Committee on Payment and Settlement Systems of the central banks of the Group of Ten countries, März 2013
- Bank for International Settlements (BIS), Recent Innovations in International Banking, April 1986
- Bank for International Settlements (BIS), Settlement Risk in Foreign Exchange Transactions. Report prepared by the Committee on Payment and Settlement Systems of the central banks of the Group of Ten countries, März 1996
- Bank for International Settlements (BIS), The crypto ecosystem: key elements and risks, Report submitted to the G20 Finance Ministers and Central Bank Governors, Juli 2023
- Bank for International Settlements (BIS)/Basel Committee on Banking Supervision (BCBS), Report on open banking and application programming interfaces, November 2019
- Bank for International Settlements (BIS)/Basel Committee on Banking Supervision (BCBS), Management and Supervision of Cross-Border Electronic Banking Activities, Juli 2003
- Bank for International Settlements (BIS)/Basel Committee on Banking Supervision (BCBS), Prudential treatment of cryptoasset exposures, Dezember 2022
- Bank for International Settlements (BIS)/Basel Committee on Banking Supervision (BCBS), Cryptoasset standard amendments. Consultative Document, Dezember 2023
- Bank for International Settlements (BIS)/Committee on Payment and Settlement Systems (CPSS), Payment, clearing and settlement systems in the CPSS countries. Red Book. Switzerland, Bd. 1, September 2011, 387-428

- Bank for International Settlements (BIS)/Committee on Payment and Settlement Systems (CPSS), Cross-Border Securities Settlements, März 1995
- Bank for International Settlements (BIS)/Committee on Payments and Market Infrastructures (CPMI), Distributed ledger technology in payment, clearing and settlement. An analytical framework, Februar 2017
- Bank for International Settlements (BIS)/Committee on Payments and Market Infrastructures (CPMI)/Market Committee (MC), Central bank digital currencies, März 2018
- Bank for International Settlements (BIS)/Committee on Payments and Market Infrastructures (CPMI), Digital Currencies, November 2015
- Bank for International Settlements (BIS)/SIX Group AG (SIX)/Swiss National Bank (SNB), Project Helvetia. Settling tokenized assets in central bank money, Dezember 2020
- Bank for International Settlements-Committee on Payment and Settlement Systems (BIS-CPSS)/Technical Committee of the International Organization of Securities Commissions (IOSCO), Recommendations for securities settlement systems, November 2001
- Bank for International Settlements-Committee on Payment and Settlement Systems (BIS-CPSS)/Technical Committee of the International Organization of Securities Commissions (IOSCO), Recommendations for Central Counterparties, November 2004
- Bank for International Settlements-Committee on Payment and Settlement Systems (BIS-CPSS)/Technical Committee of the International Organization of Securities Commissions (IOSCO), Principles for financial market infrastructures, April 2012
- Basle Committee on Banking Supervision (BCBS)/Offshore Group of Banking Supervisors (OGBS), The Supervision of Cross-Border Banking, Oktober 1996
- Better Regulation Task Force (BRTF), Imaginative Thinking for Better Regulation, London 2003
- Botschaft des Bundesrates an die Bundesversammlung betreffend den Entwurf eines Bundesgesetzes über die Banken und Sparkassen vom 2. Februar 1934, BBl 1934 I 171-224
- Botschaft des Bundesrates an die Bundesversammlung über die Revision des Bankengesetzes vom 13. Mai 1970, BBl 1970 I 1144-1203
- Botschaft über die Änderung des Schweizerischen Strafgesetzbuches (Gesetzgebung über Geldwäscherei und mangelnde Sorgfalt bei Geldgeschäften) vom 12. Juni 1989, BBl 1989 II 1061-1100
- Botschaft über die Revision des Nationalbankengesetzes vom 26. Juni 2002, BBl 2002, 6097-6303
- Botschaft über eine neue Bundesverfassung vom 20. November 1996, BBl 1997 I 1-642

- Botschaft zu einem Bundesgesetz über die Börsen und den Effektenhandel (Börsengesetz, BEHG) vom 24. Februar 1993, BBl 1993 I 1369–1462
- Botschaft zum Bucheffektengesetz sowie zum Haager Wertpapierübereinkommen vom 15. November 2006, BBl 2006, 9315–9420
- Botschaft zum Bundesgesetz über die Eidgenössische Finanzmarktaufsicht (Finanzmarktaufsichtsgesetz; FINMAG) vom 1. Februar 2006, BBl 2006, 2829–2916
- Botschaft zum Bundesgesetz zur Anpassung des Bundesrechts an Entwicklungen der Technik verteilter elektronischer Register vom 27. November 2019, BBl 2020, 233–328
- Botschaft zum Bundesgesetz zur Bekämpfung der Geldwäscherei im Finanzsektor (Geldwäschereigesetz, GwG) vom 17. Juni 1996, BBl 1996 III 1101–1177
- Botschaft zum Finanzdienstleistungsgesetz (FIDLEG) und zum Finanzinstitutsgesetz (FINIG) vom 4. November 2015, BBl 2015 8901–9092
- Botschaft zum Finanzmarktinfrastrukturgesetz (FinfraG) vom 3. September 2014, BBl 2014, 7483–7646
- Botschaft zur Änderung des Bankengesetzes vom 6. September 2023, BBl 2023, 2165 (1–92)
- Botschaft zur Ausführungsgesetzgebung zur Neugestaltung des Finanzausgleichs und der Aufgabenteilung zwischen Bund und Kantonen (NFA), 7. September 2005, BBl 2005, 6029–6304
- Botschaft zur Neugestaltung des Finanzausgleichs und der Aufgaben zwischen Bund und Kantonen (NFA) vom 14. November 2001, BBl 2002, 2291–2559
- Botschaft zur Umsetzung der 2012 revidierten Empfehlungen der Groupe d'action financière (GAFI) vom 13. Dezember 2013, BBl 2014 605–704
- Botschaft zur Umsetzung der revidierten Empfehlungen der Groupe d'action financière (GAFI) vom 15. Juni 2007, 6269–6310
- Bundesamt für Kommunikation BAKOM, Netzneutralität. Bericht zur Arbeitsgruppe, 23. Oktober 2014
- Bundesrat, Bericht des Bundesrates zu Anpassungen des Bankengesetzes vom 15. Juni 2018. Evaluation gemäss Artikel 52a des Bundesgesetzes über die Banken und Sparkassen, 16. Dezember 2022
- Bundesrat, Bericht des Bundesrates zu virtuellen Währungen in Beantwortung der Postulate Schwaab (13.3687) und Weibel (13.4070), 25. Juni 2014
- Bundesrat, Bericht über die zentralen Rahmenbedingungen für die digitale Wirtschaft, 11. Januar 2017
- Bundesrat, Digital Finance: Handlungsfelder 2022+, Februar 2022
- Bundesrat, Digitales Zentralbankengeld. Bericht des Bundesrates in Erfüllung des Postulats 18.3159, Wermuth, vom 14.03.2018, 13. Dezember 2019

- Bundesrat, Einfluss der Schweizer Finanzmarktregulierung auf Investitionsmöglichkeiten von Schweizer KMU in Afrika. Bericht des Bundesrates in Erfüllung des Postulats 17.3842 (Chevalley) vom 28. September 2017, 2. September 2020
- Bundesrat, Einsatz innovativer Technologien im Bereich der Finanzmarktaufsicht und -regulierung (RegTech). Bericht des Bundesrates in Erfüllung des Postulats 16.3256 Landolt vom 18.03.2016
- Bundesrat, Finanzmarktpolitik für einen wettbewerbsfähigen Finanzplatz Schweiz. Bericht des Bundesrates, Oktober 2016
- Bundesrat, Kostenfolgen von FINMA-Rundschreiben. Bericht des Bundesrates in Erfüllung der Postulate 17.3566 Vogler vom 16.06.2017 und 17.3620 Germann vom 16.06.2017, 20. März 2020
- Bundesrat, MiFID-II und Zugang zum Finanzmarkt: Szenarien und Massnahmen zur Erleichterung grenzüberschreitender Finanzdienstleistungen für italienische und französische Privatkundschaft. Bericht des Bundesrates in Erfüllung des Postulates 17.3744, Merlini vom 27. September 2017, 27. Oktober 2021
- Bundesrat, Rechtliche Grundlagen für *Distributed Ledger*-Technologie und Blockchain in der Schweiz. Eine Auslegeordnung mit Fokus auf dem Finanzsektor. Bericht des Bundesrates, 7. Dezember 2018
- Bundesrat, Weltweit führend, verankert in der Schweiz: Politik für einen zukunftsfähigen Finanzplatz Schweiz, 4. Dezember 2020
- Commodity Futures Trading Commission (CFTC) v. HDR Global Trading Limited, 100x Holdings Limited, ABS Global Trading Limited, Shine Effort Inc Limited, HDR Global Services (Bermuda) Limited, Arthur Hayes, Ben Peter Delo, and Samuel Reed, Civil Action Nr. 20-cv-8132, 1. Oktober 2020
- Commodity Futures Trading Commission (CFTC), CFTC Charges BitMEX Owners with Illegally Operating a Cryptocurrency Derivatives Trading Platform and Anti-Money Laundering Violations, 1. Oktober 2020, <https://www.cftc.gov/PressRoom/Press-Releases/8270-20>
- Commodity Futures Trading Commission (CFTC), CFTC vs. ZeroEx, Inc., Order, Nr. 23-41, 7. September 2023
- Commodity Futures Trading Commission (CFTC), Order Instituting Proceedings Pursuant to Section 6(c) and (d) of the Commodity Exchange Act, Making Findings and Imposing Remedial Sanctions, in the Matter of Coinbase Inc., CFTC Docket Nr. 21-03, 19. März 2021
- Conference of State Bank Supervisors (CSBS), State Regulatory Requirements for Virtual Currency Activities. CSBS Model Regulatory Framework, 15. September 2015, <https://www.csbs.org/sites/default/files/2017-11/CSBS-Model-Regulatory-Framework%28September%2015%202015%29.pdf>

- Eidgenössische Bankenkommission (EBK), Änderung der EBK-Geldwäschereiverordnung, Bericht, Mai 2007
- Eidgenössische Bankenkommission (EBK), EBK-Geldwäschereibericht. Bericht der Eidgenössischen Bankenkommission zu ihrer Geldwäschereiverordnung vom 18. Dezember 2002, März 2003, in: Eidgenössische Bankenkommission (EBK), Sonderheft: Geldwäschereibekämpfung, Bulletin 44/2003, 95–161
- Eidgenössische Bankenkommission (EBK), Jahresbericht 1989
- Eidgenössische Bankenkommission (EBK), Jahresbericht 2003
- Eidgenössische Bankenkommission (EBK), Jahresbericht 2004
- Eidgenössische Finanzmarktaufsicht (FINMA), Ausführungsbestimmungen der FINMA zu FIDLEG und FINIG. Erläuterungen, 4. November 2020
- Eidgenössische Finanzmarktaufsicht (FINMA), Diem zieht Bewilligungsgesuch in der Schweiz zurück, Medienmitteilung vom 12. Mai 2021, <https://www.finma.ch/de/news/2021/05/20210512-mm-diem/>
- Eidgenössische Finanzmarktaufsicht (FINMA), Ergänzung der Wegleitung für Unterstellungsfragen betreffend Initial Coin Offerings (ICOs), 11. September 2019
- Eidgenössische Finanzmarktaufsicht (FINMA), Faktenblatt Crowdfunding, 1. Juli 2020
- Eidgenössische Finanzmarktaufsicht (FINMA), FINMA bewilligt erstmals Börse und Zentralverwahrer für Handel mit Token, 10. September 2021, <https://www.finma.ch/de/news/2021/09/20210910-mm-sdx/>
- Eidgenössische Finanzmarktaufsicht (FINMA), FINMA stellt illegale Tätigkeit der envion AG fest, Medienmitteilung vom 27. März 2019, <https://www.finma.ch/de/news/2019/03/20190327-mm-envion/>
- Eidgenössische Finanzmarktaufsicht (FINMA), FINMA zieht Coin-Anbieter aus dem Verkehr und warnt vor Scheinkryptowährungen, Medienmitteilung vom 19. September 2017, <https://www.finma.ch/de/news/2017/09/20170919-mm-coin-anbieter/>
- Eidgenössische Finanzmarktaufsicht (FINMA), FINMA-Aufsichtsmitteilung 02/2019. Zahlungsverkehr auf der Blockchain, 26. August 2019
- Eidgenössische Finanzmarktaufsicht (FINMA), FINMA-Aufsichtsmitteilung 08/2023. Staking, 20. Dezember 2023
- Eidgenössische Finanzmarktaufsicht (FINMA), FINMA-Aufsichtsmitteilung 04/2017. Aufsichtsrechtliche Behandlung von Initial Coin Offerings, 29. September 2017
- Eidgenössische Finanzmarktaufsicht (FINMA), FINMA-Mitteilung 52 (2013), Handel im eigenen Titel mit dem Zweck der Liquiditätsbereitstellung unter den neuen Bestimmungen zur Marktmanipulation, 18. November 2013

- Eidgenössische Finanzmarktaufsicht (FINMA), Geldwäschereiverordnung-FINMA (GwV-FINMA). Erläuterungsbericht zur Totalrevision der GwV-FINMA, 11. Februar 2015
- Eidgenössische Finanzmarktaufsicht (FINMA), Jahresbericht 2018
- Eidgenössische Finanzmarktaufsicht (FINMA), Jahresbericht 2019
- Eidgenössische Finanzmarktaufsicht (FINMA), Jahresbericht 2020
- Eidgenössische Finanzmarktaufsicht (FINMA), Jahresbericht 2021
- Eidgenössische Finanzmarktaufsicht (FINMA), Jahresbericht 2022
- Eidgenössische Finanzmarktaufsicht (FINMA), Leitlinien zur Finanzmarktregulierung, 5. Dezember 2019
- Eidgenössische Finanzmarktaufsicht (FINMA), Regulierung von Produktion und Vertrieb von Finanzprodukten an Privatkunden – Stand, Mängel und Handlungsoptionen («FINMA-Vertriebsbericht 2010»), Oktober 2010
- Eidgenössische Finanzmarktaufsicht (FINMA), Rundschreiben 2018/1 Organisierte Handelssysteme. Bericht über die Anhörung vom 28. September bis 9. November 2016 zum Entwurf des Rundschreibens «Organisierte Handelssysteme», 25. Januar 2017
- Eidgenössische Finanzmarktaufsicht (FINMA), Warnung vor möglicherweise unerlaubt tätigen Anbietern, undatiert, <https://www.finma.ch/de/finma-public/warnliste>
- Eidgenössische Finanzmarktaufsicht (FINMA), Wegleitung für Gesuche betreffend Bewilligung als DLT-Handelssystem nach Art. 73a ff. Finanzmarktinfrastrukturgesetz, 2. August 2021
- Eidgenössische Finanzmarktaufsicht (FINMA), Wegleitung für Unterstellungsfragen betreffend Initial Coin Offerings (ICOs), 16. Februar 2018
- Eidgenössische Finanzmarktaufsicht (FINMA), Wie sich Anleger gegen unerlaubt tätige Finanzmarktanbieter schützen können, 1. August 2018, <https://www.finma.ch/de/finma-public/warnliste/#:-:text=Praktische%20Tipps%20wie%20Sie%20sich%20vor%20illegalen%20Anbietern%20sch%C3%BCtzen>
- Eidgenössische Finanzmarktaufsicht (FINMA), Ziele, undatiert, <https://www.finma.ch/de/finma/ziele/>
- Eidgenössisches Finanzdepartement (EFD), Änderung der Bankenverordnung (Fintech), Erläuterungen vom 5. Juli 2017
- Eidgenössisches Finanzdepartement (EFD), Änderung des Bankengesetzes und der Bankenverordnung (FinTech). Erläuternder Bericht zur Vernehmlassungsvorlage, 1. Februar 2017
- Eidgenössisches Finanzdepartement (EFD), Bericht des Eidgenössischen Finanzdepartements über die Vernehmlassungsergebnisse zum Finanzdienstleistungsgesetz (FIDLEG) und zum Finanzinstitutsgesetz (FINIG), 13. März 2015

- Eidgenössisches Finanzdepartement (EFD), Bundesgesetz zur Anpassung des Bundesrechts an Entwicklungen der Technik verteilter elektronischer Register. Erläuternder Bericht zur Vernehmlassungsvorlage, 22. März 2019
- Eidgenössisches Finanzdepartement (EFD), Erläuterungsbericht zur Geldwäschereiverordnung (GwV) – Umsetzung der GAFI-Empfehlungen, 11. November 2015
- Eidgenössisches Finanzdepartement (EFD), Finanzdienstleistungsverordnung (FIDLEV), Finanzinstitutsverordnung (FINIV) und Aufsichtsorganisationenverordnung (AOV). Erläuterungen, 6. November 2019
- Eidgenössisches Finanzdepartement (EFD), Finanzdienstleistungsverordnung (FIDLEV), Finanzinstitutsverordnung (FINIV) und Aufsichtsorganisationenverordnung (AOV). Erläuternder Bericht zur Eröffnung des Vernehmlassungsverfahrens, 24. Oktober 2018
- Eidgenössisches Finanzdepartement (EFD), Revision der Bankenverordnung (FinTech) «FinTech-Bewilligung». Erläuterungen, 30. November 2018
- Eidgenössisches Finanzdepartement (EFD), Vernehmlassung zum Bundesgesetz zur Anpassung des Bundesrechts an Entwicklungen der Technik verteilter elektronischer Register. Ergebnisbericht, 27. November 2019
- Eidgenössisches Finanzdepartement (EFD), Vernehmlassungsverfahren zur Finanzdienstleistungsverordnung (FIDLEV), Finanzinstitutsverordnung (FINIV) und Aufsichtsorganisationenverordnung (AOV). Ergebnisbericht, 6. November 2019
- Eidgenössisches Finanzdepartement (EFD), Vernehmlassungsverfahren zur Verordnung des Bundesrates zur Anpassung des Bundesrechts an Entwicklungen der Technik verteilter elektronischer Register. Ergebnisbericht, 18. Juni 2021
- Eidgenössisches Finanzdepartement (EFD), Verordnung des Bundesrates zur Anpassung des Bundesrechts an Entwicklungen der Technik verteilter elektronischer Register. Erläuternder Bericht zur Eröffnung des Vernehmlassungsverfahrens, 19. Oktober 2020
- Eidgenössisches Finanzdepartement (EFD), Verordnung des Bundesrates zur Anpassung des Bundesrechts an Entwicklungen der Technik verteilter elektronischer Register. Erläuterungen, 18. Juni 2021
- Eidgenössisches Finanzdepartement (EFD), Verordnung zum Finanzmarktaufsichtsgesetz. Erläuterungen, 13. Dezember 2019
- Eidgenössisches Finanzdepartement (EFD)/Eidgenössische Finanzverwaltung (EFV)/Kontrollstelle für die Bekämpfung der Geldwäscherei, Praxis der Kontrollstelle für die Bekämpfung der Geldwäscherei zu Art. 2 Abs. 3 GwG. Der Geltungsbereich des Geldwäschereigesetzes im Nichtbankensektor, 29. Oktober 2008 (UK KSt GwG, Rz.)

- Eidgenössisches Finanzdepartement (EFD)/Staatssekretariat für internationale Finanzfragen (SIF), Evaluation des Finanzmarktinfrastrukturgesetzes – FinfraG-Review, Bericht des EFD, 30. September 2022
- Eidgenössisches Finanzdepartement (EFD)/Staatssekretariat für international Finanzfragen (SIF), Wesentliche Änderungen an FIDLEV/FINIV/AOV, September 2019
- Eidgenössisches Justiz- und Polizeidepartement (EJPD)/Bundesamt für Polizei fedpol, National Risk Assessment (NRA), Risiko der Geldwäscherei und Terrorismusfinanzierung durch Krypto-Assets, Januar 2024
- European Central Bank (ECB), Report on a digital euro, Oktober 2020
- European Central Bank (ECB)/Bank of Japan (BOJ), Securities settlement systems: delivery-versus-payment in a distributed ledger environment. STELLA – a joint research project of the European Central Bank and the Bank of Japan, März 2018
- European Commission (EC), Communication from the Commission on an Action Plan for a comprehensive Union policy on preventing money laundering and terrorist financing, 13. Mai 2020, C 164/21–C164/33
- European Commission (EC), Communication from the Commission to the European Parliament, the Council, the European Central Bank, the European Economic and Social Committee and the Committee of the Regions. FinTech Action plan: For a more competitive and innovative European financial sector, 8. März 2018
- European Commission (EC), Decentralized Finance: information frictions and public policies. Approaching the regulation and supervision of decentralized finance, Written by Prof. Tarik Roukny, Juni 2022
- European Commission (EC), Proposal for a Regulation of the European Parliament and of the Council on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, COM(2021) 420 final, 20. Juli 2021, <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52021PC0420>
- European Data Protection Board (EDPB), Letter to the European Commission on the protection of personal data in the AML-CFT legislative proposals, 19. Mai 2021
- European Parliament (EP), Blockchain and the General Data Protection Regulation. Can distributed ledgers be squared with European data protection law?, Study. Panel for the Future of Science and Technology, Juli 2019
- European Parliament (EP), Crypto-assets. Key developments, regulatory concerns and responses, Study. Policy Department for Economic, Scientific and Quality of Life Policies, April 2020
- European Parliament (EP), Cryptocurrencies and blockchain. Legal context and implications for financial crime, money laundering and tax evasion, Study. Policy Department for Economic, Scientific and Quality of Life Policies, Juli 2018
- European Securities and Markets Authority (ESMA), Call for Evidence on Periodic Auctions, Final Report, 11. Juni 2019

- European Securities and Markets Authority (ESMA), Report: The Distributed Ledger Technology Applied to Securities Markets, 7. Februar 2017
- Financial Action Task Force (FATF), 12-Month Review of the Revised FATF Standards on Virtual Assets and Virtual Asset Service Providers, Juni 2020
- Financial Action Task Force (FATF), Draft updated Guidance for a risk-based approach to virtual assets and VASPs, März 2021
- Financial Action Task Force (FATF), FATF Report on Professional Money Laundering, Juli 2018
- Financial Action Task Force (FATF), FATF Report on Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing, September 2020
- Financial Action Task Force (FATF), FATF Report on Virtual Currencies. Key Definitions and Potential AML/CFT Risks, Juni 2014
- Financial Action Task Force (FATF), FATF Report to the G20 Finance Ministers and Central Bank Governors on So-called Stablecoins, Juni 2020
- Financial Action Task Force (FATF), Guidance for a Risk-Based Approach to Virtual Currencies, Juni 2015
- Financial Action Task Force (FATF), Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers, Juni 2019
- Financial Action Task Force (FATF), High-Level Synopsis of the Stocktake of the Unintended Consequences of the FATF Standards, 27. Oktober 2021
- Financial Action Task Force (FATF), Opportunities and Challenges of New Technologies for AML/CFT, Juli 2021
- Financial Action Task Force (FATF), Second 12-Month Review of the Revised FATF Standards on Virtual Assets and Virtual Asset Service Providers, Juli 2021
- Financial Action Task Force (FATF), The FATF Recommendations. International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation, Oktober 2020
- Financial Action Task Force (FATF), Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers, Oktober 2021
- Financial Industry Regulatory Authority (FINRA), Distributed Ledger Technology: Implications of Blockchain for the Securities Industry, Januar 2017
- Financial Industry Regulatory Authority (FINRA), Letter of Acceptance, Waiver, and Consent, Nr. 2020066971201, 30. Juni 2021
- Financial Stability Board (FSB), Crypto-asset markets. Potential channels for future financial stability implications, 10. Oktober 2018
- Financial Stability Board (FSB), Crypto-assets. Report to the G20 on work by the FSB and standard-setting bodies, 16. Juli 2018

- Financial Stability Board (FSB), Decentralised financial technologies. Report on financial stability, regulatory and governance implications, 6. Juni 2019
- Financial Stability Board (FSB), FinTech and market structure in financial services: Market developments and potential financial stability implications, 14. Februar 2019
- Financial Stability Board (FSB), Financial Stability Implications from FinTech. Supervisory and Regulatory Issues that Merit Authorities' Attention, 27. Juni 2017
- Financial Stability Board (FSB), High-level Recommendations for the Regulation. Supervision and Oversight of Crypto-Asset Activities and Markets, Final Report, 17. Juli 2023
- Financial Stability Board (FSB), Regulation, Supervision and Oversight of «Global Stablecoin» Arrangements. Final Report and High-Level Recommendations, 13. Oktober 2020
- Financial Stability Board (FSB), Report on Market Fragmentation, 4. Juni 2019
- Financial Stability Board (FSB), Shadow Banking: Strengthening Oversight and Regulation. Recommendations of the Financial Stability Board, 27. Oktober 2011
- Financial Stability Board (FSB), The Financial Stability Risks of Decentralised Finance, 16. Februar 2023
- Fürstentum Liechtenstein, Bericht und Antrag der Regierung an den Landtag des Fürstentums Liechtenstein betreffend die Schaffung eines Gesetzes über Token und VT-Dienstleister (Token- und VT-Dienstleister-Gesetz; TVTG) und die Abänderung weiterer Gesetze, Nr. 54/2019
- G7 Working Group on Stablecoins, Investigating the impact of global stablecoins, Oktober 2019
- Government Office for Science, Distributed Ledger Technology: beyond block chain. A Report by the UK Government Chief Scientific Adviser, London 2016
- Group of Thirty, Clearance and Settlement Systems in the World's Securities Markets, New York/London 1988
- Group of Thirty, Global Clearing and Settlement. A Plan of Action, Washington 2003
- Human Rights Committee, General comment Nr. 34. Article 19: Freedoms of opinion and expression, CCPR/C/GC/3, 12. September 2011
- Interdepartementale Koordinationsgruppe zur Bekämpfung der Geldwäscherei und der Terrorismusfinanzierung (KGGT), National Risk Assessment (NRA), Bericht über die nationale Beurteilung der Geldwäscherei- und Terrorismusfinanzierungsrisiken in der Schweiz. Bericht der interdepartementalen Koordinationsgruppe zur Bekämpfung der Geldwäscherei und der Terrorismusfinanzierung (KGGT), Oktober 2021
- Interdepartementale Koordinationsgruppe zur Bekämpfung der Geldwäscherei und der Terrorismusfinanzierung (KGGT), National Risk Assessment (NRA), Bericht über die Bargeldverwendung und deren Missbrauchsrisiken für die Geldwäscherei und Ter-

- rorismusfinanzierung in der Schweiz. Bericht der interdepartementalen Koordinationsgruppe zur Bekämpfung der Geldwäscherei und der Terrorismusfinanzierung (KGGT), Oktober 2018
- Interdepartementale Koordinationsgruppe zur Bekämpfung der Geldwäscherei und der Terrorismusfinanzierung (KGGT), National Risk Assessment (NRA), Risiko der Geldwäscherei und Terrorismusfinanzierung durch Krypto-Assets und Crowdfunding. Bericht der interdepartementalen Koordinationsgruppe zur Bekämpfung der Geldwäscherei und der Terrorismusfinanzierung (KGGT), Oktober 2018
- Interdepartementale Koordinationsgruppe zur Bekämpfung der Geldwäscherei und der Terrorismusfinanzierung (KGGT), Bericht über die nationale Beurteilung der Geldwäscherei- und Terrorismusfinanzierungsrisiken in der Schweiz. Bericht der interdepartementalen Koordinationsgruppe zur Bekämpfung der Geldwäscherei und der Terrorismusfinanzierung (KGGT), Juni 2015
- International Monetary Fund (IMF), Global Financial Stability Report 2021. Chapter 2: The Crypto Ecosystem and Financial Stability Challenges, 2021, 41–57
- International Organization of Securities Commissions (IOSCO), Discussion Paper on the Role of Investor Education in the Effective Regulation of CIS and CIS operators, März 2001
- International Organization of Securities Commissions (IOSCO), Final Report with Policy Recommendation for Decentralized Finance (DeFi), Dezember 2023
- International Organization of Securities Commissions (IOSCO), Investigating and Prosecuting Market Manipulation, Mai 2000
- International Organization of Securities Commissions (IOSCO), Investor Education on Crypto-Assets. Final Report, Dezember 2020
- International Organization of Securities Commission (IOSCO), IOSCO Decentralized Finance Report, Public Report, März 2022
- International Organization of Securities Commissions (IOSCO), IOSCO Research Report on Financial Technologies (Fintech), Februar 2017
- International Organization of Securities Commissions (IOSCO), Issues, Risks and Regulatory Considerations Relating to Crypto-Asset Trading Platforms. Final Report, Februar 2020
- International Organization of Securities Commissions (IOSCO), Methodology. For Assessing Implementation of the IOSCO Objectives and Principles of Securities Regulation, Mai 2017
- International Organization of Securities Commission (IOSCO), Policy Recommendations for Crypto and Digital Asset Markets, Final Report, 16. November 2023
- International Organization of Securities Commissions (IOSCO), Regulatory Issues Raised by Changes in Market Structure, Final Report, Dezember 2013

- International Organization of Securities Commissions (IOSCO), Transparency and Market Fragmentation, November 2001
- International Organization of Securities Commissions (IOSCO)/Organisation for Economic Co-operation and Development (OECD), Core Competencies Framework on Financial Literacy for Investors, 2019
- Internet Governance Forums (IGF), Internet Rights & Principles Coalition, the charter of human rights and principles for the internet, 7. Aufl., 2019
- Office of the Attorney General of the State of New York (OAG), Settlement Agreement in the Matter of iFinex Inc., BFXNA Inc., BFXWW Inc., Tether Holdings Limited, Tether Operations Limited, Tether Limited, and Tether International Limited, 18. Februar 2021
- Office of the Comptroller of the Currency (OCC), Authority of a National Bank to Provide Cryptocurrency Custody Services for Customers, Interpretive Letter Nr. 1170, 22. Juli 2020
- Office of the New York State Attorney General (OAG), Virtual Markets Integrity Initiative, Bericht vom 18. September 2018
- Ontario Securities Commission, Statement of Allegations, in the Matter of Coinsquare Ltd., Cole Diamond, Virgile Rostand and Felix Mazer, 16. Juli 2020
- Organisation for Economic Co-operation and Development (OECD), The Economic and Social Role of Internet Intermediaries, April 2010
- Organisation for Economic Co-operation and Development (OECD), The Tokenisation of Assets and Potential Implications for Financial Markets, OECD Blockchain Policy Series, 2020
- Organisation for Economic Co-operation and Development (OECD), Institutionalisation of crypto-assets and DeFi-TradFi interconnectedness, 2022
- Organisation for Economic Co-operation and Development (OECD), Why Decentralised Finance (DeFi) Matters and the Policy Implications, 2022
- Schweizerische Nationalbank (SNB), Merkblatt über den Zugang zum SIC-System und zu Girokonten, 2. September 2019
- Staatssekretariat für internationale Finanzfragen (SIF), Evaluation des Finanzmarktinfrastrukturgesetzes (FinfraG), 7. November 2019, <https://www.sif.admin.ch/sif/de/home/dokumentation/fachinformationen/archiv/evaluation-des-finanz-marktinfrastrukturgesetzes-finfrag-.html>
- UNIDROIT, UNIDROIT Legislative Guide on Intermediated Securities. Implementing the Principles and Rules of the Geneva Securities Convention, 2017
- U.S. Department of Justice (DOJ), Report of the Attorney General's Cyber Digital Task Force, Cryptocurrency, Enforcement Framework, Oktober 2020

- U.S. Department of Justice (DOJ), U.S. Attorney's Office, Southern District of New York, Founders And Executives Of Off-Shore Cryptocurrency Derivatives Exchange Charged With Violation Of The Bank Secrecy Act, 1. Oktober 2020, <https://www.justice.gov/usao-sdny/pr/founders-and-executives-shore-cryptocurrency-derivatives-exchange-charged-violation>
- U.S. Department of the Treasury, Illicit Finance Risk Assessment of Decentralized Finance, April 2023
- U.S. Department of the Treasury, Treasury Sanctions Mixer Used by the DPRK to Launder Stolen Virtual Currency, 29. November 2023, <https://home.treasury.gov/news/press-releases/jy1933>
- U.S. Department of the Treasury, U.S. Treasury Issues First-Ever Sanctions on a Virtual Currency Mixer, Targets DPRK Cyber Threats, 6. Mai 2022, <https://home.treasury.gov/news/press-releases/jy0768>
- U.S. Department of the Treasury, U.S. Treasury Sanctions Notorious Virtual Currency Mixer Tornado Cash, 8. August 2022, <https://home.treasury.gov/news/press-releases/jy0916>
- U.S. District Court for the District of Columbia, U.S. Securities and Exchange Commission (SEC) vs. Binance Holdings Limited et al., Civil Action, Nr. 1:23-cv-01599, 5. Juni 2023
- U.S. District Court for the Western District of Texas Austin Division, Van Loon et al. vs. Department of Treasury et al., Order, Nr. 1:23-cv-00312-RP, 17. August 2023
- U.S. District Court Northern District of California, Commodity Futures Trading Commission (CFTC) vs. Ooki DAO, Complaint for Injunctive and Other Equitable Relief and Civil Monetary Penalties, Nr. 3:22-cv-05416, 22. September 2022
- U.S. District Court Northern District of California, Commodity Futures Trading Commission (CFTC) vs. Ooki DAO, Order Granting Motion for Default Judgment, Nr. 3:22-cv-05416, 8. Juni 2023
- U.S. District Court Northern District of Florida Pensacola Division, Coin Center et al. vs. Janet Yellen et al., Nr. 3:22-cv-20375-TKW-ZCB, 30. Oktober 2023
- U.S. District Court Southern District of New York, Risley et al. vs. Universal Navigation et al., Opinion and Order, Nr. 1:22-cv-02780-KPF, 29. August 2023
- U.S. District Court Southern District of New York, U.S. Securities and Exchange Commission (SEC) vs. Samuel Bankman-Fried, Civil Action, Nr. 1:22-cv-10501, 13. Dezember 2022
- U.S. District Court Southern District of New York, U.S. Securities and Exchange Commission (SEC) vs. Coinbase, Inc. et al., Complaint, Nr. 1:23-cv-04738, 6. Juni 2023
- U.S. District Court Southern District of New York, United States of America (USA) vs. Roman Storm and Roman Semenov, Sealed Indictment, Nr. 1:23-cr-00430, 23. August 2023

- U.S. Financial Crimes Enforcement Network (FinCEN), Assessment of Civil Money Penalty in the Matter of Larry Dean Harmon d/b/a Helix, Nr. 2020-2, 19. Oktober 2020
- U.S. Financial Crimes Enforcement Network (FinCEN), FinCEN Guidance FIN-2019-G001, Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies, 9. Mai 2019
- U.S. Financial Crimes Enforcement Network (FinCEN), First Bitcoin «Mixer» Penalized by FinCEN for Violating Anti-Money Laundering Laws, 19. Oktober 2020, <https://www.fincen.gov/news/news-releases/first-bitcoin-mixer-penalized-fincen-violating-anti-money-laundering-laws>
- U.S. President's Working Group on Financial Markets (PWG)/Federal Deposit Insurance Corporation (FDIC)/Office of the Comptroller of the Currency (OCC), Report on Stablecoins, November 2021
- U.S. Securities and Exchange Commission (SEC), Amendments Regarding the Definition of «Exchange» and Alternative Trading Systems (ATs) That Trade U.S. Treasury and Agency Securities, National Market System (NMS) Stocks, and Other Securities, Nr. 34-94062, 26. Januar 2022, <https://www.sec.gov/rules/proposed/2022/34-94062.pdf>
- U.S. Securities and Exchange Commission (SEC), Cyber Enforcement Actions, undatiert, <https://www.sec.gov/spotlight/cybersecurity-enforcement-actions>
- U.S. Securities and Exchange Commission (SEC), Framework for «Investment Contract» Analysis of Digital Assets, 3. April 2019
- U.S. Securities and Exchange Commission (SEC), Further Definition of «As a Part of a Regular Business» in the Definition of Dealer and Government Securities Dealer in Connection with Certain Liquidity Providers, Nr. 34-99477, 6. Februar 2024, <https://www.sec.gov/files/rules/final/2024/34-99477.pdf>
- U.S. Securities and Exchange Commission (SEC), Order Instituting Cease-and-Desist Proceedings in the Matter of ShapeShift AG, Nr. 99676, 5. März 2024
- U.S. Securities and Exchange Commission (SEC), Order Instituting Cease-and-Desist Proceedings in the Matter of Zachary Coburn, Nr. 84553, 8. November 2018
- U.S. Securities and Exchange Commission (SEC), Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934: The DAO, Nr. 81207, 25. Juli 2017
- U.S. Securities and Exchange Commission (SEC), SEC Charges EtherDelta Founder With Operating an Unregistered Exchange, Press Release 2018-258, 8. November 2018, <https://www.sec.gov/news/press-release/2018-258>
- U.S. Securities and Exchange Commission (SEC), Staff Report on Equity and Options Market Structure Conditions in Early 2021, 14. Oktober 2021

- U.S. Securities and Exchange Commission (SEC), Statement on Digital Asset Securities Issuance and Trading, 16. November 2018, <https://www.sec.gov/news/public-statement/digital-asset-securities-issuance-and-trading>
- U.S. Securities and Exchange Commission (SEC), Statement on Potentially Unlawful Online Platforms for Trading Digital Assets, 7. März 2018, <https://www.sec.gov/news/public-statement/enforcement-tm-statement-potentially-unlawful-online-platforms-trading>
- U.S. Securities and Exchange Commission (SEC), Supplemental Information and Reopening of Comment Period for Amendments Regarding the Definition of «Exchange», Nr. 34-97309, 14. April 2023, <https://www.sec.gov/files/34-97309.pdf>
- U.S. Supreme Court, SEC vs. W.J. Howey Co. et al., 328 U.S. 293, 27. Mai 1946
- United Nations (UN), General Assembly, Human Rights Council, The promotion, protection and enjoyment of human rights on the Internet, A/HRC/20/L.13, 29. Juni 2012
- United Nations (UN), General Assembly, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, A/HRC/17/27, 16. Mai 2011
- United Nations (UN), General Assembly, Report of the Special Rapporteur on the rights to freedom of peaceful assembly and of association, Maina Kai, A/HRC/20/27, 21. Mai 2012
- Verordnung (EU) 2023/1114 des Europäischen Parlaments und des Rates vom 31. Mai 2023 über Märkte für Kryptowerte und zur Änderung der Verordnungen (EU) Nr. 1093/2010 und (EU) Nr. 1095/2010 sowie der Richtlinien 2013/36/EU und (EU) 2019/1937, ABl. L 150
- White House, FACT SHEET: White House Releases First-Ever Comprehensive Framework for Responsible Development of Digital Assets, 16. September 2022, <https://www.whitehouse.gov/briefing-room/statements-releases/2022/09/16/fact-sheet-white-house-releases-first-ever-comprehensive-framework-for-responsible-development-of-digital-assets/>
- World Bank, Global Financial Development Report 2019/2020: Bank Regulation and Supervision a Decade after the Global Financial Crisis, 2020

Abkürzungsverzeichnis

a.A.	andere Ansicht
a.E.	am Ende
a.M.	andere Meinung am Main
ABl.	Amtsblatt
ABS	Asset-Backed Security
Abs.	Absatz
ABV-FINMA	Verordnung der Eidgenössischen Finanzmarktaufsicht über die ausländischen Banken in der Schweiz vom 21. Oktober 1996, SR 952.111
abw.	abweichend
ACM	Association for Computing Machinery
AcP	Archiv für die civilistische Praxis
AFT	Advances in Financial Technologies
AG	Aktiengesellschaft
AGB	Allgemeine Geschäftsbedingungen
AI	Artificial Intelligence
AJP	Aktuelle Juristische Praxis
AML	Anti Money Laundering
AMM	Automated Market Making Automated Market Maker
AöR	Archiv des öffentlichen Rechts
AOV	Verordnung über die Aufsichtsorganisationen in der Finanzmarktaufsicht vom 6. November 2019, SR 956.134
API	Application Programming Interface
Art.	Artikel (im Singular oder Plural)
ASR	Abhandlungen zum Schweizerischen Recht
Aufl.	Auflage
BA	Blockchain Association
BAKOM	Bundesamt für Kommunikation

BankG	Bundesgesetz über die Banken und Sparkassen vom 8. November 1934, SR 952.0
BankV	Verordnung über die Banken und Sparkassen vom 30. April 2014, SR 952.02
BAS	Bitcoin Association Switzerland
BAT	Basic Attention Token
BBl	Bundesblatt der Schweizerischen Eidgenossenschaft
BCBS	Basel Committee on Banking Supervision
Bd.	Band
BEG	Bundesgesetz über Bucheffekten vom 3. Oktober 2008, SR 957.1
BEHG	Bundesgesetz über die Börsen und den Effektenhandel vom 24. März 1995, SR 954.1
BGE	Entscheidungen des Schweizerischen Bundesgerichts (Amtliche Sammlung)
BGer	Bundesgericht
BIP	Bitcoin Improvement Proposal
BIS	Bank for International Settlements
BJM	Basler juristische Mitteilungen
BK	Berner Kommentar
BKR	Zeitschrift für Bank- und Kapitalmarktrecht
BoJ	Bank of Japan
BR-KR	Bank- und Kapitalmarktrecht (iusNet)
BSK	Basler Kommentar
Bsp.	Beispiel
bspw.	beispielsweise
BStRA	Basler Studien zur Rechtswissenschaft Reihe A
BTC	bitcoin
BV	Bundesverfassung der Schweizerischen Eidgenossenschaft vom 18. April 1999, SR 101
BVGer	Bundesverwaltungsgericht
bzw.	beziehungsweise
CAP-Theorem	Consistency-Availability-Partitioning-Theorem
CBDC	Central Bank Digital Currency

CDO	Collateralized Debt Obligation
CDS	Credit Default Swap
CEDIDAC	Centre du droit de l'entreprise de l'Université de Lausanne
CFTC	Commodity Futures Trading Commission
CMTA	capital markets and technology association
CNIL	Commission Nationale de l'Informatique et des Libertés
coala	Coalition of Automated Legal Applications
COM	Commission (Europäische Union)
CPMI	Committee on Payments and Market Infrastructures
CPSS	Committee on Payment and Settlement Systems
CSBS	Conference of State Bank Supervisors
CVA	Crypto Valley Association
CVA CWG	Crypto Valley Association Cybersecurity Working Group
CVA RWG	Crypto Valley Association Regulatory Working Group
d.h.	das heisst
DAO	Decentralized Autonomous Organization
DApp	Decentralized Application
DCS-Theorem	Decentralization-Consensus-Scalability-Theorem
DeFi	Decentralized Finance
DEX	Decentralized Exchange
DINO	Decentralized In Name Only
Diss.	Dissertation
DLT	Distributed Ledger Technology
DNS	Domain Name System
DOJ	U.S. Department of Justice
DoS	Denial of Service
DPoS	Delegated Proof-of-Stake
DSGVO	Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG, ABl. L 119/1
DTCC	Depository Trust & Clearing Corporation
DuD	Datenschutz und Datensicherheit

E.	Erwägung(en)
EBK	Eidgenössische Bankenkommission
EBOR	European Business Organization Law Review
EC	European Commission
ECB	European Central Bank
EDPB	European Data Protection Board
EFD	Eidgenössisches Finanzdepartement
EFF	Electronic Frontier Foundation
EFV	Eidgenössische Finanzverwaltung
EIP	Ethereum Improvement Proposal
EJPD	Eidgenössisches Justiz- und Polizeidepartement
EMRK	Europäischen Menschenrechtskonvention
EOA	Externally Owned Account
EP	European Parliament
ERC	Ethereum Request for Comments
ESMA	European Securities and Markets Authority
et al.	et alii (und weitere)
ETC	Ethereum Classic
etc.	et cetera
ETF	Exchange Traded Fund
ETH	ether
ETP	Exchange Traded Product
EU	Europäische Union
EUBOF	EU Blockchain Observatory and Forum
EuZ	Zeitschrift für Europarecht
EVM	Ethereum Virtual Machine
E-Geld	Elektronisches Geld
E-Geld- Richtlinie	Richtlinie 2009/110/EG des Europäischen Parlaments und des Rates vom 16. September 2009 über die Aufnahme, Ausübung und Beaufsichtigung der Tätigkeit von E-Geld-Instituten, zur Änderung der Richtlinien 2005/60/EG und 2006/48/EG sowie zur Aufhebung der Richtlinie 2000/46/EG, ABl. L 267
f./ff.	und folgende Seite/Seiten

FAANG	Facebook, Amazon, Apple, Netflix, Google
FAQ	Frequently Asked Question(s)
FATF	Financial Action Task Force
FDIC	Federal Deposit Insurance Corporation
FIDLEG	Bundesgesetz über die Finanzdienstleistungen vom 15. Juni 2018, SR 950.1
FIDLEV	Verordnung über die Finanzdienstleistungen vom 6. November 2019, SR 950.11
FinCEN	Financial Crimes Enforcement Network
FinfraG	Bundesgesetz über die Finanzmarktinfrastrukturen und das Marktverhalten im Effekten- und Derivatehandel vom 19. Juni 2015, SR 958.1
FinfraV	Verordnung über die Finanzmarktinfrastrukturen und das Marktverhalten im Effekten- und Derivatehandel vom 25. November 2015, SR 958.11
FinfraV-FINMA	Verordnung der Eidgenössischen Finanzmarktaufsicht über die Finanzmarktinfrastrukturen und das Marktverhalten im Effekten- und Derivatehandel vom 3. Dezember 2015, SR 958.111
FINIG	Bundesgesetz über die Finanzinstitute vom 15. Juni 2018, SR 954.1
FINIV	Verordnung über die Finanzinstitute vom 6. November 2019, SR 954.11
FINMA	Eidgenössische Finanzmarktaufsicht
FINMAG	Bundesgesetz über die Eidgenössische Finanzmarktaufsicht vom 22. Juni 2007, SR 956.1
FINMAV	Verordnung zum Finanzmarktaufsichtsgesetz vom 13. Dezember 2019, SR 956.11
FINRA	Financial Industry Regulatory Authority
FN	Fussnote(n)
FS	Festschrift
FSB	Financial Stability Board
FSI	Financial Stability Institute (BIS)
G7	Group of Seven
GAFI	Groupe d'action financière

GDPR	Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, OJ L 119/1
GesKR	Zeitschrift für Gesellschafts- und Kapitalmarktrecht
gl.M.	gleiche Meinung
GmbH	Gesellschaft mit beschränkter Haftung
GUI	Graphical User Interface
GwG	Bundesgesetz über die Bekämpfung der Geldwäscherei und der Terrorismusfinanzierung vom 10. Oktober 1997, 955.0
GwV	Verordnung über die Bekämpfung der Geldwäscherei und der Terrorismusfinanzierung vom 11. November 2015, SR 955.01
GwV-FINMA	Verordnung der Eidgenössischen Finanzmarktaufsicht über die Bekämpfung von Geldwäscherei und Terrorismusfinanzierung im Finanzsektor vom 3. Juni 2015, SR 955.033.0
h.L.	herrschende Lehre
h.M.	herrschende Meinung
HAVE	Haftung und Versicherung
HGer	Handelsgericht
HP	Handelsplattform(en)
Hrsg.	Herausgeber
HTLC	Hash Time Locked Contracts
i.d.F.	in der Fassung
i.d.R.	in der Regel
i.S.	in Sachen im Sinne
i.S.d.	im Sinne des/der
i.V.m.	in Verbindung mit
ICO	Initial Coin Offering
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IGF	Internet Governance Forums
IMF	International Monetary Fund

Inc.	Incorporated Incorporation
insb.	insbesondere
InTeR	Zeitschrift zum Innovations- und Technikrecht
IOSCO	International Organization of Securities Commissions
IoT	Internet of Things
IRIS	Internationales Rechtsinformatik Symposium
IOU	I Owe You
IP	Internet Protocol
IPFS	InterPlanetary File System
ISO	International Organization for Standardization
ISP	Internet Service Provider
ITSL	Center for Information Technology, Society, and Law, Universität Zürich
JZ	JuristenZeitung
KAG	Bundesgesetz über die kollektiven Kapitalanlagen vom 23. Juni 2006, SR 951.31
KGGT	Interdepartementale Koordinationsgruppe zur Bekämpfung der Geldwäscherei und der Terrorismusfinanzierung
KKV	Verordnung über die kollektiven Kapitalanlagen vom 22. November 2006, SR 951.311
KMU	Kleine und mittlere Unternehmen
KYC	Know Your Customer
KYT	Know Your Transaction
LIPICs	Leibniz International Proceedings in Informatics
lit.	litera
LLC	Limited Liability Company
LMP	Law & Management Praxis
LNCS	Lecture Notes in Computer Science
m.a.W.	mit anderen Worten
m.E.	meines Erachtens
m.Verw.	mit Verweis
m.w.H.	mit weiteren Hinweisen

m.w.N.	mit weiteren Nachweisen
MC	Market Committee
MEV	Miner Extractable Value Maximum Extractable Value
MHS	Multilaterales Handelssystem
MiCAR	Verordnung (EU) 2023/1114 des Europäischen Parlaments und des Rates vom 31. Mai 2023 über Märkte für Kryptowerte und zur Änderung der Verordnungen (EU) Nr. 1093/2010 und (EU) Nr. 1095/2010 sowie der Richtlinien 2013/36/EU und (EU) 2019/1937, ABl. L 150
MiFID II	Richtlinie 2014/65/EU des Europäischen Parlaments und des Rates vom 15. Mai 2014 über Märkte für Finanzinstrumente sowie zur Änderung der Richtlinien 2002/92/EG und 2011/61/EU, ABl. L 173/349
MiFIR	Verordnung (EU) Nr. 600/2014 des Europäischen Parlaments und des Rates vom 15. Mai 2014 über Märkte für Finanzinstrumente und zur Änderung der Verordnung (EU) Nr. 648/2012, ABl. L 173/84
MMR	Multimedia und Recht
MSchG	Bundesgesetz über den Schutz von Marken und Herkunftsangaben vom 28. August 1992, SR 232.11
N	Note(n) Randnote(n)
NASDAQ	National Association of Securities Dealers Automated Quotations
NBG	Bundesgesetz über die Schweizerische Nationalbank vom 3. Oktober 2003, SR 951.11
NBV	Verordnung zum Bundesgesetz über die Schweizerische Nationalbank vom 18. März 2004, SR 951.131
NFA	Neugestaltung des Finanzausgleichs und der Aufgaben zwischen Bund und Kantonen
NFT	Non-Fungible Token
NIST	National Institute of Standards and Technology
NJW	Neue Juristische Wochenschrift
Nr.	Nummer
NRA	National Risk Assessment
NSA	National Security Agency
NZG	Neue Zeitschrift für Gesellschaftsrecht

NZZ	Neue Zürcher Zeitung
OAG	Office of the Attorney General of the State of New York
OCC	Office of the Comptroller of the Currency
OECD	Organisation for Economic Co-operation and Development
OFAC	Office of Foreign Assets Control
OFK	Orell Füssli Kommentar
OGBS	Offshore Group of Banking Supervisors
OHS	Organisiertes Handelssystem
OJ	Official Journal
OR	Bundesgesetz vom 30. März 1911 betreffend die Ergänzung des schweizerischen Zivilgesetzbuches (Fünfter Teil: Obligationenrecht), SR 220
OR AT	Obligationenrecht Allgemeiner Teil
OTC	Over The Counter
P2O	Peer-to-Operator
P2P	Peer-to-Peer
PBFT	Practical Byzantine Fault Tolerance
PGP	Pretty Good Privacy
PIRR	Perspectives on Innovation, Risk and Responsibility
PoS	Proof-of-Stake
PoW	Proof-of-Work
PWG	President's Working Group
resp.	respektive
RFQ	Request for Quote(s)
RD <i>i</i>	Recht Digital
RIW	Recht der internationalen Wirtschaft
RL	Richtlinie
RNT	Recht der neuen Technologien
RS	Rundschreiben
RWP	Rechtswissenschaft für die Praxis
Rz.	Randziffer(n)
s.	siehe
SA	Société Anonyme

SBF	Swiss Blockchain Federation
SBT	Schweizerische Bankrechtstagung
SBVg	Schweizerische Bankiervereinigung
SEC	U.S. Securities and Exchange Commission
SECOM	Settlement Communication System
SegWit	Segregated Witness
SFTA	Swiss Finance + Technology Association
SFTI	Swiss Fintech Innovations
SGK	St. Galler Kommentar
SGPHW	St. Galler Studien zum Privat-, Handels- und Wirtschaftsrecht
SGRW	St. Galler Schriften zur Rechtswissenschaft
SGSF	St. Galler Schriften zum Finanzmarktrecht
SHK	Stämpflis Handkommentar
SIC	SIX Interbank Clearing
SIF	Staatssekretariat für internationale Finanzfragen
SIX	Swiss Infrastructure and Exchange SIX Group AG
SJZ	Schweizerische Juristen-Zeitung
SK	Schulthess Kommentar
SMTTP	Simple Mail Transfer Protocol
SNB	Schweizerische Nationalbank Swiss National Bank
sog.	sogenannt(e)
SoK	Systematization of Knowledge
SPoC	Sinlge Point of Control
SPoF	Single Point of Failure
SR	Systematische Sammlung des Bundesrechts (Systematische Rechtssammlung)
SRIEL	Swiss Review of International and European Law
SRLR	Schriften zum Recht des ländlichen Raums
SRO	Selbstregulierungsorganisation
SSB	Schweizer Schriften zum Bankrecht
SSFM	Schweizer Schriften zum Finanzmarktrecht

SSHW	Schweizer Schriften zum Handels- und Wirtschaftsrecht
ST	Der Schweizer Treuhänder
StGB	Schweizerisches Strafgesetzbuch vom 21. Dezember 1937, SR 311.0
STLA	Swiss LegalTech Association
SWIFT	Society for Worldwide Interbank Financial Telecommunication
SZW	Schweizerische Zeitschrift für Wirtschaftsrecht
TCP	Transmission Control Protocol
TSP	Telecommunications Service Provider
TVTG	Gesetz über Token und VT-Dienstleister vom 3. Oktober 2019, LR 950.6
u.a.	unter anderem / anderen
UASF	User Activated Soft Fork
UK KSt GwG	Unterstellungskommentar der Kontrollstelle für die Bekämpfung der Geldwäscherei
ULC	Uniform Law Commission
UNIDROIT	International Institute for the Unification of Private Law
UN(O)	United Nations (Organization)
URG	Bundesgesetz über das Urheberrecht und verwandte Schutzrechte vom 9. Oktober 1992, SR 231.1
USDC	US-Dollar Coin
USDT	US-Dollar Tether
usw.	und so weiter
UTXO	Unspent Transaction Output
UWG	Bundesgesetz gegen den unlauteren Wettbewerb vom 19. Dezember 1986, SR 241
v.a.	vor allem
VA	Virtual Asset
VAG	Bundesgesetz betreffend die Aufsicht über Versicherungsunternehmen vom 17. Dezember 2004, SR 961.01
VASP	Virtual Asset Service Provider
VGer	Verwaltungsgericht
vgl.	vergleiche
VO	Verordnung

VQF	Verein zur Qualitätssicherung von Finanzdienstleistungen
VSb	Vereinbarung über die Standesregeln zur Sorgfaltspflicht der Banken
WBTC	Wrapped BTC
WEF	World Economic Forum
WETH	Wrapped ETH
WSJ	Wallstreet Journal
WWW	World Wide Web
WZG	Bundesgesetz über die Währung und die Zahlungsmittel vom 22. Dezember 1999, SR 941.10
XRP	Ripple
z.B.	zum Beispiel
ZBJV	Zeitschrift des Bernischen Juristenvereins
ZBl	Schweizerisches Zentralblatt für Staats- und Verwaltungsrecht
ZGB	Schweizerisches Zivilgesetzbuch vom 10. Dezember 1907, SR 210
ZGR	Zeitschrift für Unternehmens- und Gesellschaftsrecht
ZHR	Zeitschrift für das gesamte Handelsrecht und Wirtschaftsrecht
Ziff.	Ziffer(n)
ZIK	Publikationen aus dem Zentrum für Informations- und Kommunikationsrecht der Universität Zürich
zit.	zitiert
ZK	Zürcher Kommentar
zk-SNARK	Zero-Knowledge Succinct Non-Interactive Argument of Knowledge
ZK, zk	Zero Knowledge
ZKP	Zero-Knowledge Proof
ZLB	Zero Lower Bound
ZSR	Zeitschrift für Schweizerisches Recht
ZStP	Zürcher Studien zum Privatrecht
ZUM	Zeitschrift für Urheber- und Medienrecht

I. Einführung

Und jedem Anfang wohnt ein Zauber inne[.]

– Hermann Hesse¹

1. Einleitung

Technologie macht Märkte, Märkte benötigen Regeln. Diese Formel beschreibt in verkürzter Weise die in der Praxis häufig feststellbaren, faktischen Entstehungszusammenhänge einerseits zwischen Technologie und Markt und andererseits zwischen Markt und dessen Erfassung als Regelungsgegenstand.² Technologie wird demnach als ursprünglich für neue Waren und Dienstleistungen gesehen, für welche sich bei genügender Nachfrage ein eigenständiger Markt ausbilden kann.³ Wo ein solcher entsteht, taucht die Frage auf, nach welchem Regelwerk sich die Teilnehmer zu richten haben. Denn Regeln sind letztlich nichts anderes als Koordinationsmechanismen menschlichen Handelns. Die zur Anwendung gelangenden Regeln können dabei unterschiedlicher Natur sein: Soziale Normen stehen am Anfang der Marktentwicklung und begleiten sie fortwährend. Sie werden sodann typischerweise im Laufe der Zeit durch die Initiative der betroffenen Marktteilnehmer kodifiziert, wofür

¹ Hermann Hesse, *Glasperlenspiel*, 405.

² Freilich vereinfacht die Formel die nichtlinearen Zusammenhänge realer Erscheinungen; vgl. etwa zum Bsp. des aufkommenden Börsenhandels standardisierter Aktienoptionskontrakte in den USA in den 1970er Jahren Nobel/Zimmermann, in: Möslin, *Finanzinnovationen*, 49–50 (*«Die Entwicklung der Technologie, die Etablierung der völlig neuartigen Marktstruktur, die Erarbeitung des dafür erforderlichen regulatorischen Rahmens sowie des finanzmarkttheoretischen Knowhows seitens der partizipierenden Banken gingen Hand in Hand.»*); grundlegend für die Entwicklung der Wertpapiermärkte war jedoch die Erkenntnis, dass Technologie und Recht keine Gegenspieler sein müssen; vgl. Hess, *Penn State Law Review* 2024, 7–8.

³ In diesem Sinne ist das *Saysche Theorem* korrekt, wonach das Angebot von Waren und Dienstleistungen (hier: Technologie) die Nachfrage nach weiteren Waren und Dienstleistungen schafft. Bereits beim französischen Ökonomen Jean-Baptiste Say geht es letztlich um die Frage, welchen Einfluss der technische Fortschritt auf die Gesellschaft hat; vgl. hierzu Say, *Treatise on Political Economy*, insb. 134.

heute der Begriff der Selbstregulierung verwendet wird. Der Inhalt vieler dieser selbstaufgelegten Regeln endet schliesslich in den Erlassen hoheitlicher Regelsetzung.

Im modernen Gesellschaftskontext kommt dem Staat eine zentrale Rolle in der Festlegung des Regelwerks zu.⁴ Kaum ein Bereich menschlicher Interaktion ist derart staatlich reguliert wie das heutige Banken- und Finanzsystem sowie das heutige Geldwesen. Dies trifft auch auf die Märkte finanztechnologischer Entwicklungen zu. Die Finanzintermediation bildet dabei heute den massgeblichen Anknüpfungspunkt für die regulatorische Erfassung dieser Märkte.

Allerdings stellen moderne Technologien, wie namentlich die Blockchain, welche auch als Distributed Ledger Technologie bzw. DLT bezeichnet wird, den oben gemachten Entstehungszusammenhang infrage. Was, wenn Technologie zwar Märkte macht, die derart entstandenen Märkte jedoch in erster Linie den Regeln gehorchen, die sich aus der Technologie selbst ergeben? Dass Technologie selbst das Regelwerk darstellen kann, ist eine bereits länger vertretene These: Software kann etwa als eigenständige Regelordnung im Cyberspace betrachtet werden. Code tritt mit anderen Worten im Internet und World Wide Web (WWW) neben die staatliche Rechtsordnung, überkommene soziale Normen und Märkte bzw. deren Preissignale. LAWRENCE LESSIG bezeichnet sie als Regulierungsmodalitäten.⁵ Code bildet in diesem Fall lediglich eine dieser vier regulierenden Kräfte von Aktivitäten im Cyberspace.

Der vorliegenden Arbeit liegt die implizite Frage zugrunde, inwieweit die durch Blockchains ausgelösten dezentralen Prozesse und Strukturen – nachfolgend ist von *dezentralen Systemen* die Rede – zu einer Verschiebung in den Verhältnissen der erwähnten vier Regulierungsmodalitäten führen könnten. Gerade mit Blick auf das Finanzmarktrecht und besonders den Anleger- und Funktionsschutz scheint das Verständnis für die Effektivität staatlicher Regulierung zentral zu sein. Wenn Technologie an die Stelle der heute ubiquitären Finanzintermediation tritt und diese dadurch zum Gegenstand der Disintermediation macht, wirft dies letztlich die Frage auf, was dies für die Finanzmarktregulierung bedeutet.⁶

⁴ Siehe hierzu die Beiträge in Kessler/Kappeler, Null-Risiko-Gesellschaft, *passim*.

⁵ So bereits Lessig, Code, 87–89.

⁶ Davon zu unterscheiden ist die Frage, wie der Gesetzgeber auf die Innovation der Blockchain reagiert bzw. reagieren kann, vgl. hierzu Jutzi/Abbühl, Fintech und DLT, Rz. 12–15.

Dezentrale Systeme erinnern in ihrem Verhalten an ein geschlossenes Ökosystem. Anders als ihr biologisches Pendant basieren diese soziotechnischen Ökosysteme jedoch zu einem wesentlichen Grad auf Softwarecode. Die Notwendigkeit und Wirksamkeit systemexterner Regeln wird dadurch in gewissem Masse hinfällig. Dies scheint allerdings nur dann der Fall zu sein, wenn die Technologie zu einem Markt führt, der gemeinschaftlich verwaltet wird. Die Rede ist vorliegend von dezentralen Netzwerken und Applikationen, über welche keine Einzelperson oder Gruppe miteinander verbundener Personen die Kontrolle innehat. Solche Märkte sind öffentlich im doppelten Sinne: Sie sind einerseits frei zugänglich, indem jede Person unabhängig ihrer persönlichen Eigenschaften auf ihnen aktiv werden und zu ihrem Bestand beitragen kann; andererseits weisen sie im wirtschaftswissenschaftlichen Sinne Ähnlichkeiten mit Allgemeingütern auf, welche sich erfahrungsgemäss nur bei effizienter gemeinschaftlicher Verwaltung langfristig in einem stabilen Gleichgewicht halten können.

Diese anfänglichen Ausführungen mögen auf viele Leser idealisierend wirken. Und tatsächlich handelt es sich um eine Thematik, die bei realistischer Betrachtungsweise zu Recht viele Fragen aufwirft: Bitcoin⁷ ist heute die bedeutendste Kryptowährung, deren Protokoll aufgrund des technischen Designs aber nur bedingt als Zahlungsmittel im globalen Kontext dienen kann. Die Ethereum Blockchain hat Smart Contracts und Decentralized Finance (DeFi) popularisiert – ein System, das in regelmässigen Zeitabständen Opfer von millionenschweren Hackerangriffen ist. Blockchains/DLTs sind Teil eines enormen Hypes, was sich daran zeigt, dass sich diese kostspieligen «Datenbanken» in vielen Bereichen nicht durchsetzen konnten. Initial Coin Offerings bzw. ICOs haben in den Jahren 2017-18 Heerscharen kluger Werber und teils rücksichtsloser Betrüger angelockt, welche ihre Versprechungen nicht einhalten konnten oder wollten.

Gleichzeitig ist die innovative und transformative Natur dieses Ökosystems überwältigend: Mit Lightning existiert ein Computerprotokoll, das auf dem Bitcoin Netzwerk aufbaut, welches ein Transaktionsvolumen weit über denjenigen moderner Zahlungssysteme ermöglicht. Auch der traditionelle Finanzsektor interessiert sich inzwischen für den Einsatz von Smart Contracts für die unterschiedlichsten Anwendungen: Traditionelle Finanzintermediäre drängen

⁷ Üblicherweise wird «Bitcoin» grossgeschrieben, wenn das Protokoll, das dezentrale Netzwerk oder die Blockchain gemeint ist, wohingegen die Kleinschreibung «bitcoin» (oder das Kürzel BTC) für die Kryptowährung und deren Einheiten bevorzugt wird. Analoges gilt regelmässig auch für andere Kryptowährungen.

in die Welt von DeFi vor; Finanzmarktinfrastrukturen nutzen DLT im Handel sowie zur Abrechnung und Abwicklung von Effektengeschäften. Sodann stellen Blockchainsysteme, die gemeinschaftlich verwaltet und entwickelt werden, eine neuartige konzeptionelle Entwicklung dar; für solche Netzwerke muss gerade auf global verteilte, offene Datenbanken abgestellt werden, damit die dem System inhärenten kollektiven Handlungsprobleme überwunden werden können. Und schliesslich sind aus der «ICO-Gründerzeit» einige sehr zukunftssträchtige Projekte hervorgegangen, welche erste gut funktionierende Produkte entwickelt haben.

Gut Ding will also Weile haben? Oder doch eher «caveat emptor»? Zwischen Innovation und gesellschaftlichem Risiko besteht offenbar ein schwieriges Verhältnis. Der Frage, ob und inwieweit dem Recht eine Rolle in der wertenden Gewichtung dieses Verhältnisses zukommen soll und kann, wird in der vorliegenden Arbeit nachgegangen.

2. Untersuchungsgegenstand

Das traditionelle Finanzsystem setzt sich aus einer Vielzahl von Akteuren zusammen. In dessen Mittelpunkt stehen Finanzintermediäre und Finanzmarktinfrastrukturen bzw. – ökonomisch gesprochen – Hierarchien und Märkte. Dabei weisen die heutige Finanzintermediation und Marktorganisation *zentralisierte* Prozesse und Strukturen auf. Der wirtschaftliche Austausch von Finanzkontrakten findet mit anderen Worten lediglich ganz ausnahmsweise unmittelbar zwischen den endbegünstigten Parteien statt, sondern durchläuft üblicherweise ein komplexes Netz von Intermediären, bevor die Vermögenswerte den eigentlichen Berechtigten gutgeschrieben werden.

Hierarchien und Märkte als historisch⁸ gewachsene Institutionen gelten in aller Regel als volkswirtschaftlich effizient. Zudem bieten zentralisierte Prozesse und Strukturen leicht anknüpfbare Schnittstellen für die Rechtsordnung und damit für Eingriffe in die Wirtschaftsordnung. An diesem Knotenpunkt wirtschaftlicher Austauschbeziehungen erreicht die Regulierung mit andere Worten ihre grösste «Hebelwirkung»: Die allermeisten Finanzintermediäre und Finanzmarktinfrastrukturen haben angemessene Eigenmittel und je nach Regulierungsstatus auch angemessene Liquidität vorzuhalten, Risikomanagementsysteme und interne Kontrollen einzurichten und Regeln der Corporate Governance umzusetzen. Die Rechtsordnung soll unsere berechtigten Erwartungen in die Leistungen dieser Intermediäre schützen. Trotz der rechtlichen Vorgaben gilt der Finanzsektor, ähnlich wie dessen Regulierung, gemeinhin als intransparent und komplex⁹ und als fragil¹⁰. Die regelmässig undurchsichtige Interdependenz der verschiedenen Komponenten des Finanzsystems macht die Strukturierung und den Transfer wirtschaftlicher Risiken zwischen

⁸ Für eine ausführliche *rechthistorische* Darstellung der Finanzintermediation und Marktorganisation unter besonderer Berücksichtigung der Entwicklung des Anlegerschutzes siehe Sethe, Anlegerschutz, 208–415.

⁹ Siehe etwa Haldane/Madouros, in: Federal Reserve Bank of Kansas, *The Dog and the Frisbee*, 110, 149; Hettich, *Kooperative Risikovorsorge*, Rz. 384 m.w.N.; ferner Nobel, *Finanzmarktrecht*, § 1 N 35, der vom «regulatorischen Zeitalter» spricht.

¹⁰ So bspw. Nassim Taleb, *Black Swan*, 225–226; ferner Taleb, *Antifragile*, 5–6; ferner Nobel/Zimmermann, in: Möslin, *Finanzinnovationen*, 84–85 («[...] die systemischen Risiken ergeben sich aus der komplizierten Interaktion der verschiedenen Ebenen»).

den Marktteilnehmern sehr fehleranfällig.¹¹ Der Ruf nach einer grundlegenden Neuorientierung des Finanzsystems ist infolgedessen – nicht zuletzt wegen der Finanzkrise 2007-08 – stärker geworden.¹² Als wesentliche treibende Kraft hinter dieser Neuorientierung wird allgemein der technologische Fortschritt betrachtet.¹³

Historisch hat Innovation seit jeher die Prozesse und Strukturen der Gesellschafts- und Wirtschaftsordnung verändert, ja teils auf den Kopf gestellt. Von einem eigentlichen Zeitalter bzw. Paradigma der Informationstechnologie wird seit der Erfindung des modernen Computers Mitte des letzten Jahrhunderts und spätestens mit der Verbreitung des Internets gesprochen. Innovation ist nunmehr überwiegend digital oder wird zumindest durch digitale Verfahren ermöglicht. Dabei scheint Finanzinnovation sich besonders nachhaltig auf die Form und Struktur der zugrundeliegenden Märkte auszuwirken.¹⁴

Blockchains/DLTs sind Teil dieser Digitalisierungswelle, in deren Folge mit einer Umgestaltung der heutigen Finanzintermediation zu rechnen ist. Die grössten Veränderungen durch Blockchains werden gemeinhin für den Finanzmarktinfrastrukturbereich – d.h. im Handel, in der Abrechnung und Abwicklung sowie in der Verwahrung von Finanzinstrumenten und anderen Vermögenswerten – erwartet.¹⁵ Die heute bekanntesten Anwendungsbereiche der Blockchain-Technologie sind Kryptowährungen, allen voran Bitcoin und Ethereum, sowie Smart Contracts, die beispielsweise auf der Ethereum Blockchain zur automatisierten Ausführung von Rechtsgeschäften oder sonstigen Prozessen gelangen. Kryptowährungen und Smart Contracts stellen dabei nicht bloss

¹¹ Ähnlich in Bezug auf verbrieftes Kreditrisiken etwa Sethe/Lehmann, in: Tietje/Nowrot, § 15 Rz. 2, die von einer «Verkomplizierung» und der Zunahme von Risiken sprechen. Vgl. aber auch Stillhart, Theorie der Finanzintermediation, 2, der auf die Meinung hinweist, dass erst die ausgeprägte staatliche Regulierung die Bankenindustrie besonders macht.

¹² Siehe z.B. die Vorschläge betreffend höhere Eigenmittelanforderungen für Banken von Admati/Hellwig, The Bankers' New Clothes, 81–99; betreffend höhere Liquiditätsanforderungen King, End of Alchemy, 269–281; betreffend die Abschaffung der Buchgeldschöpfung durch Geschäftsbanken Reiser/Wyss, SZW 2018, *passim*; betreffend die Einführung von Konten für Sichtguthaben der Bürger bei der Zentralbank und die aktive Finanzierungsrolle letzter in der Volkswirtschaft Omarova, The People's Ledger, Vanderbilt Law Review 2021, 1238 («It is especially important to recognize that taking a more limited, piecemeal approach to reform is not necessarily the most prudent or practically feasible option.»).

¹³ Siehe z.B. McMillan, The End of Banking, 111–133; ferner Ali/Haldane/Nahai-Williamson, Towards a common financial language, insb. 18 («An information web, linked by a common language, makes that disintermediated model of finance a more realistic possibility.»).

¹⁴ Siehe hierzu ausführlich unten, [II.3.3b](#).

¹⁵ So etwa Bärtschi/Hirschi, SZW 2017, 790; ferner auch Bundesrat, DLT-Bericht 2018, 39 («mögliche Vorteile»).

Anwendungen der Blockchain dar, sondern bei den ihnen zugrundeliegenden Computerprotokollen handelt es sich überdies um die elementaren Bausteine dezentraler Systeme.

Damit sind wir beim *Untersuchungsgegenstand* dieser Arbeit angelangt: Dezentrale Systeme setzen sich nach vorliegendem Verständnis aus Netzwerken und Applikationen zusammen, die jeweils frei zugänglich (open bzw. permissionless) und deren Transaktionen grundsätzlich manipulationsresistent und unveränderlich sind (censorship-resistant und immutable), deren Funktionen im Wesentlichen auf quelloffenem Computercode basieren (trust-minimized) und die Funktionen des Finanzsystems, insb. der traditionellen Finanzintermediation, in dezentraler Weise reproduzieren. Das Zusammentreffen dieser Eigenschaften wird unter dem Begriff der Decentralized Finance bzw. DeFi zusammengefasst.¹⁶ Mit Kryptowährungen finden Prozesse, die bisher insb. von zentralisierten Zahlungssystemen sowie Geschäfts- und Zentralbanken übernommen worden sind, neuerdings innerhalb eines dezentralen Computernetzwerkes statt. Mit Smart Contracts können zudem weitere finanzintermediäre Tätigkeiten innerhalb eines dezentralen Netzwerks abgebildet werden, wie etwa die Errichtung und Herausgabe sowie die Verwahrung von Kryptowährungen einschliesslich Stablecoins und synthetischen Vermögenswerten (in Form von Tokens), die Errichtung und Abwicklung von Treuhandverhältnissen, das Pooling von Vermögenswerten mit dem Ziel der Vergabe von Krediten, die mit Token überbesichert werden, sowie der unmittelbare Austausch von Kryptowährungen und tokenisierten Vermögenswerten. Damit lässt sich grundsätzlich irgendein beliebiger immaterieller Wert, der mithilfe der Blockchain künstlich verknappt wird, je nach Anwendungsfall fortan ohne traditionelle zentrale Instanzen erschaffen, herausgeben, verwahren, ausleihen oder übertragen. Diese dezentralen Applikationen können sodann aufgrund der Quelloffenheit der verwendeten Computerprotokolle in beliebiger Weise miteinander kombiniert werden (composable bzw. interoperable). Es drängt sich nach dem Gesagten die Frage auf, ob und in welchem Masse dezentrale Systeme Funktionen des traditionellen Finanzsystems künftig ersetzen können. Die vorliegende Arbeit greift sich dabei als Untersuchungsgegenstand einen der neuen Anwendungsbereiche heraus: *dezentrale Handelsplattformen*.

Wie anfänglich angedeutet, finden sich Innovation und Risiko regelmässig in einem schwierigen Verhältnis wieder. Die Disintermediation, d.h. die Auflösung einer Industrie mit zentralisierten Akteuren zugunsten eines offenen Ökosystems mit dezentraler Governance, stellt das *innovative* Element de-

¹⁶ Zu den Konturen des Begriffs siehe unten, [II.4.2.](#)

zentraler Systeme dar.¹⁷ Dabei sind die Erwartungen an dezentrale Systeme durchaus hoch: Sie sollen nicht nur die Kosten ineffizienter Geschäftsprozesse senken, sondern darüber hinaus die an den Finanzmärkten vorherrschende Komplexität durch den Wegfall der heute zahlreichen involvierten Intermediäre reduzieren und schliesslich sogar für einen «demokratischeren» Zugang zu Finanzdienstleistungen sorgen.¹⁸ Die Neigung der Menschen, neue Produkte, Dienstleistungen und Verfahren zu erfinden, bringt allerdings nicht nur Chancen für die Gesellschaft mit sich, sondern ist untrennbar mit Risiken verbunden.¹⁹ Wirtschaftswissenschaftler sprechen von den negativen Externalitäten privaten Handelns, deren Kosten alle oder zumindest ein wesentlicher Teil der Gesellschaft zu tragen hat.²⁰

Innovation ist darum insoweit akzeptabel, als dass die damit verbundenen Konsequenzen aus der Perspektive der Gesellschaft noch sozialverträglich sind – und von dieser im demokratischen Prozess auch tatsächlich getragen werden. Der moderne Präventionsstaat scheint auf den ersten Blick besonders befähigt zu sein, die Externalitäten neuer Technologien durch Regulierung zu begrenzen.²¹ Die Finanzmarktregulierung bildet hier historisch betrachtet keine Ausnahme.²²

Dabei muss risikowissenschaftlich zwischen zwei grundsätzlich verschiedenen Risikotypen unterschieden werden: das individuelle Risiko des einzelnen Marktteilnehmers und das kollektive bzw. systemische Risiko der Gesamtheit der an einer Wirtschaftsordnung Beteiligten.²³ Letztere Fälle wirken sich auf die Gesellschaft als Ganzes aus, weshalb ihnen im Rahmen der staatlichen Risikovorsorge besonderes Augenmerk zukommt. Im Finanzmarktrecht werden nach einer ähnlichen Lesart gemeinhin Anleger- und Funktionsschutz unterschieden.²⁴ Dezentrale Handelsplattformen betreffen beide Risiko- bzw.

¹⁷ Siehe etwa Harvey/Ramachandran/Santoro, DeFi, 2; Nobel, SZW 2018, 596; Wagner/Weber, SZW 2017, 69–70; ferner Weber, Jusletter vom 18. Mai 2017, Rz. 5.

¹⁸ Siehe etwa Ito/Narula/Ali, The Blockchain Will Do to the Financial System What the Internet Did to Media, Harvard Business Review, *passim*; Harvey/Ramachandran/Santoro, DeFi, 2–5.

¹⁹ Siehe Bernstein, Risk, 11–12; ferner Beck, Risikogesellschaft, *passim*.

²⁰ Siehe statt vieler Samuelson/Nordhaus, Economics, 36.

²¹ Zum Begriff des Präventionsstaates siehe Hettich, Kooperative Risikovorsorge, Rz 96; ferner Hoffmann-Riem, Innovation und Recht, 18–19.

²² Siehe etwa Contratto, in: Weber et al., Technologie und Finanzmarktregulierung, 439, die das Bestehen eines co-evolutiven Verhältnisses zwischen Technologie und Finanzmarktregulierung feststellt.

²³ Grundlegend hierzu Seiler, Recht und technische Risiken, 41–43.

²⁴ Siehe hierzu unten, [VI.3.](#)

Schutzebenen: Die von ihnen potenziell ausgehende Autonomie²⁵ stellt im Extremfall ein Kontrollverlust für die Entwickler und Nutzer sowie – in systemischer Hinsicht – die Gesellschaft und den Staat dar. Im Rahmen der Risikoregulierung neuer Technologien ist letztlich aber auch den negativen Externalitäten staatlichen Handelns Rechnung zu tragen.²⁶

²⁵ Vorliegend ist allerdings nicht die Rede von *Autonomierisiken*, wie sie Teil der Diskussionen zur Künstlichen Intelligenz (KI) sind; vgl. hierzu Zech, in: Gless/Seelmann, Einsatz von Robotern, 175–176; ferner Teubner, AcP 2018, 164; sodann in informationstechnischer Hinsicht Buterin, DAOs and More, *passim*.

²⁶ Ausführlich Sunstein, Precautionary Principle, 29–33.

3. Forschungsfrage

Die Einordnung dezentraler Handelsplattformen in den bestehenden Rechtsrahmen bereitet in mehrerer Hinsicht Schwierigkeiten: (i) Dezentrale Handelsplattformen sind nutzungs- und teilnahmeoffen, d.h., es bestehen grundsätzlich keinerlei Einschränkungen in der Nutzung der Plattform oder der Teilnahme daran (dies im Gegensatz zu den heute intermediatisierten Infrastrukturen). (ii) Die Vermögenswerte werden sodann anders als bei Nutzung traditioneller Finanzmarktinfrastrukturen nicht mehr zwingend zentral verwahrt, sondern sie können grundsätzlich jederzeit beim jeweiligen Nutzer der Plattform verbleiben. (iii) Ferner verbinden dezentrale Handelsplattformen im Sinne eines *One-Stop-Shops*²⁷ nicht nur die Verwahrung und den Handel von Vermögenswerten, sondern auch deren Abrechnung und Abwicklung, soweit solche Prozesse überhaupt noch voneinander unterschieden werden können. (iv) Der verwendete Softwarecode ist schliesslich frei zugänglich und kann grundsätzlich von jedermann bearbeitet werden, was mit dem Begriff der Entwicklungs Offenheit umschrieben werden kann.

Im Ergebnis erschwert, ja verhindert die dezentrale Struktur die Möglichkeit, die Verantwortlichkeit für rechtswidrige Aktivitäten und Ergebnisse einer bestimmten Person zuzuordnen. Damit droht aber ein zentrales Anknüpfungselement der heutigen Finanzmarktregulierung wegzufallen. Der Finanzmarkt und somit das Finanzmarktrecht scheinen besonders von dieser Entwicklung betroffen zu sein. Das etablierte Rechtskonzept der *Finanzintermediation* scheint dort an seine Grenzen zu stossen, wo Intermediäre zunehmend durch Computercode abgelöst werden: Protokolle und Smart Contracts ersetzen Aktivitäten, die bislang ausschliesslich durch regulierte Finanzintermediäre erbracht worden sind.

Die *Forschungsfrage* dieser Arbeit kann nach den vorangegangenen Ausführungen wie folgt formuliert werden:

Stellen dezentrale Handelsplattformen unter Berücksichtigung der mit ihnen verbundenen Innovationschancen und der von ihnen ausgehenden Risiken einen Regulierungsanlass dar und, falls ja, mit welchen Regulierungsmodalitäten (bzw. -modi) kann darauf reagiert werden?

²⁷ So wörtlich Kramer/Oser/Meier, Jusletter vom 6. Mai 2019, Rz. 107 FN 157.

Im Rahmen der Beantwortung der Forschungsfrage sollen den konkreten Auswirkungen dezentraler Handelsplattformen die derzeitigen Zielsetzungen der schweizerischen Finanzmarktpolitik²⁸ sowie die Ziele der Finanzmarktaufsicht, namentlich der Anleger- und Funktionsschutz,²⁹ soweit sie mit Blick auf dezentrale Handelsplattformen von Bedeutung sind, sozusagen als «Benchmark» entgegengehalten werden. Es zeigt sich im Rahmen der vorliegenden Arbeit, dass auf Grundlage eines zu erarbeitenden *Rechtsprinzips der Dezentralität* ein Dezentralitätstest entwickelt werden sollte mit dem Ziel, der Beantwortung der Forschungsfrage schärfere Konturen zu verleihen.

²⁸ Siehe Bundesrat, Finanzmarktpolitik 2016, 30–31; ferner Bundesrat, Finanzmarktpolitik 2020, 4.

²⁹ Siehe FINMA, Leitlinien Finanzmarktregulierung, 3–4.

4. Aufbau der Arbeit

Die Arbeit ist in acht Kapitel unterteilt, wovon das erste die vorliegende Einführung darstellt.

Das *zweite Kapitel (II)* widmet sich den Grundlagen der Intermediation: Begonnen wird mit einem historischen Rückblick auf intermediäre Prozesse und Strukturen in Gesellschaft und Wirtschaft. Dabei wird ein Schwerpunkt auf die Finanzintermediation gelegt. Anschliessend erfolgt eine vertiefte Auseinandersetzung mit den wirtschaftswissenschaftlichen Begründungen für die Existenz der Finanzintermediation. Im Vordergrund dieses Kapitels stehen auch die unterschiedlichen Organisationsformen wirtschaftlicher Austauschprozesse, wobei typischerweise zwischen Markt, Hierarchie und Netzwerk unterschieden wird. In einem weiteren Abschnitt wird das Konzept der Disintermediation am Beispiel jüngerer Entwicklungen in der Finanzbranche und im Geldwesen betrachtet. Der Folgeabschnitt widmet sich ausführlich dem Phänomen der Decentralized Finance (DeFi). Im Zentrum der Ausführungen stehen die Vorgeschichte und die Vorläufer sowie der Begriff und die Funktionen von DeFi. Ein weiterer Abschnitt verortet DeFi in ökonomischer und soziotechnischer Hinsicht, was zur Formulierung eines Konzepts der netzwerkbasierten Intermediation sozialer und wirtschaftlicher Aktivitäten führt. Geschlossen wird das Kapitel mit Ausführungen zum Begriff der Reintermediation sowie zu potenziellen Reintermediationseffekten in dezentralen Systemen.

Das *dritte Kapitel (III)* verschafft dem Leser einen Überblick über die technischen Grundlagen dezentraler Systeme. An erster Stelle werden die wesentlichen Eigenschaften solcher Systeme herausgearbeitet, wozu die verteilte, gemeinschaftliche Verwaltung, offene, interoperable Protokolle und kryptografisch abgesicherte Vermögenswerte gehören. Sodann werden nacheinander die beiden Hauptkomponenten solcher Systeme dargestellt: dezentrale Netzwerke und dezentrale Applikationen. Dabei wird ein Schwerpunkt auf den technischen Aufbau und die technische Struktur, die beteiligten Personen sowie die groben Elemente der Governance der Systeme gelegt. Das Kapitel endet mit einem Abschnitt zu Skalierungslösungen dezentraler Netzwerke.

Im *vierten Kapitel (IV)* widmet sich die Arbeit ausführlich dezentralen Handelsplattformen als spezifische Ausprägung dezentraler Applikationen. Das Kernstück des Kapitels bildet der Abschnitt zu den unterschiedlichen Platt-

formkategorien, die in der Praxis feststellbar sind. Darauffolgend werden die Gemeinsamkeiten und Unterschiede dezentraler Handelsplattformen herausgearbeitet. Ein Grossteil des Kapitels bilden sodann auch Ausführungen zu den Chancen und Risiken dezentraler Handelsplattformen im Besonderen und dezentraler Systeme im Allgemeinen. Der letzte Abschnitt stellt den Versuch auf, dezentrale Handelsplattformen in technischer Hinsicht zu definieren.

Im *fünften Kapitel (V)* werden nach einigen wenigen Ausführungen zu vorliegend relevanten finanzmarktrechtlichen Konzepten dezentrale Handelsplattformen in Bezug auf die wichtigsten Rechtsgebiete des Finanzmarktrechts eingeordnet: In erster Linie handelt es sich um die Regeln zur Verhinderung von Geldwäscherei und Terrorismusfinanzierung. Darauf folgt ein Abschnitt zum Finanzmarktinfrastrukturrecht. Bank- und Finanzinstitutsrecht werden sodann jeweils in einem eigenen Abschnitt behandelt. Geschlossen wird mit der Einordnung dezentraler Handelsplattformen ins Finanzdienstleistungsrecht.

Das *sechste Kapitel (VI)* entwickelt vor dem Hintergrund der gewonnenen Erkenntnisse mögliche Ansätze für die Regulierung dezentraler Handelsplattformen. Die technologiebedingte Abkehr vom Finanzintermediationsmodell bringt erkennbare Herausforderungen für Aufsicht und Regulierung dezentraler Handelsplattformen mit sich. In Form eines Einschubes werden ausserdem grundrechtliche Überlegungen zur Unmöglichkeit eines allfälligen Technologieverbots angestellt. Auf einige Ausführungen zu den Implikationen für den Anleger- und Funktionsschutz folgen sodann solche zu möglichen Regulierungsansätzen. Angesichts der zu Beginn des Kapitels hervorgehobenen Herausforderungen bieten sich insb. marktorientierte Regulierungsansätze an.

Das *siebte Kapitel (VII)* widmet sich sodann der Dezentralität als neuem Rechtsprinzip. Es wird vorab untersucht, an welchen Orten der Wirtschafts- und Rechtsordnung Dezentralität in Form eines Ordnungsprinzips bereits Spuren hinterlassen haben könnte. Sodann werden im Folgeabschnitt die Konturen des Rechtsprinzips der Dezentralität für die Finanzmarktordnung herausgearbeitet. Als Orientierungspunkte eines allfälligen Dezentralitätstests sollen die Konzepte der Vertrauensminimierung und Entmachtung bzw. Kontrollverteilung dienen. Das Kapitel schliesst mit der Ausarbeitung eines funktionalen Dezentralitätstests, der belastbare Aussagen darüber erlauben soll, ob eine dezentrale Handelsplattform dem schweizerischen Finanzmarktrecht unterstellt ist oder nicht.

Am Ende der Kapitel II-VII werden die Erkenntnisse des jeweiligen Abschnitts kurz zusammengefasst.

Das letzte und *achte Kapitel* (VIII) fasst die Ergebnisse der Arbeit in Form von Schlussthesen zusammen.

II. Intermediation und Disintermediation

Banking is necessary, but bankers are not.

– Bill Gates³⁰

I don't believe we shall ever have a good money again before we take the thing out of the hands of government, that is, we can't take them violently out of the hands of government, all we can do is by some sly roundabout way introduce something they can't stop.

– Friedrich A. von Hayek³¹

1. Grundlagen der Intermediation und Dinsintermediation

1.1 Begriff der Intermediation

Der Begriff der *Intermediation* wird vorliegend im etymologisch ursprünglichen Sinne verwendet. Er setzt sich aus dem lateinischen «inter» und «medium» bzw. «medius» zusammen, was einerseits mit «zwischen» und andererseits mit «die Mitte» bzw. «in der Mitte befindlich» übersetzt wird.³² Der Vollständigkeit halber sei erwähnt, dass der vorliegend verwendete Intermediationsbegriff nichts mit dem rechtlichen Konzept der Finanzintermediation zu tun hat.

Intermediation beschreibt eine Kette bestehend aus Gliedern, die sich in sog. End- und Binde- bzw. Zwischenglieder einteilen lassen. Historisch betrachtet sind die jeweiligen Zwischenglieder in erster Linie personaler bzw. institutioneller Natur. Die Zwischenglieder bestehen mit anderen Worten aus einzelnen Personen oder aus irgendwie gearteten institutionalisierten Personenzu-

³⁰ Dieses Zitat wird in vorliegender oder ähnlicher Form dem Co-Gründer von Microsoft Bill Gates zugeschrieben, allerdings scheint keine eindeutige Quellenlage zu bestehen.

³¹ Cato Institute/Blanchard, Interview with F. A. Hayek.

³² Siehe Stowasser/Petschenig/Skutsch, Lateinwörterbuch, 272, 312.

sammenschließen, die bspw. als Familien, die Zivilgesellschaft, Gemeinwesen, Körperschaften, Anstalten, Rechtsgemeinschaften oder sonstigen Personenverbindungen in Erscheinung treten. Die Endglieder können ihrerseits sehr unterschiedlicher Natur sein. *Intermediation kann demnach als die Existenz von personalen oder institutionellen Prozessen und Strukturen definiert werden, die in der Regel im Hinblick auf die Erfüllung eines bestimmten Zwecks zwei oder mehrere Personen miteinander verbinden oder zwischen deren Interessen vermitteln.*

Um das hohe Abstraktionsniveau dieser Definition zu veranschaulichen, mag folgendes Beispiel dienen: Die Bank im Rechtskleid einer körperschaftlichen Aktiengesellschaft wird allgemein als das volkswirtschaftlich idealtypische institutionelle Zwischenglied aufgefasst, indem sie in Bezug auf den Kapitalfluss einer Volkswirtschaft Haushalte und Unternehmen als deren Endglieder miteinander verbindet.³³

1.2 Intermediation und Disintermediation als ubiquitäre Phänomene

Intermediation ist ein *ubiquitäres* Phänomen, das sich durch alle Perioden der Menschheitsgeschichte zieht. Dabei ist das Phänomen nicht auf die Wirtschaft oder das Finanzwesen beschränkt, sondern es ist auch im familiären, religiös-spirituellen oder staatlichen Bereich weit verbreitet. Einige Beispiele mögen diese Tatsache beleuchten:

So vertrat etwas der *pater familias* als Intermediär die weltlichen Anliegen der römischen Grossfamilie gegenüber der Gesellschaft.³⁴ Im religiös-spirituellen Bereich zu erwähnen sind bspw. die Orakel aus dem griechischen Delphi, die aufgrund ihrer Rolle als Informationszentrum zusammen mit der lokalen Priesterschaft einen erheblichen Einfluss auf das politische Geschehen der damaligen Zeit ausgeübt haben sollen.³⁵ Ferner ist auf die römische Praxis der Vogelschau (*auspicia*) hinzuweisen, welche dazu verwendet wurde, die kaiserliche Staatsräson mit dem Willen der Götter zu legitimieren.³⁶

³³ Siehe zur Finanzintermediation im Besonderen unten, [II.2.1](#).

³⁴ Siehe Honsell, Römisches Recht, 182.

³⁵ Siehe Scott, Delphi, 26–30, 96–97.

³⁶ Siehe Fögen, Wahrsager, 34.

Die heute wohl bedeutsamste Form der Intermediation ist diejenige des modernen demokratischen *Staatswesens*. Spätestens seit den grossen politischen Vertragstheorien der Frühneuzeit sind Funktion und Legitimation staatlicher Macht notorisch: Im entscheidenden Punkt unterscheiden sich die beiden Staatsphilosophen Thomas Hobbes und John Locke nicht. Sie beide bringen zum Ausdruck, wenn auch mit unterschiedlichen Begründungen und Schlussfolgerungen, dass dem Staat das Gewaltmonopol zukommen solle.³⁷ Zwar wird dieses vertraglich konstruierte Monopol heute kaum mehr als eine Form der Intermediation wahrgenommen, doch zumindest in philosophischer Hinsicht bildet die autonome «Selbstregierung» eines jeden Menschen den natürlichen Ausgangszustand der sozialen Ordnung.³⁸ Aus dem Gewaltmonopol ergeben sich eine Reihe von institutionellen Prozessen und Strukturen: Dazu gehört namentlich das objektive Recht, das zwischen den unterschiedlichen Interessen der Rechtsunterworfenen zu vermitteln versucht.³⁹ Deutlich erkennbar ist der Einsatz von politischen Intermediären sodann in der repräsentativen bzw. indirekten Demokratie. Das Volk übt die Herrschaft im Staat nur noch mittelbar über die Wahl ihrer Vertreter aus. In der halbdirekten Demokratie wird ebenfalls eine personale Ebene der Vertretung eingeschoben, welche neben dem Wahlzyklus durch Referenden und Volksinitiativen durchbrochen wird.⁴⁰ Idealerweise nehmen die gewählten Repräsentanten ausschliesslich die Interessen der Wählerschaft wahr und bringen dadurch deren Willen in der Gesetzgebung und Staatsführung zum Ausdruck. Zur demokratischen Willensbildung tragen sodann die politischen Parteien, Wirtschaftsverbände und Gewerkschaften sowie die Massenmedien bei, die darum als «intermediäre Gewalten» bezeichnet werden.⁴¹

³⁷ Siehe Hobbes, in: Gaskin, *Leviathan*, 119 («For before constitution of sovereign power [as hath already been shown] all men had right to all things; which necessarily causeth war: and therefore this propriety, being necessary to peace, and depending on sovereign power, is the act of that power, in order to the public peace.»); sodann Locke, in: Goldie, *Second Treatise of Government*, 29 («[...] the end of Law is not to abolish or restrain, but to preserve and enlarge Freedom: For in all the states of created Beings capable of Laws, where there is no Law, there is no Freedom. For Liberty is to be free from Restraint and Violence from others; which cannot be, where there is no Law [...] a Liberty to dispose, and order as he lists, his Person, Actions, Possessions, and his whole Property, within the Allowance of those Laws [...]»).

³⁸ Siehe Buchanan, in: *Liberty Fund, Paradox*, 117; ferner Barzel, *A Theory of the State*, 13–14.

³⁹ Vgl. auch Weber, *Sozialökonomik*, 29, 369.

⁴⁰ Siehe Haller/Kölz/Gächter, *Staatsrecht*, Rz. 265–266, 268, 281. Vgl. dagegen hinsichtlich des Konzepts der sog. *Liquid Democracy* als einen neuen Ansatz zur demokratischen Mitbestimmung Schiener, *Liquid Democracy*, Medium, *passim*.

⁴¹ So etwa Haller/Kölz/Gächter, *Staatsrecht*, Rz. 1221.

Intermediation	Zwischenglieder		Endglieder
	Personale	Institutionelle	
Soziale	<i>pater familias</i>	–	Mitglieder der römischen Grossfamilie und Gesellschaft
Religiös-spirituelle	Orakel von Delphi, Priester bei Vogelschau im antiken Rom	Katholische Kirche, Rechtsschulen im Islam	Gläubige und Gott-heit(en)
Politische	Gewählte Vertreter in einer repräsentativen Demokratie	Staat (insb. die Verwaltung), politische Parteien, Medien	Angehörige eines Volks
Wirtschaftliche	Kaufmann, Bankier	Unternehmen	Produzent und Konsument

Die Intermediation ist ubiquitär, weil sie Ausdruck des menschlichen Drangs zur Kooperation ist.⁴² Aus der Allgegenwärtigkeit der Intermediation darf jedoch nicht auf ihre Unumgänglichkeit geschlossen werden: Phasen der Intermediation werden historisch von Phasen der Disintermediation abgelöst. Ein bedeutsames Beispiel für eine Phase der Disintermediation ist die Erfindung des modernen *Buchdrucks* mit beweglichen Metalllettern durch Johannes Gutenberg Mitte des 15. Jahrhunderts. Diese Erfindung ermöglichte einerseits die Reformation⁴³, deren Lehren den Gläubigen *neu* erlaubte, ohne auf die Römische Kurie angewiesen zu sein, direkt mit Gott in Kontakt zu treten (*solae*).⁴⁴ Andererseits verstärkte der moderne Buchdruck die Renaissance und löste in der Folge die aufklärerischen Bewegungen des 18. Jahrhunderts aus.⁴⁵ Disintermediation stand somit am Anfang der politischen Neuorganisation des Westens in der Gestalt rechtsstaatlicher Demokratien.

⁴² Aristoteles spricht vom Menschen als ein von Natur aus politisches Wesen (sog. *zōon politikón*); siehe hierzu Aristoteles, in: Wolf, Politik, 46–47.

⁴³ Interessanterweise wurde die Phase seit der Erfindung von Bitcoin auch bereits mit der Periode der Reformation verglichen; vgl. Demeester, The Bitcoin Reformation, *passim*.

⁴⁴ Siehe Di Fabio, in: Di Fabio, Reformatorische Ethik, 72; ausführlich hierzu Wheeler, From Gutenberg to Google, 27–32; ferner unter Berücksichtigung von Argumenten der ökonomischen Theorie der Politik Ekelund/Hébert/Tollison, Journal of Political Economy 2002, 668 («The advent of Protestantism as a belief system meant that consumers seeking redemption could take a more direct, less expensive path to salvation. Protestantism made redemption cheaper, and it increased benefits to believers by reducing transaction costs.»).

⁴⁵ Siehe etwa Eisenstein, Printing Revolution, *passim*; ferner Dittmar/Seabold, Journal of Political Economy 2021/22, *passim*.

Die angesichts ihres umfassenden Disintermediationseffekts bedeutendste Technologie bleibt bis heute das *Geld*.⁴⁶ Zwar besteht wenig Einigkeit in der Lehre über die historischen Ursprünge von Geld – namentlich darüber, ob Geld ein Markt-⁴⁷ oder ein obrigkeitliches⁴⁸ Phänomen darstellt –,⁴⁹ doch kann ungeachtet dessen angenommen werden, dass das erstmalige Auftreten von Geld in einer Gesellschaft deren wirtschaftliche Funktionsweise nachhaltig verändert haben muss.⁵⁰ Ohne Geld in Form eines allgemein anerkannten Tausch- und Zahlungsmittels haben die Mitglieder einer Gesellschaft, um ihre in aller Regel unterschiedlichen Bedürfnisse vollständig zu befriedigen, eine Vielzahl aufwendiger Tauschgeschäfte mit verschiedenen Personen vorzunehmen. In vielen Fällen kommen Austauschgeschäfte mangels geografischer oder temporaler Übereinstimmung der Bedürfnisse gar nicht erst zustande. Mithilfe von Geld können die Teilnehmer einer Wirtschaft demgegenüber auf intermediäre Austauschhandlungen überwiegend verzichten und stattdessen ihre Waren direkt in Geld tauschen, um anschliessend ihre eigentlichen Bedürfnisse zu befriedigen.⁵¹ Geld ermöglicht mit anderen Worten den «vermit-

⁴⁶ Vgl. Omlor, ZHR 2019, 297, der zu Recht von der Geldgeschichte als «Technikgeschichte» spricht.

⁴⁷ Im Wesentlichen wird in den Wirtschaftswissenschaften kontrovers diskutiert, ob Geld anfänglich aus Waren, insb. Edelmetallen, entstanden und damit ein organisches oder spontanes Produkt des Marktes oder in Form von Kredit entstanden und damit ein geplantes Produkt des Staates sei; siehe hinsichtlich der ersten Auffassung, die als *Markttheorie* bezeichnet wird, Menger, *The Economic Journal* 1892, 250, 255; von Mises, *Theorie des Geldes*, 2–6, 44, 242–263; Rothbard, *Treatise on Economics*, 189–195.

⁴⁸ Siehe hinsichtlich dieser Auffassung, die auch als *Chartalismus* oder *Staatstheorie* bezeichnet wird, Knapp, *State Theory*, 1; Ingham, *Nature of Money*, 90–96; Lerner, *The American Economic Review* 1947, 313. Sodann wird auch im *Keynesianismus* typischerweise die zweite Ansicht vertreten; vgl. diesbezüglich insb. Keynes, *Treatise on Money*, 4–5. Die *Rechtswissenschaften* haben sich grossmehrheitlich dieser Theorie angeschlossen; vgl. insb. Proctor, *Legal Aspect of Money*, insb. 1.24, 1.27, 1.29.

⁴⁹ Siehe für eine überzeugende «Vereinigungstheorie», welche die Rolle des Staates im Markt berücksichtigt, Salter/Luther, *Advances in Austrian Economics* 2014, 168–174. Das «Problem» erkannt, aber doch nicht ganz erkannt, hat Minsky, *Unstable Economy*, 255, wenn er schreibt «Money not only arises in the process of financing, but an economy has a number of different types of money: everyone can create money; the problem is to get it accepted.» (Hervorhebungen des Verfassers). Ungeachtet dessen nehmen die *anthropologische* und *ethnologische* Forschung ganz eigene, teilweise vermittelnde Positionen ein; vgl. insb. Hart, *Man* 1986, 638–639; ferner Chapman, *L'Homme* 1980, *passim*; Humphrey, *Man* 1985, *passim*; Sillitoe, *Ethnology* 2006, *passim*.

⁵⁰ Vgl. zum Übergang von der Subsistenz- zur geldbasierten Marktwirtschaft Luhmann, *Wirtschaft der Gesellschaft*, 43, 97.

⁵¹ Vgl. Menger, *Volkswirtschaftslehre*, 250–255, der das *Problem der Doppelkoinzidenz der Wünsche* und die Entstehung von Warengeld daraus ausführlich beschreibt.

telten Tausch»⁵² und stellt darum ein Instrument der Disintermediation dar. Dies trifft v.a. auf im Markt entstandenes Warengeld zu, wohingegen Kreditgeld aufgrund des Vertrauens in den Herausgeber noch deutliche Züge der Intermediation aufweist.⁵³ Diese Differenzierung ist sodann überraschenderweise auch zentral für die Unterscheidung zwischen Kryptowährungen, wie Bitcoin, und Fiat-hinterlegten Stablecoins.⁵⁴

Die Entstehung der Geldwirtschaft bedeutete allerdings alles andere als das Ende aller übrigen wirtschaftlichen Intermediation, sondern sie war gerade der Auslöser einer völlig neuartigen Form der Intermediation, nämlich der Finanzintermediation (siehe hierzu sogleich). Der Rechtsordnung – hier in Form der Geld- und Währungsordnung sowie der Gewährleistung von Privatautonomie und Privateigentum – kommt sodann eine koordinierende Rolle zu, um die Disintermediationseffekte von Geld abzusichern.⁵⁵ Darüber hinaus weisen die Institutionen des Privatrechts auch eine *dezentral-diskursive* Struktur auf.⁵⁶ In diesem Sinne scheinen sich Intermediation und Disintermediation in komplexer Weise gegenseitig zu bedingen.

Die Wechselwirkungen zwischen Intermediation und Disintermediation sind in aller Regel das Ergebnis des ungeplanten Zusammenwirkens einer Vielzahl von Menschen. In FRIEDRICH A. VON HAYEKS Worten: «*Living as members of society and dependent for the satisfaction of most of our needs on various forms of co-operation with others, we depend for the effective pursuit of our aims clearly on the correspondence of the expectations concerning the actions of others on which our plans are based with what they will really do. This matching of the intentions and expectations that determine the actions of different individuals is the form in which order manifests itself in social life [...]*»⁵⁷ In historischer Hinsicht scheint ein relativ ausgeprägter Zusammenhang zwischen Intermediation und geplanter Organisation auf der einen Seite sowie Disintermediation und spontaner Ordnung auf der anderen Seite zu bestehen. Während intermediäre Prozesse und Strukturen von Natur aus eher Elemente zentraler Planung

⁵² von Mises, *Theorie des Geldes*, 2.

⁵³ Vgl. etwa Graeber, *Debt*, 73, 213.

⁵⁴ Siehe unten, [II.3.2e](#).

⁵⁵ Siehe Menger, *Volkswirtschaftslehre*, 259–260. Vgl. zum Wirtschaftsrecht als Koordinationsrecht Schluep, in: Jagmetti/Schluep, *Wirtschaftsrecht*, 80–81, 85; ähnlich Meier-Schatz, ZSR 1982 I, 295–296 m.w.H., welcher den dem Wirtschaftsrecht inhärenten Steuerungsprozess betont, der sich letztlich aus der Interdependenz zwischen Staat und Wirtschaft ergibt; sodann hinsichtlich der Funktion des Eigentums als Grundlage der Koordination von Entscheidungen Müller, ZSR 1981 II, 77.

⁵⁶ So Dürr, in: Walder/Jaag/Zobl, *Strukturwandel*, 52–56.

⁵⁷ von Hayek, *Rules and Order*, 36.

aufweisen, sind Disintermediationseffekte primär von polyzentrischer, verteilter Natur.⁵⁸ Auf das Verhältnis zwischen Disintermediation und Dezentralisierung wird zu einem späteren Zeitpunkt zurückzukommen sein.⁵⁹

1.3 Finanzintermediation im Besonderen

Die der Wirtschaftsordnung inhärente Intermediation findet ihre Wurzeln in der gesellschaftlichen Spezialisierung und Arbeitsteilung.⁶⁰ ADAM SMITH führte diese Entwicklungen auf die jedem Menschen inhärente «*propensity to truck, barter, and exchange one thing for another*» zurück.⁶¹

Die frühesten Formen der Finanzintermediation sind für das 3. Jahrtausend v. Chr. belegt.⁶² Daraufhin deuten schriftliche Aufzeichnungen von Zahlungsverpflichtungen auf Tontafeln und Papyri, die von der Priesterklasse in den Hochkulturen Mesopotamiens und Ägyptens verwaltet oder zumindest mit deren Hilfe erstellt wurden.⁶³ Im Griechenland und Rom der Antike bestand ein vergleichsweise ausgebautes Bankwesen, das erstmals auf geprägten Metallmünzen fusste und primär das Gewerbe und den internationalen Handel finanzierte.⁶⁴ Nach dem Zusammenbruch des Römischen Westreiches bildeten sich ab dem Frühmittelalter Intermediäre mit dem Ziel heran, um den seit der Antike erstmals wiederauflebenden Zahlungsströmen im grenzüberschreitenden Fernhandel gerecht zu werden.⁶⁵ In dieser Phase entstanden neue Zahlungs- und Schuldinstrumente, namentlich der Vorläufer des heutigen Wech-

⁵⁸ Vgl. zum Konzept der polyzentrischen spontanen Ordnung Polanyi, *Logic of Liberty*, 159–165, 170–179, 186; ferner zur Unterscheidung zwischen *geplanter* und *spontaner Ordnung* von Hayek, *Rules and Order*, 37, 46–47; eine sehr gute historische Übersicht zum Begriff der spontanen Ordnung findet sich bei Barry, *Literature of Liberty* 1982, *passim*.

⁵⁹ Siehe unten, [II.3.1](#).

⁶⁰ Siehe Smith, in: Campbell/Skinner, *Wealth of Nations*, 13–24; ferner North, *Institutions*, 118–130; Reisman, *Capitalism*, 464–466; sodann auch Omlor, ZHR 2019, 300–301, welcher Arbeitsteilung und Geldwirtschaft in einem engen gegenseitigen Entwicklungszusammenhang sieht.

⁶¹ Siehe Smith, in: Campbell/Skinner, *Wealth of Nations*, 25.

⁶² Siehe Sethe, *Anlegerschutz*, 208 m.w.N.

⁶³ Siehe Davies, *History of Money*, 48–55; Eagleton/Williams, *Money History*, 16–22. Graeber, *Debt*, 214, 217–218, und Harari, *Sapiens*, 181–182, vertreten darum die These, dass Geld aus *Schuld* entstanden sein müsse, was bei Wirtschaftshistorikern allerdings umstritten ist; siehe hierzu etwa Ferguson, *Ascent of Money*, 31.

⁶⁴ Siehe Sethe, *Anlegerschutz*, 208 m.w.N.; ferner Ward/Heichelheim/Yeo, *Roman People*, 133; ausführlich Eagleton/Williams, *Money History*, 23–61.

⁶⁵ Siehe Lopez, *Commercial Revolution*, 70–79; ferner Sethe, *Anlegerschutz*, 209–211.

sels, und in der Folge die ersten organisierten Kreditmärkte,⁶⁶ ohne dass sich daraus jedoch ein eigentlicher Wertpapiermarkt entwickelt hatte.⁶⁷

Zwischen dem 15. und 18. Jahrhundert traten demgegenüber erstmals Frühformen der modernen Aktiengesellschaft sowie Handelsplätze in Form von mehr oder weniger organisierten *Anleihen- und Aktienbörsen* in Erscheinung, um den wachsenden Kapitalbedarf von Politik und Wirtschaft in der Alten und Neuen Welt zu befriedigen.⁶⁸ Neue Handelsplätze wurden vor dem Hintergrund gegründet, den bereits existierenden Austausch zu formalisieren: Der künftige Handel sollte in örtlicher, zeitlicher und personeller Hinsicht konzentriert und einem einheitlichen Regelwerk unterstellt werden.⁶⁹ Parallel zur steigenden Spezialisierung der Intermediation an den Handelsplätzen verbesserten sich auch die Liquidität und Preistransparenz der zugrundeliegenden Märkte. Die Tätigkeit an einem organisierten Handelsplatz setzte in der Regel eine *Mitgliedschaft* voraus. In diesem Rahmen verpflichteten sich die Intermediäre, bei der Berufsausübung die jeweiligen Marktregeln einzuhalten.⁷⁰ Die meisten Handelsplätze basierten somit anfänglich auf einem mitgliedschaftlichen System, das die Aktivitäten seiner Mitglieder überwiegend selbst regulierte.⁷¹ Das mitgliedschaftliche System hat sich in der Schweiz trotz Demutualisierung der Börsen in gewandelter Form bis heute gehalten: So besteht das Aktionariat der SIX Group AG aus 120 national und international tätigen Finanzintermediären, die mehrheitlich auch als Händler an den von den Tochtergesellschaften der SIX Group AG betriebenen Börsen tätig sind.⁷²

Im 17. Jahrhundert wurden sodann die ersten *Zentralbanken* ins Leben gerufen, deren Hauptzweck gerade zu Beginn überwiegend fiskalpolitischer Natur

⁶⁶ Siehe Gilomen, *Wirtschaftsgeschichte*, 92, 115; *ausführlich* Geva, in: Fox/Ernst, *Order to Pay*, 410–411, 418–428.

⁶⁷ Siehe Michie, *Securities Regulation*, 17–21.

⁶⁸ *Ausführlich* Sethe, *Anlegerschutz*, 220–227, 237–248; Walker, in: Blair/Walker/Willey, *Financial Markets and Exchanges*, N 1.01–1.156, 1.15; Attack, in: Attack/Neal, *Financial innovations and crises*, 11–17 m.w.N.; in Bezug auf die Entwicklung nach der *Glorious Revolution* von 1688 in England North/Weingast, *The Journal of Economic History* 1989, 824–828; vgl. für die *Schweizer Börsengeschichte* Meier, in: Boemle et al., *Börse*, 206.

⁶⁹ Siehe Knorr Cetina/Preda, in: Knorr Cetina/Preda, *Sociology of Financial Markets*, 6–7; *ausführlich* Michie, *Securities Regulation*, 38–50.

⁷⁰ Vgl. für den Londoner Börsenplatz Michie, *London Stock Exchange*, insb. 20–23, 35–38.

⁷¹ Siehe Stringham, *Private Governance*, 61–78; ferner für das New York Stock & Exchange Board (NYSE) Hess, *Penn State Law Review* 2024, 6.

⁷² Siehe SIX Group Ltd, *Annual Report 2022*, März 2023, 33. Zum Begriff der *Demutualisierung* Nobel/Zimmermann, in: Möslin, *Finanzinnovationen*, 89.

war.⁷³ Zentralbanken übernahmen ferner die Funktion der Liquiditätsversorgung in Krisen, was sie seither zu sog. *Lenders of Last (and Only) Resort* (LOLR) gegenüber Geschäftsbanken macht.⁷⁴ Im internationalen Zahlungsverkehr nimmt die Bank for International Settlements (BIS) seit den 1930er Jahren eine Vermittlerrolle zwischen den nationalstaatlichen Zentralbanken im Hinblick auf die monetäre und finanzielle Stabilität der globalen Wirtschaft ein.⁷⁵ Des Weiteren sind Zentralbanken durch das Führen von Depositenkonten für Geschäftsbanken bis zum heutigen Tag um die finale Abrechnung und Abwicklung von Zahlungsverpflichtungen besorgt. Zentralbanken agieren darum als das *Clearinghouse* für die Teilnehmer einer Volkswirtschaft.⁷⁶

Der immense Kapitalbedarf der Industrialisierung prägte schliesslich das damalige Bankwesen und die damaligen Kapitalmärkte als Vorläufer des modernen Finanzsystems, das nach zwei Weltkriegen in den 1970er Jahren seinen Lauf nimmt.⁷⁷ Als einstweiliger historischer Höhepunkt der Finanzintermediation kann die Entwicklung von global bedeutenden Finanzinstituten betrachtet werden, die aufgrund ihrer Grösse und Vernetzung ein systemisches Risiko für die Wirtschaft und das Finanzsystem darstellen. Dieses Risiko realisierte sich u.a. eindrücklich in der Finanzkrise von 2007-08.⁷⁸ Über diesen systemrelevanten Marktteilnehmern stehen nur noch die Zentralbanken und Einlagenversicherungssysteme als die Intermediäre der Intermediäre. Sie greifen letztlich in der Funktion eines *Deus ex Machina* in das Finanzsystem ein mit dem Ziel, die «Alchemie» der Finanzintermediation aufrechtzuerhalten.⁷⁹

⁷³ Siehe Goodhart, in: Eatwell/Milgate/Newman, Central Banking, 88; hinsichtlich der Gründung der Bank of England Rothbard, *Mystery of Banking*, 177–183; in Bezug auf den Fall *John Laws* in Frankreich Velde, in: Attack/Neal, *John Law*, 101–103.

⁷⁴ Siehe Bagehot, *Lombard Street*, 92–101 («In ordinary times the Bank [of England] is only one of many lenders, whereas in a panic it is the sole lender, and we want, as far as we can, to bring back the unusual state of a time of panic to the common state of ordinary times.»); ferner Nobel, in: Walder/Jaag/Zobl, *Lender of Last Resort*, 508–509.

⁷⁵ Siehe Borio/Toniolo, in: Borio/Toniolo/Clement, *Central Bank Cooperation*, 18.

⁷⁶ Siehe etwa für die historische Entwicklung in England Matthews, *Clearing House*, 34–36; ferner Shafik, *Payment Systems*, 1; ausführlich Goodhart, *Central Banks*, 29–46. Vgl. zu dieser Funktion von Zentralbanken Haene/Sturm, *Finanzmarktinfrastuktur*, 4, 8.

⁷⁷ Siehe Schmoeckel/Maetschke, *Rechtsgeschichte*, Rz. 49–51; Walker, in: Blair/Walker/Willey, *Financial Markets and Exchanges*, N 1.17–1.18; Michie, in: Neal/Williamson, *Financial Capitalism*, 231–232, 243–250; ferner Rajan/Zingales, *Journal of Financial Economics* 2003, 6–7.

⁷⁸ Siehe etwa Nobel, SZW 2018, 592; ferner ausführlich King, *End of Alchemy*, 111–119. Zur Frage der Regulierung systemrelevanter Banken in verfassungsrechtlicher Hinsicht von der Crone/Beeler, ZSR 2011 I, *passim*.

⁷⁹ So King, *End of Alchemy*, 8; vgl. auch Diamond/Dybvig, *The Journal of Political Economy* 1983, 402, 404, 417.

Aufgrund der herausragenden Bedeutung der Finanzintermediation für die Wirtschaftsordnung bilden gesellschaftspolitische Friktionen seit jeher eine beinahe physikalische Konstante: Moralvorstellungen, was Finanzgeschäfte beinhalten dürfen und was nicht;⁸⁰ Finanz- und Wirtschaftskrisen;⁸¹ Zyklen von Regulierung und Deregulierung sowie Marktversagen und Staatsversagen;⁸² sowie die Tendenz von Regierungen, mithilfe des (Zentral-)Bankensystems fiskalpolitische Interessen zu verfolgen.⁸³ Diese Entwicklungen waren historisch und sind in aller Regel bis heute ständige Begleiterscheinungen der Finanzintermediation.

1.4 Intermediation als historische Gesetzmässigkeit

Die bisherigen Ausführungen haben gezeigt, dass Intermediation und Finanzintermediation historisch betrachtet immer an eine bestimmte Person oder eine bestimmte Institution (z.B. ein Unternehmen oder den Staat) gebunden sind. Sie sind damit in aller Regel mit einem bestimmten Ort und einer bestimmten Rechtsordnung verknüpft. Die unterschiedlich starken Schwankungen im Intermediationsgrad an den Kapitalmärkten der letzten rund tausend Jahre ändern nichts an der grundsätzlichen Richtigkeit dieser Feststellung.⁸⁴

Dies trifft historisch namentlich auch auf den Handel und besonders *Handelsplätze* zu: Um die gewünschten Güter auszutauschen, mussten sich die Marktteilnehmer in regelmässigen Zeitabständen an im Voraus bestimmten Orten treffen.⁸⁵ Es handelt sich dabei nach MAX WEBER um den «im Idealtypus konstruiert[en]» Fall sozialen Handelns.⁸⁶ Dies galt für die Amsterdamer Börse des 17. Jahrhunderts und gilt bis zum heutigen Tag für den Parketthandel an der

⁸⁰ In Bezug auf die herrschenden Moralvorstellungen im Mittelalter siehe Wittreck, in: Fox/Ernst, *Medieval Philosophy*, 54–59; ferner Ferguson, *Ascent of Money*, 34–38.

⁸¹ Siehe etwa von Mises, *Theorie des Geldes*, 374–375; von Hayek, *Prices and Production*, insb. 85–99; demgegenüber finden sich anderslautende Erklärungsansätze für Bankenkrisen in der *keynesianischen* Tradition bspw. in Keynes, in: Robinson/Moggridge, *General Theory*, 315–320; ferner Minsky, *Unstable Economy*, 279–282; Aliber/Kindleberger, *Financial Crises*, 38–52.

⁸² Siehe zu diesen Wechselphasen Senn, *Non-State Regulatory Regimes*, 11–17.

⁸³ Siehe etwa von Hayek, *Denationalisation of Money*, 33–36; Goodhart, *Central Banks*, 19–28; in empirischer Hinsicht vgl. Bernholz, *Monetary Regimes and Inflation*, 11–14, der von einem «inflationary bias of political systems» spricht.

⁸⁴ Vgl. betreffend die These, dass «decentralized private networks» historisch gesehen ein *wiederkehrendes* Phänomen darstellen, Donald, *The Journal of Corporation Law* 2018, 62.

⁸⁵ Siehe für eine historische Darstellung der co-evolutiven Entwicklung von Handel und Märkten Bernstein, *Exchange*, *passim*.

⁸⁶ Siehe Weber, *Sozialökonomik*, 4.

New York Stock Exchange. Seit dem Aufkommen des organisierten elektronischen Handels an der NASDAQ zu Beginn der 1970er Jahre hat die traditionelle Präsenzbörse jedoch nahezu vollständig an Bedeutung eingebüsst.⁸⁷ An die Orts- und Zeitgebundenheit des Handels ist durch die Computerisierung vermehrt dessen Systemgebundenheit getreten.⁸⁸ Trotz der Digitalisierung und Virtualisierung des Handels steht hinter traditionellen elektronischen Handelsplattformen weiterhin ein Betreiber, der in aller Regel über ein geografisch eindeutiges Domizil verfügt.⁸⁹ Bei diesen Umständen entscheidet letztlich die Rechtsordnung darüber, an welchem Ort sich eine Handelsplattform befindet. Zwar mag es in der Praxis der Finanzmarktaufsicht bei Personenmehrheiten und Gruppentatbeständen im Einzelnen durchaus zu Zuordnungsproblemen kommen, doch war es bisher nahezu ausgeschlossen, dass eine konkrete Finanzdienstleistung letztlich keiner bestimmten Person zugeschrieben werden konnte.⁹⁰

Es kann aufgrund der vorstehenden Ausführungen festgehalten werden, dass die personale und institutionelle Intermediation und somit auch die Finanzintermediation einer historischen Gesetzmässigkeit entsprechen.⁹¹ Dabei bilden mit Blick auf wirtschaftliche Sachverhalte typischerweise natürliche und juristische Personen den Nukleus der Intermediation.

1.5 Zentralisierung von Entscheidungsgewalt und Kontrolle

Personale und institutionelle Intermediation weisen eine folgenreiche Begleiterscheinung auf, die organisationstheoretisch mit *logischer Zentralisierung*

⁸⁷ Siehe etwa Gorham/Singh, *Electronic Exchanges*, 13–14.

⁸⁸ Vgl. hierzu Meier, in: Boemle et al., *Börse*, 205–206; Bühler, *OTC-Handel mit nichtkотиerten Aktien*, Rz. 293–295; zur *Evolution der Börsensysteme* ausführlich Kollmann, *Wertpapierhandelssysteme*, 9–33.

⁸⁹ Dies gilt selbst für zentralisierte Kryptobörsen, die in regulatorischer Hinsicht einen bewusst diffusen Ansatz verfolgen, indem sie über Rechtsstrukturen in verschiedenen Jurisdiktionen verfügen und dabei die Kunden und Aufsichtsbehörden über die konkrete Dienstleistungserbringerin im Unklaren lassen; vgl. hierzu del Castillo, *Binance*, Forbes, *passim*.

⁹⁰ Siehe hierzu unten, [V.1.5](#).

⁹¹ G.L.M. Gorton/Winton, in: Constantinides/Haris/Stulz, *Financial Intermediation*, 433 («*Financial intermediation is a pervasive feature of all of the world's economies.*»); Lin, *Wake Forest Law Review* 2015, 643 («*Intermediation is a fundamental fact of finance.*»).

umschrieben werden kann.⁹² Gegenstand dieser Zentralisierung bildet in erster Linie die Entscheidungsgewalt über die intermediären Aktivitäten. Diese wird bei einer Person oder einer Verbindung von Personen, die rechtlich, wirtschaftlich oder in irgendeiner anderen Form miteinander verbunden sind, konzentriert. In rechtlicher Hinsicht massgeblich ist der Umstand, dass eine konkrete Person oder Gruppe von Personen die fraglichen Aktivitäten kontrolliert oder zumindest kontrollieren könnte.⁹³

	Zentralisierung
Definition	Eine Person oder eine Gruppe miteinander verbundener Personen verfügt über die Entscheidungsgewalt und Kontrolle hinsichtlich einer Aktivität.

Demgegenüber stellen die Grundlagen der Erfindung von Bitcoin in den Jahren 2008-09 die traditionellen personalen bzw. institutionellen Elemente der Intermediation grundsätzlich infrage. Indem die Aktivitäten nicht mehr zwingend an eine bestimmte Person oder Institution anknüpfen, verlieren die räumliche und zeitliche Begrenzungen der Intermediation weiter an Bedeutung. An die Stelle der Zentralisierung von Entscheidungsgewalt und Kontrolle über eine intermediäre Aktivität tritt die *Verteilung von Entscheidungsgewalt und Kontrolle* innerhalb eines Netzwerks bestehend aus unzähligen Personen und Computern. Unbestrittenermassen besteht hier eine gewisse Nähe zur politischen Dezentralisierung,⁹⁴ welche in bedeutenden Punkten über die betriebswirtschaftliche hinausgeht.⁹⁵

In dezentralen Systemen besitzt keine der beteiligten Personen mehr die Fähigkeit, im Alleingang Entscheidungen für das Gesamtsystem zu treffen. Die Einseitigkeit der Kontrolle in der traditionellen Intermediation wird anders ausgedrückt durch einen multilateralen Mechanismus der Machtverteilung abgelöst. Obwohl zwar jede der involvierten Personen zwangsläufig über einen bestimmbareren physischen Standort verfügt, wäre eine solche Einzelbetrachtung mit Blick auf das Netzwerk als Ganzes wenig zielführend.

⁹² Vgl. Frese et al., Grundlagen der Organisation, 188-189; Jones, Organizational Theory, 125-126, 154-155; ferner Daft, Organization Theory, 17, 93.

⁹³ Dabei ist für die vorliegende Analyse nicht weiter notwendig, zwischen Entscheidungs- und Kontrollrechten zu unterscheiden, wie es etwa typisch für die Aktiengesellschaft ist; vgl. hierzu Ricketts, Business Enterprise, 261-262.

⁹⁴ Vgl. Shapiro, Control Revolution, 55, 57-59; ausführlich zur politischen Dezentralisierung Treisman, Political Decentralization, 21-27.

⁹⁵ Vgl. Picot et al., Die grenzenlose Unternehmung, 97.

	Dezentralisierung
Definition	Die Entscheidungsgewalt und Kontrolle hinsichtlich einer Aktivität werden innerhalb einer Gruppe von Personen (bspw. über ein Computernetzwerk) verteilt.

Im Ergebnis erscheint es als sachgerecht, Intermediation nicht mehr ausschliesslich personal bzw. institutionell zu verstehen. Vielmehr muss der Intermediationsbegriff, wie noch aufzuzeigen sein wird, um *netzwerkbasierte* Formen erweitert werden.⁹⁶

⁹⁶ Siehe unten, [II.5.](#)

2. Ökonomische Begründung der Finanzintermediation

2.1 Begriff der Finanzintermediation

Der Begriff der Finanzintermediation wird nach wohl herrschender Auffassung in den Wirtschaftswissenschaften als die professionelle Zusammenführung von Kapitalangebot und -nachfrage bezeichnet. Konkret erleichtern Finanzintermediäre den Kapitalfluss zwischen den Haushalten als Überschusseinheiten und den Unternehmen sowie dem Staat als Defiziteinheiten einer Volkswirtschaft. Die Finanzintermediäre sind in ihrer Rolle unmittelbar an der Produktion oder am Austausch von Kapital (sog. *Finanzkontrakte*) beteiligt. Zu den Finanzintermediären gemäss dieser Begriffsbestimmung zählen in erster Linie Banken, Versicherungen, Wertpapierhäuser, Investmentgesellschaften und Anlagefonds.⁹⁷

Von dieser Form der Finanzintermediation *im engeren Sinne* können Aktivitäten unterschieden werden, in denen nicht Finanzkontrakte, sondern etwa Informationen Gegenstand von Produktions- und Austauschhandlungen bilden.⁹⁸ Diese Form der reinen Informationsintermediation, die typischerweise durch Finanzanalysten und Ratingagenturen erbracht wird, ist vorliegend als Finanzintermediation *im weiteren Sinne* zu verstehen.⁹⁹

Entgegen der herkömmlichen Auffassung werden *Handelsplätze* und deren Nachhandelsinfrastrukturen in der vorliegenden Arbeit der Finanzintermediation zugerechnet. Denn, obwohl diese nicht unmittelbar in die Erstellung oder den Austausch von Finanzkontrakten oder der sie betreffenden Informationen involviert sind, ermöglichen sie Schuldner und Gläubigern durch das Zusammenführen von Kapitalangebot und -nachfrage eine effiziente Allokation von Finanzkontrakten. Sie übernehmen in diesem Rahmen die Funktionen der Ver-

⁹⁷ Ausführlich zum Ganzen Breuer, Finanzintermediation, 5–22; ferner Dietrich/Vollmer, Finanzintermediation, 1–2; Boemle et al., Finanzintermediäre, 442; Müller, in: Boemle et al., Intermediationsfunktion der Banken, 596–597; Zobl/Kramer, Kapitalmarktrecht, Rz. 1; Spremann/Gantenbein, Finanzmärkte, 50–51; Kaiser, Finanzintermediation, 119; Banks, Dictionary of Finance, 277; Smullen/Hand, Dictionary of Finance, 217.

⁹⁸ Siehe etwa Allen, Journal of Financial Intermediation 1990, 22.

⁹⁹ So etwa Bodie/Merton/Cleeton, Financial Economics, 60; a.M. Breuer, Finanzintermediation, 16. Ausführlich zur Finanzanalyse als Informationsintermediation Schaller, Finanzanalysten-Recht, 44–48.

mittlung bzw. Aggregation von Kapital und der Informationsverarbeitung, die vergleichbar mit derjenigen von Finanzintermediären im engeren und weiteren Sinne sind.¹⁰⁰

Ferner führt die netzwerkbasierte Intermediation *dezentraler Handelsplattformen*, wie noch zu vertiefen sein wird, selbst zur Produktion und zum Austausch von Finanzkontrakten. Eine klare Dichotomie zwischen reiner Intermediation und reinem Infrastrukturbetrieb besteht m.E. darum nicht mehr; Finanzintermediäre scheinen insoweit obsolet zu werden, als dass dezentrale Handelsplattformen einen Teil ihrer Funktionen integrieren.¹⁰¹

Teilweise wird in der Literatur zwischen ökonomischer Intermediation als Bezeichnung für die Vorhandelsphase und rechtlicher Intermediation als Sammelbegriff für die Prozesse der Nachhandelsphase unterschieden.¹⁰² Diese Arbeit folgt indessen dieser Unterscheidung nicht, da sie den Schwerpunkt auf die gesamte Handelsphase legt.

Finanzintermediäre im engeren Sinne stellen letztlich selbst den verschiedenen Marktteilnehmern einen «Marktplatz» zur Verfügung, an dem Angebot von und Nachfrage nach Kapital, Risiko und Dienstleistungen zusammengeführt werden.¹⁰³ Die ökonomische Literatur spricht in diesem Zusammenhang von zwei- oder mehrseitigen Märkten. Dabei beeinflussen sich die Entscheidungen der Teilnehmer der unterschiedlichen Marktseiten gegenseitig.¹⁰⁴ Dasselbe gilt in untergeordneter Weise auch für Effektenabwicklungs- und Zahlungssysteme.¹⁰⁵ Zentrale Gegenparteien sind demgegenüber am Austausch von Finanzkontrakten unmittelbar beteiligt und gelten darum als Finanzintermediäre im engeren Sinne.¹⁰⁶

BEAT BERNET fasst die unterschiedlichen Akteure der Finanzintermediation – d.h. Finanzintermediäre und Handelsplätze inkl. deren Nachhandelsinfrastrukturen – unter dem Oberbegriff des Finanzintermediationssystems zu-

¹⁰⁰ GLM. Bernet, Finanzintermediation, 20–23, 29–32; Achleitner, Investment Banking, 29–30; ferner offenbar auch Spremann/Gantenbein, Finanzmärkte, 51, 53; sodann Bodie/Merton/Cleeton, Financial Economics, 24–26, 30.

¹⁰¹ Siehe unten, [II.4.5](#).

¹⁰² So etwa Ter-Sahakyan, Economic and Legal Risks, Rz. 2, 31–34 m.w.N.

¹⁰³ Siehe Bernet, Finanzintermediation, 118, 129.

¹⁰⁴ Siehe hinsichtlich dieser Netzwerkexternalitäten Rochet/Tirole, Journal of the European Economic Association 2003, 990–994; ferner Rysman, Journal of Perspectives 2009, 125–128.

¹⁰⁵ Siehe Bernet, Finanzintermediation, 32–34.

¹⁰⁶ Siehe Breuer, Finanzintermediation. 18.

sammen.¹⁰⁷ Auch WOLFGANG HÜGLE unterscheidet aufgrund einer funktionalen Betrachtung zwischen bank- und marktbasierter Formen der Finanzintermediation.¹⁰⁸ Für ROBERT C. MERTON ist schliesslich eine funktionale Betrachtungsweise gegenüber einem institutionenbasierten Ansatz der Finanzintermediation gerade in Zeiten raschen technologischen Wandels geboten.¹⁰⁹

Nach dem Gesagten umfasst der Begriff der Finanzintermediation alle Prozesse und Strukturen im Zusammenhang mit der Organisation der Produktion und des Austausches von Finanzkontrakten und -informationen durch die Marktteilnehmer. Erfasst werden somit auch Handelsplätze, die nach konventioneller Auffassung nicht Teil des Finanzintermediationssystems sind. Ob der Intermediation schliesslich personale, institutionelle oder netzwerkbasierte Prozesse und Strukturen zugrunde liegen, ist grundsätzlich nicht weiter relevant.

	Finanzintermediation
Definition	Finanzintermediation umfasst alle intermediären Prozesse und Strukturen im Zusammenhang mit der Organisation der Produktion und des Austausches von Finanzkontrakten und Finanzinformationen durch die Marktteilnehmer.

2.2 Eigenschaften und Bedeutung der Finanzintermediation

Die personale und institutionelle Intermediation entspricht gemäss den Ausführungen zu Beginn dieses Kapitels einer historischen Gesetzmässigkeit. Eine arbeitsteilige und spezialisierte Wirtschaftsordnung wäre ohne einen seinerseits arbeitsteiligen und spezialisierten Finanzsektor undenkbar. Der Finanzsektor stellt in erster Linie den Transfer von Kapital und Risiken durch Zeit und Raum zwischen den Marktteilnehmern sicher.¹¹⁰ Dabei ist in einer

¹⁰⁷ Zur Definition des Begriffs Bernet, Finanzintermediation, 19–20; ebenfalls sehr weitgehend Dietrich/Bienert, in: Abegg/Bärtschi/Dietrich, § 1 Rz. 4, 15–17

¹⁰⁸ Siehe Hügle, Finanzsysteme, 77–78.

¹⁰⁹ Siehe Merton, Financial Management 1995, 24 («[...] with the current rate of technological advance and integration of world financial markets, [a functional] approach may prove especially useful in predicting the future direction of financial innovation, changes in financial markets and intermediaries, and the places for regulatory bottlenecks.»), 38–39.

¹¹⁰ Siehe Bernet, Finanzintermediation, 2; ferner Achleitner, Investment Banking, 23; Dietrich/Bienert, in: Abegg/Bärtschi/Dietrich, § 1 Rz. 5; ausführlich Bodie/Merton/Cleeton, Financial Economics, 26–34 m.w.H.

marktwirtschaftlich geprägten Ordnung in aller Regel das Preissystem für die effiziente Allokation dezentral verteilter Ressourcen besorgt.¹¹¹

Im Zentrum dieser Vorgänge steht der Finanzintermediär als Produzent von Produkten und Dienstleistungen, die im Vergleich zu den Gütern anderer Sektoren *besondere Eigenschaften* aufweisen:

- Die von Finanzintermediären produzierten Produkte und Dienstleistungen sind überwiegend immateriell und informationsbasiert,¹¹² weshalb die Finanzintermediation besonders von der Digitalisierung betroffen ist.¹¹³
- Banken etwa produzieren im Rahmen ihrer Depositen- und Kreditstätigkeit ein liquides elektronisches Tausch- und Zahlungsmittel mit je nach Bedarf des Kunden unterschiedlichen Fristen und Losgrößen (sog. Buchgeld)¹¹⁴ – dadurch produzieren Banken letztlich Kaufkraft, die es den Inhabern des Buchgelds erlaubt, Waren und Dienstleistungen der Realwirtschaft zu erwerben;¹¹⁵
- Versicherungen stellen Vereinbarungen über die Allokation von individuellen oder kollektiven Risiken basierend auf deren mathematischen Eintrittswahrscheinlichkeit her (sog. Policen),¹¹⁶
- Investmentgesellschaften und Anlagefonds begründen schliesslich professionell verwaltete Investitionskontrakte, die es einer Vielzahl von Personen erlaubt, in diversifizierter Weise an der volkswirtschaftlichen Produktivität zu partizipieren.¹¹⁷

Die erwähnten Güter gelten theoretisch und empirisch als fundamentale Stützen einer modernen Volkswirtschaft, weshalb von der Finanzintermediation als einer Institution mit *gesamtwirtschaftlicher* Bedeutung gesprochen wird.¹¹⁸

¹¹¹ Siehe statt vieler Stigler, *Theory of Price*, 11–17.

¹¹² Ausführlich hierzu Bernet, *Finanzintermediation*, 140–145, ferner 60.

¹¹³ Vgl. unten, [II.3.3b](#).

¹¹⁴ Siehe Schumpeter, *Theorie*, 109–110; Tobin, in: Eatwell/Milgate/Newman, *Financial Intermediaries*, 157–174, 162–165; vgl. ferner Dwyer/Samartín, *Journal of Financial Stability* 2009, 154–155; anschaulich zur Geldschöpfungsfunktion von Geschäftsbanken Adrian/Heidorn, *Bankbetrieb*, 13–14.

¹¹⁵ Siehe etwa Borio, *BIS Working Papers* Nr. 395, Dezember 2012, 11.

¹¹⁶ Siehe Bodie/Merton/Cleeton, *Financial Economics*, 27; ferner für eine v.a. *historische* Betrachtung Bernstein, *Risk*, 92–95, 144, 203–204.

¹¹⁷ Siehe MacNeil, *Law on Financial Investment*, 6–7; Meier-Hayoz/Forstmoser, *Schweizerisches Gesellschaftsrecht*, § 22 N 5; ferner für eine *historische* Darstellung dieser Anlagevehikel v.a. aus US-amerikanischer Perspektive Fink, *Mutual Funds*, insb. 7–29.

¹¹⁸ Siehe etwa Botschaft FINMAG 2006, 2833 («Schlüsselfunktionen einer Volkswirtschaft»); ferner Hettich, *GesKR* 2013, 388, der den Schutz der Funktion von Finanzintermediären dem Funktionsschutz zuordnet; Bärtschi/Hirschi, *SZW* 2017, 775, die unter Verweis auf die

Vor diesem Hintergrund ist es wenig überraschend, wenn das Bundesgericht in einem Urteil aus dem Jahr 1985 verlauten liess: «Die Verwicklung in rechts- oder sittenwidrige Geschäfte kann das Vertrauen nicht nur in die betroffene Bank, sondern in die Schweizer Banken ganz allgemein beeinträchtigen.»¹¹⁹

2.3 Organisationsformen

a. Einleitung

In der ökonomischen und soziologischen Literatur wird ein Konnex zwischen der Organisation wirtschaftlicher Austauschprozesse sowie Regel- und Handlungsstrukturen hergestellt. Je nach Autor werden letztere als *Governance*¹²⁰, *Ordnung*¹²¹ oder *Institutionen*¹²² bezeichnet.

Das Ziel von Regel- und Handlungsstrukturen ist es, auf der Basis von wirtschaftlichen oder rechtlichen Handlungs- und Verfügungsrechten (sog. *Property Rights*) und unter Berücksichtigung der dabei anfallenden Kosten ökonomische Austauschgeschäfte in effizienter Weise zu ordnen und strukturieren.¹²³ Wie noch näher auszuführen sein wird, können in dezentralen Systemen nunmehr auch *technologiebasierte* Handlungs- und Verfügungsrechte ökonomische Ergebnisse herbeiführen, die nicht unähnlich sind zu denjenigen, die sich aus der Allokation von *Property Rights* durch die Rechtsordnung ergeben.¹²⁴

b. Markt vs. Hierarchie

Die ökonomische Theorie unterscheidet hinsichtlich der Organisation der Wirtschaftsordnung zwischen zentralen und dezentralen Institutionen. Dabei kontrastiert grundsätzlich jede Form der Hierarchie, wie etwa Familie, Unternehmen und Staat, als zentrale Institution mit dem Markt als dezentralem

Botschaft FINMAG 2006, 2859, das Vertrauen in die Leistungsfähigkeit u.a. der am Kapitalmarkt agierenden Intermediäre betonen.

¹¹⁹ BGE 111 Ib 126, E. 2a.

¹²⁰ So insb. Williamson, *Economic Institutions*, 18; ferner Benz, in: Benz, *Governance*, 16.

¹²¹ So etwa Weber, *Sozialökonomik*, 16; sodann insb. auch Eucken, *Nationalökonomie*, 50.

¹²² So etwa North, *Institutions*, 3.

¹²³ Siehe etwa hinsichtlich der Perspektive der Neuen Institutionenökonomik Furubotn/Richter, *New Institutional Economics*, 6, 11–12.

¹²⁴ Siehe unten, [II.5.2d](#).

System.¹²⁵ Diese Dichotomie kann typischerweise anhand der Informationen, über welche die Wirtschaftsakteure solcher Institutionen verfügen, und der Anreize, die für das Handeln innerhalb solcher Institutionen massgeblich sind, untersucht werden.¹²⁶

- Die *Neoklassische Theorie* geht vom Menschenbild aus, dass alle Marktteilnehmer über stabile Präferenzen und vollständige Information verfügen. Vor dieser Ausgangslage maximieren die Marktteilnehmer ihren persönlichen Nutzen bzw. Gewinn (sog. *Rational Choice*-Theorie). Daraus resultiert in der Theorie ein allokatationseffizienter Markt mit optimalen Wettbewerbsbedingungen.¹²⁷ In einem solchen Umfeld vollkommener Finanzmärkte bedarf es grundsätzlich weder des Dazwischenschaltens von Finanzintermediären noch staatlicher Interventionen. Der Austausch von Gütern findet grundsätzlich über den Marktpreismechanismus unmittelbar zwischen den Endbegünstigten statt.¹²⁸
- Realitätsnähere Erklärungsansätze, insb. der *Informationsökonomik* und der *Neuen Institutionenökonomik*, unterstellen demgegenüber jeder wirtschaftlichen Austauschhandlung Informations- bzw. Transaktionskosten.¹²⁹ Dabei setzen diese Erklärungsansätze in ihren Governance- und Vertragsmodellen die beschränkte Verfügbarkeit von Informationen voraus, weswegen die Akteure nur beschränkt rational agieren können. Zudem wird in den Modellannahmen regelmässig davon ausgegangen, dass sich Marktteilnehmer opportunistisch verhalten.¹³⁰ Neben der beschränkten Verfügbarkeit von Informationen wird zudem auch die un-

¹²⁵ Siehe Benz, in: Benz, *Governance*, 15–16.

¹²⁶ Siehe Malinvaud, in: Eatwell/Milgate/Newman, *Decentralization*, 71; grundlegend hierzu Williamson, *Markets and Hierarchies*, 8–10, der zudem zwischen «environmental factors» und «human factors» unterscheidet.

¹²⁷ Siehe etwa Mankiw, *Microeconomics*, 6–7, 66–67, 320; Breyer, *Mikroökonomik*, 131–143; Cooter/Ulen, *Law and Economics*, 18–24, 28–29, 37–38; kritisch aus einer praxeologischen Sicht demgegenüber bereits von Mises, *Human Action*, 62–64, 241, 646–647; sodann in verhaltensökonomischer Hinsicht kritisch Simon, *The Quarterly Journal of Economics* 1955, 114; Tversky/Kahneman, *Science* 1981, 457; Kirchgässner, *Homo Oeconomicus*, 69–70 m.w.N.

¹²⁸ Siehe Bernet, *Finanzintermediation*, 84–85.

¹²⁹ Siehe Furubotn/Richter, *New Institutional Economics*, 36, 47; Ménard/Shirley, in: Ménard/Shirley, *Introduction*, 1–2; grundlegend Williamson, *Economic Institutions*, 18–22.

¹³⁰ Siehe etwa Furubotn/Richter, *New Institutional Economics*, 3–5; Milgrom/Roberts, *Organization*, 129–130; ausführlich Williamson, *Governance*, 55–57.

gleichmässige Verteilung von Information in Gesellschaft und Wirtschaft unter realen und somit dynamischen Bedingungen betont.¹³¹

- Demgegenüber gehen verhaltensökonomische Theorien, auf welche nachfolgend jedoch nicht weiter eingegangen werden soll, davon aus, dass Marktteilnehmer bei Entscheidungen regelmässig entweder auf komplexitätsreduzierende Heuristiken zurückgreifen oder kognitiven Verzerrungen (sog. *Biases*) unterliegen.¹³² Mit diesen Erkenntnissen lassen sich unter Umständen Marktanomalien erklären, die im neoklassischen Theoriengebäude keinen Niederschlag finden.¹³³

Die Kosten des «Wirtschaftens», wozu namentlich Kosten im Zusammenhang mit der Suche von Vertragspartnern und Verhandlungen mit diesen, der Abwicklung des Vertrages, der Kontrolle der Vertragspartner, der allfälligen Anpassung des Vertrages an die geänderten Umstände sowie die Sanktionierung gehören, fallen je nach Art der Transaktion und der Art ihrer Organisation unterschiedlich hoch aus (sog. *Transaktionskosten*).¹³⁴ Dabei können grundsätzlich Markttransaktionen von Transaktionen in Hierarchien bzw. Firmen unterschieden werden.¹³⁵ Finanzintermediation findet in der Form von *Hierarchien* statt. Wenn die Nutzung des Marktes Kosten von x und der Einsatz eines Finanzintermediärs Kosten von y erzeugen, dann rechtfertigt sich der Einsatz des Finanzintermediärs, sobald $y < x$ ist. Das Einschalten von Intermediären ist

¹³¹ Siehe von Hayek, *American Economic Review* 1945, 524–525 («We cannot expect that this problem will be solved by first communicating all this knowledge to a central board which, after integrating all knowledge issues its orders. We must solve it by some form of decentralization [...] We need decentralization because only thus can we ensure that the knowledge of the particular circumstances of time and place will be promptly used. But the 'man on the spot' cannot decide solely on the basis of his limited but intimate knowledge of the facts of his immediated surroundings. There still remains the problem of communicating to him such further information as he needs to fit his decisions into the whole pattern of changes of the larger economic system.»); ausführlich sodann Sunstein, *Infotopia*, 118–121, der sodann auf sog. Vorhersagemärkte (*Prediction Markets*) eingeht.

¹³² Siehe Gigerenzer, *Bauchentscheidungen*, 25–26; ferner die Aufsätze im Sammelband Kahneman/Slovic/Tversky, *Heuristics and biases*, *passim*.

¹³³ Siehe Shleifer, *Inefficient Markets*, 10–25; ferner Shiller, *Journal of Economic Perspectives* 2003, 90–91.

¹³⁴ Siehe Coase, *Economica* 1937, 390–392 («[the] cost of using the price mechanism»); Arrow, in: Haveman/Margolis, *Market Allocation*, 501 («cost of running the economic system»); Williamson, *The American Journal of Sociology*, 1981, 552–553; Williamson, *Journal of Economic Literature* 1981, 1547; Milgrom/Roberts, *Organization*, 28–29.

¹³⁵ Weitere Kategorien von ökonomischen Transaktionen, die unterschieden werden können, sind die *Bürokratie* und die *Familie*; siehe hierzu Spremann/Gantenbein, *Kapitalmärkte*, 47, 52.

darum kein Selbstzweck, sondern Ausdruck einer im Vergleich zu unmittelbaren, indessen nicht friktionsfreien Markttransaktionen kostengünstigeren Strukturierung von wirtschaftlichen Prozessen.¹³⁶ Der Einsatz eines Finanzintermediärs kann zudem regelmässig auch eine Nutzensteigerung für den Kunden darstellen (z.B. indem dieser Anlagefehler durch Beizug eines Experten avoided), welche die allenfalls höheren Kosten der Finanzintermediation aufwiegt.

Wie noch auszuführen sein wird, ist die transaktionskostenökonomische Aufteilung in Märkte und Hierarchien zentral für das Verständnis von Austauschhandlungen in dezentralen Systemen.¹³⁷ Bereits RONALD H. COASE hat indessen darauf hingewiesen, dass eine eindeutige Abgrenzung der unterschiedlichen Modelle in der Praxis nicht immer möglich ist: An modernen Handelsplätzen etwa werden dezentrale Markttransaktionen in der hierarchischen Governance-Struktur der Betreiberin des Handelsplatzes konzentriert.¹³⁸ Zudem betont auch OLIVER E. WILLIAMSON, dass es sich bei der Dichotomie von Markt und Hierarchie um eine solche der «Extremformen» handelt.¹³⁹

c. ... vs. Netzwerk

Das dichotomische Modell von Markt und Hierarchie wurde bereits früh erweitert, um weitere im Wirtschaftsleben beobachtbare Organisationsformen in adäquaterer Weise zu beschreiben. WALTER W. POWELL setzte in den 1990er Jahren *Netzwerke* als Alternative neben Märkte und Hierarchien.¹⁴⁰ Netzwerke unterscheiden sich von den beiden anderen Organisationsformen darin, dass Austauschprozesse horizontal und vertikal zwischen einer Mehrzahl von Netzwerkteilnehmern erfolgen, wobei diese in wirtschaftlicher Hinsicht zu einem gewissen Grad voneinander abhängig sind. Sie bringen Ressourcen in das Netzwerk regelmässig auf der Grundlage von Gegenseitigkeit und Langfris-

¹³⁶ Siehe Spremann/Gantenbein, Kapitalmärkte, 50; Bernet, Finanzintermediation, 117; Gordon/Winton, in: Constantinides/Haris/Stulz, Financial Intermediation, 437.

¹³⁷ Siehe unten, [II.5.2a](#).

¹³⁸ Ausführlich Coase, Firm, Market, Law, 8–10; ferner Furubotn/Richter, New Institutional Economics, 315 m.w.N.; so bereits in allgemeiner Weise mit Blick auf die Existenz unterschiedlicher Arten von «Marktregulierungen» Weber, Sozialökonomik, 43.

¹³⁹ Siehe Williamson, Economic Institutions, 83–84.

¹⁴⁰ Siehe Powell, Research in Organizational Behavior 1999, *passim*.

tigkeit ein. Die Kommunikation zwischen den Teilnehmern eines Netzwerks erfolgt typischerweise ausserhalb von Preisen und hierarchischen Kontrollstrukturen.¹⁴¹

Auch die traditionelle Finanzintermediation kann netzwerkartig strukturiert sein: Banken und Versicherungen haben sich in den letzten Jahren stärker auf ihre Kernkompetenzen fokussiert und alle übrigen Funktionen, die sie – etwa aus regulatorischen Gründen –¹⁴² nicht zwingend selbst zu erfüllen haben, an andere Anbieter ausgelagert. FinTech ist ein wesentlicher Treiber dieser Entwicklung.¹⁴³ In Finanzintermediationsnetzwerken werden Finanzkontrakte und Finanzdienstleistungen zu einem gewissen Grad gemeinsam produziert und ausgetauscht.¹⁴⁴ Finanzintermediäre, erhoffen sich aus der Netzwerkkoope-
ration insb. die Senkung von Transaktionskosten, namentlich durch Spezialisierung und die Ausnutzung von Skalen- und Netzwerkeffekten.¹⁴⁵

Bei dezentralen Systemen, wie noch aufzuzeigen ist, handelt es sich transaktionskostenökonomisch um einen organisatorischen Hybrid bestehend aus Elementen von Märkten, Hierarchien und Netzwerken.¹⁴⁶

2.4 Vorteile und Nachteile der Finanzintermediation

a. Kosten- und Informationsvorteile

Die Organisation von wirtschaftlichen Prozessen in Form der Finanzintermediation bietet intermediationsspezifische Kosten- und Informationsvorteile. Unter Berücksichtigung von *Economies of Scale, Scope and Skills* sowie der Diversifikation betrieblicher Risiken stellen diese Kosten- und Informationsvorteile eine theoretisch und empirisch fundierte Begründung für die Existenz von Finanzintermediären dar.¹⁴⁷

¹⁴¹ Ausführlich Powell, Research in Organizational Behavior 1999, 300–305.

¹⁴² Vgl. FINMA-RS 18/3 «Outsourcing», Rz. 7–13.3.

¹⁴³ Siehe hierzu unten, [II.3.3b](#).

¹⁴⁴ Siehe Bernet, Finanzintermediation, 173–174.

¹⁴⁵ Siehe Bernet, Finanzintermediation, 174–175.

¹⁴⁶ Siehe unten, [II.5.2a](#).

¹⁴⁷ Eine Übersicht der Gründe findet sich in Spremann/Gantenbein, Kapitalmärkte 50; ausführlich mit Bezug zu den unterschiedlichen wirtschaftswissenschaftlichen Erklärungsansätzen Bernet, Finanzintermediation, 90–116, sodann spezifisch 116–134; Achleitner, Investment Banking, 44–54; Bodie/Merton/Cleeton, Financial Economics, 58; ferner zu den intermediationsspezifischen Hindernissen auch Kaiser, Finanzintermediation, 97–118; insb. in Bezug auf Investmentbanken Jacob/Klein, Investment Banking, 23–30.

- *Suche und Selektion von an einer Transaktion interessierten Marktteilnehmern:* Finanzintermediäre dienen Marktteilnehmern als Anlauf- und Konzentrationsstelle, wobei sie kontraktwillige Marktteilnehmer in effizienter Weise miteinander in Verbindung bringen (sog. *Matching*).¹⁴⁸ Diese Funktion von Finanzintermediären ist nicht unähnlich zu derjenigen von Handelsplätzen.¹⁴⁹ An Märkten bieten typischerweise spezialisierte Finanzintermediäre ihre Dienstleistungen den übrigen Marktteilnehmern an.¹⁵⁰
- *Produktion von Finanzkontrakten, Gestaltung der Vertragsinhalte, Bestimmung der Preise und Abgabe von Garantien:* Finanzintermediäre produzieren kostengünstige und liquide Finanzkontrakte zur inter- und intratemporalen Befriedigung von Konsumententscheidungen;¹⁵¹ Finanzintermediäre, namentlich Banken, überwinden die Informationsasymmetrien zwischen den Marktteilnehmern und reduzieren dadurch in erster Linie das *Moral Hazard*-Risiko¹⁵² für Kapitalgeber und unter Umständen auch für andere Finanzintermediäre;¹⁵³ Finanzintermediäre, namentlich Investmentfonds, können in effizienter Weise den verbleibenden Wert von am Markt verfügbaren Informationen ausnutzen;¹⁵⁴ durch den Einsatz von Finanzintermediären und deren Reputation (sog. *Signaling*) können Geschäftsge-

¹⁴⁸ Siehe Cosimano, *Economica* 1996, 141; ebenfalls Fama, *Journal of Monetary Economics* 1980, 46.

¹⁴⁹ Gl.M. Bernet, *Finanzintermediation*, 118.

¹⁵⁰ Vgl. die Arbeiten zu sog. *Intermediated Markets* von Rubinstein/Wolinsky, *The Quarterly Journal of Economics* 1987, 581-582; Gehrig, *Journal of Economics & Management Strategy* 1993, 97, 100; Yavaş, *Journal of Economics & Management Strategy* 1996, 196-197; ferner Schwartz/Francioni, *Equity Markets*, 191.

¹⁵¹ Siehe Benston/Smith, *The Journal of Finance* 1976, 217-220; ferner Diamond/Dybvig, *The Journal of Political Economy* 1983, 403, 405, welche indessen die Risiken von *Bank Runs* in einem solchen System hervorheben.

¹⁵² Das ökonomische Konzept des *Moral Hazard* besagt, dass ein «Versicherungsnehmer» sich aufgrund der i.d.R. finanziellen Zusagen des «Versicherers» *ex post* weniger verantwortungsbewusst verhält, als wenn er selbst für die Kosten seiner Entscheidungen aufkommen müsste; vgl. hierzu Arrow, *The American Economic Review* 1963, 961-962. *Moral Hazard*-Risiken können aufgrund der ungleichen Informationsverteilung zu einer *ex ante*-Negativauslese der «Versicherungsnehmer» seitens der «Versicherer» führen, was letztlich in Pareto-ineffiziente Ergebnisse, d.h. inkorrekte Preisgestaltung von «Versicherungsrisiken», im Markt resultieren kann (sog. *Adverse Selection*); vgl. hierzu Akerlof, *The Quarterly Journal of Economics* 1970, 492-494.

¹⁵³ Siehe Leland/Pyle, *The Journal of Finance* 1977, 382-384; ähnlich Ramakrishnan/Thakor, *The Review of Economic Studies* 1984, 416.

¹⁵⁴ Siehe Allen, *Journal of Financial Intermediation* 1990, 22-25.

heimnisse von Kunden effizient geschützt werden (z.B. im Rahmen von Finanzierungen).¹⁵⁵ Finanzintermediäre, insb. Ratingagenturen, können in effizienter Weise Informationen sammeln und auswerten, was ihnen erlaubt, die Qualität von Finanzkontrakten zu beurteilen;¹⁵⁶ Finanzintermediäre verfügen schliesslich über die Expertise und Verhandlungsmacht, effiziente und anreizkompatible Finanzkontrakte mit Vertragspartnern abzuschliessen und diese Verträge aufgrund ihrer strukturellen Unvollständigkeit und Lückenhaftigkeit bei Bedarf in effizienter Weise nachzuverhandeln (sog. *Contractual Incompleteness*).¹⁵⁷

- *Unterstützung bei der Ausführung und Überwachung des Finanzkontraktes*: Banken etwa verringern die Überwachungskosten und damit das Moral Hazard-Risiko im Rahmen der Kreditvermittlung zwischen Einlegern und Darlehensnehmern, was letztlich auch die Kreditkosten für die Darlehensnehmer senkt;¹⁵⁸ Investmentfonds, Pensionskassen und Finanzanalysten können in effizienter Weise die Führungsorgane der von ihnen als Investitionen gehaltenen oder empfohlenen Unternehmen überwachen;¹⁵⁹ Finanzintermediäre, wie v.a. Banken, reduzieren das Moral Hazard-Risiko darüber hinaus auch für die Teilnehmer des Kapitalmarktes.¹⁶⁰

Diese Ansätze der Informations- und Transaktionskostenökonomik stellen nachvollziehbare Erklärungen für die in der Realität beobachtbare Existenz von Finanzintermediären dar. Finanzintermediäre können unter Umständen die Transaktionskosten wirtschaftlicher Prozesse im Vergleich zu reinen Markttransaktionen deutlich reduzieren.

¹⁵⁵ Siehe Campbell/Kracaw, *The Journal of Finance* 1980, 880.

¹⁵⁶ Siehe Millon/Thakor, *The Journal of Finance* 1985, 1416–1417; in Bezug auf die vorherrschende Informationsflut bzw. den *Information Overload* Bernet, *Finanzintermediation*, 151–152.

¹⁵⁷ Siehe Hart, *Contracts*, 4. Finanzintermediäre können somit dazu beitragen, das *Hold-up*-Problem zu beheben, das sich u.a. im opportunistischen Ausnutzen von Vertragslücken manifestiert; vgl. hierzu Bernet, *Finanzintermediation*, 92, 118–123, 125, 131–132.

¹⁵⁸ Siehe bereits Schumpeter, *Business Cycles*, 116–117; *grundlegend* Diamond, *The Review of Economic Studies* 1984, 395; ferner unter Berücksichtigung von Konjunkturzyklen Williamson, *Journal of Political Economy* 1987, 1197, 1214.

¹⁵⁹ Siehe hierzu Jensen/Meckling, *Journal of Financial Economics* 1976, 354–355.

¹⁶⁰ Siehe Seward, *The Journal of Finance* 1990, 367–369.

b. Kontroll- und Vertrauensrisiken

Die Inanspruchnahme der Finanzintermediation verursacht *ihrerseits* Transaktionskosten für die Marktteilnehmer. Die Kosten können einerseits beim Empfänger der intermediatisierten Leistung, andererseits aber auch gesamtgesellschaftlich anfallen.¹⁶¹

Die individuellen Transaktionskosten lassen sich einerseits auf die *Immaterialität* von Finanzintermediationsprodukten zurückführen. Die Immaterialität macht die qualitativen Merkmale eines Produktes für den Käufer oder Auftraggeber nur unter erschwerten Bedingungen wahrnehmbar. Namentlich handelt es sich bei vielen Finanzdienstleistungen um Erfahrungs- und Vertrauensgüter. Bei Erfahrungsgütern erfolgt der Lernprozess des Empfängers anders als bei Suchgütern erst während des Konsums des Gutes (z.B. beim Aktienkauf); bei Vertrauensgütern kann der Lernprozess hingegen deutlich länger dauern und in der Folge auch den Zeitpunkt des Konsums übersteigen (z.B. beim Kauf einer Lebensversicherung). Daraus folgt, dass der Käufer eines Finanzprodukts oder der Empfänger einer Finanzdienstleistung deren Qualität in aller Regel erst *ex post* beurteilen können.¹⁶² Technische Standardisierungen der Produktpalette sowie Informationen zur Spezifizierung der Finanzprodukte können das Risiko des Nachfragers erheblich verringern, jedoch nicht gänzlich ausschliessen.¹⁶³

Andererseits bringt die Finanzintermediation zahllose *Kontroll- und Vertrauensrisiken* mit sich:¹⁶⁴ Wer als Prinzipal für die Erreichung seiner Ziele auf die Tätigkeiten eines Dritten, d.h. Agenten, zurückgreift, muss in aller Regel sicherstellen, dass der Dritte tatsächlich im Interesse des Prinzipals tätig wird. Konkret delegiert der Prinzipal, der vom Agenten Handlungen in seinem Interesse erwartet, bestimmte Entscheidungen an den Agenten und räumt ihm in diesem Rahmen den notwendigen Entscheidungsspielraum ein. Es existie-

¹⁶¹ Siehe ausführlich Judge, *The University of Chicago Law Review* 2015, 577–579, 594–614, 614–624, welche individuelle und soziale Kosten letztlich auf die Informations- und Positionsvorteile von Finanzintermediären zurückführt; ferner Bernet, *Finanzintermediation*, 128; Diamond, *The Review of Economic Studies* 1984, 399, 404, der diese als «delegation costs» des Empfängers der Dienstleistung bezeichnet.

¹⁶² Siehe Ogus, *Regulation*, 132–133; ferner Paccos, *International Review of Law and Economics* 2000, 483, 485.

¹⁶³ Siehe Bernet, *Finanzintermediation*, 60.

¹⁶⁴ Vgl. zum Begriff Ripperger, *Ökonomik des Vertrauens*, 63; sodann Fischer, *Interessenkonflikte*, 140; die zentrale Rolle von Kontrolle in Agency-Beziehungen betonend schliesslich Eisenhardt, *Management Science* 1985, 136–137; ähnlich Dietrich/Bienert, in: Abegg/Bärtschi/Dietrich, § 1 Rz. 17 («Informations- und Vertrauensprobleme»).

ren in solchen Konstellationen ubiquitäre Kontroll- und Vertrauensrisiken für den Prinzipal, die er in irgendeiner Form zu kontrollieren bzw. überwachen hat.¹⁶⁵ Diese Risiken lassen sich auf die einer Agency-Beziehung inhärenten Möglichkeit zu opportunistischem Verhalten des Agenten aufgrund von dessen Informationsvorsprung gegenüber dem Prinzipal zurückführen.¹⁶⁶ Der Informationsvorsprung des Agenten ist letztlich aufgrund von zwei praktischen Umständen bedeutsam: Prinzipal und Agent weisen entweder unterschiedliche Wünsche und Ziele oder voneinander abweichende Risikopräferenzen auf. In beiden Fällen ist es für den Prinzipal i.d.R. nicht leicht, die bestehenden Unterschiede überhaupt erkennen zu können.¹⁶⁷

Nach der ökonomischen Theorie treten Kontroll- und Vertrauensrisiken in einem breiten Spektrum von Beziehungen auf, die weit über das hinausgehen können, was typischerweise als auftragsrechtlich oder auftragsrechtsähnlich qualifiziert wird.¹⁶⁸ Kontroll- und Vertrauensrisiken sind grundsätzlich auch den meisten Formen der traditionellen Finanzintermediation inhärent.¹⁶⁹ Sie lassen sich aufgrund der ubiquitären Informationsasymmetrien zwischen Kunde und Intermediär nicht aus dem Weg schaffen, will man nicht grundsätzlich auf den Finanzintermediär verzichten. Dabei akzentuieren sich die Kontroll- und Vertrauensrisiken zulasten des Prinzipals, wenn dieser im Rahmen der Intermediationsleistung die Verfügungsmacht über seine Vermögenswerte

¹⁶⁵ Siehe Hopt, ZGR 2004, 2–3, 51 m.w.N.; ferner Abegglen/Andreotti, GesKR 2020, 36.

¹⁶⁶ Nach ursprünglicher Auffassung wird unter der *Prinzipal-Agent-Beziehung* das Verhältnis zwischen den Unternehmenseigentümern und der Geschäftsleitung verstanden, wobei im Extremfall erstere lediglich noch über Eigentumstitel verfügen (Ownership), während letztere die effektive Kontrolle über das Unternehmen ausübt (Control); siehe Berle/Means, *Modern Corporation*, 6, 66–68; bereits Smith, in: Campbell/Skinner, *Wealth of Nations*, Bd. 2, 741.

¹⁶⁷ Siehe Eisenhardt, *Academy of Management Review* 1989, 58–59; vgl. ferner Bernet, *Finanzintermediation*, 93, der m.Verw. auf Arrow zwischen «hidden characteristics», «hidden intentions» und «hidden actions» der Vertragsparteien differenziert.

¹⁶⁸ *Agency-Beziehungen* beinhalten in den unterschiedlichsten Kontexten das Risiko opportunistischen Verhaltens durch den Agenten; siehe etwa Ross, *The American Economic Review* 1973, 134 («*Examples of agency are universal.*»); Jensen/Meckling, *Journal of Financial Economics* 1976, 309; Alchian/Demsetz, *The American Economic Review* 1972, 780–781 («*team production*»); in *körperschaftlich organisierten Strukturen* Armour/Hansmann/Kraakman, in: Kraakman et al., *Agency Problems*, 29; sodann Easterbrook/Fischel, *Corporate Law*, 1; in *spieltheoretischer Hinsicht* Salanié, *Contracts*, 5–6.

¹⁶⁹ Ausführlich Bodie/Merton/Cleeton, *Financial Economics*, 31–34; Hopt, ZGR 2004, 2–4; so dann Gruber/Palma, in: Schäfer/Sethe/Lang, § 48 Rz. 2; *differenzierend* MacNeil, *Law on Financial Investment*, 7, der zwischen Intermediation im finanzökonomischen und rechtlichen Sinne unterscheidet.

aufgibt, die Umstände der Intermediation komplex sind und der Intermediär über einen grossen Entscheidungs- und Handlungsspielraum sowie Informationsvorsprung gegenüber dem Prinzipal verfügt.¹⁷⁰

Als Beispiel dafür, wie allgegenwärtig Kontroll- und Vertrauensrisiken bei der Nutzung traditioneller Handelsplattformen sind, dient der Kauf kotierter Aktien über die Schweizer Börse SIX Swiss Exchange:

- Auf Käufer- und Verkäuferseite ist mindestens je eine Bank bzw. ein Wertpapierhaus beteiligt, welche entsprechende Kauf- und Verkaufsaufträge in eigenem Namen auf Rechnung des Kunden in das Börsensystem der SIX Swiss Exchange AG eingeben.
- Zwischen die beiden Wertpapierhäuser tritt zwecks Reduktion der Gegenparteiisiken die zentrale Gegenpartei SIX x-clear AG, welche gegenüber der verkaufenden Partei als Käuferin und gegenüber der kaufenden Partei als Verkäuferin auftritt.¹⁷¹
- Die Abrechnung und Abwicklung der Aktienlieferung erfolgen über das Effektenabwicklungssystem SECOM der SIX SIS AG.¹⁷²
- Die Aktie, die als Bucheffekte ausgestaltet sein muss, wird dem Effektenkonto des Verkäufers bei dessen Verwahrungsstelle belastet und dem Effektenkonto des Käufers bei dessen Verwahrungsstelle gutgeschrieben. Bei den Verwahrungsstellen handelt es sich um die depotführenden Banken der beiden Parteien. Die SIX SIS AG als zentrale Verwahrungsstelle nimmt sodann eine Umbuchung der Bucheffekten in den Effektenkonten der beiden Verwahrungsstellen vor.¹⁷³
- Die Abrechnung und Abwicklung der Kaufpreiszahlung erfolgen über das Zahlungssystem Swiss Interbank Clearing (SIC) der SIX Interbank Clearing AG.¹⁷⁴ Die Schweizerische Nationalbank führt zu diesem Zweck Girokonten der am SIC-System teilnehmenden Finanzinstitute.¹⁷⁵

Mit anderen Worten: Der Vollzug des Kaufvertrages über die betreffenden Aktien bedarf des Einbezugs und Zusammenwirkens von mindestens *sieben* Intermediären. Alle diese Intermediäre müssen von den endbegünstigten Kunden in irgendeiner Form kontrolliert werden.

¹⁷⁰ Allgemein Fischer, Interessenkonflikte, 101, 128 m.w.N.; in Bezug auf die Vermögensverwaltung Sethe, Anlegerschutz, 141-142.

¹⁷¹ Siehe Oleschak, x-clear, 3.

¹⁷² Siehe Haene, SECOM, 4.

¹⁷³ Siehe Haene, SECOM, 4.

¹⁷⁴ Siehe Mägerle/Oleschak, SIC, 6.

¹⁷⁵ Siehe Mägerle/Oleschak, SIC, 3.

Wie noch zu vertiefen sein wird, büssen Hierarchien bzw. Firmen in Form von Finanzintermediären in dezentralen Systemen an Bedeutung ein.¹⁷⁶ Auf traditionelle hierarchische Strukturen kann durch den Einsatz von verteilten Computernetzwerken verzichtet werden. In der Folge scheinen gewisse Arten von Transaktionskosten in dezentralen Systemen an Bedeutung zu verlieren, denn die Möglichkeit zu opportunistischem Verhalten der Marktteilnehmer im Sinne von WILLIAMSON¹⁷⁷ und damit Moral Hazard-Risiken werden zu weiten Teilen durch protokollbasierte Automatisierungen und die Transparenz solcher Systeme eliminiert. Andererseits können neuartige Agency-Probleme in bisher wenig untersuchten Bereichen auftreten.¹⁷⁸

c. Mittel zur Verringerung von Kontroll- und Vertrauensrisiken

Um die Kontroll- und Vertrauensrisiken zu minimieren, muss der Prinzipal Anreizsysteme vorsehen, die den Agenten trotz der Möglichkeit zu opportunistischem Verhalten dazu veranlassen sollen, ausschliesslich im Interesse des Prinzipals tätig zu werden.¹⁷⁹

Die Kontrolle des Finanzintermediärs kann einerseits *direkt* durch den Kunden erfolgen, indem letzterer als Prinzipal das Verhalten des Agenten präventiv überwacht (sog. *Screening* und *Monitoring*) und dessen Leistung *ex post* analysiert (sog. *Auditing*). Ein solches Vorgehen ist für den Prinzipal in den meisten Fällen mit hohen Transaktionskosten verbunden und aufgrund des Informationsvorsprungs des Agenten in den wenigsten Fällen praktikabel. Die Kontrolle des Agenten durch den Kunden kann aber auch *indirekt* stattfinden, namentlich aufgrund von Informationen, die der Agent oder ein Dritter dem Markt zur Verfügung stellt. Hierzu gehören etwa Informationen zur Ausbildung und Expertise sowie der Reputation des Agenten (sog. *Signaling*), die Qualitätsprüfung des Agenten durch einen Dritten (sog. *Rating*) und die Abgabe von Ga-

¹⁷⁶ Siehe unten, [II.4.](#)

¹⁷⁷ Siehe hierzu ausführlich Williamson, *Managerial and Decision Economics* 1993, *passim*.

¹⁷⁸ Siehe unten, [IV.5.2.](#)

¹⁷⁹ Siehe Bernet, *Finanzintermediation*, 98–99; Bodie/Merton/Cleeton, *Financial Economics*, 33; ferner Jensen/Meckling, *Journal of Financial Economics* 1976, 308; Stiglitz, in: Eatwell/Milgate/Newman, *Principal and Agent*, 242 («The principal-agent problem is, then, the central problem of economic incentives.»).

rantien oder den Abschluss von Versicherungen durch den Agenten.¹⁸⁰ Freilich fallen auch in solchen Fällen Kosten an, die allerdings je nach Ausprägung vom Agenten, dem Prinzipal oder von beiden zu tragen sind.

Da für Marktteilnehmer nachvollziehbare und von ihnen akzeptierte Verhaltensvorgaben zur Stabilisierung ihrer Erwartungen führen können (und sollen), kann insb. auch privater und staatlicher *Finanzmarktregulierung* der Effekt der Vertrauensbildung der Allgemeinheit in die Finanzintermediation und somit transaktionskostenreduzierende Wirkung zukommen.¹⁸¹ Selbstredend kann Regulierung auch neuartige Kontroll- und Vertrauensrisiken schaffen, die sodann zu gesamtgesellschaftlichen Kosten führen können.¹⁸²

Schliesslich kann auch der anbieterseitige *Wettbewerb* eine disziplinierende Wirkung auf die Höhe der Transaktionskosten der Nachfrager sowie einen positiven Einfluss auf die Konsumentensouveränität im Finanzintermediationssystem haben.¹⁸³

¹⁸⁰ Siehe Akerlof, *The Quarterly Journal of Economics* 1970, 499–500; hinsichtlich *Signaling* Spence, *The Quarterly Journal of Economics* 1973, 358; ausführlich Bernet, *Finanzintermediation*, 93–94, vgl. ferner 119, 124–125; in *historischer* Hinsicht Stringham, *Private Governance*, 56–58 m.w.N.

¹⁸¹ So insb. Emmenegger/Döbeli, *SZW* 2017, 758–759, 759–767, welche die Rolle des Aufsichts- und Vertragsrechts für den praktischen und strategischen Vertrauensschutz betonen; ferner Weber, *Journal of International Banking Law and Regulation* 2017, 253–254, 259 m.w.N.; Fischer, *Interessenkonflikte*, 136; ferner Ruffner, *Ökonomische Grundlagen*, 18–19. Zwischen Reputation und Regulierung besteht indessen ein komplexes Verhältnis; vgl. hierzu von der Crone/Vetsch, in: Klewes/Wreschniok, *Reputation*, 182–183.

¹⁸² Vgl. hinsichtlich der Schaffung potenzieller Moral Hazard-Risiken am Beispiel von *Einlagensicherungssystemen* Sethe, *SZW* 2012, 508–509; ferner Sethe/Fahrländer, *SZW* 2019, 640–641; sodann am Fall der Kaupthing-Bank Schweiz Dietrich/Bienert, in: Abegg/Bärtschi/Dietrich, § 1 Rz. 67–70.

¹⁸³ Siehe Bernet, *Finanzintermediation*, 101–102; *spezifisch* mit Blick auf den Anlegerschutz Inderst, *EBOR* 2009, 461–464; vgl. ferner unten, [VI.4.2b](#).

3. Formen der Disintermediation in Finanzmärkten

3.1 Begriff der Disintermediation

Der Begriff der Disintermediation (auch Desintermediation oder Disintermediatisierung) wird in der Literatur sehr unterschiedlich definiert:¹⁸⁴

Ausgehend vom banktypischen Zinsdifferenzgeschäft wird Disintermediation traditionellerweise als die *Verschiebung des bilanzmässigen zum indifferenten Bankgeschäft* verstanden. Es ist damit der Rückgang des Kreditgeschäfts zugunsten von Bankdienstleistungen, wie etwa Brokerage, Anlageberatung und Vermögensverwaltung, gemeint. Als Gründe für die Verschiebungen werden die im Vergleich zu klassischen Bankprodukten grössere Auswahl an Finanzinstrumenten, höhere Renditen und steuerliche Begünstigungen von Investitionen am Kapitalmarkt erwähnt.¹⁸⁵

Nach einem allgemeineren Verständnis wird unter Disintermediation die Übernahme von ursprünglich bankmässig erbrachten Finanzintermediationsfunktionen durch Anbieter ausserhalb des Bankensystems verstanden. Die Produktion und der Austausch von Finanzkontrakten verlagert sich von den klassischen Finanzintermediären, namentliche Banken und Versicherungen, zu den Kapitalmärkten und deren Teilnehmern. Unternehmen und Investoren erlangen «direkten Zugriff» auf den Kapitalmarkt.¹⁸⁶ Auch hier wird mit anderen Worten die *Verschiebung zum Kapitalmarkt* betont, wo sich sodann neue Anbieter um kapital anbietende und kapitalsuchende Marktteilnehmer kümmern.¹⁸⁷

Nach dem vorliegenden Verständnis wird unter Disintermediation der *vollständige Verzicht* auf traditionelle Finanzintermediäre durch die Marktteil-

¹⁸⁴ Siehe v.a. Rennig, Finanztechnologische Innovationen, 119–137 m.w.N.

¹⁸⁵ Siehe Müller, in: Boemle et al., Desintermediation, 306; in Bezug auf die Vermögensverwaltung Sethe, Anlegerschutz, 351–353.

¹⁸⁶ So Nobel/Zimmermann, in: Möslein, Finanzinnovationen, 69 FN 58.

¹⁸⁷ Siehe Bernet, Finanzintermediation, 54; Achleitner, Investment Banking, 62; ferner auch Staub, GesKR 2009, 500; ähnlich Banks, Dictionary of Finance, 159; Smullen/Hand, Dictionary of Finance, 118.

nehmer verstanden.¹⁸⁸ Anstelle des Einschlebens eines Zwischenglieds in eine wirtschaftliche Produktions- oder Austauschhandlung kommt es zur Eliminierung solcher Glieder aus bestehenden finanzintermediären Prozessen und Strukturen. In der Informatik wird vom Ersatz vertrauenswürdiger Instanzen durch computergestützte Verfahren gesprochen.¹⁸⁹ Anbieter und Nachfrager von Finanzkontrakten stehen am Ende dieser Entwicklung in einer beschränkt unmittelbaren Produktions- und Austauschbeziehung. Die Beziehung ist insoweit lediglich *beschränkt* unmittelbar, als dass sie noch von den Leistungen eines Computernetzwerks abhängig ist.¹⁹⁰

	Disintermediation
Definition	Marktteilnehmer verzichten im Zusammenhang mit der Organisation der Produktion und des Austausches von Finanzkontrakten und Finanzinformationen vollständig auf Finanzintermediäre.

Das FINANCIAL STABILITY BOARD (FSB) spricht in diesem Zusammenhang von «decentralised financial technologies». Das FSB scheint implizit Disintermediation mit Dezentralisierung gleichzusetzen.¹⁹¹ Vorliegend werden die beiden Konzepte allerdings *auseinandergehalten*: Demnach beschreibt Disintermediation den vollständigen Verzicht auf traditionelle intermediäre Prozesse und Strukturen, während Dezentralisierung die Verteilung von Entscheidungsgewalt und Kontrolle über ein System auf mehrere voneinander unabhängige Personen meint.¹⁹² Oder anders gewendet: Disintermediation ist eine Bedingung für die Dezentralisierung eines Systems.

3.2 Beispiele von Disintermediation

Das Aufkommen der Finanzintermediation ist, wie oben festgestellt, v.a. eine Reaktion der Marktteilnehmer auf die Unvollkommenheiten des Marktes. Falls effizientere und kostengünstigere Transaktionen ohne oder mit weniger Finanzintermediären möglich sind, ist zu erwarten, dass Finanzintermediäre an

¹⁸⁸ GLM. wohl Jacquemart, Offene Blockchainsysteme, Rz. 329, 332 («vollständig oder teilweise zu ersetzen»).

¹⁸⁹ Vgl. Bonneau et al., Proceedings 2015 IEEE Symposium on Security and Privacy, 118 («We use the term *disintermediation* to refer to the general process of designing transactions that remove the need for a trusted intermediary.»).

¹⁹⁰ Vgl. zur netzwerkbasierten Intermediation in dezentralen Systemen unten, [II.5](#).

¹⁹¹ Siehe FSB, Decentralised financial technologies, 2 FN 7.

¹⁹² Siehe hierzu oben, [II.1.5](#).

Relevanz einbüßen.¹⁹³ Die Finanzintermediation ist darum einem stetem Wandel von Intermediation, Disintermediation und Reintermediation (siehe hierzu später) unterworfen, wobei seit Aufkommen von Informations- und Kommunikationstechnologien eine sinkende Bedeutung traditioneller Finanzintermediäre beobachtbar ist.¹⁹⁴

a. Asset Securitization

Disintermediation wurde lange als Ausfluss von Finanzinnovation betrachtet. Seit den 1970er Jahren wird die finanzintermediäre Transformation von Kapital und Risiken aufgrund neuartiger Verbriefungstechniken zunehmend von den Kapitalmärkten selbst übernommen, ohne dass dafür auf Banken zurückgegriffen werden muss (sog. *Asset Securitization*).¹⁹⁵ Kreditrisiken werden dabei nicht mehr ausschliesslich von Banken, sondern vermehrt durch andere Marktteilnehmer refinanziert. Die dabei zur Anwendung gelangenden Vorgänge des Originate-to-Distribute-Geschäftsmodells gelten als komplex, bedürfen Kreditverbriefungen doch des Zusammenspiels einer *Vielzahl* von Akteuren, die den Verbriefungs- und Risikobewertungsprozess begleiten.¹⁹⁶ In der globalen Finanzkrise von 2007-08 spielten v.a. Finanzinnovationen in den Bereichen der Verbriefung von Hypothekarforderungen und anderen Vermögenswerten durch das Schattenbankensystem und der Herausgabe von Kreditausfallversicherungen durch Banken eine bedeutende Rolle.¹⁹⁷

Diese Form der Disintermediation, die überwiegend den Banken- und Versicherungsbereich betrifft, hat zu einer zunehmenden Verwischung der Grenzen zwischen Kredit- und Kapitalmarkt geführt.¹⁹⁸ Die Verbriefung von ursprünglich wenig liquiden Finanzkontrakten begründet die Handelbarkeit dieser Ansprüche an

¹⁹³ Vgl. Achleitner, *Investment Banking*, 53; ferner Bernet, *Finanzintermediation*, 174–175.

¹⁹⁴ Siehe Bernet, *Finanzintermediation*, 167.

¹⁹⁵ Siehe Kielholz, *Trend zur Disintermediation*.

¹⁹⁶ Siehe Mishkin/Eakins, *Financial Markets*, 489–490; Avgouleas, *Global Financial Markets*, 41–43, siehe auch die aufschlussreiche Grafik zu *Asset-Backed Securities (ABS)*, 44; Hastenpflug, *Securitizationsphänomen*, 18–42; ferner Schwarcz, *Cornell Law Review* 2016, 116–117.

¹⁹⁷ Ausführlich zum Einsatz dieser Finanzinstrumente in der Finanzkrise WEF, *Rethinking Financial Innovation*, 24–31; vgl. zur Abgrenzung von sog. *Asset-Backed Securities (ABS)*, *Collateralized Debt Obligations (CDOs)* und *Credit Default Swaps (CDS)* Wierichs/Smets, *Lexikon*, 11, 49, 51.

¹⁹⁸ Siehe Giovanoli, *SZW* 1999, 132–133; Zobl/Kramer, *Kapitalmarktrecht*, Rz. 3; Sethe/Lehmann, in: Tietje/Nowrot, § 15 Rz. 2 FN 7.

einem Sekundärmarkt.¹⁹⁹ Im Ergebnis führt dies anstelle einer bilanz- bzw. bankorientierten zu einer kapitalmarktorientierten Finanzintermediation,²⁰⁰ wobei die Verbriefungsmechanik und deren Akteure funktionell an die Stelle der traditionellen Finanzintermediäre treten.²⁰¹ Entsprechend definiert das FSB «Shadow Banking» als «the system of credit intermediation that involves entities and activities outside the regular banking system».²⁰² Es handelt sich darum lediglich oberflächlich um Disintermediation im oben beschriebenen Sinne.

b. Crowdfunding bzw. Peer-to-Peer-Lending

Ein weiteres Beispiel der Disintermediation hat sich in den letzten Jahren aufgrund der Einsatzmöglichkeiten des Internets entwickelt: *Crowdfunding* bzw. *Peer-to-Peer-Lending*.²⁰³ Dabei übernehmen Internetplattformen in aller Regel die Rolle der Vermittlerin von Geldern zwischen Investoren und Unternehmen.²⁰⁴ Diese Plattformen üben jedoch keine klassische Banktätigkeit aus, weshalb ihr Geschäftsmodell typischerweise die mit dem Zinsdifferenzgeschäft verbundenen Liquiditäts- und Zinsrisiken nicht aufweist.²⁰⁵

In der Schweiz bedurfte es allerdings einer Anpassung des Bankenrechts, hätten doch sonst Anbieter solcher Dienstleistungsplattformen in vielen Fällen eine Bankbewilligung benötigt.²⁰⁶ Besonders relevant für Crowdfunding-Geschäftsmodelle war die Ausdehnung der Frist auf 60 Tage für die Entgegennahme der für den Empfänger bestimmten Geldmittel und deren vorübergehende Aufbewahrung auf Abwicklungskonten des Finanzintermediärs. Solche Habensaldi auf Kundenkonten des Finanzintermediärs, die einzig der Abwicklung von Kundengeschäften dienen, qualifizieren dann nicht als bankenrechtlich relevante Einlagen, wenn für sie kein Zins bezahlt wird.²⁰⁷ Alternativ kann

¹⁹⁹ Siehe Achleitner, *Investment Banking*, 65; Fabozzi/Modigliani/Jones, *Financial Markets*, 537.

²⁰⁰ Siehe zur Unterscheidung dieser beiden Intermediationssysteme Bernet, *Finanzintermediation*, 45–48.

²⁰¹ Siehe Fabozzi/Modigliani/Jones, *Financial Markets*, 536–537; ferner Hügle, *Finanzsysteme*, 77–78, der zwischen bank- und marktbasierter Finanzintermediation unterscheidet.

²⁰² Siehe FSB, *Shadow Banking*, 3.

²⁰³ Ausführlich Rennig, *Finanztechnologische Innovationen*, 180–187.

²⁰⁴ Siehe Günther/Riethmüller, *Crowdfunding*, 1–3; Burton, in: Dresner, *Crowdfunding*, 157–158; Gullifer/Payne, *Corporate Finance Law*, 32.

²⁰⁵ Statt vieler Leimgruber/Flückiger, *Jusletter* vom 6. November 2017, Rz. 4–5; vgl. zur Rolle der Kreditrisikotransformation von Geschäftsbanken Adrian/Heidorn, *Bankbetrieb*, 6–11.

²⁰⁶ Vgl. zu den Gründen beim *Crowdlending* statt vieler Reiser, *AJP* 2018, 812–813.

²⁰⁷ Art. 5 Abs. 3 lit. c BankV; ferner FINMA-RS 08/3 «Publikumseinlagen bei Nichtbanken», Rz. 16; ausführlich zur Revision EFD, Änderung der Bankenverordnung (Fintech), 13, 22.

die Plattformbetreiberin bei unverzinslichen Crowdfunding-Beträgen von bis zu 1 Mio. Franken vom *Sandbox*-Regime profitieren, wobei sie den Investoren gegenüber eine Informationspflicht trifft.²⁰⁸

Anders als bei der Verbriefung von Krediten und deren Emission am Kapitalmarkt führt das Crowdfunding effektiv zum Wegfall der Rolle von Banken im Bereich der Kreditvermittlung.²⁰⁹ Jedoch tritt an deren Stelle mit der Betreiberin der Internetplattform eine neue Intermediärin.²¹⁰ Auch in diesem Fall handelt es sich darum gerade nicht um Disintermediation nach vorliegendem Verständnis.²¹¹

c. Robo-Advice

Robo-Advice kann als softwaregestützte Anlageberatung oder Vermögensverwaltung definiert werden, bei welcher ein Computer auf Basis der vom Kunden eingegebenen Informationen und einer anschliessenden Analyse dieser Inputdaten eine Anlageempfehlung abgibt oder eine Anlagestrategie entwickelt und diese sodann in aller Regel umsetzt.²¹² Dabei werden unterschiedliche Grade der Automatisierung unterschieden.²¹³

Zwar sehen die heute angebotenen Robo-Advice-Geschäftsmodelle in den meisten Fällen noch eine menschliche Intervention in der einen oder anderen Form im Beratungs- und Vermögensverwaltungsprozess vor.²¹⁴ Doch erscheint es absehbar, dass die technologischen Fortschritte zu einer weiteren Automatisierung in Form der «Algorithmisierung» führen werden, sodass die histori-

²⁰⁸ Art. 6 Abs. 2 BankV; hierzu FINMA, Faktenblatt Crowdfunding, 1–2.

²⁰⁹ Siehe Werlen/Hertner, in: Gschwend et al., Crowdfunding, 325, die von einer «markt-basierten Finanzierungsmethode» sprechen.

²¹⁰ Siehe etwa Alt/Puschmann, Digitalisierung der Finanzindustrie, 95; Hettich, GesKR 2013, 392; Kunz, Jusletter vom 25. August 2014, Rz. 8; von der Crone/Projer, in: Gericke, Crowdfunding, 23–24; Spacek, sic! 2013, 279; Reichmuth/von der Crone, SZW 2017, 259; Ancelle/Fischer, Jusletter vom 22. Februar 2016, Rz. 4; nach Rolle der Plattformbetreiberin differenzierend Poskriakov, Jusletter vom 13. März 2017, Rz. 13–15; insb. in geldwäschereirechtlicher Hinsicht Schneuwly, AJP 2014, 1624–1626; ebenso Essebier/Auf der Maur, Jusletter vom 28. September 2015, Rz. 18; spezifisch hinsichtlich Crowdinvesting Baumann, Crowdinvesting, Rz. 2; ferner Maizar/Kühne, in: Reutter/Werlen, Crowdinvesting, 92–93.

²¹¹ Vgl. die Hinweise bei Fritschi, Crowdfunding, Rz. 91 m.w.H.

²¹² Vgl. Weber/Baisch, AJP 2016, 1066–1067, welche die Vermögensverwaltung allerdings als «Robo-Portfolio-Management» bezeichnen.

²¹³ Siehe etwa EFD, Änderung der Bankenverordnung (Fintech), 7; ferner van Gammeren, Robo-Advice, N 24–28.

²¹⁴ Siehe Iannarone, Chicago-Kent Law Review 2018, 152–153.

sche Konstante der Intermediation auch in den Bereichen der Anlageberatung und Vermögensverwaltung zunehmend aufgelöst wird. Autonom handelnde Robo-Advisors werden voraussichtlich gestützt auf intelligente Algorithmen die Rolle von Kundenberatern weitgehend obsolet machen.²¹⁵

d. DLT-Handelssysteme

Ein weiteres Beispiel entstammt der neuen Regulierung von Finanzmarktinfrastrukturen bei Einsatz von DLT im Bereich des Effektenhandels. DLT kann in doppelter Hinsicht Disintermediationseffekte aufweisen:

Einerseits lösen DLT-Handelssysteme eine *Konvergenz* im Bereich der Handels- und Nachhandelsinfrastrukturen aus.²¹⁶ Davon sind neben dem Handel namentlich die Abrechnung und Abwicklung von Effektingeschäften inkl. der Zahlungsseite sowie die zentrale Verwahrung der Vermögenswerte betroffen. Die heute eigens mit diesen Funktionen befassten Intermediäre werden bei Verwendung solcher Handelssysteme überflüssig.²¹⁷ Dies betrifft in der Terminologie des FinfraG einerseits Effektenabwicklungssysteme und zentrale Verwahrungsstellen, die je für sich oder zusammen einen Zentralverwahrer bilden, und andererseits Zahlungssysteme, nicht jedoch zentrale Gegenparteien.²¹⁸ Diese Konvergenz stellt im Grundsatz eine Abkehr von dem bisherigen Regime der Trennung der einzelnen Finanzmarktinfrastруктурfunktionen dar.²¹⁹

Andererseits soll der Handel von DLT-Effekten an DLT-Handelssystemen neu potenziell *allen Marktteilnehmern* offenstehen (vgl. Art. 73c Abs. 1 lit. e FinfraG). Damit können erstmals, worin ein Bruch mit der historischen Konstante des mitgliedschaftlichen Systems von Handelsplattformen gesehen werden kann,²²⁰ nicht nur Effekthändler bzw. Wertpapierhäuser unmittelbar an ei-

²¹⁵ Siehe für eine konzeptionelle Übersicht der in der Praxis zur Anwendung gelangenden Algorithmen Prantl, Robo Advice, N 17–21 m.w.N. Weniger weitgehend als hier demgegenüber Arslanian/Fischer, Future of Finance, 41.

²¹⁶ Siehe Botschaft DLT 2019, 272.

²¹⁷ Siehe FSB, Decentralised financial technologies, 5; ferner BIS/CPMI, Distributed ledger technology, 19; eine ausführliche Übersicht über die verschiedenen Funktionen findet sich bei Pinna/Ruttenberg, European Central Bank Occasional Paper Series Nr. 172, April 2016, 22–27, wobei nach Meinung der Autoren zumindest die «notary function» von Zentralverwahrern und die «clearing function» bei Derivatgeschäften notwendig bleiben.

²¹⁸ Siehe Botschaft DLT 2019, 311.

²¹⁹ Vgl. etwa IOSCO, Crypto-Asset Trading Platforms, 13, 24–25 m.w.H.

²²⁰ Siehe hierzu oben, [II.1.3](#).

nem organisierten Markt teilnehmen, sondern auch natürliche und juristische Personen ohne finanzmarktrechtlichen Bewilligungsstatus.²²¹

e. Central Bank Digital Currency (CBDC)

Schliesslich tangieren auch die Diskussionen um die Einführung von *Central Bank Digital Currency* (CBDC) neben Fragen der Finanzstabilität insb. die Thematik der Bankintermediation. Dies ist hauptsächlich auf den Umstand zurückzuführen, dass digitale Währungen, die unmittelbar von Zentralbanken herausgegeben werden, voraussichtlich in einen Wettbewerb mit Bankeinlagen als Zahlungsmittel treten würden.²²²

CBDCs sind anders als elektronisches Bankbuchgeld Forderungen gegen die Zentralbank. Sie sind damit mit gesetzlichem Zahlungsmittel in Form von Münzen und Banknoten vergleichbar.²²³ Dabei existieren im Wesentlichen zwei Arten von CBDC: Zentralbanken können solche entweder als Token über das bestehende Finanzintermediationssystem an die Endkunden herausgeben (*Wholesale*) oder unmittelbar Konten für die Endkunden führen (*Retail*).²²⁴

Zu den von CBDCs betroffenen Banktätigkeiten gehören in erster Linie die Entgegennahme von Depositen, die Vergabe von Krediten und der Zahlungsverkehr. Je nach Modellvorschlag konkurrieren CBDCs unmittelbar mit diesen Intermediationsfunktionen der Geschäftsbanken.²²⁵ Damit würden CBDCs allerdings auch das gesetzliche Privileg von Geschäftsbanken im heutigen Mindest- bzw. Teilreservesystem, Buchgeld quasi *ex nihilo* schöpfen zu können,²²⁶ infrage stellen.²²⁷

²²¹ Siehe Abegglen/Andreotti, GesKR 2020, 36 m.w.H.; ferner Botschaft DLT 2019, 272.

²²² Siehe Mancini-Griffoli et al., in: Brummer, Central Bank Digital Currency, 322.

²²³ Vgl. Art. 2 lit. a und b WZG.

²²⁴ Eine ausführliche Übersicht findet sich bei BIS/CPMI/MC, Central bank digital currencies, 5–7.

²²⁵ Siehe für eine Übersicht der Herausforderungen BIS/CPMI/MC, Central bank digital currencies, 14–17; ferner Mancini-Griffoli et al., IMF Staff Discussion Note, November 2018, 21–25.

²²⁶ Die Rechtsgrundlagen für die Mindestreservevorgaben befinden sich in Art. 17–18 NBG i.V.m. Art. 12–17 NBV; vgl. zur Geldschöpfungsfunktion von Banken Sturny, in: Kommentar NBG/WZG, Art. 17 NBG N 4. Kritisch bezüglich dieser Rolle von Geschäftsbanken aus rechtlicher Sicht Huerta de Soto, Money, 115–165, 706–712; aus volkswirtschaftlicher Sicht siehe etwa Fisher, 100% Money, 33–59.

²²⁷ Vgl. Dyson/Hodgson, Digital Cash, 29–30; ferner die Hinweise zu *Narrow Banking* und *Vollreservesystem* BIS/CPMI/MC, Central bank digital currencies, 16; eine gute Übersicht der unterschiedlichen Vorschläge findet sich zudem bei Niepelt, International Journal of Central Banking 2020, 213–216.

Schliesslich können CBDCs auch als Zahlungsmittel für die Zug-um-Zug-Abwicklung von Effektentransaktionen eingesetzt werden, was im Falle von Wholesale-CBDCs die traditionelle Finanzintermediation allerdings nicht negativ beeinträchtigen, sondern in erster Linie den Einsatz von zentralen Gegenparteien und den heutigen Nachhandelsinfrastrukturen obsolet machen würde.²²⁸ Aufgrund der schwer abschätzbaren Risiken für die Finanzintermediation und Finanzstabilität haben bedeutende Zentralbanken gewisse Mindeststandards formuliert.²²⁹

Hingegen ist heute davon auszugehen, dass die Liveversionen von CBDC nicht innerhalb von dezentralen Netzwerken herausgegeben werden, so dass zumindest in dieser Hinsicht von keinem oder einem sehr geringen Disintermediationseffekt auszugehen ist.²³⁰ Es ist ausserdem wahrscheinlich, dass CBDCs ganz auf Blockchain-Technologie verzichten, da es aufgrund der Tatsache, dass die Zentralbank als Emittentin fungiert, gar kein inhärentes Vertrauensproblem zu lösen gilt.²³¹ Davon geht korrekterweise auch der Bundesrat in seinem Bericht zu digitalem Zentralbankengeld aus.²³²

Die Öffentlichkeit betrachtet CBDCs regelmässig als blosser Weiterentwicklung von Kryptowährungen und Stablecoins, was aber aufgrund der verschiedenartigen Qualität der involvierten Emittenten, der Ausgabeparität von CBDCs zu bestehendem gesetzlichem Zahlungsmittel und der absehbar komplett unterschiedlichen technologischen Infrastruktur verfehlt ist.²³³ CBDCs sind in erster Linie eine Reaktion auf das Aufkommen von Stablecoins, wie allen voran das mit Facebook assoziierte Projekt *Libra*, das inzwischen in *Diem* umbenannt

²²⁸ Siehe BIS/SIX/SNB, Project Helvetia, 10–11, 18, 21–22, 23, 25; ausführlich Bech et al., BIS Quarterly Review März 2020, 74–75, ferner 78, 81–83, die jedoch die wichtige Rolle von Finanzintermediären, die Liquidität den Handelssystemen zuführen, betonen.

²²⁹ Siehe BIS, CBDC principles, 8, 16; ebenso ECB, digital euro, 16–18.

²³⁰ G.L.M. Geva, in: Brummer, Evolution, 35. Die Nutzung von offenen bzw. permissionless Blockchains war scheinbar von Anfang an umstritten; vgl. hierzu Bech/Garratt, BIS Quarterly Review September 2017, 58; Broadbent, Central banks and digital currencies, 6.

²³¹ G.L.M. Berentsen/Schär, Federal Reserve Bank of St. Louis Review 2018, 103–104; ferner Auer/Böhme, BIS Quarterly Review März 2020, 91–93; vgl. für einen konkreten Vorschlag Chaum/Grothoff/Moser, SNB Working Papers 3/2021, 3, welche für ihr CBDC-Design gänzlich auf DLT verzichten; a.M. Calle/Eidan, Central Bank Digital Currency, 13–15.

²³² Siehe Bundesrat, Bericht digitales Zentralbankengeld, 8.

²³³ Siehe zur Abgrenzung zwischen CBDCs und Stablecoins Arner/Auer/Frost, BIS Working Papers Nr. 905, November 2020, 5, 21–22; Dell’Erba, New York University Journal of Legislation and Public Policy 2019, 38–45; ausführlich zu unterschiedlichen CBDC-Designs Auer/Cornelli/Frost, BIS Working Papers Nr. 880, August 2020, 17–20.

wurde.²³⁴ Das ursprünglich in Genf angesiedelte Projekt wurde auf internationalen politischen Druck hin zuerst komplett überarbeitet und sodann aufgegeben.²³⁵ Am Beispiel von Libra bzw. Diem wird letztlich die machtpolitische Dimension im Geld- und Zahlungswesen gut sichtbar.²³⁶

Digitale Währungen von Zentralbanken sollen nach dieser Sichtweise die Funktion von privat emittierten, mit einer oder mehreren *Fiatwährungen* hinterlegten Stablecoins ersetzen. Der Fokus auf Fiat-Stablecoins ist wohl im Umstand begründet, dass diese sich geld- und fiskalpolitisch primär auf den Geldmarkt und dort insb. auf Repogeschäfte auswirken können. Demgegenüber nicht direkt betroffen sind voraussichtlich dezentral herausgegebene Stablecoins, welche entweder mit Kryptovermögenswerten hinterlegt sind oder deren Angebot algorithmisch stabilisiert ist.²³⁷

Die derzeitigen Diskussionen um die inhaltliche Ausgestaltung und Umsetzung von CBDCs scheinen in erster Linie geld- und fiskalpolitisch motiviert zu sein.²³⁸ Angesichts des langfristigen Null- und Negativzinsumfelds, das die herkömmliche Geldpolitik, die wesentlich auf Leitzinsen beruht, praktisch verunmöglicht,²³⁹ ist es nicht unwahrscheinlich, dass die eine oder andere Zentralbank CBDCs für Direktzahlungen an die Haushalte einer Volkswirtschaft

²³⁴ Siehe insb. G7 Working Group on Stablecoins, Stablecoins, iii («The G7 believes that no global stablecoin project should begin operation until the legal, regulatory and oversight challenges and risks outlined above are adequately addressed, through appropriate designs and by adhering to regulation that is clear and proportionate to the risks. That said, depending on the unique design and details of each stablecoin arrangement, approval may be contingent on additional regulatory requirements and adherence to core public policy goals.»); sodann FSB, Global Stablecoin Arrangements, 1–2.

²³⁵ Siehe FINMA, Diem zieht Bewilligungsgesuch zurück, *passim*; vgl. auch Zellweger-Gutknecht/Weber, Jusletter vom 11. Januar 2021, Rz. 1–2 m.w.H.

²³⁶ Vgl. auch Müller/Ong, AJP 2020, 204; ferner Weber, in: Gortsos/Sethe, Global Financial Architecture, 28–29, der festhält, dass der politische Währungswettbewerb innerhalb globaler CBDC-Netzwerke tendenziell zunehmen wird.

²³⁷ Vgl. für eine Übersicht der existierenden Projekte The Stablecoin Index, *passim*; ausführlich sodann die *Taxonomie* in Moin/Sekniqi/Gun Sirer, in: Bonneau/Heninger, Stablecoin Designs, insb. 177–178, 179.

²³⁸ Vgl. die Diskussion in Alloway/Weisenthal, Benoît Cœuré on Central Bank Digital Currencies, Odd Lots Podcast, *passim*.

²³⁹ Dies ist auf das sog. Zero Lower Bound (ZLB)-Konzept zurückzuführen, wonach weitere Zinssenkungen im Negativbereich zumindest solange nicht möglich sind, als die Bevölkerung Bargeldbezüge tätigen kann; vgl. hierzu etwa Bernanke, Deflation, *passim*; hinsichtlich der verschiedenen Möglichkeiten, die limitierende Rolle von Bargeld einzuschränken, siehe sodann Rogoff, Journal of Economic Perspectives 2017, 57.

einsetzen könnte (sog. Helikoptergeld).²⁴⁰ Ähnliche geld- und fiskalpolitische Überlegungen werden schliesslich aufgrund der scheinbar verbreiteten Angst vor einer «Cryptoization» einzelner Nationalstaaten angestellt.²⁴¹

3.3 Technologische Innovation als Treiberin von Disintermediation

a. Digitalisierung und Intermediation

Wirtschaftshistorisch betrachtet hat technologische Innovation seit jeher die Prozesse und Strukturen der Gesellschafts- und Wirtschaftsordnung verändert, ja teils auf den Kopf gestellt.²⁴² Von einem eigentlichen Zeitalter bzw. Paradigma der Informationstechnologie wird seit der Erfindung des modernen Computers Mitte des letzten Jahrhunderts und spätestens mit der Verbreitung des Internets und Webs gesprochen. Innovation scheint nunmehr überwiegend digital zu sein oder wird zumindest durch digitale Verfahren ermöglicht.²⁴³ Die digitale Wettbewerbsfähigkeit eines Unternehmens ist heute wesentlich für den langfristigen Geschäftserfolg verantwortlich.²⁴⁴

Die Digitalisierung hat auch einen massgeblichen Einfluss auf den Grad und die Struktur der Intermediation und dadurch auf die Marktstrukturen. Technologie hat insb. die persönlichen und räumlichen Distanzen zwischen den Menschen verkürzt. Wenn immer möglich und opportun, verzichtet Technologie auf nicht notwendige intermediäre Prozesse und Strukturen. Das Internet ermöglicht etwa den unmittelbaren Informationsaustausch zwischen Computern, ohne dass es eines Medienhauses, einer Druckerei oder eines Postbe-

²⁴⁰ Vgl. zum parabelähnlichen, theoretischen Konstrukt des Helikoptergelds Friedman, *Quantity of Money*, 4–7, der darin indessen keinen Politikvorschlag sah.

²⁴¹ Vgl. IMF, *Crypto Ecosystem*, insb. 52.

²⁴² Am bekanntesten ist wohl Joseph A. Schumpeters Konzept der schöpferischen Zerstörung bzw. *creative destruction*; siehe hierzu Schumpeter, *Capitalism*, 83 («*This process of Creative Destruction is the essential fact about capitalism. It is what capitalism consists in and what every capitalist concern has got to live in.*»); heute spricht die Managementliteratur demgegenüber von *disruptiven Technologien*; vgl. hierzu Christensen, *The Innovator's Dilemma*, xvii–xx.

²⁴³ Siehe Castells, *Information Age*, 38–39, 69–76 m.w.N.; ferner Gilder, *Knowledge and Power*, 13–14, 29–30, der aus der gesellschaftlichen Bedeutung der Informationstechnologie die Entstehung einer *information economy* ableitet; schliesslich von einem «*techno-economic paradigm*» ausgehend Perez, *Cambridge Journal of Economics* 2010, 194–195.

²⁴⁴ Vgl. etwa bereits Porter, *Competitive Advantage*, 166–176.

triebes für die Erstellung und den Versand der Informationsträger bedürfte. Allerdings ist das Internet nicht gänzlich frei von Intermediären: An die ursprüngliche Stelle von Offline-Intermediären sind nunmehr neue Intermediäre getreten, allen voran Fernmeldediensteanbieter (*Telecommunications Service Provider*, TSPs), Internetdienstleister (*Internet Service Providers*, ISPs) und Online-Dienstleistungserbringer, wie beispielsweise Suchmaschinen, soziale Netzwerke und Cloudservices, deren Angebote für die Nutzung des Internets als Infrastruktur zentral geworden sind und deren Position als Mittelmänner ihnen die faktische Kontrolle über die Datenströme einräumt.²⁴⁵ Online- bzw. Internet-Intermediäre, wie diese Rollen teilweise bezeichnet werden, bringen Anbieter von und Nachfrager nach digitalen Informationen näher zusammen.²⁴⁶ Dies kann weitreichende Konsequenzen für die Einordnung von Internet-Intermediären in den regulatorischen Rahmen haben.²⁴⁷ Das Internet in seiner heutigen Form weist damit einen ausgeprägten Grad an personaler und institutioneller Intermediation auf.²⁴⁸

b. FinTech im Allgemeinen

Die Finanzintermediation ist historisch – und nicht erst seit dem Aufkommen des Begriffs der Financial Technology (FinTech) – besonders von technologischer Innovation betroffen.²⁴⁹ Unter *FinTech* wird gemeinhin «[...] *technology-enabled innovation in financial services that could result in new business mo-*

²⁴⁵ Siehe etwa Riordan, *Internet Intermediaries*, N 2.40–2.86; Gasser/Schulz, *Governance of Online Intermediaries*, 1 («a new type of powerful institution»); kritisch gegenüber einer klaren Rollenverteilung zwischen Mittelmännern und Endpunkten im Internet Zittrain, *Future of the Internet*, 167.

²⁴⁶ Siehe OECD, *Internet Intermediaries*, 9, 37.

²⁴⁷ Ausführlich hierzu die Beiträge von Eifert, in: Eifert/Gostomzyk, *Netzwerkdurchsetzung*, *passim*; Wielsch, in: Eifert/Gostomzyk, *Ordnungen der Netzwerke*, *passim*; ferner Belli/Sappa, *Journal of Intellectual Property, Information Technology and E-Commerce Law* 2017, *passim*; Mansell, *info* 2015, *passim*.

²⁴⁸ Vgl. allerdings die Ausführungen zum Web 3.0 unten, [II.4.3b](#).

²⁴⁹ Eine historische Übersicht des jahrhundertelangen Einsatzes von Technologie im Finanzsektor findet sich bei Arner/Barberis/Buckley, *University of New South Wales Law Research Series* 2016, Nr. 62, 19. Dezember 2019, 4–20; ferner Alt/Puschmann, *Digitalisierung der Finanzindustrie*, 36–40; Jutzi/Abbühl, *Fintech und DLT*, Rz. 1–5; ausführlich zur *historischen Permanenz* der Finanzinnovation Möslin, in: Möslin, *Finanzinnovation und Rechtsordnung*, 6–8. Kritisch demgegenüber Bernet, *Finanzintermediation*, 67–68, der von einem tiefen Grad echter Finanzinnovation seit den 1980er Jahren ausgeht; ferner Perez, *Technological Revolutions*, 110.

dels, applications, processes or products with an associated material effect on the provision of financial services [...]» verstanden.²⁵⁰ Die Definition zeigt die Heterogenität der möglichen FinTech-Geschäftsmodelle.²⁵¹

Da die Finanzindustrie und ihre Produkte bereits nahezu vollständig informationsbasiert sind und somit keiner weiteren Übersetzung der Informationen von der analogen in die digitale «Sprache» bedürfen, wirken sich insb. Fortschritte in der Informationstechnologie grundlegend auf die Finanzintermediation aus.²⁵² Die Finanzintermediation profitiert überdurchschnittlich von tieferen Informations- und Transaktionskosten aufgrund von technologischer Innovation.²⁵³ Die BIS hat diesen Trend bereits in einem Bericht aus dem Jahr 1986 aufgearbeitet.²⁵⁴ Der Einsatz moderner Kommunikationsmittel hat die persönlichen und räumlichen Distanzen zwischen den Marktteilnehmern verkürzt. In der Folge kam es zur Globalisierung des Handels mit Finanzinstrumenten.²⁵⁵

In der ökonomischen Theorie werden diese Entwicklungen aus dem Blickwinkel von Effizienzverbesserungen betrachtet.²⁵⁶ Die gesteigerte Fähigkeit der Märkte, preisrelevante Informationen risiko- und renditeadjustiert verarbeiten zu können, liegt in erster Linie im Aufkommen dichter und schneller Kommunikationsnetzwerke begründet (informationelle Effizienz).²⁵⁷ So dann konnten Transaktionshindernisse abgebaut werden, indem der Zugang von Emittenten und Anlegern zu inländischen und ausländischen Märkten verbessert wurde (operationelle Effizienz). Schliesslich haben technisch zuverlässige Computersysteme die Nutzung des Marktmechanismus für die Marktteilnehmer vereinfacht (institutionelle Effizienz). Es ist darum anzunehmen, dass der Einsatz von Technologie die Allokationseffizienz der Kapitalmärkte in den letzten Jahrzehnten stark erhöht hat. Hinzu kommt die Konvergenz unter-

²⁵⁰ FSB, Financial Stability Implications FinTech, 7; ferner, jedoch produktspezifischer IOSCO, Fintech Report, 4; sodann Schueffel, Journal of Innovation Management 2016, 45; Walker, The International Lawyer 2017, 140–142.

²⁵¹ Siehe Schilling de Carvalho, Journal of Financial Regulation 2022, 117 m.w.H.

²⁵² Siehe Alt/Puschmann, Digitalisierung der Finanzindustrie, 36.

²⁵³ Siehe etwa Bernet, Finanzintermediation, 145, 150–151, 152.

²⁵⁴ Siehe BIS, Recent Innovations, 8, 181–182.

²⁵⁵ Siehe Sethe/Lehmann, in: Tietje/Nowrot, § 15 Rz. 4; Kaplan, in: Berg Olsen/Pedersen/Hendricks, Technology and Globalization, 327; vgl. ferner für die jüngeren Entwicklungen an den US-amerikanischen Kapitalmärkten Brummer, Fordham Law Review 2015, 1020–1035.

²⁵⁶ Für eine Übersicht der unterschiedlichen Markteffizienztypen siehe Zobl/Kramer, Kapitalmarktrecht, Rz. 12–18 m.w.N.; ferner Andreotti, Produktverbote, 2–4 m.w.N.

²⁵⁷ Siehe Achleitner, Investment Banking, 69–70; ferner Bernet, Finanzintermediation, 70.

schiedlicher datengetriebener Innovationen, wie etwa Smartphones, Big Data, Cloud Computing, DLT, IoT und AI, was umso radikalere Umwälzungen in der Finanzindustrie auslösen kann.²⁵⁸

Diese Entwicklungen zeitigen entsprechende Konsequenzen für die traditionelle Finanzintermediation, indem es zu Verschiebungen der Aktivitäten von Banken und Versicherungen zu Kapitalmärkten und anderen Anbietern, die v.a. aus dem IT-Bereich stammen, kommt. Dies führt zur Aufspaltung traditioneller integrierter Wertschöpfungsketten der Finanzintermediation und in der Folge zur Ausbildung von neuen «Wertschöpfungsnetze[n]».²⁵⁹ BERNET spricht deshalb von «Finanzintermediationsnetzwerke[n]», welche dynamisch, komplex, kooperativ und zumindest temporär stabil seien.²⁶⁰ Die eigentlichen Aktivitäten und ökonomischen Funktionen – d.h. etwa der Geldkredit oder die Versicherung von Risiken – verschwinden dabei nicht, sie wechseln aber unter Umständen ihre Form sowie die Art und Weise der Präsentation.²⁶¹ Die finanzwirtschaftlichen Funktionen scheinen also stabiler zu sein als die *in praxi* bestehenden Institutionen.²⁶²

Allerdings können technologische Entwicklungen Disintermediationseffekte aufweisen, welche die allokative Funktion der Kapitalmärkte zumindest aus einer Makroperspektive zu beeinträchtigen drohen: Grundlegend veränderte regulatorische Bedingungen sowie die rasante Verbesserung der elektronischen Kommunikationsmittel nach der Jahrtausendwende haben etwa zu einer zunehmenden *Fragmentierung des Handels* an den etablierten Handelsplätzen beigetragen. An die Stelle einiger weniger traditioneller Wertpapierbörsen ist eine Vielzahl alternativer Handelssysteme getreten, welche die Entwicklung computerbasierter, algorithmischer Handelsstrategien und des Hochfrequenzhandels begünstigt haben. Diese Handelsinnovationen haben sodann ihrerseits das Aufkommen

²⁵⁸ Vgl. zum Konzept der Konvergenz inkrementeller Innovationen Hacklin/Raurich/Marxt, *Technological Convergence*, *passim*. Bei dezentralen Systemen handelt es sich nach vorliegender Auffassung nicht bloss um eine inkrementelle, sondern um eine disruptive Innovation; *gl.M.* wohl Puschmann/Weber, SZW 2017, 83, 94; ferner Weber, SZW 2018, 684, 686, 691, 694. Vgl. ferner hinsichtlich des Rechtsrahmens beim Einsatz künstlicher Intelligenz in der Finanzindustrie Stengel/Wirthensohn/Stäuble, SZW 2021, *passim*.

²⁵⁹ So bereits Bernet, *Finanzintermediation*, 144, ferner 142, 149, 173–176; ausführlich hinsichtlich veränderter Marktstrukturen im Finanzsektor FSB, *FinTech and market structure*, 5–10; ferner Liebenberg, *Electronic Financial Markets*, 39, die von «networked financial 'supermarkets'» spricht.

²⁶⁰ Siehe Bernet, *Finanzintermediation*, 174.

²⁶¹ Siehe Lin, *Wake Forest Law Review* 2015, 654–655, 658; ferner Schaefer, *FINMA im Fin-tech-Bereich*, 2.

²⁶² So auch Bodie/Merton/Cleeton, *Financial Economics*, 26.

alternativer Plattformen verstärkt.²⁶³ Ausserbörsliche Handelssysteme haben im Ergebnis die konzeptionelle Trennung zwischen Handelsplätzen und Intermediären zunehmend aufgeweicht.²⁶⁴

Die Fragmentierung kann die positiven Externalitäten zentralisierter Marktstrukturen etwa in den Bereichen der Risikoverteilung und Marktliquidität verringern.²⁶⁵ Institutionelle Anleger nutzen die auch als sog. *Dark Pools* bezeichneten Handelssysteme, um die Vertraulichkeit ihrer Handelsgeschäfte zu schützen, was allerdings die effiziente Preisfindung an etablierten Handelsplätzen für die übrigen Marktteilnehmer erschweren kann.²⁶⁶

In der Schweiz sieht der Gesetzgeber seit der Einführung des FinfraG im Jahr 2015 für die Mehrzahl solcher privater Wertpapiermärkte die Bewilligungsformen des multilateralen Handelssystems (MHS) sowie insb. des organisierten Handelssystems (OHS) vor.²⁶⁷ Während MHS grundsätzlich von einer separaten juristischen Entität zu betreiben sind,²⁶⁸ setzt der Betrieb eines OHS die Bewilligung als Finanzintermediär voraus.²⁶⁹ Der Bundesrat hat den Betreibern von OHS teilweise Vor- und Nachhandelstransparenzregeln auferlegt, damit die Preisfindung an den traditionellen Handelsplätzen sichergestellt ist.²⁷⁰

Technologische Entwicklungen, darunter auch Einzelereignisse wie der *Flash Crash* vom Mai 2010, wurden generell von den Gesetzgebern und Aufsichtsbehörden kritisch beobachtet. Seit der Finanzkrise 2007-08 ist zudem eine von den USA ausgehende regulatorische Erfassung von Risiken moderner Technologien, v.a. im Bereich von Handelsalgorithmen, feststellbar.²⁷¹

²⁶³ Siehe Zimmermann, in: Strebel-Aerni, Umbruch, 97–100, 120–122; ferner in Bezug auf die USA Brummer, *Fordham Law Review* 2015, 997–1020; zum komplexen Zusammenhang zwischen Hochfrequenzhandel und der Fragmentierung der Märkte sowie deren Liquidität Contratto, *GesKR* 2014, 146, 147–148; ausführlich zur Rolle des *Hochfrequenzhandels* Monsch, *Hochfrequenzhandel*, 327–331 m.w.N.; eine *historische* Darstellung des Hochfrequenzhandels findet sich bei Gesser, *Praxishandbuch Hochfrequenzhandel*, 25–48.

²⁶⁴ So bereits Maurenbrecher, *AJP* 2005, 25.

²⁶⁵ Siehe Foucault/Pagano/Röell, *Market Liquidity*, 238–239.

²⁶⁶ Siehe Foucault/Pagano/Röell, *Market Liquidity*, 236; zu den Chancen und Risiken von *Dark Pools* Baisch/Baumann/Weber, *GesKR* 2014, 191–194; kritisch sodann Nobel/Zimmermann, in: Möslin, *Finanzinnovationen*, 78–89, 83.

²⁶⁷ Siehe Botschaft *FinfraG* 2014, 7499, 7530.

²⁶⁸ Vgl. Art. 10 Abs. 1 *FinfraG*

²⁶⁹ Art. 43 *FinfraG*.

²⁷⁰ Art. 46 *FinfraG* i.V.m. Art. 42–43 *FinfraV*. Zum Ganzen ausführlich Humbel, Vor- und Nachhandelstransparenz, *passim*; sodann kritisch zur heutigen Regelung der Vorhandelstransparenzpflichten von OHS-Betreiberinnen Humbel *GesKR* 2021, 34–38.

²⁷¹ Ausführlich Hess, *Penn State Law Review* 2024, 14–23.

c. FinTech 3.0

FinTech befindet sich seit der Finanzkrise von 2007–08 bereits in der dritten Iteration. DOUGLAS ARNER, JÁNOS BARBERIS und ROSS P. BUCKLEY erwarten von dieser sog. *FinTech 3.0-Phase* die Demokratisierung der Finanzwelt.²⁷² Darunter wird einerseits verstanden, dass sich der Kreis der Anbieter von Finanzdienstleistungen verbreitert. Andererseits soll das Finanzsystem ganz grundsätzlich unmittelbarer, transparenter und zugänglicher werden. Es geht mit anderen Worten um den allgemeinen Zugang zu Märkten und Dienstleistungen sowie den Abbau von Informationsasymmetrien.²⁷³ Vermehrt drängen technologieaffine Unternehmen aufs Finanzparkett und bieten ihre Dienstleistungen direkt den Kunden an, ohne auf einen Finanzintermediär zurückzugreifen. FinTech-Innovationen erlauben darum gänzlich neue Geschäftsmodelle, weshalb der ehemalige FINMA-Direktor und jetzige Präsident der BaFin MARK BRANSON von «Banking ohne Intermediation, Banking ohne Banken» spricht.²⁷⁴

Hierzu sind nach vorliegender Ansicht auch Anbieter von privat herausgegebenen Stablecoins, die mit Fiatwährungen und kurzfristigen Wertschriften hinterlegt sind, zu zählen. Die Unternehmen hinter *Tether*, *USD Coin* oder *Paxos* üben durch die Herausgabe vollgedeckter digitaler Zahlungsmittel eine Tätigkeit aus, die an die Prinzipien des *Narrow Bankings* erinnert. Zwar bieten die Anbieter von Stablecoins ihren «Kunden» keine Kontoführung an, doch sie leihen die hinterlegten Vermögenswerte aktivseitig nicht aus, sondern halten sie in möglichst liquider Form u.a. auf Bankkonten, die auf ihren Namen lauten.²⁷⁵

²⁷² Siehe Arner/Barberis/Buckley, University of New South Wales Law Research Series 2016, Nr. 62, 19. Dezember 2019, 15; ebenso Blair, Journal of International Banking Law and Regulation 2020, 173–174; ferner Mauchle, SZW 2017, 810–830, 811; insb. bezüglich Crowdfunding Kunz, Jusletter vom 25. August 2014, Rz. 7; Hettich, GesKR 2013, 386, 391–392; so bereits Shiller, Financial Analysts Journal 2013, 22; allgemein zum Demokratisierungsgedanken Shiller, Finance and the Good Society, *passim*.

²⁷³ Siehe Arner/Barberis/Buckley, University of New South Wales Law Research Series 2016, Nr. 62, 19. Dezember 2019, 15; Shiller, Finance and the Good Society, 231–240; Weber/Baisch, Journal of International Banking Law and Regulation 2018, 350; Sixt, Schwarmökonomie und Crowdfunding, 19.

²⁷⁴ Branson, Fintech und Negativzinsen, 9.

²⁷⁵ Siehe etwa Dell’Erba, New York University Journal of Legislation and Public Policy, 9, 10–11; ferner zum Konzept des *Narrow Banking* Friedman, in: Ketchum/Kendall, Monetary Stability, *passim*.

Mit FinTech werden darüber hinaus einzel- und gesamtwirtschaftliche Effizienzsteigerungen verbunden, die letztlich zu mehr Wettbewerb und somit Kosteneinsparungen bei den Anbietern und deren Kunden führen sollen.²⁷⁶ So hat auch das Bundesgericht die volkswirtschaftliche Bedeutung innovativer Zahlungssysteme in einem Urteil aus dem Jahr 2015 betont.²⁷⁷

d. Ausbleiben vollständiger Disintermediation

Technologische Innovation hat in der Vergangenheit praktisch in keinem Fall zu einer vollständigen Disintermediation von Finanzintermediären geführt.²⁷⁸ Im Gegenteil kann historisch eher von gegenläufigen Bewegungen zwischen Intermediation, Disintermediation und Reintermediation gesprochen werden.²⁷⁹ Disintermediation im Sinne des Verzichts auf Finanzintermediäre wird zudem selten als ein Teil der sich im Gang befindenden FinTech-Entwicklungen betrachtet.²⁸⁰ LIN spricht darum von der «mirage of financial disintermediation», wonach Technologie in der Vergangenheit lediglich zur Substitution und teilweise sogar zur Addition neuer Intermediäre geführt habe.²⁸¹

Demgegenüber werden dezentrale Systeme nicht von traditionellen Finanzintermediären unterhalten. Der Verzicht auf solche Intermediäre ist bereits im Design dieser Netzwerke angelegt.²⁸² Die vorliegende Arbeit spricht von netzwerkbasierter Intermediation.²⁸³ Die Eliminierung bestehender intermediärer Prozesse und Strukturen könnte nochmals zu weit grösseren Kosteneinsparungen und in der Folge zu einer nochmals verbesserten allokativen Effizienz sowohl für den Einzelnen als auch für die Allgemeinheit führen. Zudem, worauf

²⁷⁶ Siehe Frost, BIS Working Paper Nr. 838, Februar 2020, 6–7 m.w.N.; Alt/Puschmann, Digitalisierung der Finanzindustrie, 22, 33–31; Puschmann/Weber, SZW 2017, 83–84; Branson, Fintech and Blockchain, 2 m.w.H.; Arner/Barberis/Buckley, University of New South Wales Law Research Series 2016, Nr. 62, 19. Dezember 2019, 40; Weber, SZW 2018, 686; ausführlich bereits Bernet, Finanzintermediation, 149–164, 167–171.

²⁷⁷ Siehe BGer 2C_345/2015 vom 24. November 2015, E. 4.2 m.w.H.

²⁷⁸ GLM. Lin, Wake Forest Law Review 2015, 655, der von «infinite financial intermediation» spricht; Harvey/Ramachandran/Santoro, DeFi, 10–12.

²⁷⁹ Vgl. hinsichtlich Marktstrukturen seit dem Mittelalter Donald, The Journal of Corporation Law 2018, 30–31 m.w.H.

²⁸⁰ Vgl. etwa Lehmann, Boston University International Law Journal 2020, 124; Weber/Baumann, FinTech, Jusletter vom 21. September 2015, Rz. 1, 6, 10; Flühmann/Hsu/Ender, GesKR 2017, 6.

²⁸¹ Siehe Lin, Wake Forest Law Review 2015, 657, der von «substitution» und «layering» bestehender finanzintermediärer Prozesse und Strukturen spricht.

²⁸² Dies scheinbar anerkennend Lin, Wake Forest Law Review 2015, 657.

²⁸³ Siehe unten, [II.5](#).

noch vertieft einzugehen ist, weisen *disintermediatisierte* Prozesse und Strukturen die Möglichkeit uneingeschränkter Partizipation der Marktteilnehmer auf. Der Zugang zu solchen Finanzdienstleistungen wird, um die oben eingeführte Terminologie aufzunehmen, weitgehend «demokratisiert».²⁸⁴ Demokratisierung wird im vorliegenden Kontext nicht in einem politikwissenschaftlichen Sinne verstanden, sondern als die Tatsache, dass die Öffentlichkeit an der technologischen Innovation unmittelbar partizipieren kann. Dies führt zur Herausbildung neuartiger Formen der *gemeinschaftlichen* Produktion informationstechnologischer Güter u.a. im Finanzbereich.²⁸⁵

Zwar ist es gerade charakteristisch, dass FinTech-Dienstleistungen der dritten Iteration global verfügbar sind,²⁸⁶ doch stösst ihre grundsätzliche Ubiquität durchaus auch an territoriale Grenzen. Dadurch, dass FinTech-Anbieter weiterhin über eine physische Präsenz verfügen und typischerweise körperchaftlich organisiert sind, sind sie mindestens an die lokalen Regeln der jeweiligen Jurisdiktion gebunden. Darüber hinaus haben FinTech-Unternehmen regelmässig auch die Regeln der Zielmärkte einzuhalten. Dezentrale Systeme führen demgegenüber auch in diesem Aspekt zu einer verstärkten *Delokalisierung* von Finanzdienstleistungen. Sowohl die Disintermediation als auch die Delokalisierung der Finanzdienstleistungserbringung sind auf die Dezentralität solcher Systeme zurückzuführen.

Dezentrale Systeme sind mit anderen Worten frei von eindeutig identifizierbaren Intermediären.²⁸⁷ THOMAS PUSCHMANN und ROLF H. WEBER erkennen darin das Potenzial, die Finanzindustrie in mikro- und makroökonomischer Hinsicht zu verändern, und sprechen darum von der «Neuerfindung des Finanzsektors»,²⁸⁸ während YVES MAUCHLE den Vorgang als «Revolution» der Art und Weise, wie Finanzdienstleistungen erbracht werden, bezeichnet.²⁸⁹ Aus diesem Grund ist nachfolgend davon auszugehen, dass sich die vorliegende Arbeit bereits mit den Entwicklungen von *FinTech 4.0* befasst, soweit man einen solchen

²⁸⁴ Siehe etwa Rohr/Wright, *Hastings Law Journal* 2019, 484–485; vgl. auch Rifkin, *Zero Marginal Cost Society*, 259–262.

²⁸⁵ Siehe etwas von Hippel, *Democratizing Innovation*, 95–97, 121–131, der die Entwicklung zu «innovation communities» nachzeichnet; ferner Benkler, *Wealth of Networks*, 59–90, welcher von «commons-based peer production» spricht.

²⁸⁶ Siehe Lehmann, *Boston University International Law Journal* 2020, 123–124; Weber/Baisch, *Journal of International Banking Law and Regulation* 2018, 350; bereits Bernet, *Finanzintermediation*, 144, 145.

²⁸⁷ Siehe FINMA, *Jahresbericht 2021*, 20 («echte[...] DeFi-Applikationen»).

²⁸⁸ Siehe Puschmann/Weber, *SZW* 2017, 79, 94; demgegenüber zurückhaltender Weber, *Jusletter IT* vom 18. Mai 2017, Rz. 55–56.

²⁸⁹ Siehe Mauchle, *SZW* 2017, 830; ähnlich Simmchen, *MMR* 2017, 165.

Begriff für sinnvoll hält. Durch die praktisch uneingeschränkte Öffnung der Produktion und des Austausches von Finanzkontrakten gegenüber dem Publikum kommt es zu einem exponentiellen Wachstum des Einflusses technologischer Innovation auf die Finanzintermediation. Es ist darum für die vierte Iteration von FinTech – die sog. *Decentralized Finance* – davon auszugehen, dass es zu einer Hyperdigitalisierung des Finanzwesens kommt, infolgedessen die bisherige Rolle der Finanzintermediation neu bestimmt werden muss.²⁹⁰

²⁹⁰ Ähnlich Klebeck/Dobrauz-Saldapenna, in: Klebeck/Dobrauz-Saldapenna, Einleitung, 2–3; Rennig, Finanztechnologische Innovationen, 132, der unter Bezugnahme auf die Funktionen der Finanzintermediation lediglich für *vollkommene Märkte* gemäss ökonomischem Modell von einem Wegfall der Finanzintermediäre ausgeht; ferner bereits zur umfassenden Transformation des Systems der Finanzintermediation Bernet, Finanzintermediation, 143, 146–147.

4. Decentralized Finance (DeFi)

4.1 Vorgeschichte und Vorläufer

a. Cypherpunks und Hightech-Hayekians

Die historischen Wurzeln von Bitcoin im Allgemeinen und Decentralized Finance im Besonderen liegen in den ideologischen Entwicklungen, die Anfang der 1990er Jahre in eine lose Bewegung kulminierten, deren Anhänger der Öffentlichkeit als *Cypherpunks* bekannt wurden. Bei den Cypherpunks handelte es sich einerseits um Akademiker, Coder und Hacker, die *Free* bzw. *Open-Source-Software* für die Öffentlichkeit entwickelten.²⁹¹ Andererseits gehörten politische Aktivisten dazu, welche sich publizitätswirksam für Meinungsfreiheit und Privatsphäre im *Cyberspace* und darüber hinaus einsetzten.²⁹²

Die Cypherpunks waren damals der Überzeugung, dass das Internet an einem Wendepunkt angelangt sei, an dem es entweder zu einem dystopischen Überwachungsstaat im *Orwell'schen* Sinne²⁹³ führe oder aber instrumental für die Verwirklichung der persönlichen Freiheiten sei.²⁹⁴ Daraus schlossen sie, dass staatliche und privatwirtschaftliche Kontrolle und Macht mithilfe von Technologie zurückgedrängt werden müsse. Besonders in der Mathematik in Form der Kryptografie sahen sie eine Möglichkeit zur Befreiung des Einzelnen, was politischen und gesellschaftlichen Wandel erlauben solle, der letztlich für das Fortbestehen liberaler Demokratien in einer globalisierten Welt notwendig sei.²⁹⁵

Kryptografie beschreibt Systeme, die Information durch Transposition und Substitution von Zeichen und Zahlen sowie durch Kodierung so verändern, dass die Information für Nichtberechtigte unverständlich wird.²⁹⁶ Kryptografie als Methode zur bewussten Verschleierung von Nachrichten und somit der Wahrung der Privatsphäre ist bereits für den Entstehungszeitpunkt der ersten

²⁹¹ Siehe Stallman, *Free Software*, 251–270; ferner Raymond, *Cathedral and Bazaar*, 11, 67–71, 175–176.

²⁹² Vgl. Barlow, in: Ludlow, *Independence of Cyberspace*, *passim*.

²⁹³ Siehe Orwell, *Nineteen Eighty-Four*, *passim*.

²⁹⁴ Siehe Narayanan, *IEEE Security & Privacy* 2013 II, 75.

²⁹⁵ Ausführlich zum ideologischen Fundament der Cypherpunks Levy, *crypto*, 236–281.

²⁹⁶ Siehe Kahn, *The Codebreakers*, xiii–xv; ferner Dooley, *History of Cryptography*, 5–6.

Schriften nachgewiesen.²⁹⁷ Im Unterschied zu diesen überwiegend linguistischen Vorläufern griffen Cypherpunks auf moderne Verschlüsselungsverfahren zurück, die auf computergestützten mathematischen Algorithmen basierten.²⁹⁸

Bezeichnend für diese frühe Phase der Cypherpunks war ein Aufsatz des Computerwissenschaftlers DAVID CHAUM von 1985. Er warnte in seinem Beitrag davor, dass ohne Änderung des aktuellen Kurses die Verstärkung zentripetaler Kräfte in allen Lebensbereichen absehbar sei. Demgegenüber müsse man das dezentalisierende Potenzial aus der Verbindung von Computern mit Informationstechnologie im Interesse der Menschen nutzbar machen.²⁹⁹ CHAUM erhielt schliesslich mit der Aufdeckung des NSA-Überwachungsprogramms PRISM durch Edward Snowden³⁰⁰ und des Skandals um Facebook und Cambridge Analytica Recht.

Darüber hinaus vertraten gewisse Cypherpunks, die sich selbst als *Kryptoanarchisten* bezeichneten, idealisierte Visionen einer neuen Welt ausschliesslich basierend auf Computercode: Sie konzipierten für das *Cyberspace* neue Formen der gesellschaftlichen Organisation, in denen nationalstaatliche Grenzen aufgehoben und staatliche Rechtsnormen vollständig durch die Gesetze der Mathematik ersetzt und diese durch Computercode vollstreckt würden.³⁰¹

Zu Erreichung eines freien *Cyberspace* wurde in den 1990er Jahren auch gerichtlich gegen staatliche Einschränkungen von Verschlüsselungssoftware, wie etwa *Pretty Good Privacy* (PGP) des Computerwissenschaftlers Philipp R. Zimmermann, vorgegangen. Die US-amerikanische Regierung argumentierte in diesem Fall, dass Computercode dem *Arms Export Control Act* unterstehe, da Hardware und Software, die kryptografische Verfahren verwenden, von ausländischen Staaten und Terroristen zur Verschleierung ihrer Kommunikation verwendet werden können.³⁰² Die jahrzehntelange Auseinandersetzung zwischen Softwareingenieuren und politischen Aktivisten auf der einen Seite sowie dem US-amerikanischen Staat auf der anderen Seite, die auch als *Crypto*

²⁹⁷ Siehe Kahn, *The Codebreakers*, 84.

²⁹⁸ Siehe zur Unterscheidung zwischen klassischer und moderner Kryptologie Bauer, *Secret History*, xvii–xxi; ferner Rubinstein-Salzedo, *Cryptography*, 1.

²⁹⁹ Siehe Chaum, *Communications of the ACM* 1985, 1044.

³⁰⁰ Siehe hierzu Greenwald, Edward Snowden, *passim*.

³⁰¹ Siehe Narayanan, *IEEE Security & Privacy* 2013 II, 76.

³⁰² Siehe Dooley, *History of Cryptography*, 232. Die Argumentation der US-amerikanischen Regierung ist v.a. in den Erfahrungen im Zweiten Weltkrieg und dem Kalten Krieg begründet; vgl. bspw. zur Verschlüsselungsmaschine *Enigma* Dooley, *History of Cryptography*, 151–165.

Wars bezeichnet wird,³⁰³ endete in wichtigen Grundsatzentscheidungen, die überwiegend zugunsten der uneingeschränkten Entwicklung und Veröffentlichung von Computercode, der kryptografische Verfahren beinhaltet, ausgingen.³⁰⁴ Im Kern kamen die Richter etwa in *Bernstein vs. U.S. Department of Justice* zum Schluss, dass Computercode *Speech* darstellt und somit vom Ersten Zusatzartikel der US-amerikanischen Verfassung geschützt ist.³⁰⁵ Philipp R. Zimmermann hat 1995 den Source Code von PGP in einem eigens erstellten Buch abdrucken lassen, um die Bedeutung von Computercode als Protected Speech hervorzuheben.³⁰⁶

Schliesslich war aus ideellen und ökonomischen Überlegungen auch der Kampf gegen Patent- und Urheberrechte an Software und anderen kreativen Erzeugnissen ein zentrales Anliegen der Cypherpunk-Bewegung.³⁰⁷

Inhaltlich ging es anfänglich – wie heute –³⁰⁸ zwar in erster Linie um den freien Austausch von Ideen sowie den Schutz der Privatsphäre des Einzelnen im Cyberspace, doch spielte auch die ökonomische Güterverteilung eine zunehmend bedeutende Rolle: Viele der damaligen Cypherpunks träumten von einem frei zugänglichen und damit global verfügbaren Zahlungsmittel für die virtuellen Gemeinschaften des Internets.³⁰⁹ Tatsächlich finden sich erste Gedanken zu den heutigen Kryptowährungen und Smart Contracts bereits bei den Kryptoanarchisten Timothy C. May und Eric Hughes in ihrem jeweiligen politischen Manifest.³¹⁰

Parallel zu den Cypherpunks bildete sich eine Forschungsgruppe, deren Angehörige als *Hightech-Hayekians* bezeichnet wurden. Anders als die Cypherpunks, die sich in erster Linie mit der künftigen Gestaltung des virtuellen Cyberspace

³⁰³ Siehe hierzu Levy, *crypto*, 367–373; für einen guten Überblick sorgt ferner die vierteilige Videoserie über Cypherpunks in ReasonTV, *Cypherpunks Write Code*, Youtube, *passim*; ferner zu den verschiedenen Phasen der Crypto Wars aus rechtlicher Sicht Koops/Kosta, *Computer Law & Security Review* 2018, 892–898.

³⁰⁴ Siehe für eine Übersicht Stay, *Georgia State University Law Review* 1997, *passim*.

³⁰⁵ Siehe Camp/Lewis, *Ethics and Information Technology* 2001, 24–27; weiterführend Van Valkenburgh, *Electronic Cash*, 32–45; ferner Dame-Boyle, *Remembering the Case*, *passim*. Vgl. Zimmermann, *PGP Source Code*, *passim*.

³⁰⁷ Vgl. Salin, *Freedom of Speech*, *passim*; ferner Lessig, *The Future of Ideas*, 19–23, 85–86, 214–215, der das Spannungsverhältnis zwischen «innovation commons» und «anti-commons» aufzeigt.

³⁰⁸ Vgl. Snowden, *Permanent Record*, *passim*.

³⁰⁹ Siehe May, in: Ludlow, *Crypto Anarchy*, 73–74, 76, der jedoch noch davon ausging, dass Digital Cash am schwierigsten umzusetzen ist.

³¹⁰ Siehe May, in: Ludlow, *Crypto Anarchist Manifesto*, 63; Hughes, in: Ludlow, *A Cypherpunk's Manifesto*, 82.

beschäftigten, erkannten die Hightech-Hayekians im Internet ökonomische Lösungen für real existierende Wirtschaftsprobleme. Sie entwickelten die agoristische Idee von internetbasierten Märkten, indem sie bestehende ökonomische Konzepte der Informationsökonomik mitberücksichtigten.³¹¹ Das Internet soll dabei die Koordination zwischen den Marktteilnehmern verbessern, indem es die Informations- und Transaktionskosten von Austauschbeziehungen sowie die Opportunitätskosten von Entscheidungen verringert.³¹² Auch den Hightech-Hayekians ging es aber letztlich darum, den Einfluss des Staates auf den Markt und somit auf das Leben des Einzelnen zu verringern.

Ähnlich wie für die damaligen Cypherpunks und Hightech-Hayekians stehen in ideologischer Hinsicht auch für viele der heutigen Verfechter von Decentralized Finance das Bottom-up- und Peer-to-Peer-Design von Entscheidungsprozessen im Vordergrund. Grundlage dafür bildet die uneingeschränkte Nutzung des Internets. Auf diese Aspekte wird im Verlauf dieser Arbeit nochmals zurückkommen sein.³¹³

Am 31. Oktober 2008 wurde endlich das Whitepaper über die technischen Grundlagen der Kryptowährung Bitcoin veröffentlicht.³¹⁴ Darauf folgte die Schaffung des Genesis-Blocks der Bitcoin Blockchain am 3. Januar 2009.³¹⁵ Ganz in der Tradition der Cypherpunks ist bis heute unklar, wer hinter dem Bitcoin-Erfinder mit dem Nom de Plume *Satoshi Nakamoto* steckt. Selbst der Zeitpunkt der Inbetriebnahme des Bitcoin Netzwerks scheint angesichts der Finanz- und Bankenkrise, die Anfang 2009 in vollem Gange war, nicht völlig zufällig gewählt gewesen zu sein.³¹⁶

Mit der Realisierung von Bitcoin ging ein langjähriger Traum der Cypherpunks in Erfüllung: ein Zahlungsmittel, das gemeinschaftlich verwaltet wird, staatlich unabhängig ist und transnational funktioniert, eine mit Bargeld vergleichbare Privatsphäre gewährleistet und dessen primärer *locus operandi* das Internet ist.³¹⁷ Die implizite Kritik Bitcoins am heutigen Finanzsystem ist dabei offen-

³¹¹ Siehe etwa Miller/Drexler, in: Huberman, *Markets and Computation*, 140; ferner Lavoie/Baetjer/Tulloh, in: Birner/Garroste, *High-tech Hayekians*, 98–105 m.w.N.

³¹² Siehe Salin, *Release 1.0*, 13–17.

³¹³ Siehe etwa unten, III.2.2.

³¹⁴ Siehe Nakamoto, *Bitcoin*, *passim*.

³¹⁵ Der Genesis-Block lässt sich mit einem Blockchain-Explorer finden, z.B. unter <https://www.blockchain.com/btc/block/00000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f>.

³¹⁶ Siehe Champagne, *Book of Satoshi*, 3–4; ferner Assange, *Cypherpunks*, 96–101.

³¹⁷ Siehe Antonopoulos, *Internet of Money*, Bd. 1, 8, 19; Narayanan et al., *Bitcoin*, 175–176; Brito, *The Case for Electronic Cash*, 21–25; vgl. ferner Brunton, *Digital Cash*, 42, 63–65, 155; kri-

sichtlich nicht rein technischer Natur, sondern weist eine grundsätzlich politische und philosophische Dimension auf.³¹⁸

b. Digital Cash und Smart Contracts

i. Kryptowährungen

Erfindungen wie Bitcoin und darauf aufbauend Ethereum sind erst aufgrund der technologischen Fortschritte in den Computerwissenschaften der letzten Jahrzehnte realisierbar geworden.³¹⁹ Im Folgenden werden einige der wichtigsten Eckpunkte kurz dargestellt:

- Grundlegend waren die Arbeiten zur *Public-Key- asymmetrischen Kryptografie* in den 1970er Jahren. Die Public-Key-Kryptografie erlaubt es dem Absender von Informationen, diese durch Anwendung eines bestimmten kryptografischen Verfahrens mit dem öffentlichen Schlüssel des Empfängers zu verschlüsseln, so dass lediglich der Empfänger aufgrund des Besitzes des korrespondierenden privaten Schlüssels die Informationen entschlüsseln kann. Zu diesem Zweck teilt der Empfänger der Mitteilung seinen öffentlichen Schlüssel vorab dem Absender mit. Der öffentliche Schlüssel (Public Key) dient mit anderen Worten als Signierschlüssel, der private Schlüssel (Private Key) als Verifikationsschlüssel. Zudem kann mit demselben Mechanismus auch die Authentizität des Absenders einer Mitteilung verifiziert werden (sog. *Digitale Signaturen*).³²⁰ Anders als bei der symmetrischen Kryptografie kann der öffentliche Schlüssel bedenkenlos über unsichere Netzwerke geteilt werden, da mit ihm allein die Entschlüsselung der übertragenen Mitteilung nicht möglich ist.³²¹

Kryptografische Verfahren sind heute ein zentraler Bestandteil, um die Integrität und Vertraulichkeit der Kommunikation im Internet (z.B. mittels des Protokolls TLS, sog. *Transport Layer Security*) und, zwar erst

tisch hingegen Narayanan IEEE Security & Privacy 2013 II, 76; ferner Swartz, Cultural Studies 2018, 634–641.

³¹⁸ Siehe etwa Roy, National Affairs 2021, Nr. 49, 79–80.

³¹⁹ Siehe für eine nützliche grafische Übersicht der unterschiedlichen Innovationen Narayanan/Clark, acmqueue 2017, 2; ferner Brunton, Digital Cash, 97–117, 155–156.

³²⁰ Siehe Diffie/Hellman, IEEE Transactions on Information Theory 1976, *passim*; ferner Rivest/Shamir/Adleman, Communications of the ACM 1978, *passim*.

³²¹ Siehe Merkle, Communications of the ACM 1978, 295–296; ausführlich Dooley, History of Cryptography, 185–186.

ansatzweise, per E-Mail zu gewährleisten. In dezentralen Systemen, namentlich Bitcoin und Ethereum, wird asymmetrische Kryptografie zwar nicht für die Verschlüsselung der Kommunikation über das Netzwerk verwendet; die Netzwerkteilnehmer kommunizieren grundsätzlich unverschlüsselt miteinander.³²² Transaktionen wären in dezentralen Systemen allerdings ohne kryptografische Verfahren (*Hash-Funktionen*³²³ usw.) und ohne digitale Signaturen technisch und ökonomisch undenkbar.³²⁴ Sie bilden die Grundlage für das schlüsselbasierte Identitätssystem der Nutzer, die manipulationsresistente Aneinanderreihung von Transaktionen und Blocks in einem verteilten Register und den Konsensmechanismus solcher Protokolle.³²⁵

- Erstmals wurde ein kryptografisch abgesichertes Zahlungssystem namens *DigiCash* sodann durch den bereits erwähnten Computerwissenschaftler CHAUM in den 1980er Jahren entwickelt. Bei *DigiCash* handelte es sich um ein System mit überwiegend anonymisierten Vermögenswerten und Transaktionen.³²⁶ In diesem Sinne stellte *DigiCash* einen ersten Prototyp digitalen Bargelds dar. Anders als Bitcoin setzte dieses Zahlungssystem noch durchgehend auf die zentrale Serverinfrastruktur einer Bank oder eines sonstigen Intermediärs, und jede Einheit von *DigiCash* repräsentierte letztlich eine bestehende Buchgeldeinheit, die von einem Intermediär verwahrt werden musste.³²⁷
- Der Kryptograf und Hacker ADAM BACK entwickelte sodann mit *hashcash* einen Mechanismus, der systematischen E-Mail-Spam und andere Denial of Service (DoS)-Attacken verhindern sollte. Die Lösung bestand darin,

³²² Eine Ausnahme hierzu bildet bspw. das Dazwischenschalten der *The Onion Router* (Tor)-Netzwerkknoten, deren Kommunikation mehrfach verschlüsselt ist; vgl. hierzu <https://www.torproject.org/>.

³²³ Eine *Hash-Funktion* ist der in einem kryptografischen Kompressionsverfahren berechnete «Fingerabdruck» (*Output*) einer bestimmten Information (*Input*). Eine Hashfunktion einer Information kann leicht erstellt bzw. berechnet werden, die umgekehrte Ableitung der Information aus der Hashfunktion ist allerdings mit einem grossen, ja sogar prohibitiven Aufwand verbunden; vgl. hierzu Buchmann, *Kryptographie*, 234; in Bezug auf Kryptowährungen Narayanan et al., *Bitcoin*, 2–10.

³²⁴ Siehe Antonopoulos, *Mastering Bitcoin*, 55–57; Antonopoulos/Wood, *Programming Ethereum*, 59–62; Narayanan et al., *Bitcoin*, 15–20.

³²⁵ Für eine Übersicht siehe Narayanan/Clark, *acmqueue* 2017, 15–19.

³²⁶ Siehe Chaum, in: Chaum/Rivest/Sherman, *Blind Signatures*, *passim*.

³²⁷ Siehe Berentsen/Schär, *Bitcoin*, 65; ausführlich Schuster/Färber/Eberl, *Digital Cash*, 59–62.

dass der Absender einer E-Mail aufwendige, jedoch nicht prohibitiv aufwendige Hash-Funktionen berechnen musste, bevor er die E-Mail versenden konnte.³²⁸ Dieser Proof-of-Work-Mechanismus wurde von Satoshi Nakamoto zum Konsensmechanismus in Bitcoin weiterentwickelt (sog. *Nakamoto-Konsens*).³²⁹ Der Nakamoto-Konsens und darauf basierende Iterationen erlauben verteilten Netzwerken, sich auf eine für *alle* Teilnehmer autoritative Transaktionshistorie einigen zu können, wobei angenommen wird, dass eine gewisse Anzahl der Netzwerkteilnehmer fehlerhaft oder sogar böswillig ist.³³⁰

Der Nakamoto-Konsens stellt somit eine Lösung für das als *Byzantinischer Fehler* bekannte Kommunikationsproblem in verteilten Netzwerken dar. Der Name geht auf ein Gedankenexperiment zurück, in welchem mehrere byzantinische Generäle bei der Belagerung einer feindlichen Stadt ihren Angriff zu koordinieren haben, sie allerdings davon ausgehen müssen, dass sich fehlerhafte Informationen im Umlauf befinden.³³¹ Die Angriffshypothese ist zentral für Kryptowährungen.³³² Sie ist letztlich gleichzusetzen mit der wirtschaftswissenschaftlichen Modellannahme, dass die Teilnehmer eines Marktes, wenn immer lohnenswert, opportunistisch handeln.³³³

- Der Nakamoto-Konsens weicht von klassischen Konsensmodellen in verteilten Netzwerken – namentlich Paxos und *Practical Byzantine Fault Tolerance* (PBFT) –³³⁴ darin ab, dass der Konsens in Bitcoin probabilistischer Natur ist. Die probabilistische Natur des Nakamoto-Konsens bezieht sich dabei einerseits auf die Wahrscheinlichkeit, dass ein Netzwerkteilnehmer

³²⁸ Siehe Back, Hashcash, *passim*; ferner Dwork/Naoor, in: Brickell, *Combating Junk Mail*, *passim*.

³²⁹ Siehe Berentsen/Schär, Bitcoin, 66; vgl. ferner bereits Back, Hashcash, 7, der auf Wei Dais *b-money* Bezug nimmt (siehe hierzu sogleich).

³³⁰ Siehe Nakamoto, Bitcoin, 2–3; ferner Narayanan et al., Bitcoin, 28–32.

³³¹ Siehe Lamport/Shostak/Pease, *ACM Transactions on Programming Languages and Systems* 1982, 382–383.

³³² SATOSHI NAKAMOTO hat die Angriffshypothese dezentraler Systeme zu einem Kernanliegen von Bitcoin gemacht; vgl. Nakamoto, Bitcoin, 4 («If a greedy attacker is able to assemble more CPU power than all the honest nodes, he would have to choose between using it to defraud people by stealing back his payments, or using it to generate new coins.»).

³³³ Siehe hierzu oben, [II.2.4b](#).

³³⁴ Siehe zu Paxos Lamport, *ACM Transactions on Computer Systems* 1998, *passim*; sodann Lamport, *ACM SIGACT News* 2001, Nr. 4, *passim*; ferner zur PBFT siehe Castro/Liskov, *Proceedings of the Third Symposium on Operating Systems Design and Implementation* (OSDI) 1999, *passim*.

einen korrekten Block findet, und andererseits auf die über die Zeit exponentiell abnehmende Wahrscheinlichkeit, dass der Konsens zwischen den Netzwerkteilnehmern rückgängig gemacht werden kann.³³⁵ Anders als die klassischen Vorläuferprotokolle, die grundsätzlich auf einem einvernehmlichen Abstimmungsmechanismus mit autorisierten und somit bekannten Teilnehmern beruhen, macht das Nakamoto-Protokoll ein offenes Netzwerk möglich, in dem die bürgerlichen Identitäten der Teilnehmer für den Konsens nicht relevant sind.³³⁶

Dank des Nakamoto-Konsens kann auch die inhärente Anfälligkeit von anonymen offenen Netzwerken auf sog. *Sybil-Attacken* erheblich reduziert werden. Normalerweise kann ein Teilnehmer eines verteilten P2P-Netzwerks dieses untergraben, indem er eine grosse Anzahl von Pseudonymen, d.h. Identitäten, erstellt, die einfach und billig zu generieren sind. Aus Sicht des Netzwerks erweckt dies den falschen Eindruck, dass Teilnehmer mit unterschiedlichen Identitäten existieren.³³⁷ Proof-of-Work löst dieses Problem weitgehend.³³⁸

- Der Computerwissenschaftler WEI DAI war sodann für die Ausarbeitung von *b-money* verantwortlich, gemäss welcher die verschiedenen Teilnehmer eines dezentralen Zahlungsnetzwerks ein konsistentes, jedoch separat geführtes Register über alle Transaktionen führen. DAIs *b-money* kann als Vorläufer von Distributed Ledgers bzw. Blockchains betrachtet werden, die sicherstellen sollen, dass jedem Netzwerkteilnehmer alle Transaktionen des Netzwerks bekannt sind. Auch bei DAI sind kryptografische Verfahren zentral für die Absicherung der Transaktionen, namentlich um das sog. *Double Spending-Problem*³³⁹ zu lösen. Ferner greift der Compu-

³³⁵ Siehe Nakamoto, Bitcoin, 3, 6–8; Narayanan et al., Bitcoin, 32, 33–34, die von «random node selection» sprechen; ausführlich Wattenhofer, Blockchain, 79–87.

³³⁶ Siehe zu den Unterschieden zwischen klassischen Konsensmodellen und dem Nakamoto-Konsens Narayanan et al., Bitcoin, 31–34.

³³⁷ Siehe hierzu Douceur, in: Druschel/Kaashoek/Rowstron, Sybil Attack, *passim*.

³³⁸ Siehe Narayanan/Clark, *acmqueue* 2017, 11.

³³⁹ Das sog. *Double-Spending-Problem* ist allen elektronischen Zahlungssystemen inhärent, denn die in einem solchen System existierenden Vermögenswerte bestehen ausschliesslich aus digitalen Daten oder werden durch solche vermittelt, die ohne entsprechende Vorkehrungen durch einfaches Kopieren der Daten mehrfach ausgegeben werden können. In traditionellen Zahlungssystemen wird zur Lösung dieses Problems ein Finanzintermediär in Form eines zentralen Clearinghouse eingesetzt; vgl. hierzu Nakamoto, Bitcoin, 2, 3; ferner Karame et al., ACM Transactions on Information and System Security 2015, 2:3–2:4.

terwissenschaftler auf Schlüsselpaare der asymmetrischen Kryptografie zurück, die anstelle von echten Identitäten über die digitalen Vermögenswerte des Netzwerks verfügen können.³⁴⁰

- BACKS und DAIS Arbeiten zu hashcash und b-money kulminierten in der Folge im Konzept eines wiederverwertbaren Token des Kryptografen und Hackers HAL FINNEY. Er nannte diese als Zahlungsmittel verwendbaren Token «Reusable Proofs of Work».³⁴¹
- Schliesslich entwickelte der Computer- und Rechtswissenschaftler NICK SZABO im Jahr 2005 mit *Bit Gold* ein Prototyp von Bitcoin, der allerdings nie über das Konzeptstadium hinauskam. *Bit Gold* war als digitales Zahlungssystem konzipiert, das im Wesentlichen auf digitalen Signaturen, einer verteilten Beurkundungsfunktion mithilfe von Zeitstempeln, einem verteilten Register und einer Proof-of-Work-Funktion basierte.³⁴² SZABO orientierte sich für das Design an physischem Gold: «*It would be very nice if there were a protocol whereby unforgeably costly bits could be created on-line with minimal dependence on trusted third parties, and then securely stored, transferred, and assayed with similar minimal trust.*»³⁴³ Mangels zentraler Parteien sollten die *Bit Gold*-Einheiten von den Netzwerkteilnehmern gemeinsam ausgegeben werden; zudem sollte die Transaktionshistorie von den Netzwerkteilnehmern durch Lösung von Proof-of-Work-Rechenaufgaben autoritativ mit Wirkung für alle Teilnehmer festgelegt werden.³⁴⁴

Bitcoins eigentliche Errungenschaft besteht in der praktischen *Zusammenführung* der oben dargestellten Komponenten zu einem selbständigen dezentralen Zahlungsnetzwerk.³⁴⁵ Das Protokoll unterscheidet sich insofern von früheren digitalen Zahlungssystemen, wie etwa *e-gold*, *Liberty Dollar* und *Liberty Reserve*, die noch auf zentralisierte Modelle angewiesen waren und deren Betrieb letztlich von den US-amerikanischen Strafverfolgungsbehörden eingestellt wurde.³⁴⁶ Selbst *PayPal*, dessen digitale Wallets nach PETER THIELS ur-

³⁴⁰ Siehe Dai, b-money, *passim*.

³⁴¹ Siehe Finney, RPOW, *passim*.

³⁴² Siehe Szabo, *Bit Gold*, *passim*.

³⁴³ Szabo, *Bit Gold*, *passim*.

³⁴⁴ Siehe Szabo, *Bit Gold*, *passim*.

³⁴⁵ Siehe Narayanan/Clark, *acmqueue* 2017, 3, 15–17, 24.

³⁴⁶ Zu den Unterschieden zwischen diesen früheren Modellen und Bitcoin und anderen Kryptowährungen siehe Dowd, *Private Monies*, 15–24, 27–37; Brito/Castillo, *Bitcoin*, 39, 42–43; kritisch hingegen bereits Güring/Grigg, *Bitcoin & Gresham's Law*, 5–6, deren Befürch-

sprünglicher Idee durchaus Ähnlichkeiten mit Bitcoin aufwiesen,³⁴⁷ ist letztlich intermediarisiert und somit zentralisiert. Demgegenüber ist Bitcoin das erste digitale Zahlungssystem, dem es trotz der Tatsache, dass kein Intermediär für die Vermittlung zwischen den Netzwerkteilnehmern vorgesehen ist, einen globalen Konsens über die Transaktionshistorie herzustellen gelingt.³⁴⁸

Damit zusammenhängend besteht eine weitere Errungenschaft des Bitcoin Protokolls im wirksamen Einsatz von ökonomischen Anreizen in verteilten Netzwerken. Solche Anreize werden implementiert, um den erwähnten globalen Konsens zu erreichen und die langfristige Stabilität des Systems zu gewährleisten (sog. Cryptoeconomics).³⁴⁹ Dies wird im Wesentlichen durch die Verwendung einer nativen, d.h. blockchain-eigenen Kryptowährung erreicht, welche einerseits das Resultat eines Schöpfungsmechanismus ist und andererseits für die Bezahlung von Transaktionsgebühren verwendet wird. Netzwerkteilnehmer, welche den Protokollregeln zum Durchbruch verhelfen, können die Kryptowährungseinheiten einbehalten. Ein derartiger Leistungsanreiz wurde in den Vorläufermodellen von Bitcoin nicht oder nur ungenügend realisiert.³⁵⁰

ii. Smart Contracts und DAOs

Eine weitere zentrale Komponente von dezentralen Systemen sind Smart Contracts. Dabei handelt es sich um Computerprogramme, die auf einem dezentralen Netzwerk (z.B. Ethereum) in deterministischer Weise zur Ausführung gelangen, weshalb die Korrektheit der Ausführung von jedermann überprüft werden kann.³⁵¹ Smart Contracts gelten nach verbreiteter Auffassung weder als «smart» noch als «contracts» im rechtlichen Sinne.³⁵² Smart Contracts

tungen sich allerdings bisher nicht bewahrheitet haben; ferner ausführlich Trautman, Richmond Journal of Law and Technology 2014, 85–91.

³⁴⁷ Siehe hierzu Jackson, PayPal Wars, insb. Kapitel 1.

³⁴⁸ Siehe Antonopoulos, Mastering Bitcoin, 3, 4–5; Bonneau et al., Proceedings 2015 IEEE Symposium on Security and Privacy, 106, die den «Nakamoto consensus» für die Kerninnovation von Bitcoin halten. Einige Autoren heben konkret das Element der *einheitlichen Zeitmessung* innerhalb eines verteilten Netzwerks als die zentrale Innovation hervor; so etwa Gigi, Bitcoin Is Time, *passim*.

³⁴⁹ Siehe Barber et al., in: Keromytis, Bitter to Better, 400–401.

³⁵⁰ Vgl. Narayanan/Clark, acmqueue 2017, 11, 14, 16, 17; ferner Azouvi/Hicks, Cryptoeconomic Systems, 2, 7–9.

³⁵¹ Siehe Antonopoulos/Wood, Mastering Ethereum, 127–128.

³⁵² Vgl. etwa Buterin, Twitter, *passim* («To be clear, at this point I quite regret adopting the term 'smart contracts'. I should have called them something more boring and technical, perhaps something like 'persistent scripts'»).

werden demgegenüber hauptsächlich als Mittel zur Ausführung des zwischen den Parteien vereinbarten Vertragsinhalts betrachtet.³⁵³ Ihr Einsatz ist mit anderen Worten auf den tatsächlichen *Vollzug* einer Vereinbarung gerichtet. Aufgrund der Tatsache, dass der in einer Applikation verwendete Computercode grundsätzlich immer Fehler enthält und die Intentionen des Programmierers oder der Nutzer eines Smart Contracts in aller Regel nur unvollständig festgestellt werden können, beschlagen Smart Contracts aber oftmals auch die Konsensebene in der Praxis. Zudem kann gerade im Falle von DeFi-Anwendungen mangels persönlicher Interaktion der Parteien regelmässig nur aufgrund des Codes und allfälliger dazugehöriger Dokumentationen auf die «wahren» Intentionen der Parteien geschlossen werden. An den unterschiedlichen Auffassungen in der Community darüber, ob es sich bei einem ausgenutzten Softwarefehler um einen Hack oder lediglich um die kluge Verwendung des Codes handelte, wird dies regelmässig sehr gut sichtbar.

Smart Contracts haben darum gewisse Ähnlichkeiten mit dem von IAN GRIGGS entwickelten Konzept der *Ricardian Contracts*. Dabei handelt es sich um eine Methode einer gleichsam für Mensch und Computer lesbaren verbindlichen Vereinbarung zwischen den Parteien.³⁵⁴ Solche Vereinbarungen sollen mit anderen Worten sowohl in rechtlicher als auch in Softwareform wirksam sein. Deren Bestimmungen können, müssen aber nicht in einem verteilten Register (Blockchain) abgebildet und über ein dezentrales Netzwerk ausgeführt werden.³⁵⁵ Das Konzept der Smart Contracts widerspricht allerdings insoweit der Methode von Ricardian Contracts, als dass erstere typischerweise als ein technisch geschlossenes System intendiert sind. Smart Contracts können grundsätzlich jede Form von Transaktionslogik verarbeiten, solange die dafür notwendigen Inputdaten innerhalb des Systems vorhanden sind.³⁵⁶ Bei Verwendung von Ricardian Contracts ist es hingegen oft gerade die Absicht der Parteien, dass die Vereinbarung gegenüber manuellem Dateninput oder nachträglichen menschlichen Veränderungen, wie etwa ein Gerichtsurteil, offen ist.³⁵⁷

³⁵³ So bereits Wood, Ethereum Yellow Paper, 2 («algorithmic enforcement of agreements»).

³⁵⁴ Siehe Grigg, Ricardian Contract, *passim* («The Ricardian Contract delivers a rich source of primary, complete information. The full story is right there in textual form, in parsable parameters, and in the signature chain.»)

³⁵⁵ Siehe Dobrauz-Saldapenna/Schrackmann, in: Kaili/Psarrakis, Economics of Smart Contracts, 44

³⁵⁶ Siehe hierzu unten, [II.4.4.](#)

³⁵⁷ Vgl. Grigg, Ricardian and Smart Contracts, *passim* («[Smart contracts and Ricardian contracts] are trying to improve our agreements at different points and in different ways, within the overall framework of a contract in law. In practical terms we can now look at the original

Obwohl das Bitcoin Protokoll selbst einfache Formen von Smart Contracts zulässt,³⁵⁸ wurde die Programmierung von Turing-vollständigen³⁵⁹ Applikationen grundsätzlich erst mit Ethereum möglich.³⁶⁰ Die ursprüngliche Idee von Smart Contracts geht auf den bereits erwähnten Computerwissenschaftler und Juristen SZABO zurück: «A smart contract is a computerized transaction protocol that executes the terms of a contract. The general objectives of smart contract design are to satisfy common contractual conditions (such as payment terms, liens, confidentiality, and even enforcement), minimize exceptions both malicious and accidental, and minimize the need for trusted intermediaries.»³⁶¹ Dabei sollen in Anlehnung an das Common Law-Prinzip der Rechtsbeziehung (privity of contract) nur so viele Personen um das Bestehen eines Vertrages und dessen Inhalt wissen müssen sowie die Kontrolle über die Vertragsausführung ausüben können, wie es gerade noch für die Durchsetzung des Vertrages nötig ist.³⁶² Die Relativierung der Rolle von Mittelmännern liegt somit bereits der ursprünglichen Konzeption von Smart Contracts zugrunde.³⁶³

Eine der ersten DeFi-Anwendungen auf Basis von Smart Contracts bildete sodann der The DAO. Die Abkürzung DAO steht für Decentralized Autonomous Organization. Gegründet wurde The DAO von Slock.it. Beim The DAO handelte sich um ein Investmentvehikel, deren Investitionen in verschiedene Krypto-Projekte nach Plan der Gründer überwiegend automatisiert werden sollten. Weder bestand ein eigentliches Management des Investmentvehikels noch wurde die Struktur innerhalb einer Rechtsordnung inkorporiert. In funktionaler Hinsicht war The DAO am ehesten noch mit einem Investmentclub ver-

Ricardo system as a system with infinite semantic ability but capable of handling by assumption only one form of action – perhaps the Alice to Bob payment [...]. Whereas Bitcoin can handle a multitude of smart-enabled transaction forms but in only one semantically trivial unit: assumed to be the bitcoin [...].»).

³⁵⁸ Siehe z.B. bezüglich der Funktionen Multisignature, Pay-to-Script-Hash und Timelocks Antonopoulos, *Mastering Bitcoin*, 149–170; ferner Swanson, *Great Chain*, 16, der Bitcoin als Smart Contracts der ersten Generation bezeichnet.

³⁵⁹ Zum Begriff siehe unten, [III.3.1b](#).

³⁶⁰ Siehe Ethereum, *Ethereum Whitepaper*, *passim*.

³⁶¹ Siehe Szabo, *Smart Contracts*, *passim*; ferner Szabo, *Public Networks*, *passim*. Eine Übersicht weiterer Definitionsversuche in der Rechtsliteratur findet sich bei Braegelmann/Kaulartz, in: Braegelmann/Kaulartz, *Einleitung*, § 1 N 17–29; sodann de Caria, in: DiMatteo/Cannarsa/Poncibò, *Definitions*, 21–24; ausführlich Gyr, *Blockchain und Smart Contracts*, N 214–239 m.w.H.

³⁶² Siehe Szabo, *Digital Markets*, *passim*.

³⁶³ Vgl. auch Voshmgir, in: Braegelmann/Kaulartz, *Smart Contracts*, § 2 N 4; skeptisch diesbezüglich Mik, *Law, Innovation and Technology* 2017, 9–10, 31–32.

gleichbar.³⁶⁴ The DAO nahm im Sommer 2016 seine Aktivitäten auf, nachdem er anlässlich eines Token-basierten Crowdfundings Vermögenswerte in Millionenhöhe bei Investoren eingesammelt hatte. Aufgrund eines Programmierfehlers konnte ein Hacker rund einen Drittel der eingesammelten Vermögenswerte in die von ihm kontrollierten Smart Contracts abfließen lassen.³⁶⁵ Im Anschluss daran kam es zur berühmten Teilung des Ethereum Netzwerks in zwei neue Blockchains (sog. Hard Fork).³⁶⁶

Die Idee hinter DAOs kann als eine Weiterentwicklung von Smart Contracts betrachtet werden, welcher künftig insb. in rechtlicher Hinsicht grosse Bedeutung zukommen dürfte. Während einfache Smart Contracts die Übertragung von Vermögenswerten erlauben, können DAOs auch unternehmerische Risiken verwalten und die Kontrolle darüber in effizienter Weise auf eine Vielzahl von Personen verteilen. Dies erlaubt eine stärkere Humanisierung von Smart Contracts. So ist es etwa denkbar, dass künftig die dynamischen Prozesse und Strukturen eines Unternehmens in einer DAO organisiert werden. Je nach Anschlussmöglichkeit von DAOs an die Rechtsordnung liessen sich dadurch auch Ricardian Contracts in einer disintermediatisierten Weise realisieren.³⁶⁷

Das Internet hat, wie oben ausgeführt, die persönlichen und räumlichen Distanzen zwischen den Menschen stark relativiert, indem es neue Kommunikationswege geschaffen hat. Doch erst anlässlich von Kryptowährungen und Smart Contracts sind disintermediatisierte Systeme zur *Wertübertragung* Realität geworden. Dies ist möglich geworden, weil Personen aufgrund der mathematischen Funktionslogik dezentraler Systeme Informationseinheiten einen ökonomischen Wert zuschreiben können.³⁶⁸ Anders gewendet: Computerda-

³⁶⁴ Vgl. Art. 2 Abs. 2 lit. f KAG und Art. 1a KKV.

³⁶⁵ Siehe Antonopoulos/Wood, Mastering Ethereum, 325–326.

³⁶⁶ Siehe hierzu unten, [IV.5.2e.ii](#).

³⁶⁷ Vgl. Grigg, Ricardian and Smart Contracts, *passim* («We can now see that the real challenge between smart contracts and Ricardian Contracts or legal documents is not to choose, but to incorporate. The Bitcoin world will benefit from adding the semantic richness of legal documentation into its service.»); ferner Goodenough, in: Capiello/Carullo, Integrating Smart Contracts, 194.

³⁶⁸ Vgl. Okamoto/Ohta, in: Feigenbaum, Universal Electronic Cash, 324 («The security of electronic cash systems cannot depend on any physical condition, but must be guaranteed by mathematics. Here, cryptographic techniques are essentially used to guarantee security. Then, information itself has a value, and electronic cash can be transferred through networks.»).

ten werden zu digitalen Handlungs- und Verfügungsrechten im Sinne der ökonomischen Theorie.³⁶⁹

Im Ergebnis kommt es durch den Rückgriff auf gemeinsame Computerprotokolle zu einer starken Integration der Finanzwelt mit dem Internet. Die für die Finanzintermediation in ihren derzeitigen Ausprägungen typische personale und institutionelle Intermediation wird in diesem Rahmen zumindest relativiert.

4.2 Begriff von Decentralized Finance

Decentralized Finance (DeFi) – in der Literatur selten auch als *Open Finance* bezeichnet – beruht auf computer- bzw. softwarebasierten Anwendungen für den Finanzbereich. Dies setzt die Nutzung der Blockchain-Technologie und somit von Kryptowährungen und Smart Contracts voraus.³⁷⁰

An Definitionen des Begriffs mangelt es in der Literatur nicht:

- Nach ANDREAS M. ANTONOPOULOS handelt es sich bei DeFi um «programmable money», dessen Anwendungsbereich in der Finanzwelt beinahe unbegrenzt sei.³⁷¹
- Gemäss FABIAN SCHÄR bezieht sich der Begriff auf «[...] an open, permissionless, and highly interoperable protocol stack built on public smart contract platforms, such as the Ethereum blockchain [...]».³⁷²
- STROPONIATI et al. verstehen sodann unter DeFi «[...] a complex array of platforms on the Ethereum blockchain through which borrowers, lenders and investors can execute financial transactions without the use of traditional financial institutions.»³⁷³
- DIRK A. ZETZSCHE, DOUGLAS W. ARNER und ROSS P. BUCKLEY fassen unter dem Begriff «[...] the decentralized provision of financial services [...]»³⁷⁴

³⁶⁹ So auch Yermack, *Review of Finance* 2017, 10–11; Berentsen/Schär, *Federal Reserve Bank of St. Louis Review* 2018, 1–2, 14–15 («digital property rights»); Catalini/Gans, *Communications of the ACM* 2020, 86–87, 89. Vgl. ferner unten, [II.5.2d](#).

³⁷⁰ Siehe Werner et al., *Decentralized Finance*, 2.

³⁷¹ Antonopoulos, *Internet of Money*, Bd. 1, 8.

³⁷² Schär, *Federal Reserve Bank of St. Louis Review* 2021, 153.

³⁷³ Stroponiati et al., *Decentralized governance*, 1; ferner *ähnlich* Popescu, in: Vlăduțescu/Bunăiașu/Negrea, *Decentralized Finance*, 323.

³⁷⁴ Zetzsche/Arner/Buckley, *Journal of Financial Regulation* 2020, 173.

- «[...] through a mix of infrastructure, markets, technology, methods, and applications [...]»³⁷⁵
- Ähnlich klingt es bei AMLER et al., wonach DeFi «[...] a whole ecosystem of financial services realized through smart contracts deployed on public distributed ledgers [...]» darstellt.³⁷⁶
 - MATTHIAS NADLER und FABIAN SCHÄR verstehen unter DeFi «[...] a composable and trust-minimized protocol stack that is built on public Blockchain networks and uses smart contracts to create a large variety of publicly accessible and interoperable financial services.»³⁷⁷
 - WERNER et al. definieren den Begriff schliesslich über seine Eigenschaften: «[...] DeFi is non-custodial[,] [...] permissionless[,] openly auditable [and] composable [...]».³⁷⁸
 - Das WORLD ECONOMIC FORUM (WEF) verfolgt einen ähnlichen Ansatz, indem es die Unterscheidungskriterien zum traditionellen Finanzwesen hervorhebt: Bei DeFi handelt es sich danach um (1) Finanzdienstleistungen oder Finanzprodukte gestützt auf (2) vertrauensminimierte Operationen und Abwicklung über eine permissionless Blockchain in einem (3) Non-custodial-Design und basierend auf (4) programmierbarer, offener und interoperabler Softwarearchitektur.³⁷⁹
 - DAVID MEIRICH kommt schliesslich zur folgenden Definition: «[DeFi ist] die Smart Contract-basierte Infrastruktur zur intermediärslosen und automatisierten Inanspruchnahme von Finanzdienstleistungen auf einer öffentlichen und zugangsfreien Blockchain [...], die den Nutzern die alleinige Verwaltung ihrer virtuellen Vermögenswerte belässt.»³⁸⁰

DeFi ist nach vorliegender Auffassung die Erbringung von Dienstleistungen innerhalb eines dezentralen Systems, die bisher, soweit sie überhaupt existiert haben, von Finanzintermediären erbracht worden sind.³⁸¹ DeFi ist somit die dezentrale Replikation traditioneller finanzintermediärer Aktivitäten mittels

³⁷⁵ Buckley/Arner/Zetzsche, FinTech, 131.

³⁷⁶ Amler et al., DeFi-ning DeFi, 2.

³⁷⁷ Nadler/Schär, Decentralized Finance, 1.

³⁷⁸ Werner et al., Decentralized Finance, 1.

³⁷⁹ Siehe WEF, Decentralized Finance, 6–7.

³⁸⁰ Meirich, Decentralized Finance, Rz. 270, der sodann aufgrund des Dezentralitätsgrades zwischen «DeFi im weiteren Sinne» und «DeFi im engeren Sinne» unterscheidet; ähnlich Maurenbrecher/Leisinger, SJZ 2022, 648 («Intermediationsfreiheit»).

³⁸¹ Siehe auch Schär, Federal Reserve Bank of St. Louis Review 2021, 153, 172; Coelho-Prabhu, Decentralized Finance, *passim*; DeFi Pulse, Defi, *passim*; ConsenSys, Decentralized Finance, *passim*; EthHub, Decentralized Finance, *passim*.

offener und interoperabler Computerprotokolle.³⁸² Darüber hinaus kann DeFi zu neuartigen Aktivitäten und Geschäftsmodellen führen, die ebenfalls auf den vorgenannten Protokollen basieren.

	Decentralized Finance
Definition	Decentralized Finance umfasst Dienstleistungen, die bisher typischerweise von Finanzintermediären erbracht worden sind, in einer dezentralen Art und Weise auf der Grundlage offener Computerprotokolle.

4.3 Abgrenzung

a. Begriff der Centralized Finance

Zum besseren Verständnis des Begriffs mag es hilfreich sein, die personalen und institutionellen Prozesse und Strukturen der traditionellen Finanzintermediation als Centralized Finance bzw. CeFi (oder auch TradFi für Traditional Finance) aufzufassen.³⁸³

Die Hauptunterschiede zwischen DeFi und CeFi lassen sich an zwei Merkmalen erläutern: (i) Erstens sind finanzintermediäre Dienstleistungen in CeFi *logisch zentralisiert*, typischerweise in der Form einer juristischen Person. Die Zentralisierung erfasst dabei nicht nur die Erbringung der Dienstleistung an sich, sondern schliesst i.d.R. auch die Kontrolle über die in diesem Rahmen involvierten Vermögenswerte und Informationen bzw. Daten mit ein. (ii) Zweitens können juristische Personen in CeFi innerhalb der Schranken der Rechtsordnung³⁸⁴ *frei darüber entscheiden*, welchen Kunden sie ihre Dienstleistungen

³⁸² Siehe auch Carter/Jeng, in: Coen/Maurice, DeFi Protocol Risks, 2 («[...] platforms and protocols that seek to replicate existing financial services by using crypto/blockchain technology with limited centralization.»); Bitkom, Decentralized Finance, 7 («The long-term vision of DeFi is [...] a fully-functioning and fully-automated trustless financial system.»).

³⁸³ Vgl. für eine differenzierende Ansicht von CeFi als Bindeglied zwischen dem traditionellen Finanzsektor und DeFi Hays/Yorke/Rosenberg, DeFi Adoption, 7–8; siehe ferner für eine nützliche Übersicht zur Abgrenzung von DeFi von CeFi und TradFi Aramonte/Huang/Schrimpf, BIS Quarterly Review Dezember 2021, 23.

³⁸⁴ Ein Kontrahierungszwang bzw. eine derartige Pflicht kann sich gemäss Rechtsprechung des Bundesgerichts aus ausdrücklichen Gesetzesbestimmungen, aber ausnahmsweise auch aus den allgemeinen Prinzipien des Privatrechts ergeben; vgl. etwa: (i) Anspruch auf Aufnahme in einen Verein wegen Verstosses gegen das Persönlichkeitsrecht nach Art. 28 ZGB aufgrund der Boykottierung einer Marktteilnehmerin (BGE 82 II 292, E. 7); (ii) Anspruch auf Transport einer Massensendung durch die Post wegen Verstosses gegen

anzubieten gedenken. Damit zusammenhängend sind sie in aller Regel nicht dazu verpflichtet, die im Rahmen ihrer Dienstleistungen bearbeiteten Daten Dritten zur Verfügung zu stellen. Letztlich liegt, wie bereits erwähnt,³⁸⁵ die Entscheidungsgewalt und Kontrolle in CeFi bei der juristischen Person, welche die Dienstleistung erbringt.

Diese für CeFi massgeblichen Elemente werden nun durch DeFi grundlegend infrage gestellt: DeFi setzt (i) die gemeinschaftliche Erbringung finanzintermediärer Dienstleistungen und deren datenmässige Abbildung innerhalb eines Netzwerks, (ii) die unmittelbare Kontrolle über die Vermögenswerte durch deren Inhaber sowie (iii) der offene, uneingeschränkte Zugang zu diesen Dienstleistungen und der damit zusammenhängenden Daten über das Internet voraus.³⁸⁶ Diese Eigenschaften bedingen sich sodann gegenseitig: Da DeFi-Aktivitäten gemeinschaftlich erbracht werden und ihnen somit keine Person vorsteht, kann grundsätzlich niemand von ihrer Nutzung ausgeschlossen werden. Und, *vice versa*, weil DeFi jedermann offensteht, steht letztlich keine Person den Aktivitäten vor. In DeFi wird somit Entscheidungsgewalt und Kontrolle auf mehrere Personen verteilt bzw. dezentralisiert.

b. Web 3.0

Wie die Bezeichnung «DeFi» vermuten lässt, beziehen sich die Aktivitäten auf den *Finanzbereich* bzw. finanzintermediäre Dienstleistungen. Allerdings ist gerade die Eingrenzung auf den Finanzbereich mit Problemen verbunden. Problematisch daran ist der Umstand, dass dezentrale Applikationen auch Vermögenswerte zum Gegenstand haben können, die an traditionellen Finanzmärkten typischerweise nicht gehandelt werden. Hierzu gehören etwa

das Verbot sittenwidrigen Verhaltens (BGE 129 III 35, E. 6.); (iii) Anspruch auf Vertragsabschluss mit marktbeherrschenden Unternehmen wegen einer Verletzung von Art. 7 Abs. 2 lit. a KG (vgl. hierzu Gohari, Geschäftsbeziehungen, 765 m.w.N.); (iv) Anspruch auf grundlegende Finanzdienstleistungen der Post im Bereich des Zahlungsverkehrs gestützt auf Art. 32 Abs. 1 PG i.V.m. Art. 43 Abs. 1 VPG (vgl. auch BGer 4A_417/2009 vom 26. März 2010, E. 3.4, wobei sich der Anspruch des Postkunden noch auf Art. 2 Abs. 2 PG stützte); ferner betreffend Zürcher Kantonbank, wobei die Beschwerdeführer für die Durchsetzung eines allfälligen Kontrahierungszwanges auf den Zivilprozess verwiesen wurden (BGer 2C_966/2018, 2C_967/2018, vom 29. Januar 2019, E. 3.6); (v) Eintritt in eine Genossenschaft ist nicht übermässig zu erschweren (Art. 839 Abs. 2 OR, sog. *Prinzip der offenen Tür*), wobei darunter ein Ordnungsprinzip und kein klagbares Recht auf Eintritt zu verstehen ist (vgl. hierzu Meier-Hayoz/Forstmoser, Schweizerisches Gesellschaftsrecht, § 19 N 40).

³⁸⁵ Siehe oben, [II.1.5](#).

³⁸⁶ Siehe hierzu ausführlich unten, [III.2](#).

dezentral zur Verfügung gestellte Computerleistung oder auf diesem Weg zur Verfügung gestellter Computerspeicher, welche in aller Regel in Form eines Nutzungs-Tokens verfügbar gemacht werden.³⁸⁷ Darüber hinaus können etwa digitale Kunst, Eintrittskarten, Universitätsdiplome, digitale Identitäten und vergleichbare einmalige Werte über eine Blockchain tokenisiert werden. In letzteren Fällen ist die Rede von Non-Fungible Tokens bzw. NFTs, welche je nach Ausgestaltung finanzmarktrechtlich ebenfalls als Nutzungs-Token gelten.³⁸⁸

In der Tat stellen DeFi und Open Finance nur einen Teilbereich einer grösseren Bewegung dar, die letztlich das Fundament eines an den Interessen des Nutzers orientierten Internets und Webs bilden sollen. Diese als Web 3.0 bezeichnete Entwicklung kann als eine Reaktion auf die im Zusammenhang mit FAANG (Facebook, Amazon, Apple, Netflix und Google) und staatlichen Nachrichtendiensten stehende Datenschutzsituation gesehen werden. Das inoffizielle Motto der Bewegung «Redecentralize the Web» soll an die Anfänge des Internets zurückerinnern.³⁸⁹ Demnach soll neben der Infrastrukturebene des Internets die Applikationsebene des Webs redezentralisiert werden.³⁹⁰

Web 3.0-Softwareentwickler verfolgen mit ihren Protokollen und Applikationen das Ziel, Nutzern die Hoheit und Kontrolle über ihre Daten einzuräumen.³⁹¹ Über den privaten und kommerziellen Umgang mit persönlichen Daten sollen demnach anders als heute ausschliesslich und autonom die betroffenen Nutzer entscheiden.³⁹² Dieses auch als Self-Sovereign Identity be-

³⁸⁷ Treffender ist hingegen der Begriff des Applikations-Token; vgl. hierzu MME, Conceptual Framework, 7, 10.

³⁸⁸ Siehe hierzu die Ausführungen in Aref/Fábián/Weber, GesKR 2021, 394–396; ausführlich auch FINMA, Jahresbericht 2022, 20–21; ferner Harvey/Ramachandran/Santoro, DeFi, 37–38; Mauchle, iusNet BR-KR 28.10.2021, *passim*, der von «Speziestoken» spricht; sodann auch Reymond, Jusletter vom 31. Mai 2021, Rz. 5.

³⁸⁹ Vgl. etwa <https://redcentralize.org/>.

³⁹⁰ Siehe Ibanez et al., IEEE Intelligent Systems, Institute of Electrical and Electronics Engineers 2017, 94.

³⁹¹ Siehe Kim, in: Park/Fong/Pan/Sung, Future of the Internet, 289–294, *passim*; ul Hassan et al., Future of the Internet, 9. Für eine Übersicht der Unterschiede zwischen Web 1.0, Web 2.0 und Web 3.0 siehe Ragnedda/Destefanis, in: Ragnedda/Destefanis, Disruptive Technology, 2–4.

³⁹² Siehe Wood, Web 3.0, *passim* («As a user of Web 3.0, all interactions will be carried out pseudonymously, securely and for many services, trustlessly. Those that require third party(-ies), the tools will give the users and DApp-developers the ability to spread the trust among multiple different, possibly competing, entities, massively reducing the amount of trust one must place in the hands of any given single entity.»); Makridakis/Christodoulou, Future In-

kannte Konzept ist eine Form des Identitätsmanagements.³⁹³ Zu den vom Web 3.0 erfassten nutzerbezogenen Informationen gehören nicht nur gewöhnliche Personen- und Sachdaten, sondern auch digitale Identitäten (z.B. der Twitter-Nutzername @...) sowie dessen kryptografisch abgesicherten Vermögenswerte. Das Web 3.0 will eine umfassende Umgestaltung der personalen und institutionellen Intermediation im Internet und über dezentrale Systeme sodann auch im Finanzwesen auslösen.³⁹⁴ Die heute stark zentralisierten Anwendungen sollen mit anderen Worten dezentralisiert werden.

Dank Kryptowährungen existiert nunmehr auch ein natives Zahlungsmittel für das Internet. Das Ziel von Verfechtern des Web 3.0 ist es, dass Internetnutzer selbst darüber entscheiden können, ob sie für die Nutzung von Webanwendungen mit ihren persönlichen Daten, wie heute etwa bei Facebook und Co., oder stattdessen bspw. mit eigens dafür herausgegebenen Token *bezahlen* wollen.³⁹⁵ Ein Projekt, das in den Webbrowser Brave integriert ist, ist der Basic Attention Token (BAT), der auf der Ethereum Blockchain herausgegeben wurde. Nutzer erhalten von Werbeinserenten BAT für ihre Bereitschaft, deren Inserate im Internet zu betrachten. Sie können sodann mit den so verdienten Token die Autoren von Inhalten bezahlen oder ihnen diese spenden.³⁹⁶

Ein weiteres Beispiel für das Web 3.0 ist das Protokoll *InterPlanetary File System* (IPFS). Dabei handelt es sich um ein verteiltes System für die Speicherung von und den Zugriff auf Dateien, Websites und Anwendungen. Grundlage bildet ein offenes P2P-Netzwerk bestehend aus unzähligen Computern.³⁹⁷ Es soll nach den Plänen der Entwickler dereinst das heutige Web ablösen.³⁹⁸ Einige Blockchain-Projekte, wie etwa Filecoin³⁹⁹, nutzen ebenfalls IPFS als dezentrale Datenbank, wobei mit der Herausgabe einer eigenständigen Kryptowährung den Teilnehmern des Netzwerks ein Anreiz zur dauerhaften Aufbewahrung von Daten gesetzt wird.⁴⁰⁰ Der zentrale Vorteil von IPFS, Filecoin und vergleichbaren Projekten gegenüber dem heute verbreiteten Cloud-Hosting-Mo-

ternet 2019, 13–14; ferner bereits auf die Risiken für die Privatsphäre im Internet hinweisend Berners-Lee, Computer 1996, 76–77.

³⁹³ Siehe EUBOF, Digital Identity, 14–16; *skeptisch*, allerdings auf eine private Blockchain abstellend, Yansen, in: Ragnedda/Destefanis, Blockchain, 170.

³⁹⁴ Gl.M. Voshmgir, in: Braegelmann/Kaulartz, Smart Contracts, § 2 N 21–24, 42.

³⁹⁵ Siehe Leising, MetaMask, *passim*; ferner Essential1, Web 3.0, *passim*.

³⁹⁶ <https://basicattentiontoken.org/>.

³⁹⁷ Siehe IPFS, What is IPFS?, *passim*.

³⁹⁸ So Benet, IPFS, 11.

³⁹⁹ <https://filecoin.io/>.

⁴⁰⁰ Siehe Filecoin, What is Filecoin?, *passim*.

dell liegt in der Beseitigung zentraler Knotenpunkte, welche die Nutzerdaten kontrollieren sowie die Zugangsrechte von Nutzern beliebig einschränken können.⁴⁰¹

Zwischen den Intentionen des Web 3.0 und den Zielen aktueller Datenschutzgesetzgebungen, wie namentlich der Europäischen Datenschutzgrundverordnung (DSGVO), besteht durchaus ein Gleichlauf. Das Web 3.0 integriert in aller Regel das Konzept von *Privacy by Design and Default*, das mit Art. 25 in die DSGVO Eingang gefunden hat und nunmehr auch ausdrücklich in Art. 7 des revidierten Datenschutzgesetzes enthalten ist.⁴⁰²

c. Open Finance und Open Banking

Von der vorliegenden Auffassung von DeFi bzw. Open Finance weicht das in der traditionellen Finanzindustrie verwendete Konzept des Open Bankings und der Open Finance ab.

Anschliessend an den Begriff von Open Banking⁴⁰³ wird unter *Open Finance* gemeinhin die Öffnung von internen Bankensystemen und der darin enthaltenen Kundeninformationen für vertrauenswürdige externe Finanzdienstleister, insb. FinTech-Unternehmen, verstanden. Die Öffnung der Systeme soll auf der Basis gemeinsamer, standardisierter Datenschnittstellen erfolgen.⁴⁰⁴ Bei Kundeninformationen kann es sich etwa um den Zugriff auf die Kontoinformationen eines Bankkunden handeln, welche ein externer Zahlungsdienstleister für das Auslösen einer Zahlung benötigt. Die Datenschnittstellen werden in der Informatik als *Application Programming Interfaces* (APIs) bezeichnet. APIs können definiert werden als ein Regelwerk mitsamt Spezifikationen für die Kommunikation von Softwareprogrammen untereinander, das eine Schnittstelle zwischen verschiedenen Programmen bildet, um deren Interaktion zu erleichtern. Solche Schnittstellen können offen (Open API) oder proprietär (Inter-

⁴⁰¹ Siehe Benet, IPFS, 1; Protocol Labs, Filecoin, 4, 8, 24; ferner Clayburgh/Zumwalt/Benet, Distributed file storage, *passim*.

⁴⁰² Vgl. zum revidierten Datenschutzgesetz Rosenthal, Jusletter vom 16. November 2020, Rz. 43–52.

⁴⁰³ Ausführlich hierzu SwissBanking, Open Banking, *passim*; ferner hinsichtlich des Zahlungsverkehrs Essebie/Bourgeois, EuZ 2018, *passim*.

⁴⁰⁴ Siehe für einen Überblick der unterschiedlichen Konzepte sowie deren Gemeinsamkeiten und Unterschiede Ankenbrand/Bieri, Architekturrahmen, *passim*; ferner Nicholls, Banking & Finance Law Review 2019, 123; sodann aus bankwirtschaftlicher Sicht Wildi, in: Emmenegger, Open Banking, *passim*; ausführlich zum Schweizer Ansatz hinsichtlich Open Finance Bundesrat, Digital Finance, 16–17.

nal/Closed API) ausgestaltet sein oder nur ausgewählten Parteien offenstehen (Partner API).⁴⁰⁵ Das Dienstleistungsangebot über die eigenen Unternehmensgrenzen hinweg wird nunmehr auch als *Embedded Finance* bezeichnet.⁴⁰⁶

Die wesentliche Gemeinsamkeit zwischen Open Finance und DeFi liegt darin, dass jeweils der Kunde des Finanzdienstleisters bzw. der Nutzer eines dezentralen Systems als Entscheidungsträger fungiert.⁴⁰⁷ Ob und wohin die Daten fließen, liegt in der Entscheidungsmacht der betroffenen Personen. Der Hauptunterschied der beiden Konzepte ist in der Motivation der beteiligten Akteure begründet. Quelloffene APIs sind ein unentbehrliches Merkmal dezentraler Systeme, um bei den Marktteilnehmern überhaupt Vertrauen schaffen zu können. Sie sind mit anderen Worten nicht bloss Ausdruck der Präferenz, mit der Zustimmung des Kunden gewisse Datenströme vertrauenswürdigen Drittunternehmen zur Verfügung zu stellen. DeFi schafft *grundlegend* interoperable und offene Finanzökosysteme. Jedermann kann für seine Anwendungen an dieses Ökosystem andocken. Demgegenüber setzt Open Finance nach herkömmlicher Auffassung nicht voraus, dass Finanzinstitute auf proprietäre Softwaresysteme und Datenschnittstellen verzichten.⁴⁰⁸ APIs dieser Art haben den Nachteil, dass der Anbieter sie grundsätzlich, vorbehaltlich einer anderslautenden Regulierung oder Vereinbarung, jederzeit ausschalten kann, was selbstredend die Interessen der Drittunternehmen tangiert, die sich für ihre Geschäftsaktivitäten auf die API verlassen haben.⁴⁰⁹

Um Missverständnisse zu vermeiden, spricht die vorliegende Arbeit ausschliesslich von Decentralized Finance bzw. DeFi.

4.4 Inhalt und Umfang

Wie bereits erwähnt, wird DeFi in der vorliegenden Arbeit als die Reproduktion traditioneller Finanzintermediation in dezentraler Weise verstanden. DeFi beschäftigt sich inhaltlich mit zwei Grundfunktionen der traditionellen Finanzintermediation:

⁴⁰⁵ Siehe für weitere Informationen BIS/BCBS, Open banking, 15–16, 19.

⁴⁰⁶ Siehe SwissBanking/SFTI, Open Finance, 3; ausführlich zu den Implikationen sodann SFTI, Future of Financial Institutions. View 2030, Discussion Paper, 2020, 74–76.

⁴⁰⁷ So auch Ankenbrand/Bieri, Architekturrahmen, *passim*; auch auf die Unterschiede hinweisend Weber, SZW 2022, 3–4.

⁴⁰⁸ Siehe Ankenbrand/Bieri, Architekturrahmen, *passim*; ausführlich Zachariadis/Ozcan, API Economy, SWIFT Institute Working Paper Nr. 2016-001, 15. Juni 2017, 10, 11–13.

⁴⁰⁹ Siehe etwa für den Fall der Twitter-API Newton, Third-party apps, *passim*.

- In erster Linie übernimmt DeFi die dauerhafte oder vorübergehende Verwahrung bzw. Aufbewahrung oder Verwaltung von Finanztiteln, welche Intermediäre im heutigen Finanzsystem im Auftrag ihrer Kunden ausüben (sog. *Custodian-Funktion*).⁴¹⁰ Darunter fallen bspw. Banken, Escrow-Anbieter und Wertpapierhäuser sowie (zentrale) Verwahrungsstellen im Bereich der Verwahrung von Effekten und Finanzinstrumenten, die an einem Handelsplatz gehandelt werden.
- Darüber hinaus sind aber auch Intermediäre, welche die für den Austausch von Effekten und Finanzinstrumenten zugrundeliegenden Märkte bzw. Infrastrukturen betreiben, von dieser Entwicklung betroffen (sog. *Exchange-Funktion*). Darunter fallen organisierte und alternative Märkte, insb. Handelsplätze und Handelssysteme mitsamt allfälligen Nachhandelsinfrastrukturen.

Insofern wirkt sich DeFi nicht nur auf Finanzintermediäre nach dem vorherrschenden ökonomischen Verständnis aus, sondern auch auf Märkte, an welchen erstgenannte Intermediäre für den Handel von Finanztiteln zusammentreten. DeFi betrifft somit das gesamte Finanzintermediationssystem gemäss vorliegendem Verständnis.⁴¹¹ ZETZSCHE, ARNER und BUCKLEY gehen ebenfalls von einem weiten Anwendungsfeld von DeFi aus, wenn sie schreiben: «[...] in this article we understand DeFi to comprise, at its core, what its simple name suggests: the decentralized provision of financial services through a mix of infrastructure, markets, technology, methods and applications.»⁴¹²

Als DeFi gelten demnach in erster Linie Computerprotokolle für:⁴¹³

- die dezentrale Herausgabe von Kryptowährungen, wie etwa bitcoin und ether, von algorithmischen oder mit Kryptovermögenswerten hinterleg-

⁴¹⁰ Zum Begriff siehe Smullen/Hand, *Dictionary of Finance*, 103; Banks, *Dictionary of Finance*, 137; *Dictionary of Banking and Finance*, 388; ferner Boemle et al., *Depotbank*, 295, welche die Custodian-Funktion der Depotbank zuordnen.

⁴¹¹ Siehe oben, II.2.1.

⁴¹² Zetzsche/Arner/Buckley, *Decentralized Finance*, 173–174; ebenfalls von einem weiten Anwendungsbereich ausgehend Schär, *Federal Reserve Bank of St. Louis Review* 2021, 153 («blockchain-based financial infrastructure»).

⁴¹³ Ein guter Überblick findet sich etwa in Wharton Blockchain and Digital Asset Project, *DeFi Beyond the Hype*, 8–17; Schär, *Federal Reserve Bank of St. Louis Review* 2021, *passim*; sehr ausführlich Harvey/Ramachandran/Santoro, *DeFi*, 69–129; ferner Amler et al., *DeFi-ning DeFi*, 2–4; Werner et al., *Decentralized Finance*, 3–6; Bokhenek/Kamakin/Hays, *Decentralization meets finance*, *passim*; ferner Chen/Bellavitis, *Journal of Business Venturing Insights* 2020, 4–6; Leonhard, *Decentralized Finance*, *passim*.

ten Stablecoins (z.B. *Ampleforth*⁴¹⁴, *Dai*⁴¹⁵, *Rai*⁴¹⁶, *Reserve*⁴¹⁷ und *Terra*⁴¹⁸) und von tokenisierten Vermögenswerten (z.B. in Form von ERC-20-Token);

- den dezentralen Handel dieser Vermögenswerte (siehe hierzu sogleich unten);
- die dezentrale Vergabe und Ausleihung von Darlehen (z.B. *Aave*⁴¹⁹, *Compound*⁴²⁰ und *Yearn*⁴²¹), wobei zu erwähnen ist, dass solche Protokolle bestehende Kryptovermögenswerte mittels Überbesicherung der ausgeliehenen Summe verleihen und bisher, soweit ersichtlich keine Modelle entwickelt worden sind, welche die Ausgabe ungedeckter oder teilgedeckter Kredite durch Buchgeldschöpfung im bankwirtschaftlichen Sinne erlauben würden;⁴²²
- die dezentrale Emission von Derivaten (z.B. *Hegic*⁴²³ und *Synthetix*⁴²⁴); sowie
- die dezentrale kollektive Kapitalanlage (z.B. *Enzyme*⁴²⁵ und *Set*⁴²⁶).

Ferner gehören auch dezentrale Protokolle zur Einspeisung externer Informationen in ein dezentrales System zu DeFi. Dabei liegt die Herausforderung darin, zu verhindern, dass externe Informationen auf ihrem Weg in die Blockchain manipuliert werden und dadurch eine Kettenreaktion falscher Ereignis-

⁴¹⁴ <https://www.ampleforth.org/>.

⁴¹⁵ <https://makerdao.com/>.

⁴¹⁶ <https://reflexer.finance/>.

⁴¹⁷ <https://reserve.org/>.

⁴¹⁸ <https://www.terra.money/>.

⁴¹⁹ <https://aave.com/>.

⁴²⁰ <https://compound.finance/>.

⁴²¹ <https://yearn.finance/>.

⁴²² Siehe Gudgeon et al., *Loanable Funds*, 94. Demgegenüber bestehen zentralisierte Anbieter, wie etwa BlockFi (<https://blockfi.com/>), welche als Finanzintermediäre teilgedeckte Kredite basierend auf und in Kryptovermögenswerten anbieten. Kraken Bank (<https://www.kraken.com/en-us/bank/>) ist demgegenüber eine vollgedeckte «Kryptobank» in der Form einer Special Purpose Depository Institution gemäss dem Recht des US-Bundesstaates Wyoming. Vgl. zur Frage der Realisierbarkeit von Mindest- bzw. Teilreserven im Bitcoin Ökosystem Berentsen/Schär, *Bitcoin*, 259 m.w.H.; ferner ausführlich Wall, *Cryptocurrency Banks, passim*, der die Grenzen staatlicher Einlagensicherungssysteme und der LOLR-Funktion von Zentralbanken in einem System mit teilgedeckten Krypto-Banken betont.

⁴²³ <https://www.hegic.co/>.

⁴²⁴ <https://www.synthetix.io/>.

⁴²⁵ <https://enzyme.finance/>.

⁴²⁶ <https://www.setprotocol.com/>.

nisse innerhalb des dezentralen Systems auslösen.⁴²⁷ Diese Herausforderung wird in dezentralen Systemen mithilfe von Orakel-Netzwerken und Prognosemärkten angegangen:

- Orakel-Netzwerke, wie namentlich *ChainLink*⁴²⁸ und *Provable* (ehemals *Oracleize*)⁴²⁹, fungieren als Schnittstellen, um dezentralen Systemen externe Informationen einzuspeisen, die nicht innerhalb des Systems produziert werden.⁴³⁰ Oracle-Protokolle spielen etwa für die Preisbestimmung tokenisierter Derivate eine zentrale Rolle, wenn der Preis des Basiswerts an Märkten *ausserhalb* des dezentralen Systems bestimmt wird (z.B. der Marktpreis einer an der SIX Swiss Exchange kotierten Aktie oder der LMBA-Goldpreis).⁴³¹ Zudem sind auch Stablecoins, die mit Kryptowährungen hinterlegt sind, auf zuverlässige externe Datenquellen (z.B. den Marktpreis von ETH an einer Kryptohandelsplattform) angewiesen.⁴³²
- Soweit *Prognosemärkte* DeFi-Anwendungen mit externen Informationen versorgen, weisen schliesslich auch sie Relevanz für DeFi auf. Prediction Market-Protokolle, wie etwa *Augur*⁴³³ und *Gnosis*⁴³⁴, erlauben den entgeltlichen Handel mit Informationen in der Form einer binären Option mit dem Ziel, die Eintrittswahrscheinlichkeit künftiger Ereignisse vorherzusagen.⁴³⁵ Sie ermöglichen bspw. das Abschliessen von Wetten auf den Sieger einer Präsidentschaftswahl oder einen bestimmten Aktienkurswert zu einem im Voraus bestimmten Stichtag. Die Tatsache, dass die Teilnehmer solcher Märkte vor Abgabe ihrer Stimme eine finanzielle Investition tätigen müssen, soll sicherstellen, dass die Vorhersagen möglichst akkurat ausfallen und somit als verbindliche Information in dezentralen Systemen verwendet werden können.⁴³⁶

⁴²⁷ Siehe Augur, Prediction Markets, *passim*.

⁴²⁸ <https://chain.link/>.

⁴²⁹ <https://provable.xyz/>.

⁴³⁰ Siehe Werner et al., Decentralized Finance, 3.

⁴³¹ Vgl. zum Konzept und einigen Beispielen Antonopoulos/Wood, Mastering Ethereum, 253–255. Es bestehen Anstrengungen, die Funktionen von Oracles und Prediction Markets möglichst zu dezentralisieren; vgl. hierzu bspw. die Projekte in Peterson et al., Augur, 1; Ellis/Juels/Nazarov, ChainLink, 26–27; ferner Antonopoulos/Wood, Mastering Ethereum, 261–262.

⁴³² Vgl. etwa für den Stablecoin Dai MakerDAO, Maker Protocol, 10–11.

⁴³³ <https://www.augur.net/>.

⁴³⁴ <https://gnosis.io/> und ferner <https://sight.pm/>.

⁴³⁵ Vgl. für eine Übersicht Arrow et al., Science 2008, *passim*; ausführlich sodann Hanson, The Journal of Political Philosophy 2013, *passim*.

⁴³⁶ Siehe Augur, Prediction Markets, *passim*; ausführlich zu möglichen Designs von Anreizsystemen in Prognosemärkten Luckner et al., Prediction Markets, 23–24.

Abschliessend ist noch zu erwähnen, dass dezentrale Orakel-Netzwerke und Prognosemärkte offensichtlich auch mannigfaltige Anwendungsfälle ausserhalb des Finanzbereichs haben können.⁴³⁷

4.5 Dezentrale Handelsplattformen im Besonderen

Untersuchungsgegenstand der vorliegenden Arbeit sind dezentrale Handelsplattformen. In der Literatur werden sie regelmässig als *Decentralized Exchanges* (DEXes) bezeichnet. Auf die unterschiedlichen Kategorien dezentraler Handelsplattformen wird zu einem späteren Zeitpunkt eingegangen.⁴³⁸

Dezentrale Handelsplattformen weisen im Vergleich zu traditionellen Intermediationsstrukturen mit Handelsbezug drei wesentliche Unterschiede auf:

- Der Zugang zur Plattform ist nicht intermediatisiert, d.h., die Nutzer müssen grundsätzlich⁴³⁹ keine Dienstleistungen Dritter in Anspruch nehmen, um am Handel von Finanzkontrakten teilzunehmen (*Disintermediated Access*).⁴⁴⁰ Die Nutzer werden somit zu direkten Teilnehmern der Handelsplattform. In dieser Hinsicht findet ein grundlegender Bruch mit dem historisch gewachsenen mitgliedschaftlichen System von Finanzintermediären an Handelsplätzen statt.⁴⁴¹
- Die Verwahrung der gehandelten Vermögenswerte erfolgt nicht in zentralisierter Form, d.h., Nutzer sind nicht auf die Verwahrungsdienstleistungen Dritter angewiesen, sondern können ihre Vermögenswerte selbst verwahren bzw. von Smart Contracts verwahren lassen (*Self-Custody*).⁴⁴² Zudem erfolgt die «Verbuchung» der Vermögenswerte in einem *einzigem* verteilten Register, das von einer Vielzahl von Teilnehmern eines dezentralen Netzwerks unterhalten wird.⁴⁴³ In der Folge kann auch auf die

⁴³⁷ Vgl. Messari, *Methodology Token*, *passim*, welche die Protokolle darum nicht zu DeFi zählen.

⁴³⁸ Siehe unten, [IV.3](#).

⁴³⁹ Davon ausgenommen sind grundsätzlich *grafische Benutzeroberflächen*, wie etwa eine Internetseite, über welche die Smart Contracts einer Handelsplattform erreichbar sind; siehe hierzu unten, [VII.4.2b.iii](#).

⁴⁴⁰ Siehe Schär, *Federal Reserve Bank of St. Louis Review* 2021, 153, 168–169.

⁴⁴¹ Siehe oben, [II.1.3](#).

⁴⁴² Siehe Lin, *Stanford Journal of Blockchain Law & Policy* 2019, 58; Schär, *Decentralized Finance* 153, 154, 160, 169; vgl. ferner Mills et al., *Federal Reserve System, Finance and Economics Discussion Series* 2016–095, 12.

⁴⁴³ Siehe Chiu/Koepl, *The Review of Financial Studies* 2019, 1717, 1724; Benos/Garratt/Gurrola-Perez, *Ledger* 2019, 129–130; Green/Snagg, in: Gullifer/Payne, *Intermediated Secu-*

mehrfache, treuhänderische Verbuchung derselben Vermögenswerte innerhalb einer mehrgliedrigen, oftmals grenzüberschreitenden Verwahrungskette verzichtet werden.⁴⁴⁴ Auch in diesem Punkt brechen dezentrale Handelsplattformen mit der historisch gewachsenen Entkopplung der Kontrolle über elektronisch verbuchte Finanztitel und deren Verwahrung durch eine Drittperson, wie namentlich eine Depotbank, eine Verwahrungsstelle oder eine zentrale Verwahrungsstelle.⁴⁴⁵

- Abrechnung und Abwicklung eines Austauschgeschäfts erfolgen schliesslich innerhalb eines dezentralen Netzwerks, d.h. durch die Teilnehmer des Netzwerks, auf welchem die dezentrale Handelsplattform zur Ausführung gelangt. Die Abwicklung erfolgt demgegenüber nicht etwa über ein Effektenabwicklungssystem. Handelsgeschäfte werden grundsätzlich nach dem Prinzip abgewickelt, dass es entweder zum erfolgreichen Austausch kommt oder aber alle getätigten Schritte rückabgewickelt werden (*Atomic Trades*).⁴⁴⁶ Die Abwicklung erfolgt mit anderen Worten unter Ausschluss traditioneller Gegenparteirisiken.⁴⁴⁷ Nutzer dezentraler Handelsplattformen tragen nicht das wirtschaftliche Risiko, dass ein anderer Nutzer (Gegenpartei), ein effektenkontoführendes Wertpapierhaus oder letztlich die zentrale Gegenpartei ihre Verpflichtungen auf Lieferung oder Bezahlung der Finanzkontrakte nicht erfüllen kann.⁴⁴⁸ Jede abgewickelte

rities, 337, 339, 358 («the symmetry of information»). Siehe zur Kontenführung in der Verwahrungskette traditioneller Bucheffektensysteme Meier-Hayoz/von der Crone, Wertpapierrecht, N 1353–1354; Hess/Friedrich, GesKR 2008, 116.

⁴⁴⁴ Siehe zur heutigen *Drittverwahrung* bei Bucheffekten Botschaft BEG 2006, 9351; Meier-Hayoz/von der Crone, Wertpapierrecht, N 1349–1354, die von einer «Pyramide der Wertpapierverwahrung» sprechen; insb. zu den mit langen Verwahrungsketten verbundenen Risiken Reiser, SZW 2017, 455–456; ferner zur Rechtslage vor Inkrafttreten des Bucheffektengesetzes Zobl, SZW 2001, 115. Nicht ausgeschlossen ist hingegen, dass durch die Ausgestaltung von Token in Form von Bucheffekten weiterhin Verwahrungsketten realisiert werden können; vgl. hierzu Bandi-Lang/Mauchle/Spoerlé, GesKR 2021, 246, 247. Es fragt sich allerdings, ob eine solche Strukturierung die Vorteile der Tokenisierung nicht gerade wieder zunichte machen würde.

⁴⁴⁵ Gl.M. Benos/Garratt/Gurrola-Perez, Ledger 2019, 130; ferner allerdings lediglich in Bezug auf tokenisierte Aktien Panisi/Buckley/Arner, Stanford Journal of Blockchain Law & Policy 2019, 211–213; FSB, Decentralised financial technologies, 14 m.w.N.

⁴⁴⁶ Ausführlich hierzu unten, [IV.5.1c.iii](#).

⁴⁴⁷ Vgl. in technischer Hinsicht etwa Wall/Malm, Distributed Securities Depository, 31–37. Ausführlich zu den *Gegenparteirisiken* in einem solchen System unten, [IV.5.1c.iv](#).

⁴⁴⁸ Siehe Lin, Stanford Journal of Blockchain Law & Policy 2019, 58; Chiu/Koepl, The Review of Financial Studies 2019, 1716–1717, 1725, 1727; Benos/Garratt/Gurrola-Perez, Ledger 2019, 130; Schär, Federal Reserve Bank of St. Louis Review 2021, 160, 169; ferner Bonneau et al., Proceedings 2015 IEEE Symposium on Security and Privacy, 118 m.w.N.

Transaktion über die Vermögenswerte wird schliesslich in einem einzigen verteilten Register aufgezeichnet (siehe auch oben).

Der Grad der Disintermediation geht in vielen Fällen über diese drei wesentlichen Unterschiede zu traditionellen Intermediationsstrukturen hinaus: Die auf Algorithmen basierende Automatisierung der Preisstellung und des anschliessenden Order Matchings stellt etwa die Rollen von zentralen Gegenparteien und Market Makern in traditionellen Märkten in Frage. Dies schliesst allerdings nicht aus, dass gewisse Nutzer dezentraler Handelsplattformen funktional als Market Maker agieren (so z.B. die Relayers im Protokoll 0x). Ferner können dezentrale Handelsplattformen Funktionen übernehmen, die Ähnlichkeiten mit der traditionellen Portfolioverwaltung oder kollektiven Kapitalanlagen besitzen. Aufgrund der technischen Offenheit solcher Protokolle ist zu erwarten, dass dezentrale Handelsplattformen ganz grundsätzlich nicht nur ein Ort des Austausches von Kryptovermögenswerten sind, sondern dass deren Protokolle über die Zeit eine Reihe weiterer Dienstleistungen für Nutzer integrieren werden.

Zusammenfassend kann festgehalten werden, dass dezentrale Handelsplattformen Disintermediationseffekte auf mehreren Ebenen aufweisen.⁴⁴⁹ Konkret sind der Bereich der finanzintermediären Verwahrung von Finanzkontrakten sowie die vollständige Wertschöpfungskette traditioneller Finanzmarktinfrastrukturen betroffen, namentlich die Handelsfunktion, die Funktion der zentralen Gegenpartei, die Abwicklungs- und Verwahrungsfunktion sowie die Zahlungsfunktion.⁴⁵⁰ Diese unterschiedlichen Funktionen werden heute klar auseinandergehalten.⁴⁵¹ Die Disintermediation führt zudem dazu, dass die unterschiedlichen, bisher überwiegend von Finanzintermediären und Finanzmarktinfrastrukturen einzeln erbrachten Dienstleistungen auf dezentralen Handelsplattformen *ineinander übergehen*.⁴⁵² An die Stelle des im bisherigen schweizerischen Börsenhandel vertikal integrierten Silokonzepts tritt nunmehr ein vollintegriertes System interoperabler Computerprotokolle.⁴⁵³

⁴⁴⁹ GL.M. Johnstone, *Stanford Journal of Blockchain, Law & Policy* 2020, 159.

⁴⁵⁰ Siehe zur *Swiss Value Chain* Haene/Sturm, *Finanzmarktinfrastuktur*, 7; ferner Hoffmann, in: Boemle et al., *Swiss value chain*, 1011.

⁴⁵¹ Anschaulich BIS, *Delivery versus Payment in Securities Settlement Systems*, 10–12.

⁴⁵² Gemäss Art. 10 Abs. 1 FinfraG darf eine juristische Person grundsätzlich lediglich eine Finanzmarktinfrastuktur betreiben.

⁴⁵³ Vgl. zum *Silokonzept* Nobel/Zimmermann, *SZW* 2011, 513, 528.

Tatsächlich ermöglichen dezentrale Systeme alle traditionellen Funktionen des Handels von Vermögenswerten, der Abrechnung und Abwicklung von Austauschgeschäften sowie der Verwahrung von Vermögenswerten.⁴⁵⁴ FEDERICO PANISI, ROSS P. BUCKLEY und DOUGLAS ARNER bezeichnen diese Entwicklung als «mutualization of the entire financial market infrastructure».⁴⁵⁵ Der Begriff der *Mutualisierung* entstammt der Börsengeschichte und bezieht sich auf den quasi-öffentlichen und mitgliedschaftlich organisierten Betrieb eines Börsenplatzes i.d.R. in Form eines Vereins oder einer Genossenschaft.⁴⁵⁶

Grundsätzlich nicht Gegenstand der vorliegenden Untersuchung sind Einrichtungen, welche Käufer und Verkäufer zusammenbringen, damit diese Handelsgeschäfte in Kryptovermögenswerten eingehen können, wobei die Nutzer einer solchen Plattform die Vermögenswerte der Betreiberin anzuvertrauen haben. Es handelt sich dabei um *zentrale Modelle* von Kryptohandelsplattformen, welche wie traditionelle Handelsplätze und Handelssysteme von einer klar identifizierbaren Person mit klar identifizierbarem Domizil betrieben werden.⁴⁵⁷ Sie können im Einzelnen zwar wesentliche Funktionsunterschiede zu traditionellen Handelssystemen aufweisen, doch sind auch sie letztlich logisch zentralisiert, weshalb die bestehenden Prinzipien des Finanzmarktrechts, wenn auch allenfalls in modifizierter Form, weiterhin Gültigkeit besitzen.⁴⁵⁸

⁴⁵⁴ Vgl. auch Micheler/von der Heyde, *Butterworths Journal of International Banking and Financial Law* 2016, 653 («[...] merge into one real time process [...]»); ferner bezüglich Konsortium-Blockchains Peters/Panayi, in: Tasca et al., *Modern Banking Ledgers*, 272–273.

⁴⁵⁵ Panisi/Buckley/Arner, *Stanford Journal of Blockchain Law & Policy* 2019, 210 m.w.H. zum Begriff.

⁴⁵⁶ Siehe hierzu Nobel, *Finanzmarktrecht*, § 1 N 257.

⁴⁵⁷ Die vorliegende Arbeit unterscheidet zwischen *Custodial Handelsplattformen* und *Custodial OTC-Handelsplattformen (Broker)*; siehe hierzu unten, [IV.3.2.](#)

⁴⁵⁸ Vgl. in diesem Zusammenhang Bundesrat, *DLT-Bericht* 2018, 105–106, 146; ferner den Bericht der IOSCO, *Crypto-Asset Trading Platforms*, 6–9.

5. Netzwerkbasierte Intermediation

5.1 Einleitung

Als die Hauptinnovation von DeFi wird gemeinhin der Verzicht auf Finanzintermediäre betrachtet.⁴⁵⁹ Die traditionelle Finanzintermediation könnte deshalb vor einer historischen Zäsur stehen: Sie wird durch Kryptowährungen, wie namentlich Bitcoin und Ethereum, nicht nur im Bereich der Zahlungssysteme oder in ihrer Custodian-Funktion,⁴⁶⁰ sondern durch das Aufkommen dezentraler Handelsplattformen auch im Bereich ihrer Exchange-Funktion infrage gestellt.⁴⁶¹

Die weggefallenen Finanzintermediäre hinterlassen allerdings kein Vakuum. Das Gegenteil ist der Fall: Ein ganzes Netzwerk von Personen und Computern ersetzen die bisherigen Intermediäre. Entsprechend spricht die vorliegende Arbeit von der *netzwerkbasierten Intermediation*.

Die folgenden Ausführungen befassen sich hauptsächlich mit einer ökonomischen und soziotechnischen Perspektive auf die Eigenschaften dezentraler Systeme.

5.2 Ökonomische Eigenschaften

a. Neuartige Form der wirtschaftlichen Organisation

In Anlehnung an COASE, der in seinem für die modernen Wirtschaftswissenschaften bahnbrechenden Aufsatz von 1937 der Frage nachgegangen ist, weshalb Austauschgeschäfte in vielen Fällen vertikal innerhalb eines Unter-

⁴⁵⁹ Siehe etwa Schär, Federal Reserve Bank of St. Louis Review 2021, 152; Harvey/Ramachandran/Santoro, DeFi, 2; Lin, Stanford Journal of Blockchain Law & Policy 2019, 58; Tapscott/Tapscott, MIT Sloan Management Review 2017, 10–11; hinsichtlich Bitcoin bereits Andreessen, Why Bitcoin Matters, *passim*; Antonopoulos, Mastering Bitcoin, 1–5; Berentsen/Schär, Bitcoin, 51; Voshmgir, in: Braegelmann/Kaulartz, Smart Contracts, § 2 N 4; Bonneau et al., Proceedings 2015 IEEE Symposium on Security and Privacy, 106; Harvey, Cryptofinance, 2; sodann auch BIS/CPMI, Digital Currencies 2015, 5 («the key innovation»).

⁴⁶⁰ Siehe Antonopoulos, Mastering Bitcoin, 3; Berentsen/Schär, Bitcoin, 50–51; De Filippi/Wright, Blockchain and the Law, 34; Enz, Kryptowährungen, N 57 m.w.N.

⁴⁶¹ GLM. Johnstone, Stanford Journal of Blockchain, Law & Policy 2020, 168.

nehmens oder einer Gruppe von Unternehmen anstelle horizontaler Markttransaktionen abgewickelt werden,⁴⁶² steht im vorliegenden Abschnitt die Frage im Mittelpunkt, inwiefern sich dezentrale Systeme von der traditionellen Finanzintermediation in puncto Organisation ökonomischer Prozesse und Strukturen unterscheidet.⁴⁶³

DeFi-Anwendungen treten in der Praxis in den unterschiedlichsten Ausprägungen in Erscheinung. Eine einheitliche Einordnung ist kaum möglich. Nachfolgend kann es darum lediglich um die Erläuterung gewisser Gemeinsamkeiten dezentraler Systeme gehen.

Vereinfachend dargestellt besteht DeFi aus einem *dezentralen System*, deren einzelnen Komponenten, namentlich dezentrale Netzwerke und dezentrale Applikationen, von einer Vielzahl von Teilnehmern erbracht werden. Der Begriff der Erbringung ist dabei weit zu verstehen, wobei er insb. die Produktion, Unterhaltung und Weiterentwicklung eines dezentralen Systems umfasst. Eine weitere Komponente sind sodann Governance-Mechanismen, welche dazu dienen, die Produktion, Unterhaltung und Weiterentwicklung eines dezentralen Systems zu koordinieren. Grundlage eines dezentralen Systems bilden schliesslich computergestützte Regeln, typischerweise in Form eines Protokolls.⁴⁶⁴

Über die ökonomischen Eigenschaften eines dezentralen Systems besteht in der Literatur wenig Einigkeit:

- Die gemeinschaftliche Erbringung der Systemkomponenten weist daraufhin, dass es sich um eine Art (digitales) Netzwerk- bzw. Systemgut handeln könnte.⁴⁶⁵ In systemtheoretischer Hinsicht ist keine Komponente eines dezentralen Systems derart relevant bzw. «dominant», dass ihr Wegfall die Existenz oder Funktionsweise des Systems bedrohen würde.⁴⁶⁶ In den Computerwissenschaften wird in diesem Zusammenhang von der Vermeidung eines Single Point of Failure bzw. SPoF innerhalb eines Computernetzwerks gesprochen.⁴⁶⁷ Ohne Zweifel organisieren sich dezentrale Systeme in einer netzwerkartigen Weise. Dies ist offen-

⁴⁶² Vgl. Coase, *Economica*, 390 («Our task is to attempt to discover why a firm emerges at all in a specialised exchange economy.»).

⁴⁶³ In diesem Sinne auch Casey et al., *Impact of Blockchain Technology*, 13.

⁴⁶⁴ Ausführlich zu diesen Begrifflichkeiten unten, [III.2](#).

⁴⁶⁵ Zu den Begriffen siehe Clement et al., *Internet-Ökonomie*, 34–35, 41–42.

⁴⁶⁶ Vgl. von Bertalanffy, *General System Theory*, 72–73.

⁴⁶⁷ Siehe Yaga et al., *Blockchain*, 2; Berentsen/Schär, *Bitcoin*, 95–96; Jacquemart, *Offene Blockchainsysteme*, Rz. 203 m.w.N.

sichtlich der Fall bei dezentralen Netzwerken; eine netzwerkartige Organisation kann aber auch im Falle dezentraler Applikationen von Bedeutung sein. Der Einordnung als Netzwerk widerspricht allerdings die offene und frei zugängliche Natur dezentraler Systeme.⁴⁶⁸ Die Analogie zu einer öffentlichen Infrastruktur bietet sich demgegenüber an.

- Nutzer dezentraler Systeme interagieren direkt miteinander (Peer-to-Peer, P2P); ihre Interaktionen werden lediglich durch das Computernetzwerk basierend auf den Regeln eines Protokolls intermediatisiert.⁴⁶⁹ Dieser Aspekt weist also eher auf *marktbasierte* Austauschgeschäfte hin. Eine Evolution der Produktion und Koordination von Gütern und Dienstleistungen weg von Hierarchien und hin zu Märkten wird für computergestützte Technologien in der Literatur seit den 1980er Jahren festgestellt.⁴⁷⁰ Im Unterschied zu traditionellen zwei- und mehrseitigen elektronischen Märkten, wie z.B. solchen für Kreditkartenzahlungen oder Computersoftware,⁴⁷¹ weisen dezentrale Systeme aufgrund der Vielzahl an Teilnehmern und Nutzern *unzählige Seiten* auf, ohne dass zentrale Interaktions- oder Koordinationspunkte vorhanden sind.⁴⁷² Da die Märkte dezentraler Systeme frei zugänglich sind, tendieren sie viel stärker als traditionelle mehrseitige Märkte dazu, eigentliche Ökosysteme zu entwickeln, von denen sie einen Bestandteil bilden. Auch diesbezüglich besteht eine Ähnlichkeit mit öffentlichen Infrastrukturen.
- Namentlich bildet sich an der Peripherie dezentraler Systeme ein überwiegend informationsbasiertes Ökosystem⁴⁷³ aus, deren Fortentwicklung letztlich wie das Internet selbst aus dem Zusammenspiel von positiven und negativen Netzwerkeffekten bestimmt wird.⁴⁷⁴ Zu diesem Ökosystem zählen etwa Softwareentwickler, Wallet-Anbieter, Hardwarehersteller und die Betreiber von Kryptohandelsplattformen. Deren Bedeutung als

⁴⁶⁸ Vgl. Powell, Research in Organizational Behavior 1999, 305.

⁴⁶⁹ Vgl. Yaga et al., Blockchain, 2; Catalini/Gans, ACM 2020, 80; Lee, Business Horizons 2019, 775; ausführlich Bonneau et al., Proceedings 2015 IEEE Symposium on Security and Privacy, 108–109.

⁴⁷⁰ Siehe insb. Malone/Yates/Benjamin, Communications of the ACM 1987, 489–490.

⁴⁷¹ Siehe hierzu Rysman, Journal of Perspectives 2009, 125–126, 128–129; Rochet/Tirole, Journal of the European Economic Association 2003, 992.

⁴⁷² Gl.M. Berg/Davidson/Potts, frontiers in Blockchain 2020, 4.

⁴⁷³ Zum Begriff Jacobides/Cennamo/Gawer, Strategic Management Journal 2018, 10 («An ecosystem is a set of actors with varying degrees of multilateral, nongeneric complementarities that are not fully hierarchically controlled.»).

⁴⁷⁴ Eingehend zu «network externalities» bzw. «network effects» von Informationsökonomien Shapiro/Varian, Information Rules, 13–14, 183–184.

faktische Koordinationspunkte im Ökosystem sowie deren Informationsvorsprung gegenüber anderen Marktteilnehmern weisen schliesslich auf hierarchische Elemente in dezentralen Systemen hin.⁴⁷⁵

Dezentrale Systeme können nach dem Gesagten nicht ohne Weiteres in die Trichotomie von Markt, Hierarchien und Netzwerken im Sinne der Transaktionskostenökonomik eingeordnet werden.⁴⁷⁶ Im Gegenteil sind in dezentralen Systemen Elemente unterschiedlicher traditioneller Organisationsformen wiederzuerkennen, wobei gänzlich eigenständige Elemente hinzukommen.⁴⁷⁷ SINCLAIR DAVIDSON, PRIMAVERA DE FILIPPI und JASON POTTS sprechen darum in Anlehnung an die Transaktionskostenökonomik von WILLIAMSON⁴⁷⁸ und DOUGLAS C. NORTH⁴⁷⁹ zu Recht von einer «[...] new coordination technology [...] [that] compete[s] with other economic institutions of capitalism, namely] firms, markets and economies as institutional alternatives for coordinating the economic actions of groups of people [...]».⁴⁸⁰ Die drei Autoren bezeichnen Blockchain-Technologien als Decentralized Collaborative Organisations bzw. DCOs:

*«A DCO is a self-governing organisation with the coordination properties of a market, the governance properties of a commons and the constitutional, legal and monetary properties of a nation state.»*⁴⁸¹

In einer vertieften Auseinandersetzung mit der Thematik kommen die erwähnten Autoren sodann zum Schluss, dass Blockchains in erster Linie neben die bestehenden Institutionen treten, unter Umständen allerdings mit diesen konkurrieren.⁴⁸² Ähnlich klingt die Auffassung von ARUN SUNDARARAJAN, der von

⁴⁷⁵ Siehe mehr hierzu unten, IV.5.2.

⁴⁷⁶ Siehe hierzu oben, II.2.3.

⁴⁷⁷ G.L.M. MacDonald/Allen/Potts, in: Tasca et al., Self-Organized Economies, insb. 286; so auch Lumineau/Wang/Schilke, Organization Science 2021, 505–506; ferner wohl auch Catalini/Gans, Communications of the ACM 2020, 86 m.Verw. auf Catalini/Boslego, MIT Working Paper 2019, passim; vgl. ferner Seidel Marc-David L., Journal of Management Inquiry 2017, 4 m.w.H.

⁴⁷⁸ Siehe Williamson, Economic Institutions, 15.

⁴⁷⁹ Siehe z.B. North, Institutions, 64.

⁴⁸⁰ Davidson/De Filippi/Potts, Journal of Institutional Economics 2018, 646–647, 653, wobei die Autoren in der Tendenz von einer Verschiebung zu Märkten ausgehen; diesbezüglich wohl ähnlich Catalini/Gans, Communications of the ACM 2020, 89.

⁴⁸¹ Davidson/De Filippi/Potts, Journal of Institutional Economics 2018, 654.

⁴⁸² Siehe Berg/Davidson/Potts, Institutional Cryptoeconomics, Introduction («Institutional cryptoeconomics adds another institutional form to this schema: blockchains. Blockchains are an economic infrastructure, alongside markets, the firm, governments, clubs, and the commons, for coordination and exchange. They have distinct economic characteristics that

einem neuen «crowd-based capitalism» spricht, in denen eine Gemeinschaft aus Netzwerkteilnehmern Vertrauen schaffen, wo vorher kein Vertrauen bestand.⁴⁸³

Nach vorliegender Auffassung stellen DeFi-Anwendungen eine *neuartige Form der gemeinschaftlichen Organisation* wirtschaftlicher Transaktionen dar, die nicht primär auf ökonomischer Effizienz, sondern auf Vertrauensminimierung und Kontrollverteilung ausgerichtet ist (siehe zu diesen Punkten weiter unten). Diese Form der Organisation ist in erster Linie als Koordination und erst danach als Kooperation zu verstehen.

b. Überwindung kollektiver Handlungsprobleme

Allerdings bringt die Koordination einer Vielzahl von Personen im Hinblick auf ein gemeinsames Ziel strukturelle Herausforderungen für dezentrale Systeme mit sich.

Vorab ist kurz auf die unterschiedliche Natur von Gütern nach der ökonomischen Theorie einzugehen:

- Traditionell wird zwischen *öffentlichen* und *privaten* Gütern Die entscheidenden Kriterien zur Unterscheidung der beiden Güterkategorien sind die Ausschliessbarkeit und Rivalität des Konsums bzw. der Nutzung durch Dritte.⁴⁸⁴ Bei öffentlichen Gütern, wie bspw. der Landesverteidigung, können Dritte nicht vom Konsum ausgeschlossen werden; ihr Konsum führt zudem nicht zu einer Verringerung der Verfügbarkeit des öffentlichen Gutes für die übrigen Konsumenten. Demgegenüber können Dritte vom Konsum eines privaten Gutes, wie bspw. einer Fahrrades, ausgeschlossen werden; der Konsum führt zudem zur Verringerung der Verfügbarkeit des privaten Gutes für alle anderen Personen.
- Die Theorien kollektiven bzw. sozialen Handelns untersuchen, unter welchen Bedingungen Parteien kooperieren, um ein für sie gemeinsames, sozial nützliches Ziel zu erreichen. MANCUR OLSON geht dabei von der Prämisse aus, dass eine Person, die nicht von den Vorteilen eines kollektiven Guts ausgeschlossen werden kann (sog. Free-Riding-Problem), gar nicht

give them the potential to complement, and in some circumstances directly compete with, this existing suite of institutional choices.»).

⁴⁸³ Siehe Sundararajan, *The Sharing Economy*, 26–27, 60, 95–96.

⁴⁸⁴ Siehe Mankiw, *Microeconomics*, 212–213; ferner Samuelson/Nordhaus, *Microeconomics*, 272.

erst zu den Kosten und Lasten der Bereitstellung des Gutes beitragen wird. Daraus leitet er ab, dass in Fällen, in denen ein Handeln im Hinblick auf die Realisierung eines gemeinsamen Ziels nicht im rationalen Eigeninteresse der einzelnen Gruppenmitglieder ist, im Extremfall keiner handelt oder nur wenige handeln, weshalb die Gruppe das aus ihrer Sicht sozial nützliche Ziel nicht erreichen wird.⁴⁸⁵ Bei gewissen öffentlichen Gütern, wie beispielsweise einem angemessenen Klimaschutz, kann sich daraus ein *kollektive Handlungsproblem*⁴⁸⁶

Regelmässig wird der Staat darum ein *Marktversagen*⁴⁸⁷ in Form negativer oder positiver Externalitäten erkennen, was ihn zum Handeln bewegt, in dessen Folge er bspw. das öffentliche Gut selbst produziert oder Trittbrettfahrer vom Konsum auszuschliessen oder zu besteuern versucht.⁴⁸⁸ Jede Form menschlicher Kooperation im Hinblick auf ein gemeinsames Ziel ist letztlich mit Informations- und Koordinationskosten für die Beteiligten und allenfalls für Dritte verbunden.

Ferner gehen andere Ansätze davon aus, dass auch öffentliche Güter nicht in jedem Fall durch den Staat bereitgestellt werden müssen:⁴⁸⁹

- Nach JAMES M. BUCHANAN ist es ohne weiteres möglich, Personen von der Nutzung von Gütern mit Öffentlichkeitscharakter auszuschliessen (sog. *Clubs*). Clubgüter sind ökonomische Güter, die grundsätzlich ähnlich wie öffentliche Güter keine Konsumrivalität aufweisen, jedoch aufgrund ihrer Natur ähnlich wie private Güter den Ausschluss von Nichtberech-

⁴⁸⁵ Ausführlich Olson, *Collective Action*, 2.

⁴⁸⁶ Mit dem *Collective Action*-Problem eng verwandt sind das spieltheoretische Gefangenendilemma (*Prisoner's Dilemma*) und die Tragik der Allmende (*The Tragedy of the Commons*); siehe hierzu Campbell, in: Campbell/Sowden, *Background*, 4–14; Hardin, *Science* 1968, 1244.

⁴⁸⁷ Allerdings ist zu betonen, dass die Absolutheit des Begriffs des *Marktversagens* irreführend ist. Ein «Marktversagen» muss vielmehr als ein Spektrum von Unvollkommenheiten begriffen werden, welche in unterschiedlichem Masse zur Erschwerung des marktbasierten Tausches führen können; vgl. Arrow, in: Haveman/Margolis, *Market Allocation*, 513; Furubotn/Richter, *New Institutional Economics*, 73; ferner von der Crone/Beyeler/Dédeyan, ZSR 2003 I, 440 FN 131; Watter/Spillmann, *GesKR* 2006, 98 FN 40. Hinzu kommt, dass das angebliche Marktversagen die Folge staatlicher Interventionen sein kann oder dass bestehende Marktversagen durch staatliche Interventionen verschärft werden können oder ihre zeitnahe Auflösung zumindest behindert werden kann; vgl. Kirzner, in: Kirzner, *The Perils of Regulation*, 136–145.

⁴⁸⁸ Siehe Mankiw, *Microeconomics*, 213; Samuelson/Nordhaus, *Microeconomics*, 36–37, 271–277.

⁴⁸⁹ Vgl. etwa die berühmte «Leuchtturmdebatte» bei Coase, *Firm, Market, Law*, 187–191.

tigten zulassen (z.B. der Betrieb eines Schwimmbades). Der Konsum von Clubgütern ist zumindest bis zum Grad der Überlastung des Gutes nicht-trivialisierend.⁴⁹⁰ Damit ein Clubgut vorliegt, müssen genügend Berechtigte bereit sein, die gemeinsamen Kosten zu teilen und Nichtberechtigte von der Teilnahme und dem Konsum des Gutes auszuschliessen.⁴⁹¹ Clubgüter stellen damit eine Brücke zwischen reinen privaten Gütern (z.B. Fahrrad) und reinen öffentlichen Gütern (z.B. Luft) dar.⁴⁹²

- ELINOR OSTROM weist sodann für den Bereich der Gemeingüter (sog. *Common-Pool Resources*) empirisch nach, dass eine Alternative zum Markt und zur Hierarchie, womit der Staat gemeint ist, existieren kann.⁴⁹³ Als Gemeingüter gelten etwa Fischgründe. Nach OSTROMS Erkenntnissen aufgrund konkreter Untersuchungen ist kollektives Handeln in Bezug auf Gemeingüter trotz der Vielzahl der beteiligten Personen möglich, wenn gewisse Gestaltungsprinzipien eingehalten werden.⁴⁹⁴

OSTROMS Erkenntnisse wurden sodann auf die digitale Welt ausgedehnt: Die Untersuchung von als Knowledge Commons bzw. Digital Commons bezeichneten Gemeingütern fokussiert sich dabei u.a. auch auf das allgemeine Phänomen der Peer Production und im Besonderen auf die Entwicklung von Open-Source-Software.⁴⁹⁵ Hierzu sind etwa Wikipedia oder Linux-Betriebssysteme zu zählen.

Die Überwindung kollektiver Handlungsprobleme, die in *dezentralen* Systemen in unterschiedlichen Formen auftreten, kann im Prinzip anhand der ökonomischen Theorien zu Club- und Gemeingütern beschrieben werden. Es wird an mehreren Stellen dieser Arbeit darauf zurückzukommen sein.⁴⁹⁶ Hier sei lediglich beispielhaft erwähnt, dass dezentrale Netzwerke kryptoökonomische Anreizsysteme vorsehen, welche derart konzipiert sind, dass die involvierten Personen nicht in opportunistischer Weise gegen die Konsensregeln des Protokolls verstossen.⁴⁹⁷ Auf diese Weise kann etwa das kollektive Handlungsproblem der Bereitstellung des Netzwerks überwunden werden.

⁴⁹⁰ Siehe Buchanan, *Economica* 1965, 3, 7–8.

⁴⁹¹ Siehe Buchanan, *Economica* 1965, 1–3; ferner Sandler, *Constitutional Political Economy* 2013, insb. 265–266.

⁴⁹² Siehe Buchanan, *Economica* 1965, 1; Ostrom, *The American Economic Review* 2010, 644–645; ferner Leeson, *Journal of Economic Behavior & Organization* 2011, 303.

⁴⁹³ Ostrom, *Governing the Commons*, 8–18.

⁴⁹⁴ Siehe zu den Gestaltungsprinzipien unten, [IV.5.2g.i](#).

⁴⁹⁵ Siehe Hess/Ostrom, in: Hess/Ostrom, *Overview of the Knowledge Commons*, 3–26; Benkler, *Wealth of Networks*, 5, 59–90.

⁴⁹⁶ Vgl. etwa ausführlich unten, [IV.5.2g](#).

⁴⁹⁷ Siehe unten, [II.5.3b.ii](#).

c. Reduktion traditioneller Kontroll- und Vertrauensrisiken

Traditionelle Kontroll- und Vertrauensrisiken werden in dezentralen Systemen, wenn nicht vollständig eliminiert, doch massgeblich reduziert. Zwei Umstände tragen hierzu bei: Einerseits die transaktionale Transparenz, welche die Ausführung und Abwicklung von Transaktionen für die Vertragspartei beobachtbar macht. Andererseits der Abbau von Informationsasymmetrien zwischen den an einer Transaktion beteiligten Parteien, die sich insb. im Verlauf der Vertragsausführung manifestieren können.

Die Möglichkeit zur Überwachung des Verhaltens der Gegenpartei wird bei WILLIAMSON als eine Teilaufgabe von Governance angesehen und ist freilich je nach Ausgestaltung mit höheren oder tieferen Transaktionskosten verbunden.⁴⁹⁸ Die verbesserte Beobachtbarkeit des Verhaltens der Teilnehmer in dezentralen Systemen senkt grundsätzlich die mit der Governance zusammenhängenden Transaktionskosten gegenüber vergleichbaren traditionellen Prozessen und Strukturen. Erfasst werden v.a. opportunistische Verhaltensweisen, welche sich *ex post*, d.h. nach Vertragsschluss, manifestieren können. Hierzu gehören insb. auch Moral Hazard-Risiken des Prinzipals.⁴⁹⁹ Ferner sinken die Transaktionskosten wirtschaftlicher Austauschprozesse aufgrund der Möglichkeit, den Vollzug von Verträgen mithilfe von Smart Contracts zu automatisieren.⁵⁰⁰ Verdeckte Eigenschaften oder verdeckte Handlungen des Agen-

⁴⁹⁸ Siehe Williamson, *Economic Institutions*, 18, 28–29, 30–32.

⁴⁹⁹ So bereits Szabo, *Public Networks*, *passim*; siehe ferner Yermack, *Review of Finance* 2017, 26; Davidson/De Filippi/Potts, *Journal of Institutional Economics* 2018, 650–652; MacDonald/Allen/Potts, in: Tasca et al., *Self-Organized Economies*, 287–288; Werbach/Cornell, *Duke Law Journal* 2017, 348; Kaal, *University of St. Thomas (Minnesota) Legal Studies Research Paper* Nr. 19–23, 5. Dezember 2019, 23–24; vgl. ferner Chen/Bellavitis, *Journal of Business Venturing Insights* 2020, 2; kritisch Böhme et al., *Journal of Economic Perspectives* 2015, 233; ferner Vatiello, *Smart contracts*, 25. Februar 2020, 4–5, 10–13, welcher Smart Contracts aufgrund der fehlenden Anpassungsfähigkeit an geänderte Umstände als kostenineffizient im Vergleich zu traditionellen semantischen Verträgen betrachtet, die bspw. durch Nachverhandlung der Parteien oder richterliches Urteil modifiziert werden können. Der Autor vernachlässigt allerdings die Möglichkeit, Smart Contracts z.B. aufgrund einer DAO-Abstimmung nachträglich zu verändern, oder dies unter Einsatz von künstlicher Intelligenz zu tun; vgl. Wu, *Columbia Law Review* 2019, 2020–2025.

⁵⁰⁰ So bereits Surden, *University of California Davis Law Review* 2012, 689–690; sodann in Bezug auf Blockchains Lumineau/Wang/Schilke, *Organization Science* 2021, 510–511; Davidson/De Filippi/Potts, *Economics of Blockchain*, 9, die davon sprechen, dass Blockchains «[...] an economic world of complete contracts [...]» erlauben; differenzierend Murray et., *Academy of Management Perspectives* 2019, 16–22.

ten sind aufgrund der Transparenz und der Automatisierung der Vertragsabführung viel weniger relevant für den Prinzipal.⁵⁰¹

Hinzukommt, dass in dezentralen Systemen keine festen Rollen existieren. So können Nutzer einer dezentralen Applikation gleichzeitig auch Teilnehmer des zugrundeliegenden dezentralen Netzwerks sein. Die mit klassischen Agency-Beziehungen verbundene Dichotomie in Prinzipal und Agent wird dadurch stark relativiert.⁵⁰² Es ist deshalb damit zu rechnen, dass die traditionellen Transaktionskosten im Zusammenhang mit der Strukturierung von Austauschgeschäften in dezentralen Systemen deutlich verringert werden können.⁵⁰³

Demgegenüber ist mit dem Wegfall von traditionellen intermediären Prozessen und Strukturen selbstredend nicht in jedem Fall auch die Beseitigung jeglicher Form von Informationsasymmetrie verbunden. Relevant sind namentlich Asymmetrien, die sich *ex ante*, d.h. vor Vertragsschluss, auswirken können.⁵⁰⁴

d. Unmittelbare Zuordnung von Handlungs- und Verfügungsrechten

Handlungs- und Verfügungsrechte, d.h. sog. *Property Rights*, sind zentrale Bausteine der ökonomischen Theorie.⁵⁰⁵ Handlungs- und Verfügungsrechte erlauben dem Inhaber darüber zu bestimmen, welchem Zweck ein ökonomisches Gut zugeführt wird.⁵⁰⁶

⁵⁰¹ Vgl. zu diesen Faktoren Bernet, Finanzintermediation, 93.

⁵⁰² Vgl. Williamson, *Managerial and Decision Economics* 1993, 97 («But for opportunism, most forms of complex contracting and hierarchy vanish.»), 99–100; differenzierend Hodgson, *Industrial and Corporate Change* 2004, 405, 409, welcher insb. Interpretationsdefizite zwischen Prinzipal und Agent betont, die allerdings beim Einsatz von Smart Contracts gerade nicht existieren. Dies schließt allerdings nicht aus, dass Smart Contracts im Einzelfall unvollständig sind.

⁵⁰³ A.M. Lumineau/Wang/Schilke, *Organization Science* 2021, 510–511, die davon ausgehen, dass die Kosten im Zusammenhang mit der Strukturierung von Transaktionen («designing costs») tendenziell höher ausfallen dürften. Diese Einschätzung mag in einer Anfangsphase zutreffend sein, sie dürfte allerdings künftig nach genügender Standardisierung des Softwarecodes kaum mehr richtig sein.

⁵⁰⁴ Siehe zu den Informationsrisiken bei Nutzung dezentraler Handelsplattformen unten, [IV.5.2d.](#)

⁵⁰⁵ Siehe Demsetz, *The American Economic Review* 1967, 347.

⁵⁰⁶ Siehe Alchian, in: *The New Palgrave Dictionary of Economics*, Property Rights, 10892 («A property right is a socially enforced right to select uses of an economic good.»).

Handlungs- und Verfügungsrechte vermitteln dem Inhaber insb. Kontrolle, wenn Verträge unvollständig sind, was in der Praxis dem Normalfall entspricht.⁵⁰⁷ Die Definition von Property Rights ist eine zentrale Funktion der Rechtsordnung.⁵⁰⁸ Folglich können die Parteien innerhalb des rechtlichen Rahmens über die konkrete Zuordnung von ökonomischen Handlungs- und Verfügungsrechten frei bestimmen. Die privatautonome Gestaltung und Aufrechterhaltung von Handlungs- und Verfügungsrechten ist indessen mit Transaktionskosten verbunden, deren Höhe von den konkreten rechtlichen und tatsächlichen Bedingungen abhängig ist.⁵⁰⁹

Traditionelle Kontroll- und Vertrauensrisiken, wie sie etwa in intermediarisierten Effektenverwahrungssystemen verbreitet sind, werden in DeFi weitgehend beseitigt.⁵¹⁰ Demgegenüber besteht in dezentralen Systemen ein Gleichlauf zwischen den Handlungs- und Verfügungsrechten an Kryptovermögenswerten und der faktischen Kontrolle über die Vermögenswerte. Die Berechtigung an den Vermögenswerten ist direkt aus dem verteilten Register eines dezentralen Netzwerks ersichtlich. Mithilfe des Private Keys werden die Vermögenswerte sodann bewegt. Dies erlaubt im Gegensatz zum heutigen Finanzintermediationssystem die unmittelbare Zuordnung von Handlungs- und Verfügungsrechten zu einer Person.

Im Ergebnis ist davon auszugehen, dass die Transaktionskosten, die den Inhabern von Kryptovermögenswerten im Zusammenhang mit der Gestaltung und Aufrechterhaltung ihrer Rechte verbunden sind, im Vergleich zu heute abnehmen.

⁵⁰⁷ Siehe Hart, Contracts, 29–30, der von «residual control rights» spricht; ausführlich Hart, The American Economic Review 2017, 1732–1733.

⁵⁰⁸ Vgl. Alchian/Demsetz, The Journal of Economic History 1973, 18, 25; ferner Cooter/Ulen, Law and Economics, 59, die in rechtlicher Hinsicht sodann «property rights» von «contract rights» abgrenzen.

⁵⁰⁹ Siehe Allen, in: Zerbe, Transaction Costs, 1–18, 3–6 m.w.N. («*Transaction costs are the resources used to establish and maintain property rights.*»); Furubotn/Richter, New Institutional Economics, 81–83; ähnlich bereits Coase, Journal of Law and Economics 1960, 15, 19, der sich allerdings auf «legal rights» bezieht; ähnlich, aber ohne Transaktionskostenansatz sodann Hart, The American Economic Review 2017, 1733–1735.

⁵¹⁰ Vgl. in Bezug auf tokenisierte Beteiligungswerte Panisi/Buckley/Arner, Stanford Journal of Blockchain Law & Policy 2019, 213; ferner Mooney, University of Pennsylvania Journal of Business Law 2020, 390, 392, insb. 407; ferner Schwarcz/Benjamin, Duke Journal of Comparative & International Law 2002, *passim*; sodann hinsichtlich Moral Hazard Micheler, Cambridge Law Journal 2015, 532.

Handlungs- und Verfügungsrechte können allerdings dort fraglich sein, wo die in einem verteilten Register verzeichneten Kryptovermögenswerte *im Widerspruch* zur Rechtsordnung stehen. Eine solche Situation kann sich etwa aus einem Hackerangriff auf einen Smart Contract ergeben. In der Kryptogemeinschaft treffen in solchen Fällen regelmässig sehr unterschiedliche Auffassungen zur Frage aufeinander, inwieweit der rechtsrelevante Zustand sich unmittelbar aus der Anwendung des Computercodes ergibt.⁵¹¹ Eine systembedingte Friktion zwischen dezentralen Systemen und der Rechtsordnung kann darüber hinaus in denjenigen Fällen eintreten, in denen die über eine Blockchain getauschten Vermögenswerte über ein eigenständiges Leben in der realen Welt verfügen (z.B. tokenisierte Immobilien).⁵¹² Soweit die Rechtsordnung die Tokenisierung von Vermögenswerten ausserhalb der Blockchain anerkennt, können diese Friktionen allerdings auf ein Minimum reduziert werden.⁵¹³

e. Offener Plattformwettbewerb

Schliesslich weisen dezentrale Systeme und deren Ökosysteme auch in wettbewerbsökonomischer Hinsicht besondere Eigenschaften auf:

In erster Linie ist festzuhalten, dass dezentrale Systeme, deren Protokolle auf dem Internet aufbauen, einige Gemeinsamkeiten mit Internetplattformen haben.⁵¹⁴ In erster Linie ist die grundsätzliche Offenheit solcher Plattformen zu nennen. Allerdings bestehen auch wesentliche Unterschiede zu traditionellen Internetplattformen, welche von enormen Skaleneffekten (Economies of Scale) sowie von Netzwerkeffekten und Wechselkosten profitieren.⁵¹⁵

Dezentrale Systeme weisen namentlich geringere Markteintrittshürden als zentralisierte Internetplattformen auf.⁵¹⁶ Die Gründe dafür liegen insb. in den tieferen Netzwerkkosten, der symmetrischen Informationsverteilung und der

⁵¹¹ Siehe hierzu unten, [II.5.3b](#).

⁵¹² Siehe Arruñada, *European Property Law Journal* 2020, 239–240.

⁵¹³ Vgl. etwa zur Frage der Tokenisierung dinglicher Rechte Bundesrat, DLT-Bericht 2018, 52–53.

⁵¹⁴ Siehe Benkler, *Wealth of Networks*, 394–396.

⁵¹⁵ Siehe etwa Shapiro/Varian, *Information Rules*, 13–14, 21–23, 179–185; ausführlich Farrell/Klemperer, in: Armstrong/Porter, *Coordination and Lock-in, 1972–1975*; sodann für einen aktuellen Überblick der Literatur Jullien/Sand-Zantman, *Information Economics and Policy* 2020, *passim*.

⁵¹⁶ Ähnlich OECD, *Institutionalisation*, 47 m.w.N. Dies in starkem Kontrast zu permissioned bzw. private Blockchains; vgl. hierzu Yermack, *Review of Finance* 2017, 10, 12, 14.

dezentralen Datenhoheit der Nutzer.⁵¹⁷ Ferner scheint die Wettbewerbssituation deutlich ausgeprägter als in den von einigen wenigen Internetplattformen behaupteten Märkten zu sein. Konkret ist nicht nur mit einem Wettbewerb zwischen den unterschiedlichen dezentralen Systemen, sondern besonders auch innerhalb eines dezentralen Systems zu rechnen.⁵¹⁸ Die Tatsache, dass dezentrale Applikationen grundsätzlich interoperabel sind, senkt die Netzwerkeffekte einer einzelnen Applikation und somit auch die Wechselkosten der Nutzer.⁵¹⁹ Die Netzwerkeffekte eines dezentralen Systems und somit des dazugehörigen Ökosystems scheinen aber umso stärker zu sein, je grösser die Interoperabilitätseffekte der Applikationen innerhalb des betreffenden dezentralen Systems ausfallen.⁵²⁰ Dies ist etwa gut an der Marktführerposition der Ethereum Blockchain im DeFi-Bereich erkennbar.

Die Nutzer als «Konsumenten» von DeFi-Anwendungen sind zudem im Vergleich zu traditionellen Plattformnutzern in einer deutlich besseren Verhandlungsposition, wie etwa Untersuchungen zu den Märkten für Transaktionsgebühren zeigen.⁵²¹ Aufgrund der Tatsache, dass die Kontrolle über die Daten und Vermögenswerte bei den Nutzern verbleibt, können diese schliesslich zu sehr tiefen Kosten zwischen unterschiedlichen Applikationen wechseln.⁵²² Schliesslich weisen DeFi-Anwendungen eine weitere Besonderheit im Vergleich zu herkömmlichen Finanzmärkten auf: Gewöhnliche Nutzer können in dezentralen Systemen sowohl als Anbieter als auch als Nachfrager auftreten.⁵²³ Sie können etwa selbst als Liquiditätsgeber oder Market Maker über dezentrale Handelsplattformen agieren.

⁵¹⁷ Siehe Catalini/Gans, Communications of the ACM 2020, 80 («From an economics perspective, this new market design solution provides some of the advantages of a centralized digital platform [...] without some of the consequences the presence of an intermediary may introduce such as increased market power, ability to renege on commitments to ecosystem participants, control over participants' data, and presence of a single point of failure.»), 81–82, 86–88; ausführlich hierzu Lianos, in: Hacker et al., Blockchain and Competition, 336–340, 379; zurückhaltender Cong/He, The Review of Financial Studies 2019, 1754–1797, 1757–1759.

⁵¹⁸ Siehe Abadi/Brunnermeier, NBER Working Paper 25407, Dezember 2019, 20–22, die von «fork competition» zwischen dezentralen Systemen sprechen; Harvey/Ramachandran/Santoro, DeFi, 2, 60, 64.

⁵¹⁹ Vgl. hinsichtlich traditioneller Plattformen Farrell/Klemperer, in: Armstrong/Porter, Coordination and Lock-in, 1976.

⁵²⁰ So auch Harvey/Ramachandran/Santoro, DeFi, 2.

⁵²¹ Siehe Huberman/Leshno/Moallemi, The Review of Economic Studies 2021, 2.

⁵²² Siehe Catalini/Gans, Communications of the ACM 2020, 82, 86, 87, 88–89.

⁵²³ Siehe Amler et al., DeFi-ning DeFi, 2.

Der verschärfte Wettbewerb ist letztlich auf die technische Offenheit der verwendeten Protokolle zurückzuführen: So zeugt die Praxis einerseits von einem sehr dynamischen Ökosystem, das etwa von der Weiterentwicklung von Protokollen durch andere Entwickler (*Software Forks*) oder von der Aufspaltung bestehender Systeme in zwei inkompatible Versionen (*Hard Forks*) geprägt ist.⁵²⁴ Konsequenz dieser Entwicklungsoffenheit ist die Existenz tausender Coins und Tokens, die jedoch mit gewissen Ausnahmen in aller Regel kaum nennenswerte technische Unterschiede aufweisen.⁵²⁵

Im Währungs- und Zahlungsbereich kann die Wettbewerbssituation durchaus mit BENJAMIN KLEINS und VON HAYEKS Konzept des privaten Währungswettbewerbs verglichen werden.⁵²⁶ Andererseits weisen die Bitcoin und Ethereum Blockchain – in Einklang mit den Vorhersagen des Potenzgesetzes –⁵²⁷ bis heute die mit Abstand höchste Marktkapitalisierung auf, wobei erwähnt werden muss, dass der Markt für Kryptovermögenswerte insgesamt in den letzten Jahren rasant gewachsen ist.

5.3 Soziotechnische Eigenschaften

a. Dezentrale Governance

i. Verteiltheit des Konsenses

Die Kombination von Erkenntnissen aus den Computerwissenschaften mit bewährten Konzepten der Ökonomik und Spieltheorie macht es möglich, dass finanzintermediäre Dienstleistungen in gemeinschaftlicher und offener Weise erbracht werden können.⁵²⁸ Als «Spielregeln» dienen die im Protokoll enthal-

⁵²⁴ Während *Software Forks* die logische Konsequenz der Entwicklung von Software unter Open-Source-Lizenzierung darstellen, sind *Hard Forks* kontroverse Ereignisse innerhalb eines dezentralen Systems, die aufgrund einer Änderung grundlegender Protokollregeln (sog. Konsensregeln) zur Aufspaltung des Netzwerks in zwei inkompatible Versionen führen; siehe hierzu die Übersicht bei Antonopoulos, *Mastering Bitcoin*, 273–278; ferner Narayanan et al., *Bitcoin*, 73–75, 171–173.

⁵²⁵ Siehe <https://coinmarketcap.com/>.

⁵²⁶ Siehe Klein, *Journal of Money, Credit and Banking* 1974, *passim*; von Hayek, *Denationalisation of Money*, 14.

⁵²⁷ Vgl. für den Zeitraum zwischen April 2013 und Februar 2018 Wu/Wheatley/Sornette, *Royal Society Open Science* 2018, *passim*.

⁵²⁸ Siehe etwa zu den spieltheoretischen Überlegungen der Anreizmechanismen Yaga et al., *Blockchain*, 5, 37; ferner hinsichtlich Bitcoin Böhme et al., *Journal of Economic Perspec-*

tenen Konsensregeln eines Systems. Dabei wird vorausgesetzt, dass ein gewisser Anteil der Netzwerkteilnehmer ehrlich ist. In der Regel wird erwartet, dass mindestens die Hälfte oder wenigstens ein Drittel aller Teilnehmer das Protokoll korrekt ausführen.⁵²⁹

Die Teilnehmer eines dezentralen Netzwerks müssen sich nicht nur hinsichtlich der Konsensregeln selbst, sondern v.a. auch in Bezug auf die Transaktionshistorie einig sein.⁵³⁰ Diese miteinander verwandten Konsensformen werden in den Computerwissenschaften als *Distributed Consensus* bezeichnet.⁵³¹

Darüber hinaus bedarf es einer Reihe zusätzlicher Governance-Mechanismen, um etwa die Weiterentwicklung eines dezentralen Systems durch die unterschiedlichen Stakeholder zu koordinieren. Governance soll dabei als ein Mechanismus der internen Organisation und Kontrolle eines dezentralen Systems verstanden werden, der grundsätzlich unabhängig vom Rechtssystem ist und (überwiegend) getrennt von ihm abläuft, dieses jedoch nicht überlagert oder ersetzt.⁵³²

ii. Formen dezentraler Governance

In dezentralen Systemen sind zwei Grundformen der Governance zu unterscheiden:⁵³³

- *Governance i.e.S.* setzt sich zusammen aus den Regeln, welche das Systemverhalten bestimmen. Es handelt sich um Governance *durch* das System. Diese Form der Governance wird für das dezentrale Netzwerk insb. in den Konsensregeln und für dezentrale Applikationen in den jeweiligen

tives 2015, 218–219; Bonneau et al., Proceedings 2015 IEEE Symposium on Security and Privacy, 110.

⁵²⁹ Siehe Townsend, Distributed Ledgers, 64–65, 68–70.

⁵³⁰ Vgl. Kroll/Davey/Felten, Economics of Bitcoin Mining, 6–7, die ferner einen Konsens darüber verlangen, dass bitcoins ein Wert zukommt.

⁵³¹ Siehe hierzu Narayanan et al., Bitcoin, 28–30.

⁵³² So auch etwa Nabilou, Stanford Journal of Blockchain Law & Policy 2021, 28; bereits *skeptisch*, was das Verhältnis zwischen «crypto law» und dem Rechtssystem anbelangt, Zamfir, Against Szabo's Law, *passim*; differenzierend Shapiro, In defense of Szabo's Law, *passim*, der Szabos Gesetz als einen Ansatz der Minimierung des gesellschaftlich notwendigen Vertrauens auslegt («social-trust-minimization approach»).

⁵³³ In Anlehnung an De Filippi/Loveluck, Internet Policy Review 2016, 10–12, welche die sinnvolle Unterteilung in «governance by infrastructure» and «governance of infrastructure» vornehmen.

Smart Contracts festgelegt.⁵³⁴ Governance i.e.S. ist im Wesentlichen für die laufende Verhaltenssteuerung der Nutzer solcher Protokolle verantwortlich. Es handelt sich bei ihr um algorithmische Governance.⁵³⁵

- Governance i.w.S. beschäftigt sich mit der Steuerung des Systems durch die Teilnehmer, Nutzer, Entwickler und weitere interessierte Kreise des Ökosystems. Es handelt sich also um die Governance des Governance i.w.S. ist insofern regeländernd, als dass in die laufende Verhaltenssteuerung eines Systems eingegriffen wird. Diese Form der Governance regelt etwa das mehr oder weniger formalisierte Verfahren hinsichtlich Änderungen und Anpassungen an einem Protokoll im Allgemeinen und an den Konsensregeln im Besonderen sowie an Smart Contracts. Diese Form von Governance kann so weit gehen, dass sie selbst Teil der Blockchain ist. In diesem Fall ist von On-chain-Governance die Rede.⁵³⁶ Im Gegensatz zur Off-chain- oder informalen Governance werden hier die Regeln der Entscheidungsfindung *ex ante* festgelegt und die beschlossenen neuen Regeln sodann automatisch nach Erreichen eines bestimmten Quorums und zwar typischerweise auch gegen den Willen einer grösseren Minderheit durchgesetzt.⁵³⁷ Allerdings weisen gerade bedeutende Blockchains, wie etwa Bitcoin und Ethereum, keine Algorithmisierung im Bereich der Governance i.w.S. auf.⁵³⁸

iii. Bazar Governance in der Softwareentwicklung

Die Entwicklung von Computercode bildet Teil der Governance i.w.S. Die Anwendbarkeit der vorherrschenden Governance-Modelle⁵³⁹ des Marktes, der Hierarchie und des Netzwerks auf die Entwicklung von Open-Source-Software in der Literatur ausführlich geprüft und letztlich verneint.⁵⁴⁰

⁵³⁴ Siehe Antonopoulos, *Mastering Bitcoin*, 273; Antonopoulos/Wood, *Mastering Ethereum*, 2, 275, 319; Narayanan et al., *Bitcoin*, 168–170; ferner De Filippi/Hassan, *First Monday*, Dezember 2016, II.A. und II.B.; Weber, *Computer Law & Security Review* 2018, 704.

⁵³⁵ Vgl. zur *kybernetischen Dimension* dezentraler Governance unten, [II.5.3b.iii.](#)

⁵³⁶ So etwa die Tezos Blockchain; vgl. hierzu Goodman, Tezos, 9–10.; ausführlich zu den unterschiedlichen Phasen der Governance in Tezos Arluck, *Amending Tezos*, *passim*.

⁵³⁷ Vgl. für eine gute Übersicht der beiden Governance-Formen EUBOF, Governance of and with Blockchains, 13–14 m.w.H.

⁵³⁸ Vgl. für eine Kritik an On-chain-Governance Zamfir, *Against on-chain governance*, *passim*.

⁵³⁹ Siehe zu diesen oben, [II.2.3.](#)

⁵⁴⁰ So etwa Demil/Lecocq, *Organization Studies* 2006, *passim*.

Demgegenüber werden die Governance-Mechanismen im Bereich der offenen Softwareentwicklung aufgrund der eher losen Prozesse und Strukturen als *Bazar Governance* bezeichnet. Die Literatur weist daraufhin, dass Entwickler auf Basis offener Urheberrechtslizenzen kooperieren und dass innerhalb solcher Gemeinschaften lediglich schwach ausgeprägte Anreiz- und Kontrollstrukturen bestehen.⁵⁴¹ Bazar Governance stellt demnach – im Vergleich zu alternativen Governance-Modellen – eine eigenständige Organisationsform wirtschaftlicher Austauschgeschäfte dar.⁵⁴²

iv. Proof of Human

Jedes menschengemachte System muss versuchen, die Möglichkeiten der beteiligten Personen zu opportunistischem Verhalten auszuschliessen oder zumindest die langfristigen negativen Auswirkungen solchen Verhaltens zu verringern. Die Nützlichkeit eines Systems, in welchem opportunistisches Verhalten der Nutzer allgegenwärtig ist, wäre letztendlich aufgrund der einseitigen Vermögensverteilungseffekte infrage gestellt.

Dezentralen Systemen ist es indessen überwiegend verwehrt, auf die in der traditionellen Finanzintermediation etablierten Governance-Mechanismen zurückzugreifen: Da Nutzer in *pseudonymer* Weise an dezentralen Systemen teilnehmen, spielen direkte und indirekte Kontrollmechanismen, wie etwa Screening und Reputationssysteme, keine oder eine nur sehr unbedeutende Rolle.⁵⁴³ Das Ausbleiben von Reputationseffekten ist u.a. darauf zurückzuführen, dass solche Systeme heute im Wesentlichen ohne bürgerliche Identitäten oder sonstige eindeutige Identitätssysteme auskommen müssen.⁵⁴⁴ Reputations- und Identitätsmechanismen gelten als *Hard Problems* kryptobasierter Systeme, für welche heute noch keine überzeugenden Lösungen bestehen.⁵⁴⁵

Um die Offenheit dezentraler Systeme gewährleisten zu können und dennoch Sybil-Attacken auszuschliessen, arbeiten verschiedene Projekte an der Realisierung dezentraler Identitätssysteme. Solche Identitätssysteme bezwecken den *Proof of (Unique) Human* bzw. *Proof of Personhood*. Dieser Nachweis zielt darauf ab, jedem menschlichen Teilnehmer ein gleiches Mass an Partizipation

⁵⁴¹ Ausführlich Demil/Lecocq, *Organization Studies* 2006, 1452–1454.

⁵⁴² Ebenso Dalle/Jullien, *Research Policy* 2003, 2.

⁵⁴³ Siehe hinsichtlich Reputationsmechanismen Berentsen/Schär, *Bitcoin*, 97; Harvey/Ramachandran/Santoro, *DeFi*, 49–50.

⁵⁴⁴ Siehe hierzu auch unten, III.3.2.

⁵⁴⁵ Siehe für eine Übersicht solcher Herausforderungen Buterin, *Hard Problems*, *passim*.

an einem dezentralen System zu garantieren, d.h. etwa unabhängig von dessen wirtschaftlichen Investitionen in Hardware oder einen bestimmten Vermögenswert.⁵⁴⁶

Es besteht eine Vielzahl von Lösungsansätzen, welche teilweise ihrerseits verteilte Netzwerke in Anspruch nehmen. Microsoft etwa entwickelt eine Open-Source-Identitätsplattform namens Identity Overlay Network (ION)⁵⁴⁷, welche für die Speicherung von Daten IPFS verwendet und für die Gewährleistung der zeitlichen Abfolge von Dateneinträgen auf die Bitcoin Blockchain zurückgreift.⁵⁴⁸ Auf Basis «eindeutiger» digitaler Identitäten kann eine Person etwa eine Blockchain-basierte Anwendung nutzen oder an der dezentralen Governance eines Protokolls partizipieren. Reputationseffekte könnten darum künftig eine grössere Rolle in dezentralen Systemen spielen. Aufgrund solcher Effekte könnte digitalen Identitäten eine institutionalisierende Rolle im Web 3.0 zukommen.⁵⁴⁹

b. Regelbasierte Systeme

i. Code is Law

In dezentralen Systemen werden Mechanismen zur Lösung von Kontroll- und Vertrauensrisiken bereits in das Systemverhalten *eingebettet*. Sie werden namentlich als Regeln formuliert, die sich als Computercode implementieren lassen. Der Computercode wird sodann von den Netzwerkteilnehmern durch Ausführung der Konsensregeln durchgesetzt. Solche Mechanismen gehören damit zur Governance i.e.S.

⁵⁴⁶ Vgl. Borge et al., in: 2017 IEEE European Symposium on Security and Privacy Workshops 2017, 24; ausführlich Ford, in: Bernhold/Landemore/Reich, Technologizing Democracy, 284–289.

⁵⁴⁷ <https://identity.foundation/ion/>.

⁵⁴⁸ Siehe Dingle/Buchner, ION, *passim* («[...] ION has been developed as a decentralized network designed to operate independently of centralized parties and trusted intermediaries, including Microsoft. ION doesn't rely on special utility tokens, trusted validator nodes, or additional consensus mechanisms; the deterministic progression of Bitcoin's linear block chronology is the only consensus it requires. The core promise of DID technology is to empower all individuals and entities with ownership and control over their identities [...]»).

⁵⁴⁹ Vgl. in wirtschaftshistorischer Hinsicht die Bedeutung der privaten Rechtsdurchsetzung der *lex mercatoria* für die Reputation von Gilden im Fernhandel Milgrom/North/Weingast, Economics and Politics 1990, 2–3; ausführlich Greif, Institutions, 428–452.

Die Einhaltung der Regeln ist zwingende Nutzungs- und Teilnahmevoraussetzung des Systems. Aus diesem Grund hat DAVID YERMACK die Parameter eines Blockchain-Protokolls mit den Handelsregeln einer traditionellen Börse verglichen.⁵⁵⁰ Genauer ist allerdings die Charakterisierung der Entscheidungsfindung als dezentrale oder P2P-Governance, denn die Netzwerkteilnehmer entscheiden autonom über die von ihnen angewendeten Konsensregeln.⁵⁵¹

Die Verhaltenssteuerung ist in DeFi insoweit automatisiert, als dass die Vollstreckung der kodierten Regeln in Abweichung zu staatlichen Rechtsnormen *ex ante* erfolgt.⁵⁵² MAX RASKIN verwendet im Kontext von Smart Contracts den Begriff der *Self-Help* als einer ausserstaatlichen Methode der Rechtsdurchsetzung.⁵⁵³ Der Einsatz von Computercode zur Verhaltenssteuerung wurde in der Rechtsliteratur bereits früh mit dem Begriff der «lex informatica»⁵⁵⁴ oder der Formel «Code is Law»⁵⁵⁵ umschrieben. SZABO spricht sodann konzeptionell von «dry code», der in Abweichung zu «wet code» von Computern verstanden und ausgeführt werden kann.⁵⁵⁶

Die verbreitete Code-is-Law-Hypothese hinterfragt die Literatur zumindest im Falle von Hackerangriffen auf Smart Contracts.⁵⁵⁷ Andere Ausprägungen von Code is Law scheinen demgegenüber ohne Weiteres akzeptiert zu sein: Die Konsensregeln des Bitcoin Protokolls etwa setzen für die Entscheidung darüber, welche Transaktionen permanenter Teil des verteilten Registers bilden sollen, auf das Prinzip der längsten Blockchain. Bei Konflikten zwischen mehreren Versionen einer Blockchain setzt sich diejenige Version als Konsensversion durch, welche am meisten Rechenkapazitäten auf sich vereint.⁵⁵⁸

⁵⁵⁰ Siehe Yermack, *Review of Finance* 2017, 26 («These software parameters are akin to the rules and regulations of a stock exchange in which firms agree to list their shares and have them traded by third parties subject agreed-upon constraints and limitations.»).

⁵⁵¹ Vgl. Abramowicz, *Arizona Law Review* 2016, 369, der den Begriff der «peer-to-peer governance» verwendet.

⁵⁵² Siehe De Filippi/Hassan, *First Monday*, Dezember 2016, II.B.; ferner Weber, *Computer Law & Security Review* 2018, 704.

⁵⁵³ Siehe Raskin, *Georgetown Law Technology Review* 2017, 333–337.

⁵⁵⁴ Reidenberg, *Texas Law Review* 1998, 554–555.

⁵⁵⁵ Lessig, *Code*, 5.

⁵⁵⁶ Siehe Szabo, *Wet code and dry*, *passim*.

⁵⁵⁷ Siehe unten, [IV.5.2e.ii](#).

⁵⁵⁸ Siehe Antonopoulos, *Mastering Bitcoin*, 255–256, 260; Berentsen/Schär, *Bitcoin*, 57–58, 216, 217.

Der Entscheidung liegen nicht etwa Fairnesserwägungen oder dergleichen zugrunde, sondern es ist ausschliesslich der ausgeführte Code für die Bestimmung der relevanten Transaktionshistorie massgeblich.⁵⁵⁹

ii. Cryptoeconomics

Das Protokoll von Bitcoin und Ethereum sieht etwa vor, dass nur Transaktionen und Blöcke gültig sind, welche die Konsensregeln des Systems einhalten.⁵⁶⁰ Sodann kann die Teilnahme am Netzwerk von der Bereitstellung einer bestimmten Menge an Rechenkapazität (*Work*) oder der Leistung finanzieller Sicherheiten (*Stake*) abhängig gemacht werden.⁵⁶¹ Proof-of-Work bzw. Proof-of-Stake sind mit anderen Worten Mechanismen, um den Mangel an eindeutigen Identitäten in dezentralen Netzwerken zu ersetzen.

Diese Vorkehrungen allein genügen allerdings nicht, um die langfristige Stabilität und Sicherheit des Systems zu gewährleisten.⁵⁶² Die Protokolle müssen die Teilnahme insb. durch positive und negative ökonomische Anreize fördern. Pekuniäre Belohnungen sind typischerweise positive Anreize; Geldstrafen und der Verlust von Investitionen oder Sicherheiten sind demgegenüber negative Anreize.⁵⁶³ Um die Verknüpfung von Fragen des System- und Marktdesigns mit ökonomischen und spieltheoretischen Konzepten zu beschreiben, hat sich der Begriff der *Cryptoeconomics* durchgesetzt.⁵⁶⁴

Ein positiver Anreiz für die Teilnehmer wird bspw. durch die Schöpfung neuer Geldeinheiten und die Belastung von Transaktionsgebühren geschaffen. Die neu geschöpften Geldeinheiten und Transaktionsgebühren werden den Teil-

⁵⁵⁹ Siehe statt vieler Townsend, *Distributed Ledgers*, 68–70. Der Bundesrat spricht vom «Prinzip der Wahrheit»; vgl. Bundesrat, DLT-Bericht 2018, 21.

⁵⁶⁰ Siehe Antonopoulos, *Mastering Bitcoin*, 273; Antonopoulos/Wood, *Mastering Ethereum*, 2.

⁵⁶¹ Siehe Antonopoulos/Wood, *Mastering Ethereum*, 321.

⁵⁶² Vgl. Buterin, *Visions*, *passim* («to ensure that [the blockchain] keeps going and doesn't go back in time or incur any other glitch»).

⁵⁶³ Siehe Williamson, *The American Economic Review* 1983, *passim*.

⁵⁶⁴ Siehe Zamfir, *What is Cryptoeconomics?*, *passim* («A formal discipline that studies protocols that govern the production, distribution, and consumption of goods and services in a decentralized digital economy. Cryptoeconomics is a practical science that focuses on the design and characterization of these protocols.»); ferner Buterin, *Introduction to Cryptoeconomics*, *passim* («[...] a methodology for building systems that try to guarantee certain kinds of information security properties [...]»); ausführlich Brekke/Alsindi, *Policy Review* 2021, 2; sodann Halaburda et al., *Journal of Economic Literature* 2022, *passim*; ferner zur Verbindung von kryptografischen und ökonomischen Konzepten Gong/Xu, *Cryptoeconomics*, 1–13; Finck, *Blockchain Regulation*, 29–30.

nehmern im Austausch für ihre Leistungen an das Netzwerk vergütet.⁵⁶⁵ Verstöße gegen die eingebetteten Kontrollmechanismen können sodann sanktioniert werden (negativer Anreiz). Das Computerprotokoll kann z.B. für den Fall der Zuwiderhandlung die automatisierte Wegnahme und Zerstörung der geleisteten finanziellen Sicherheit vorsehen.⁵⁶⁶ In diesem Fall ist die Rede von Slashing und/oder Staking-Strafen.⁵⁶⁷

Es handelt sich bei diesen Formen der computerisierten Durchsetzung von Regeln in dezentralen Systemen letztlich um einen Anwendungsfall der *algorithmischen Regulierung* bzw. *Governance*.⁵⁶⁸ Diese Form der Governance bildet die Grundlage für die Koordination und das Zusammenwirken aller beteiligten Parteien eines dezentralen Systems. Ohne diese Regeln wären die oben erwähnten kollektiven Handlungsprobleme gar nicht erst überwindbar.⁵⁶⁹

Dabei ist die Regeldurchsetzung in dem Sinne dezentralisiert, als dass jeder Node *selbständig* darüber entscheidet, welchen Konsensregeln er letztlich folgen will. Anders als in gewöhnlichen verteilten Netzwerken ist damit jeder Teilnehmer entscheidungsautonom, was gerade den Kern dezentraler Governance ausmacht.⁵⁷⁰ Diese Form der Regeldurchsetzung kann am Konzept der sog. User Activated Soft Fork (UASF) in Bitcoin dargestellt werden: Demnach unterliegen Änderungen am Bitcoin Protokoll der Zustimmung einer qualifizierten «ökonomischen Mehrheit» der Netzwerkteilnehmer und Nutzer, und dies notfalls auch gegen den Widerstand der einflussreichen Gruppe der Mi-

⁵⁶⁵ Siehe Nakamoto, Bitcoin, 4; Antonopoulos, Mastering Bitcoin, 229–230; Berentsen/Schär, Bitcoin, 205–206.

⁵⁶⁶ Siehe etwa Antonopoulos/Wood, Mastering Ethereum, 320–321; Harvey/Ramachandran/Santoro, DeFi, 46.

⁵⁶⁷ Siehe hierzu Harvey/Ramachandran/Santoro, DeFi, 47–48.

⁵⁶⁸ Siehe zum Begriff Yeung, Regulation & Governance 2018, 507 («[...] I refer to algorithmic regulation as decisionmaking systems that regulate a domain of activity in order to manage risk or alter behavior through continual computational generation of knowledge from data emitted and directly collected [in real time on a continuous basis] from numerous dynamic components pertaining to the regulated environment in order to identify and, if necessary, automatically refine [or prompt refinement of] the system's operations to attain a prespecified goal.»), ferner hinsichtlich Sanktionen 508–509; sodann Lettieri, in: Barfield, Algorithmic Turn, 701–703; ferner hinsichtlich des Einsatzes von Machine Learning-Algorithmen Hassan/De Filippi, Field Actions Science Reports 2017, 90.

⁵⁶⁹ Siehe Antonopoulos, Mastering Bitcoin, 273; Davidson/De Filippi/Potts, Economics of Blockchain, 13.

⁵⁷⁰ Siehe unten, [III.2.2.](#)

ner.⁵⁷¹ Die ökonomische Mehrheit, wozu insb. gewöhnliche Nutzer, Händler, Wallet-Anbieter und Kryptohandelsplattformen gehören, verschafft letztlich einer Kryptowährung einen Nutzen und somit den Marktwert.⁵⁷² Mit anderen Worten kann sich diese Mehrheit durch Koordination gegen die homogene Gemeinschaft der Miner und andere einflussreiche Akteure durchsetzen.⁵⁷³ Ein Praxisbeispiel findet sich in der langjährigen, kontrovers geführten Debatte um die Skalierung der Bitcoin Blockchain, die letztlich in der Aktivierung des SegWit-Updates endete.⁵⁷⁴

Das Ethereum Protokoll sieht einen im Ergebnis ähnlichen Mechanismus vor: Bei der sog. *Difficulty Bomb* handelt es sich um eine technische Massnahme, welche das Mining der Kryptowährung zunehmend erschwert, was Miner von der «Entschärfung» des Mechanismus durch die übrigen Netzwerkteilnehmer abhängig macht. Aufgrund der Regelmässigkeit, mit welcher die Difficulty Bomb entschärft werden muss, ist das Netzwerk imstande, in kürzeren Zeitabständen neue Updates zu implementieren, und dies allenfalls auch gegen den Willen der Miner.⁵⁷⁵

Spieltheoretisch kann die soziale Dynamik in dezentralen Systemen als ein Spiel mit teils kooperativen, aber v.a. nicht-kooperativen Elementen modelliert werden, das je nach Ausgangslage und Entwicklung mehrere Gleichgewichte mit sehr unterschiedlichem Ausgang aufweisen kann.⁵⁷⁶ Kooperativ ist das Spiel insoweit, als dass Sanktionen und Kontrollmechanismen bereits im Code enthalten sind; nicht-kooperativ sind hingegen all jene Funktionen des Systems, die kompetitiv erbracht werden (Mining, Staking etc.). In beiden Fällen ergibt sich die Stabilität dezentraler Systeme letztlich aus der Mechanik ökonomischer Anreize und somit dem Eigeninteresse der Teilnehmer.⁵⁷⁷

⁵⁷¹ Siehe hinsichtlich der spieltheoretischen Dimension des UASF-Konzepts am Beispiel der Aktivierung des SegWit-Protokollupdates im Sommer 2017 Harper, Bitcoin Independence Day, Bitcoin Magazine, *passim*.

⁵⁷² Siehe statt vieler Atik/Gerro, Stanford Journal of Blockchain Law & Policy 2018, 26–27 m.w.N.

⁵⁷³ Siehe hierzu Antonopoulos, Mastering Bitcoin, 283–284; Berentsen/Schär, Bitcoin, 75–76; Nabilou, Stanford Journal of Blockchain Law & Policy 2021, 47–49.

⁵⁷⁴ Siehe van Wirdum, SegWit, Bitcoin Magazine, *passim*.

⁵⁷⁵ Siehe hierzu EthHub, Ethereum Difficulty Bomb, *passim*.

⁵⁷⁶ Zur Unterscheidung zwischen *kooperativer* und *nicht-kooperativer* Spieltheorie vgl. Holler/Illing/Napel, Spieltheorie, 6–7, 23; ferner Tadelis, Game Theory, 55.

⁵⁷⁷ Vgl. Green, in: Fox/Green, Underlying Technology, N 1.10, welche von einer Angleichung zwischen Eigeninteresse und Altruismus spricht, was zumindest vom Ergebnis her betrachtet richtig ist.

iii. Kybernetische Dimension

Algorithmische Regulierung hat ihre Ursprünge u.a. in der Kybernetik. Gegenstand der kybernetischen Forschung sind die Steuerung und Regelung von natürlichen und künstlichen dynamischen Systemen namentlich durch positive und negative Feedbackmechanismen.⁵⁷⁸ In der Literatur ist umstritten, inwieweit Märkten die homöostatische Befähigung zukommt, von sich aus nicht nachhaltige Entwicklungen zu korrigieren und dadurch wieder in ein Gleichgewicht zu gelangen.⁵⁷⁹

Während die kryptografischen Komponenten eines dezentralen Systems zeitlich rückwärtsgerichtet sind, erlauben dessen ökonomischen Komponenten zukunftsgerichtete Aussagen über das System:⁵⁸⁰ Der Computercode eines dezentralen Systems soll demnach – im Sinne der kybernetischen Theorie – stabile Rahmenbedingungen schaffen, die zu einer langfristigen Angleichung der Verhaltensweisen (nicht jedoch der Interessen oder Motivationen!) der verschiedenen Teilnehmer führen und dadurch Handlungen im kollektiven Interesse gewährleisten. Demgegenüber soll Computercode jede Abweichung vom intendierten Gleichgewicht möglichst prohibitiv kostspielig machen.⁵⁸¹ Daraus folgt, dass dezentrale Systeme – ähnlich wie Organisationen und Institutionen nach herkömmlicher Auffassung –⁵⁸² regelbasierte Systeme darstellen.⁵⁸³

⁵⁷⁸ Siehe Medina, *Kybernetes 2015*, 1006–1007; grundlegend zur *Kybernetik* Wiener, *Cybernetics*, 11–12, 18, 132–133; hinsichtlich der *Rechtsordnung* als kybernetisches System Wiener, *Cybernetics and Society*, 110.

⁵⁷⁹ Siehe etwa von Hayek, *The Mirage of Social Justice*, 124–125, der die von einer freien Marktwirtschaft geschaffenen Ordnung als eine sich selbst regulierende «Katallaxie» bezeichnet; a.M. Wiener, *Cybernetics*, 35–36, insb. 220–225.

⁵⁸⁰ Siehe Buterin, *Introduction to Cryptoeconomics*, *passim*.

⁵⁸¹ Vgl. Antonopoulos, *Mastering Bitcoin*, 254; ferner Furrer/Glarner/Linder/Müller, *Jusletter* vom 26. November 2018, Rz. 11–12 («Im Kern geht es [...] um die kryptografisch gesicherte Anwendung von Regelungstechnik mittels dezentral gespeicherter Software.»).

⁵⁸² Siehe North, *Institutions*, 3, 4 («Institutions are the rules of the game in a society or, more formally, are the humanly devised constraints that shape human interaction. [...] Like institutions, organizations provide a structure to human interaction.»); ferner, jedoch leicht abw. Hodgson, *Journal of Economic Issues* 2006, 18.

⁵⁸³ So auch Davidson/De Filippi/Potts, *Economics of Blockchain*, 6–7.

iv. Konstitutionelle Dimension

Besonders an der in dezentralen Systemen zur Anwendung gelangenden algorithmischen Regulierung ist ihre Ähnlichkeit mit den konstitutionellen Regeln anderer kollektiv organisierter Gemeinschaften, wie etwa von Nationalstaaten.⁵⁸⁴

Codebasierte Regeln, deren Existenz die Teilnehmer von DeFi durch ihren Eintritt in das System implizit anerkennen, beschränken *de facto* deren Auswahlmöglichkeiten («choices made within constraints»)⁵⁸⁵ Spieltheoretisch stellen die Konsensregeln den Rahmen dar, innerhalb welchem die Agenten zu agieren haben, um stabile kooperative Ergebnisse zu erreichen.⁵⁸⁶ Austauschgeschäfte, die in Einklang mit den Konsensregeln einer Blockchain erfolgen, werden von den Netzwerkteilnehmern akzeptiert; diejenigen, die dagegen verstossen, werden von ihnen hingegen abgelehnt.⁵⁸⁷

Die Literatur hat den Eintritt in ein dezentrales System aufgrund der ähnlichen Konsequenzen auch schon mit der einvernehmlichen Vereinbarung des anwendbaren Rechts und des Gerichtsstandes verglichen. Die faktische Möglichkeit, jederzeit das System zu verlassen, untermauert das Einstimmigkeitserfordernis.⁵⁸⁸ Im Unterschied zu den Verfassungsregeln von Nationalstaaten stellen die Regeln dezentraler Systeme darum das Ergebnis einer in aller Regel konkludent getroffenen «Abmachung»⁵⁸⁹ aller Teilnehmer zu einem beliebigen Zeitpunkt dar.⁵⁹⁰ Zwar sind Verstösse gegen die Systemregeln denkbar, doch

⁵⁸⁴ Vgl. Brennan/Buchanan, in: Liberty Fund, *The Reason of Rules*, xvii, 3–4.

⁵⁸⁵ Siehe Buchanan, *Constitutional Political Economy* 1990, 2.

⁵⁸⁶ Vgl. Schotter, *Social institutions*, 154–155.

⁵⁸⁷ So auch Berg/Davidson/Potts, in: Wagner, *Blockchains as Constitutional Orders*, 384.

⁵⁸⁸ Siehe Davidson/De Filippi/Potts, *Economics of Blockchain*, 12 («[...] mutual choice of a legal jurisdiction [...]»); ferner MacDonald, *Non-territorial political jurisdictions*, Working Paper, 1. Mai 2015, 12–13.

⁵⁸⁹ Ob es sich dabei um eine rechtlich verbindliche Vereinbarung handelt, ist in der Lehre umstritten; vgl. hierzu unten [III.2.2.](#)

⁵⁹⁰ Vgl. zum Einstimmigkeitserfordernis von Verfassungsregeln in Nationalstaaten Buchanan/Tullock, in: Liberty Fund, *The Calculus of Consent*, 248–251 («Insofar as participation in the organization of a community, a State, is mutually advantageous to all parties, the formation of a 'social contract' on the basis of unanimous agreement becomes possible. Moreover, the only test of the mutuality of advantage is the measure of agreement reached. [...] The organizing principle or theme of our whole construction is the concentration on the individual calculus, and it is easy to see that both the unanimity rule at the constitutional level and other less-than-unanimity rules at the operational level of decisions may be based directly on this calculus.»).

sind solche mit entsprechenden wirtschaftlichen Kosten und ausnahmsweise sogar Reputationsrisiken verbunden. Diese Form der anreizkompatiblen Regelsetzung⁵⁹¹ bildet einen Teil der Governance i.e.S.⁵⁹²

Eine weitere Option für die Teilnehmer stellt allerdings die Änderung der Systemregeln selbst dar, was in der konstitutionellen Ökonomik mit «choice among constraints» umschrieben wird.⁵⁹³ Diese Form der Regelsetzung ist als Governance i.w.S. bezeichnet worden.⁵⁹⁴

Im Ergebnis verfügen die Teilnehmer dezentraler Systeme über die Optionen, die bei ALBERT O. HIRSCHMAN mit Exit und Voice beschrieben werden.⁵⁹⁵ Darüber hinaus weisen dezentrale Systeme, wie bereits erwähnt, auch die Möglichkeit des Forkings auf, das als eine besondere und flexible Form des Exits in der Entwicklung von Open-Source-Software bezeichnet werden kann.⁵⁹⁶ In der Praxis wird Forking durch gegenläufige Faktoren eingeschränkt. Hierzu gehören insb. die bereits angesprochenen Netzwerkeffekte. Aufgrund solcher Effekte präferieren Teilnehmer in aller Regel dasjenige System, welches das grösste wirtschaftliche Interesse auf sich vereint, und dies zu einem gewissen Grad selbst dann, wenn die Eigenschaften des Netzwerks nicht vollständig mit ihren eigenen Präferenzen übereinstimmen.⁵⁹⁷ Im Ergebnis sind die vorgängig präsentierten Handlungsoptionen der Teilnehmer dezentraler Systeme als ein mögliches Instrument gegen opportunistisches Verhalten anderer Teilnehmer zu betrachten.⁵⁹⁸

Die Existenz algorithmischer Governance in dezentralen Systemen darf nicht darüber hinwegtäuschen, dass der sozialen, d.h. «wet» Governance weiterhin eine bedeutende, bei kollidierenden Interessen sogar eine zentrale Rolle zu-

⁵⁹¹ Siehe zur Begründung der Vorteilhaftigkeit anreizkompatibler Rechtsnormen van Aaken, in: van Aaken/Schmid-Lübbert, Normative Grundlagen, 100.

⁵⁹² Vgl. oben, [II.5.3a.ii.](#)

⁵⁹³ Siehe Buchanan, Constitutional Political Economy 1990, 3, 4.

⁵⁹⁴ Vgl. oben, [II.5.3a.ii.](#)

⁵⁹⁵ Siehe Hirschman, Exit, Voice, and Loyalty, 3–4.

⁵⁹⁶ So etwa Atik/Gerro, Stanford Journal of Blockchain Law & Policy 2018, 36–37; ebenso Berg/Berg, COSMOS + TAXIS 2020, 78–80; ferner am Beispiel der *Blocksize-Debatte* in Bitcoin aufzeigend Metz, Bitcoin Schism, Wired, *passim*.

⁵⁹⁷ Vgl. hierzu Lee/Moroz/Parkes, Political Economy of Blockchain Governance, 2–5.

⁵⁹⁸ Siehe hinsichtlich Forking von Softwarecode Nyman et al., in: Hammouda/Lundell, Forking, 3–4 («Code forking and, indeed, the mere possibility of forking, is one of the key factors that ensures that open source will continue to evolve and thus remain sustainable.»); ferner in politökonomischer Hinsicht Buchanan/Tullock, in: Liberty Fund, The Calculus of Consent, 114–115.

kommen kann.⁵⁹⁹ Die Governance dezentraler Systeme ist darum zwangsläufig ein Mischsystem aus algorithmischer Governance (i.e.S.) und realpolitischer Governance (i.w.S.), wobei sich letztere ausserhalb der Blockchain abspielt.⁶⁰⁰ Falls Interessengruppen im Einzelfall über einen besonderen Einfluss oder bessere Informationen als die übrigen involvierten Personen verfügen, können Agency-Beziehungen in neuen Erscheinungsformen auftreten.⁶⁰¹

c. Vertrauen und Komplexität

i. Technologievertrauen

Die vorherrschende und bislang sicherlich zutreffende Auffassung geht davon aus, dass ohne interpersonales Vertrauen die alltäglichsten Handlungen undenkbar wären.⁶⁰² So war die Ausführung von Finanztransaktionen historisch auf Intermediäre und somit deren korrekte und effiziente Buchführung angewiesen.⁶⁰³ Die Zentralisierung dieser Funktion setzt ein *Vertrauen* in die personale und institutionelle Intermediation voraus. Für dieses Vertrauen in den Intermediär einerseits und in das Intermediationssystem als solches andererseits wird der Begriff des sozialen Kapitals verwendet.⁶⁰⁴

Interpersonales Vertrauen ist in doppelter Hinsicht mit Transaktionskosten verbunden: Augenfällig ist die Situation, in welcher der Intermediär in opportunistischer Weise wider die Interessen seiner Kunden handelt.⁶⁰⁵ Kann aber

⁵⁹⁹ Siehe etwa De Filippi/Loveluck, Internet Policy Review 2016, 15–17.

⁶⁰⁰ Siehe Buterin, Blockchain Governance, *passim* («The approach for blockchain governance that I advocate is 'multifactorial consensus', where different coordination flags and different mechanisms and groups are polled, and the ultimate decision depends on the collective result of all of these mechanisms together.»); ebenso De Filippi/Lavayssière, in: Gear/Bollier, Decentralized Governance, 222.

⁶⁰¹ Gl.M. Voshmgir, Strategic Change 2017, 507, welche auf die besondere Rolle von Meinungsbildnern in Krisensituationen hinweist. Vgl. etwa zu *Kollusionsrisiken* von Softwareentwicklern unten, [IV.5.2e.iv](#).

⁶⁰² Siehe etwa Good, in: Gambetta, Interpersonal Relations, 31–32; Ben-Ner/Halldorsson, Journal of Economic Psychology 2010, 64.

⁶⁰³ So bereits Sombart, Der Moderne Kapitalismus, 391–397; ferner Winjum, Journal of Accounting Research 1971, 335; Yamey, The Economic History Review 1949, 100, der allerdings bezüglich der Rolle der doppelten Buchhaltung im Mittelalter und in der Frühen Neuzeit skeptisch ist.

⁶⁰⁴ Siehe Esser, in: Castiglione/van Deth/Wolleb, Social Capital, 25, der zwischen «relational capital» und «system capital» unterscheidet.

⁶⁰⁵ Siehe Williamson, Journal of Law and Economics 1993, 463–466, 485; ferner Casey et al., Impact of Blockchain Technology, xx, 13, 17 m.w.N.; ferner Granovetter, American Journal

Opportunismus eliminiert werden, so werden nach WILLIAMSON interpersonale Versprechungen plötzlich möglich.⁶⁰⁶ Andererseits ist bereits der Aufbau von Vertrauen in das Gegenüber ohne Transaktionskosten undenkbar.⁶⁰⁷ Transaktionskosten könnten darum als «Gestehungskosten» interpersonales Vertrauens im Finanzintermediationssystem betrachtet werden.

Demgegenüber spielt diese soziale Dimension von Vertrauen zwischen den beteiligten Personen in einem dezentralen System eine untergeordnete oder gar keine Rolle mehr. Indem opportunistisches Verhalten überwiegend durch technische Massnahmen eliminiert wird, kann auch die dem interpersonales Vertrauen inhärente Unsicherheit reduziert werden.⁶⁰⁸ Die britische Zeitschrift THE ECONOMIST hat darum in einem vielbeachteten Beitrag aus dem Jahr 2015 von der Blockchain als «[...] *a machine for creating trust* [...]» gesprochen.⁶⁰⁹ Damit ist nicht etwa gemeint, dass die Blockchain tatsächlich interpersonales Vertrauen zwischen sich völlig fremden Menschen schaffen kann, sondern dass für das grundlegende Funktionieren dezentraler Systeme gar nicht erst ein derartiges Vertrauen notwendig ist. Dies liegt letztlich auch an den praktischen Hürden, interpersonales Vertrauen quantifizieren und somit für Computer lesbar machen zu können.

Die Teilnehmer dezentraler Systeme haben demgegenüber den gemeinsam unterhaltenen algorithmischen Regelsystemen zu vertrauen. Dies wird vorliegend als *Technologievertrauen* bezeichnet.⁶¹⁰ In der Literatur ist teilweise auch die Rede von Distributed Trust.⁶¹¹

of Sociology 1985, 491; vgl. hinsichtlich der unterschiedlichen Auffassungen von Vertrauen Nooteboom/Six, in: Nooteboom/Six, Introduction, 3–5.

⁶⁰⁶ Siehe Williamson, Economic Institutions, 31 («[...] *contract execution goes efficiently to completion because promises of the above-described kind are, in the absence of opportunism, self-enforcing. Contract, in this context, reduces to a world of promise.*»).

⁶⁰⁷ Siehe Brescia, Nebraska Law Review 2016, 101–102 m.w.H.

⁶⁰⁸ Vgl. auch Berg/Davidson/Potts, frontiers in Blockchain 2020, 4; Lumineau/Wang/Schilke, Organization Science 2021, 506.

⁶⁰⁹ The Economist, The trust machine, *passim*.

⁶¹⁰ Siehe zur Unterscheidung von «social trust» und «technology trust» Bracamonte/Okada, in: Cunningham/Cunningham, User Trust, 1–4, *passim*; ferner bereits Earle, Risk Analysis 2009, 786, der zwischen dem sozialen «trust» und dem technischen «confidence» unterscheidet.

⁶¹¹ So etwa Chen/Bellavitis, Journal of Business Venturing Insights 2020, 2; breiter sodann Botsman, Who Can You Trust, 8–9, 257; ferner Gervais, digma 2017, 128, der davon spricht, dass Technologie das Vertrauen einer Partei auf eine andere Partei oder gar eine ganze Gruppe von Parteien erweitern kann.

Technologievertrauen ist einerseits in den kulturellen Idealen von Transparenz und Gemeinschaftlichkeit der Entwicklung von Free Software und Open-Source-Software begründet.⁶¹² Andererseits sind die ökonomischen Rahmenbedingungen bestehend aus den kryptoökonomischen Anreizen massgeblich für das anfängliche Aufkommen sowie die langfristige Glaubwürdigkeit von Technologievertrauen.⁶¹³ Dies wird als die spieltheoretisch⁶¹⁴ motivierte Anreizkompatibilität von Computerprotokollen bezeichnet.⁶¹⁵ Der Anreizkompatibilität liegt in aller Regel die mikroökonomische Annahme zugrunde, dass die Teilnehmer eines dezentralen Systems überwiegend rational und nutzenmaximierend handeln.⁶¹⁶ «Simply put, there is money at stake!»⁶¹⁷ Dies setzt voraus, dass das Protokoll auf diesen relativ simplen Grundlagen programmiert werden kann.⁶¹⁸

Die Überprüfung dieser Grundlagen erzeugt Transaktionskosten, welche letztlich bei den Nutzern dezentraler Systeme anfallen. Technologievertrauen ist ferner nicht die einzige Vertrauensdimension, die in dezentralen Systemen existiert.⁶¹⁹

ii. Entwicklervertrauen

Aufgrund der Mehrdimensionalität von dezentralen Systemen würde das Ausblenden anderer Motive als der Nutzenmaximierung nicht den tatsächlichen Umständen gerecht werden.⁶²⁰ So zeigen etwa spieltheoretische Untersuchungen, dass Menschen aus vielfältigen Beweggründen miteinander kooperieren, wobei sozialen Normen und der Reziprozität des Handelns einen zentralen Stellenwert zukommen.⁶²¹

⁶¹² Siehe Osterloh/Weibel, Investition Vertrauen, 228–229; ferner sogleich unten, [II.5.3c.ii.](#)

⁶¹³ Vgl. zur Kryptoökonomik auch oben, [II.5.3b.ii.](#)

⁶¹⁴ Vgl. Roughgarden, Communications of the ACM 2010, *passim*.

⁶¹⁵ Siehe Bonneau et al., Proceedings 2015 IEEE Symposium on Security and Privacy, 110.

⁶¹⁶ So bereits implizit Nakamoto, Bitcoin, 4; vgl. ferner Antonopoulos, Mastering Bitcoin, 271; Antonopoulos/Wood, Mastering Ethereum, 319–321; Bonneau et al., Proceedings 2015 IEEE Symposium on Security and Privacy, 104; Böhme et al., Journal of Economic Perspectives 2015, 233; Narayanan/Clark, *acmqueue* 2017, 10–11; Kroll/Davey/Felten, Economics of Bitcoin Mining, 2; Werner et al., Decentralized Finance, 8–9.

⁶¹⁷ Antonopoulos/Wood, Mastering Ethereum, 319.

⁶¹⁸ Siehe Werner et al., Decentralized Finance, 9.

⁶¹⁹ So bereits in allgemeiner Hinsicht Narayanan, IEEE Security & Privacy 2013 II, 70.

⁶²⁰ So auch Voshmgir/Zargham, Working Paper Series 1/2020, 5.

⁶²¹ Statt vieler Axelrod, Evolution of Cooperation, 118–123; ferner Axelrod, Complexity of Cooperation, 45–48.

Die enorme Bedeutung sozialer Normen für die Organisation sozialer und wirtschaftlicher Transaktionen wurde auch von Vertretern der Neuen Institutionenökonomik erkannt.⁶²² Die experimentelle Wirtschaftsforschung betont sodann die Rolle von nichtmonetären Handlungsmotiven im Wirtschaftsgeschehen, namentlich reziproke Fairness sowie Altruismus.⁶²³ Dabei wird aufgezeigt, dass die Bildung stabiler Gemeinschaften möglich ist, wenn Trittbrettfahrer für Abweichungen von sozialen Normen durch ihre Peers sanktioniert werden, was in aller Regel die Möglichkeit effektiver Überwachung voraussetzt.⁶²⁴ In diesem Kontext kommt u.a. der Reputation der beteiligten Parteien, d.h. deren Verhalten in der Vergangenheit, eine bedeutende Rolle zu.⁶²⁵

Für die Entwicklung von dezentralen Systemen bedient man sich regelmässig des Modells des *wohlmeinenden Diktators (auf Lebenszeit)*.⁶²⁶ Die Annahme des Modells besteht darin, dass der wohlmeinende Diktator die öffentlichen Güter im Zusammenhang mit der Entwicklung eines Open-Source-Projekts im Interesse aller Beteiligten verwaltet.⁶²⁷ In der DeFi-Praxis stösst man neben kalkuliertem Technologievertrauen teils auf nahezu blindes Vertrauen der Nutzer, dass die Entwickler, deren Informationsvorsprung gegenüber gewöhnlichen Nutzern naturgemäss sehr gross ist, im Rahmen der Softwareprogrammierung

⁶²² Siehe Williamson, *Economic Institutions*, 71–72, der von «relational contracting» spricht; North, *Zeitschrift für die gesamte Staatswissenschaft* 1984, 8, 10–11, welcher soziale Normen auf subjektive Wahrnehmungen der Realität durch den Menschen zurückführt (sog. *Ideologien*); Ellickson, *Order without Law*, 123–136 («system of social control»); Ostrom, *The Journal of Economic Perspectives* 2000, 143–144 («*Social norms are shared understandings about actions that are obligatory, permitted, or forbidden [...]*»); ferner Powell, *Research in Organizational Behavior* 1999, 300–305.

⁶²³ Siehe für eine Übersicht Fehr/Fischbacher, *The Economic Journal* 2002, C2–C4; sodann Frey, *Personal Motivation*, 1–3, 13–18, wonach der Zusammenhang zwischen nichtmonetärer *intrinsischer* Motivation und monetärer Vergütung sowie Intervention in den Wirtschaftswissenschaften und der Regulierungstheorie oft unterschätzt wird.

⁶²⁴ Siehe etwa Fehr/Schmidt, *Quarterly Journal of Economics* 1999, 818–819, 845–846, 855–856 («*[...] a minority of fair-minded players can force a big majority of selfish players to cooperate fully in the public good game with punishment.*»); sodann Fehr/Gächter, *The American Economic Review* 2000, 980 («*A main purpose of this paper is to show experimentally that there is indeed a widespread willingness of the cooperators to punish the free-riders.*»).

⁶²⁵ Siehe etwa Andreoni/Miller, *The Economic Journal* 1993, 571; Ostrom/Walker/Gardner, *The American Political Science Review* 1992, *passim*; Gächter/Falk, *The Scandinavian Journal of Economics* 2002, *passim*.

⁶²⁶ Vgl. zu diesem theoretischen Modell Deek/McHugh, *Open Source*, 173–174; ferner bereits Raymond, *Cathedral and Bazaar*, 101–103.

⁶²⁷ So etwa für die ersten Jahre von Bitcoin Satoshi Nakamoto und Gavin Andresen, für Litecoin Charlie Lee, für Ethereum Vitalik Buterin und für Cardano Charles Hoskinson; vgl. hierzu auch De Filippi/Loveluck, *Internet Policy Review* 2016, 12–13.

in erster Linie die kollektiven Interessen der Gemeinschaft beachten werden. Eine solche Erwartung ist aus Gründen des Reputationseffekts – zumindest bis zu einem gewissen Grad – durchaus auch plausibel.⁶²⁸

Entwicklervertrauen kann darum auch als *Governance durch Legitimität* bezeichnet werden.⁶²⁹ Die Auffassung darüber, welche Legitimität eine Person in einer bestimmten Blockchain-Community genießt, kann durchaus die Bedeutung eines spieltheoretischen Schellingpunkts zukommen,⁶³⁰ an welchem sich die Mitglieder einer solchen Gemeinschaft unter Unsicherheit orientieren werden.⁶³¹ Allerdings mahnen die Erkenntnisse der Public Choice-Theorie zur nötigen Vorsicht.⁶³²

Letztlich wird in dezentralen Systemen die traditionelle Intermediation – mit einem Menschen oder einer Institution als Nukleus – zugunsten einer computergesteuerten Intermediation aufgegeben. An die Stelle personaler bzw. institutioneller und standortgebundene Finanzintermediation tritt software- bzw. codebasierte, algorithmische Intermediation, welche in erster Linie weder personal oder institutionell noch standortgebunden ist. Dabei darf allerdings nicht die Rolle von sozialen Normen und insb. die Reputation von Entwicklergemeinschaften bis hin zu derjenigen von Einzelpersonen unterschätzt werden. In dieser Intermediation von menschlicher Interaktion und Technologievertrauen ist die *Soziotechnizität* des Systems zu erkennen.⁶³³

iii. Komplexität

Wie bereits erwähnt, sind dezentrale Systeme, die ausschliesslich auf algorithmischer Governance beruhen, heute nur unvollständig realisierbar. So erscheint die Programmierung von Protokollen, die alle möglichen zukünftigen Szenarien abdecken, als praktisch ausgeschlossen. Die meisten Projekte anerkennen darum die Notwendigkeit laufender technischer Anpassungen, indem

⁶²⁸ Vertrauen und Reputation sind gerade in sozial vernetzten Gemeinschaften wichtige Verhaltensfaktoren; siehe hierzu etwa Bowles/Gintis, in: Gintis et al., *Moral Sentiments*, 385–386; ebenso Ahn/Ostrom, in: Castiglione/van Deth/Wolleb, *Social Capital*, 83–84; in wirtschaftshistorischer Hinsicht ferner Greif, *Institutions*, 58–59.

⁶²⁹ Siehe hierzu Andreotti, in: Kessler, *Dezentrale Governance*, 133–134.

⁶³⁰ Siehe zu den unterschiedlichen Formen von Legitimität, die im Beitrag v.a. positivistisch verstanden werden, Buterin, *Legitimacy*, *passim*.

⁶³¹ Vgl. hierzu in theoretischer Hinsicht Schelling, *Strategy of Conflict*, 57.

⁶³² Siehe hierzu unten, [IV.5.1f.](#)

⁶³³ Zum Begriff siehe Whitworth, in: Ghaoui, *Social-Technical Systems*, 533 (*«Social-technical systems arise when cognitive and social interaction is mediated by information technology rather than the natural world.»*); ferner Mariani, *Complex Sociotechnical Systems*, 1.

sie etwa Regeln für die kollektive Entscheidungsfindung definieren. Zu diesem Zweck greifen viele Projekte auf Governance Token zurück, welchen den Inhabern die Möglichkeit künftiger Teilhabe gewähren.⁶³⁴ Die Unmöglichkeit von DeFi-Projekten, ausschliesslich mithilfe codierter Governance erfolgreich operieren zu können, ist sinnbildlich für die soziotechnische Komplexität dieser Systeme.

Komplexe Systeme sind Systeme (z.B. die Gesellschaft, das Klima oder ein biologisches Ökosystem), die aus mehreren Einzelteilen bestehen, wie namentlich Menschen, Technologien, Institutionen und Organismen, die sich gegenseitig beeinflussen und mit ihrer Umgebung interagieren können und dadurch zum Systemverhalten beitragen. Ferner wirkt das Systemverhalten auf die Einzelteile des Systems zurück. Dabei kann aus dem Verhalten der Einzelteile nicht auf das Verhalten des Gesamtsystems geschlossen werden; das Ganze ist demnach mehr als die Summe seiner Einzelteile (sog. *Emergenz*).⁶³⁵ Die Einzelteile, d.h. z.B. der Staat, ein Unternehmen oder ein Lebewesen, können sodann ihrerseits komplexe Systeme darstellen.⁶³⁶ Eigenschaften komplexer Systeme sind neben der bereits erwähnten Emergenz etwa die Nichtlinearität von Prozessen, die permanente Adaption an veränderte Umstände, die Selbstorganisation, die spontane Entstehung von Ordnung sowie Feedbackmechanismen.⁶³⁷

Aus der Komplexität folgt hinsichtlich der Prozesse in Wirtschaftssystemen, dass diese wenig bis gar nicht vorhersehbar und somit nur unter erschwerten Bedingungen steuerbar sind.⁶³⁸ Mit anderen Worten sind die handelnden Per-

⁶³⁴ Siehe etwa unten, [III.4.2b](#).

⁶³⁵ Siehe Bar-Yam, *Complex Systems*, 1, 8, 10; Arthur, in: Arthur, *Complexity Economics*, 3, 16–17; Simon, *Proceedings of the American Philosophical Society* 1962, 468 («In such systems, the whole is more than the sum of the parts, not in an ultimate, metaphysical sense, but in the important pragmatic sense that, given the properties of the parts and the laws of their interaction, it is not a trivial matter to infer the properties of the whole.»); ferner aus naturwissenschaftlicher Perspektive Richter/Rost, *Komplexe Systeme*, 3.

⁶³⁶ Siehe Bar-Yam, *Complex Systems*, 5.

⁶³⁷ Eine gute Übersicht findet sich bei San Miguel et al., *The European Physical Journal Special Topics* 2012, 249; ferner Caldarelli/Vespignani, in: Caldarelli/Vespignani, *Network Theory*, 14–15.

⁶³⁸ Siehe Goldenfeld/Kadanoff, *Science* 1999, 87, die zwischen Komplexität und Chaos unterscheiden; sodann Arthur, in: Arthur, *Complexity and the Economy*, 187; San Miguel et al., *The European Physical Journal Special Topics* 2012, 250; zum Kontrollproblem in soziotechnischen Systemen Franssen/Kroes, in: Olsen/Pedersen/Hendricks, *Sociotechnical Systems*, 225–226; sodann bereits von Hayek, in: Bartley, *Fatal Conceit*, 25–26, 148–151; a.M. hinsichtlich Börsenstürze Sornette, *Stock Markets Crash*, 15–25.

sonen mit «echter» Unsicherheit im Knight'schen Sinne konfrontiert.⁶³⁹ Allerdings kann nach Ansichten in der Literatur die Komplexität menschengemachter Systeme reduziert werden.⁶⁴⁰ Demgegenüber kann der Versuch der Komplexitätsreduktion, allen voran durch die Rechtsordnung, gerade neue Komplexität erzeugen.⁶⁴¹

In den Jahren seit der Finanzkrise von 2007-08 ist das traditionelle Finanzsystem vermehrt zum systemtheoretischen Untersuchungsgegenstand geworden: Dabei hat sich gezeigt, dass das Finanzintermediationssystem einen hohen Grad an struktureller Komplexität, Interdependenz und institutioneller Homogenität aufweist.⁶⁴² Aufgrund der dynamischen, innovationsgetriebenen Natur von Finanzmärkten kommt dabei dem Element der Unsicherheit eine zentrale Rolle zu.⁶⁴³ STEVEN L. SCHWARCZ hat die Komplexität der heutigen Finanzmärkte sogar als die grösste Herausforderung für die künftige Finanzmarktregulierung bezeichnet.⁶⁴⁴

Ein Beispiel aus der Finanzkrise mag veranschaulichen, wie sich bspw. nicht-lineare Feedbackmechanismen auf die Systemstabilität auswirken können: Die Weigerung von Banken, anderen Finanzinstituten auf dem Interbankenmarkt Geld zu leihen, damit sie ihre notleidenden Vermögenswerte refinanzieren können, zwang diese 2007-08 dazu, die Vermögenswerte zu veräussern, was in der Form eines positiven Feedbacks die Preise der Vermögenswerte noch

⁶³⁹ Derartige nichtmessbare Unsicherheit ist von der messbaren Unsicherheit, d.h. Risiko, zu unterscheiden; siehe hierzu Knight, *Risk, Uncertainty and Profit*, 19-20; vgl. zum Ganzen ferner Lewis, in: Aligica/Lewis/Storr, *The Ostroms and Hayek*, 40.

⁶⁴⁰ So etwa San Miguel et al., *The European Physical Journal Special Topics* 2012, 250.

⁶⁴¹ Siehe etwa Haldane/Madouros, in: Federal Reserve Bank of Kansas, *The Dog and the Frisbee*, 152 («Modern finance is complex, perhaps too complex. Regulation of modern finance is complex, almost certainly too complex. That configuration spells trouble. As you do not fight fire with fire, you do not fight complexity with complexity. Because complexity generates uncertainty, not risk, it requires a regulatory response grounded in simplicity, not complexity.»); hinsichtlich des Konzepts, wonach Komplexität nur mithilfe von Komplexität reduziert werden könne, siehe Luhmann, *Soziale Systeme*, 49.

⁶⁴² Siehe Haldane, in: Jansen/Schröter/Steher, *Rethinking*, 244, 246-248, 256-257; hinsichtlich Zahlungsnetzwerke May/Levin/Sugihara, *Nature* 2008, 895; Schweitzer et al., *Science* 2009, 424-425; Cliff/Northrop, in: Calinescu/Garlan, *Global Financial Markets*, 34, 59, welche die Thematik anhand des «Flash Crash» vom 6. Mai 2010 untersuchen; Sornette, *Stock Markets Crash*, 15.

⁶⁴³ Siehe Schneiberg/Bartley, in: Lounsbury/Hirsch, *Regulating or redesigning finance*, 283, 295.

⁶⁴⁴ Siehe Schwarcz, *Washington University Law Review* 2009, 213.

weiter unter Druck setzte, was im Ergebnis die Finanzinstitute noch weniger attraktiv für die Refinanzierung durch andere Marktteilnehmer machte.⁶⁴⁵

Dezentrale Systeme lassen sich nach dem Gesagten als komplexe, soziotechnische Systeme qualifizieren: Aus simplen kryptoökonomischen Anreizen können komplexe Ergebnisse entstehen.⁶⁴⁶ Die Zusammensetzung ihrer Einzelteile, namentlich der Teilnehmer sowie der im System verarbeiteten Informationen, ist dabei hochdynamisch, die zugrundeliegenden Protokolle lassen adaptive Prozesse als Antwort auf eine sich verändernde Umgebung zu – insb. aufgrund algorithmischer Governance – und die Steuerung des Systems basiert, wie gesehen, nicht ausschliesslich auf Computercode, sondern zu einem wesentlichen Grad auf kollektiven sozialen Prozessen der beteiligten Parteien.⁶⁴⁷ Die Emergenz des Systems kann dabei entweder in der Sicherstellung der Funktionsfähigkeit des Systems oder aber in dessen Kollaps bestehen.⁶⁴⁸ Nach dem Gesagten können dezentrale Systeme auch als *autopoietische* Systeme beschrieben werden.⁶⁴⁹ Schliesslich ist in Erinnerung zu rufen, dass Komplexität selbst die emergente Eigenschaft eines bereits komplexen Systems darstellen kann.⁶⁵⁰

Die soziotechnische Dimension von dezentralen Systemen führt den Blick auf die institutionelle Einordnung zurück: Dezentrale Systeme erlauben die *soziale Skalierbarkeit* von überwiegend anonymen globalen Gemeinschaften, deren lokalen Einzelteile keine oder nur eine geringfügige Rolle spielen.⁶⁵¹ Im Zen-

⁶⁴⁵ Siehe Haldane, in: Jansen/Schröter/Stehr, Rethinking, 252–253; ferner Schwarcz, Minnesota Law Review 2008, 396–397.

⁶⁴⁶ Vgl. Voshmgir/Zargham, Working Paper Series 1/2020, 9–10; kritisch Brekke/Alsindi, Internet Policy Review 2021, 5–6.

⁶⁴⁷ Vgl. für eine *politökonomische* Theorie der Emergenz in dezentralen Systemen Allen/Berg/Novak, Journal of Public Finance and Public Choice 2018, 106–108.

⁶⁴⁸ So auch Voshmgir/Zargham, Working Paper Series 1/2020, 1–9, die allerdings von einem komplexen, sozioökonomischen System bzw. Netzwerk sprechen.

⁶⁴⁹ Der Begriff, der v.a. in Niklas Luhmanns Rechtssoziologie und Systemtheorie breite Verwendung findet, beschreibt die *emergenten* Prozesse der Selbsterschaffung und -erhaltung eines Systems; siehe etwa Luhmann, Rechtssoziologie, 354–355.

⁶⁵⁰ Siehe zum *Composability* Risiko unten, [IV.5.2f.i](#).

⁶⁵¹ Siehe zum Konzept der sozialen Skalierbarkeit Szabo, Social scalability, *passim* («Social scalability is the ability of an institution – a relationship or shared endeavor, in which multiple people repeatedly participate, and featuring customs, rules, or other features which constrain or motivate participants' behaviors – to overcome shortcomings in human minds and in the motivating or constraining aspects of said institution that limit who or how many can successfully participate. Social scalability is about the ways and extents to which participants can think about and respond to institutions and fellow participants as the variety and numbers of participants in those institutions or relationships grow. [...] The social scalability

trum stehen Vertrauensminimierung und Kontrollverteilung. Dies hebt den besonderen Charakter von dezentralen Systemen im Vergleich zu anderen institutionellen Designs hervor, wie insb. traditionellen Märkten und Nationalstaaten.

5.4 **Fazit**

Dezentrale Systeme weisen einen beispielelosen Disintermediationseffekt für bestehende intermediäre Prozesse und Strukturen auf. Im Gegensatz zu den bisherigen Formen der Disintermediation in traditionellen Märkten tritt bei manchem DeFi-Projekt nachweislich ein *vollständiger Verzicht* auf den Einsatz von Finanzintermediären und nicht lediglich eine Substitution oder gar Überlagerung bestehender intermediärer Prozesse und Strukturen durch neue Formen der Intermediation ein. Es kommt in der Folge zur Auflösung der personalen und institutionellen Intermediation und somit, wie oben festgestellt, einer historischen Gesetzmässigkeit traditioneller Formen der Intermediation.⁶⁵²

Am Ende dieser Disintermediationswelle erwartet die Marktteilnehmer allerdings kein Intermediationsvakuum. Ihnen steht eine neuartige Form der Intermediation gegenüber, die sich auf ein Netzwerk von Computern stützt.⁶⁵³ Diese wird in der vorliegenden Arbeit als *netzwerkbasierte Intermediation* bezeichnet.

	Netzwerkbasierte Intermediation
Definition	Marktteilnehmer interagieren im Zusammenhang mit der Organisation der Produktion und des Austausches von Finanzkontrakten und Finanzinformationen unter Einbezug eines verteilten Computernetzwerks direkt miteinander.

Anstelle des bisherigen Zentralitätsparadigmas gilt neu ein Dezentralitätsparadigma. Diese Entwicklung hat weitreichende Konsequenzen für die Finanzmarktregulierung, welche traditionellerweise unmittelbar an die Person des Finanzintermediärs bzw. dessen Aktivitäten anknüpft. Insofern wird vorlie-

lity of an institutional technology depends on how that technology constrains or motivates participation in that institution, including protection of participants and the institution itself from harmful participation or attack. [...] The more an institution depends on local laws, customs, or language, the less socially scalable it is.»).

⁶⁵² Siehe oben, [II.1.4.](#)

⁶⁵³ Vgl. auch Gasiorkiewicz/Monkiewicz/Monkiewicz, Foundations of Management 2020, 145, die von «network-based finance» sprechen.

gend – zumindest umgangssprachlich –⁶⁵⁴ von einem *Paradigmenwechsel* in der Finanzintermediation und somit auch in der Finanzmarktregulierung gesprochen.⁶⁵⁵

Dennoch scheint DeFi bis auf Weiteres nicht das Ende der traditionellen Finanzintermediation darzustellen, sondern lediglich ein neues Finanzökosystem zu schaffen, das parallel zu traditionellen Prozessen und Strukturen der Finanzintermediation existiert und von dieser teilweise sogar überlagert wird.⁶⁵⁶ Aufgrund der Tatsache, dass sich DeFi noch in einer frühen Entwicklungsphase befindet, ist jedoch nicht ausgeschlossen, dass weitere Komponenten des traditionellen Finanzintermediationssystems der Disintermediation zum Opfer fallen können.

Mit Blick auf das in der Realität beobachtbare Spektrum an Dezentralität muss ausserdem festgehalten werden, dass DeFi nicht in jedem Fall als vorbehaltlos frei von Intermediären bzw. der mit diesen verbundenen Kontroll- und Vertrauensstrukturen gilt. Neue Formen der Intermediation, welche im Einzelfall Ähnlichkeiten mit dem traditionellen Finanzintermediationssystem haben, können neben die netzwerkbasierte Intermediation treten und sie im Einzelfall sogar in der praktischen Bedeutung übertreffen. Dies ergibt in finanzmarktrechtlicher Hinsicht interessante Abgrenzungsfragen, auf die zu einem späteren Zeitpunkt zurückzukommen ist.⁶⁵⁷

⁶⁵⁴ Der vorliegende *Paradigmenwechsel* ist freilich nicht im wissenschaftstheoretischen Sinne zu verstehen; vgl. hierzu Kuhn, *Scientific Revolutions*, 19.

⁶⁵⁵ So auch Bundesrat, DLT-Bericht 2018, 115–116.

⁶⁵⁶ Vgl. auch das Modell bei Malinova/Park, *Market Design*, 6.

⁶⁵⁷ Siehe unten, [VII](#).

6. Reintermediation als Gegenbewegung?

6.1 Begriff der Reintermediation

Die herkömmliche Ansicht in den Wirtschaftswissenschaften versteht unter Reintermediation den Vorgang, dass Gelder aus dem Kapitalmarkt zurückgezogen werden, um sie als Bankeinlagen erstmals oder wiederum dem Bankensystem zuzuführen.⁶⁵⁸

Demgegenüber verwendet die vorliegende Arbeit den Begriff der *Reintermediation*, um intermediäre Prozesse und Strukturen in dezentralen Systemen und im darüberhinausgehenden Ökosystem zu erfassen. Dabei kommen als Intermediäre traditionelle Finanzintermediäre oder neue Anbieter infrage. Durch Reintermediation können gegebenenfalls auch vormals verteilte Entscheidungsgewalt und Kontrolle in zentralisierte Strukturen zurückgeführt werden.

	Reintermediation
Definition	Marktteilnehmer in Krypto-Ökosystemen nehmen trotz der Möglichkeit der netzwerkbasierten Intermediation finanzintermediäre Prozesse und Strukturen im Zusammenhang mit der Organisation der Produktion und des Austausches von Finanzkontrakten und Finanzinformationen in Anspruch.

Dass mit Reintermediationseffekten in dezentralen Systemen zu rechnen ist, hat FINNEY in einem Forumsbeitrag auf BitcoinTalk bereits im Jahr 2010 vorhergesagt: *«Actually there is a very good reason for Bitcoin-backed banks to exist, issuing their own digital cash currency, redeemable for bitcoins. Bitcoin itself cannot scale to have every single financial transaction in the world be broadcast to everyone and included in the block chain. There needs to be a secondary level of payment systems which is lighter weight and more efficient. [...] Most Bitcoin transactions will occur between banks, to settle net transfers.»*⁶⁵⁹

Reintermediationseffekte können verschiedene Ebenen des DeFi-Ökosystems betreffen, allen voran periphere Dienstleister, wie etwa Kryptobörsen oder

⁶⁵⁸ Siehe Dictionary of Banking and Finance, 295; Smullen/Hand, Dictionary of Finance, 118; ähnlich Nobel/Zimmermann, in: Möslein, Finanzinnovationen, 69 FN 58.

⁶⁵⁹ Finney, Bitcoin Bank, BitcoinTalk, *passim*.

Wallet-Anbieter. Sodann treten solche Effekte zu einem gewissen Grad auch innerhalb dezentraler Systeme auf, namentlich auf der Ebene der Entwickler oder der Teilnehmer dezentraler Netzwerke. Schliesslich können auch treuhänderische Aktivitäten traditioneller Marktteilnehmer einen gewissen Einfluss auf den Disintermediationsgrad von DeFi haben. Die nachfolgende Übersicht erhebt keinen Anspruch auf Vollständigkeit, sondern will dem Leser lediglich einen ersten Eindruck der Situation vermitteln.

6.2 Ebene der peripheren Dienstleister, insb. Hosted Wallets

a. Wallet-Typen

Kryptovermögenswerte werden in sog. *Wallets* aufbewahrt.⁶⁶⁰ Dabei existieren unterschiedliche Wallet-Typen: Neben physischen Papier Wallets existieren insb. Hardware Wallets – ein Speichergerät, das speziell für die sichere, langfristige Speicherung solcher Werte angefertigt wird –, Software Wallets für Smartphones, Tablets und Desktop Computer sowie Web Wallets, in welchem Fall sich die Daten auf fremden Servern befinden.⁶⁶¹

Je nach Typ erfüllen Wallets für den Nutzer unterschiedliche Zwecke. Typischerweise verwalten sie für den Nutzer die öffentlichen Adressen, zeigen das Guthaben an und verwahren die Private Keys als verschlüsselte Datenstruktur.⁶⁶² Ferner können Wallets auch Schnittstellen zu Handelsplattformen integrieren, so dass Nutzer direkt aus ihrer Wallet heraus Vermögenswerte handeln können.⁶⁶³ Dasselbe gilt für die Integration von DeFi-Anwendungen.

Die in Wallets verwahrten Private Keys sind ein zentraler Baustein von DeFi, denn sie verschaffen den Nutzern die effektive Kontrolle und Verfügungsmacht über die Kryptovermögenswerte. Wallets ermöglichen ihren Inhabern,

⁶⁶⁰ Der Begriff des Wallets hat sich eingebürgert; technisch richtig verstanden sollte aber eher von einer *Keychain* bzw. einem Schlüsselbund gesprochen werden, denn die Wallets speichern nicht die Kryptovermögenswerte an sich ab, sondern sie gewähren lediglich die Zugriffsmöglichkeit auf die Vermögenswerte, d.h., sie speichern den Private Key ab; siehe hierzu Antonopoulos, *Mastering Bitcoin*, 93.

⁶⁶¹ Siehe für Übersichten der unterschiedlichen Wallet-Typen Antonopoulos, *Mastering Bitcoin*, 7; ausführlich Berentsen/Schär, *Bitcoin*, 309–323; Narayanan et al., *Bitcoin*, 76–83, 88.

⁶⁶² Siehe Antonopoulos, *Mastering Bitcoin*, 93; Antonopoulos/Wood, *Mastering Ethereum*, 79–80.

⁶⁶³ Siehe etwa unten, [IV.3.3](#).

Kryptovermögenswerte zu halten, aufzubewahren und darüber zu verfügen sowie mit Smart Contracts zu interagieren.⁶⁶⁴ Mit anderen Worten bilden Wallets den *Dreh- und Angelpunkt* von DeFi-Anwendungen.

b. Wallet-Anbieter

In der Praxis existieren unterschiedliche Typen von Wallet-Anbietern. Dabei handelt es sich in erster Linie um Softwareunternehmen. Falls Wallet-Anbieter auf die Kryptovermögenswerte der Nutzer Zugriff haben oder diese für Transaktionen von den Anbietern abhängig sind, stellt sich die Frage, ob Wallet-Anbieter als Finanzintermediäre zu betrachten sind.⁶⁶⁵ Hinsichtlich der *Abhängigkeit* der Nutzer von den Dienstleistungen eines Wallet-Anbieters wird zwischen zwei Grundtypen von Wallets unterschieden:

- Wie oben erwähnt, gilt in DeFi der Grundsatz der Self-Custody, d.h., die Vermögenswerte werden durch den Inhaber eigen- bzw. selbstverwahrt. Diesem Grundsatz wird mit der Redewendung «*Not your keys, not your coins*» Nachdruck verliehen.⁶⁶⁶ Man spricht in diesem Zusammenhang auch von sog. *Self-Hosted*, *Unhosted* oder *Non-Custodial Wallets*.⁶⁶⁷ Nachfolgend wird grundsätzlich ausschliesslich von Self-Hosted Wallets gesprochen, weil der Begriff die Eigenschaften des Wallet-Typs am besten beschreibt.

Bei Self-Hosted Wallets kann ausschliesslich der Inhaber des jeweiligen Private Keys über die Kryptovermögenswerte verfügen; er interagiert direkt oder allenfalls indirekt über eine dezentrale Applikation mit dem dezentralen Netzwerk. Der Nutzer ist für Verfügungen über die Vermögenswerte nicht auf eine Drittperson, wie namentlich den Wallet-Anbieter, angewiesen.⁶⁶⁸ Zwar werden auch diese Wallet-Typen letztlich von einem Softwareunternehmen entwickelt und angeboten, doch entstehen daraus in aller Regel keine finanzintermediären Reintermediationseffekte.

- Die Verwahrung von Private Keys ist allerdings mit Kosten verbunden, die sich insb. aus den informationstechnischen Risiken im Zusammenhang

⁶⁶⁴ Siehe Antonopoulos, *Mastering Bitcoin*, 55–58; Antonopoulos/Wood, *Mastering Ethereum*, 62–63; Berentsen/Schär, *Bitcoin*, 120; ferner FATF, *Virtual Currencies Report 2014*, 7.

⁶⁶⁵ Zu dieser Frage weiter unten ausführlich, [V.2.8](#).

⁶⁶⁶ Antonopoulos, *Internet of Money*, Bd. 1, 18.

⁶⁶⁷ Zu diesen Begriffen *ausführlich* Shin, *Privacy in Crypto*, *Unchained Podcast*, *passim*; ferner FinCEN, *Guidance CVC 2019*, 16; der Begriff wird ferner auch von der FATF verwendet; siehe hierzu FATF, *VASP Guidance 2019*, *passim*.

⁶⁶⁸ Siehe Bundesrat, *DLT-Bericht 2018*, 28, 146; BA, *Self-Hosted Wallets*, 5–6.

mit der Speicherung von Daten ergeben. Dies ist mitunter ein Grund, weshalb in der Praxis Verwahrungsdienstleistungen für Kryptovermögenswerte angeboten werden. Abhängig von der konkreten Ausgestaltung der Verwahrungsdienstleistungen ist mit der Verwahrung durch den Intermediär die vollständige oder teilweise Aufgabe der Kontrolle über die Vermögenswerte durch den Kunden verbunden.⁶⁶⁹ Kunden verwenden mit anderen Worten die von diesen Anbietern zur Verfügung gestellten, sog. *Hosted* oder *Custodial Wallets* für die Aufbewahrung ihrer Kryptovermögenswerte.⁶⁷⁰ Für Verfügungen über ihre Kryptovermögenswerte sind die Kunden auf die Dienstleistungen des Wallet-Anbieters angewiesen. Sie müssen deshalb dem Anbieter vertrauen, dass er instruktionsgemäss über ihre Vermögenswerte verfügt.⁶⁷¹ Die Anbieter dieses Wallet-Typs sind unter Umständen dann als Finanzintermediäre zu betrachten, wenn sie eine genügend massgebliche Rolle im Rahmen einer Verfügung über die Vermögenswerte einnehmen.⁶⁷²

Mit Blick auf *Kryptohandelsplattformen* existiert ebenfalls diese Zweiteilung in *Hosted* und *Self-Hosted Wallets*.⁶⁷³

- *Zentrale Handelsplattformen*, die vorliegend als sog. *Custodial Handelsplattformen* bezeichnet werden, bieten ihren Kunden üblicherweise ausschliesslich *Hosted Wallets* an. Sie verwahren die Kryptovermögenswerte ihrer Kunden zum Zweck des Handels über ihre Plattform in eigenen *Wallets*.⁶⁷⁴ Die Nutzer haben darum keinen Zugriff auf einen *Private Key*, der ihnen die unmittelbare Kontrolle über ihre Vermögenswerte erlauben würde.⁶⁷⁵ Bei sog. *Custodial OTC-Handelsplattformen* gibt es in der Praxis sowohl Anbieter von *Hosted Wallets* als auch solche mit *Self-Hosted Wallet-Lösungen*. Die Verwahrung stellt bei diesen Handelsplattformen eine Art Nebendienstleistung der Plattformbetreiberin dar.⁶⁷⁶

⁶⁶⁹ Siehe Berentsen/Schär, Bitcoin, 314–315, 316.

⁶⁷⁰ Siehe zum Begriff des *Hosted Wallets* FinCEN, Guidance CVC 2019, 15–16; ferner OCC, *Cryptocurrency Custody Services*, 4–5.

⁶⁷¹ Siehe Bundesrat, DLT-Bericht 2018, 28, 29, 145–146; ferner BA, *Self-Hosted Wallets*, 6, 9.

⁶⁷² Siehe hierzu unten, [V.2.8a](#).

⁶⁷³ Siehe zu den Plattformkategorien ausführlich unten, [IV.3](#).

⁶⁷⁴ In der Regel wird der Grossteil der Kryptovermögenswerte in *Cold Storage*, d.h. in Form von *Offline Wallets*, verwahrt; vgl. zu den Unterschieden zu *Hot Storage* Narayanan et al., Bitcoin, 79; Berentsen/Schär, Bitcoin, 317.

⁶⁷⁵ Siehe Berentsen/Schär, Bitcoin, 315–316; ferner Narayanan et al., Bitcoin, 88–90; ausführlich Andreotti, in: Zellweger-Gutknecht/Tschudi/MacCabe, *Handelsplattformen*, *passim*.

⁶⁷⁶ Siehe Bundesrat, DLT-Bericht 2018, 29.

- *Dezentrale Handelsplattformen* sind demgegenüber grundverschieden: Der Handel von Kryptovermögenswerten erfolgt ausschliesslich über Self-Hosted Wallets. Die Arbeit wird sich den unterschiedlichen Typen von dezentralen Handelsplattformen zu einem späteren Zeitpunkt vertieft zuwenden.⁶⁷⁷

Zusammenfassend ist festzuhalten, dass nicht jeder Einbezug eines Wallet-Anbieters einen Reintermediationseffekt aufweisen muss. Von Reintermediation kann gesprochen werden, wenn ein Anbieter beigezogen wird, welcher im Auftrag seiner Kunden die Kryptovermögenswerte verwaltet und in diesem Rahmen die Kontrolle über die Vermögenswerte erlangt (d.h. insb. Anbieter von Hosted Wallets).⁶⁷⁸

6.3 Ebene des dezentralen Netzwerks, insb. Mining Pools

Auf der Ebene dezentraler Systeme können aus verschiedenen Gründen zentripetale Kräfte bestehen, welche im Ergebnis zu einer Konzentration von Entscheidungsgewalt und Kontrolle führen können. Die Entstehungsgründe für diese Entwicklung liegen regelmässig in der Reduktion unternehmerischer Risiken und in der Realisierung von Economies of Scale durch die Netzwerkteilnehmer.

Namentlich hat sich in Bitcoin und Ethereum die Begründung von sog. *Mining Pools* als wirtschaftlich sinnvoll erwiesen. In solchen Pools wird die Rechenkapazität von kleineren Minern gebündelt, um diesen im Zeitablauf ein kontinuierliches Einkommen für die Erbringung ihrer Leistungen, d.h. das Erreichen eines Konsenses innerhalb des Netzwerks, sicherzustellen. Durch den Anschluss an einen Pool nimmt die Varianz der Erträge für den einzelnen Miner ab. Die Konzentration von Rechenkapazität in Mining Pools ist in erster Linie auf diese betriebswirtschaftlich motivierte Verringerung der Einkommensunsicherheit zurückzuführen.⁶⁷⁹

⁶⁷⁷ Siehe unten, [IV.3](#).

⁶⁷⁸ Gl.M. offenbar Micheler/von der Heyde, *Butterworths Journal of International Banking and Financial Law* 2016, 654; *unklar* hingegen Finck, *Blockchain Regulation*, 18–19.

⁶⁷⁹ Ausführlich Antonopoulos, *Mastering Bitcoin*, 267–270; Narayanan et al., *Bitcoin*, 124–130; Cong/He/Li, *The Review of Financial Studies* 2020, 2–3, 13, 36; Berentsen/Schär, *Bitcoin*, 222–224.

Ein Beispiel der Konzentration von Kapital – anstelle von Rechenkapazität – findet sich in Proof-of-Stake-Blockchains: So können Nutzer ihre Kryptowährungen Wallet-Anbietern und zentralen Kryptohandelsplattformen zur Verfügung stellen, damit diese für sie quasi als Delegierte am Konsensalgorithmus des Netzwerks teilnehmen (sog. *Staking Pools*).⁶⁸⁰ Diese Entwicklung kann wie im Falle von Mining Pools zu einer gewissen Reintermediation auf der Ebene dezentraler Netzwerke führen.⁶⁸¹ Eine Debatte über solche Effekte besteht derzeit etwa in Ethereum aufgrund der dominanten Stellung des Liquid Staking-Protokolls Lido.⁶⁸² Gewisse Protokolle, wie etwa diejenigen der Blockchains EOS, Tezos oder NEAR, sind sodann bereits designmässig weniger stark dezentral konzipiert, so dass ein (Re-)Intermediationseffekt bis zu einem gewissen Grad ganz bewusst in Kauf genommen wird.⁶⁸³

Auch für das Lightning Netzwerk, welches als sog. Layer-2-Protokoll auf dem Bitcoin Netzwerk aufbaut,⁶⁸⁴ wurde bereits mehrfach in der Vergangenheit mit Reintermediationseffekten argumentiert. Demnach soll es langfristig unumgänglich sein, dass es zur Ausbildung von ökonomisch bedeutenden *Payment Hubs* kommt, welche einen Grossteil aller Transaktionen «abwickeln».⁶⁸⁵ Auf die Frage, ob die Teilnahme am Lightning Netzwerk eine finanzintermediäre Tätigkeit darstellt, ist zu einem späteren Zeitpunkt zurückzukommen.⁶⁸⁶

6.4 Ebene der traditionellen Finanzintermediation, insb. treuhänderische Strukturen

Sodann darf nicht unerwähnt bleiben, dass viele Marktteilnehmer ihre Kryptovermögenswerte lediglich treuhänderisch über Drittpersonen erwerben, halten und veräussern, ohne dass sie in diesem Rahmen die tatsächliche Kontrolle über die Vermögenswerte erhalten.

⁶⁸⁰ Vgl. He/Tang/Wang, *Staking Pool Centralization*, 2, die davon ausgehen, dass dieselben ökonomische Anreize in Bitcoin und Ethereum gelten.

⁶⁸¹ Vgl. Cong/He/Li, *The Review of Financial Studies* 2020, 34–35; ähnlich Lianos, in: Hacker et al., *Blockchain and Competition*, 344, der solchen Systemen eine «*plutocratic governance*» unterstellt.

⁶⁸² Vgl. bspw. Morgan, *Lido Dominance Prompts Warnings*, Decrypt, *passim*.

⁶⁸³ Siehe Snider/Samani/Jain, *Delegated Proof of Stake*, 2, 3 («*[Delegated Proof of Stake] can be seen as a form of 'controlled semi-centralization' [...]*»).

⁶⁸⁴ Siehe ausführlich zu Layer-2-Netzwerken unten, [III.5.2.](#)

⁶⁸⁵ Siehe etwa Martinazzi/Flori, *PLoS ONE* 2020, 2–3, 6; ferner Torpey, *Centralization Risks*, *passim*; zusammenfassend Gudgeon et al., in: Bonneau/Heninger, *Layer-Two Blockchain Protocols*, 210.

⁶⁸⁶ Siehe unten, [V.2.10d.](#)

Ein treuhänderischer Erwerb von Kryptovermögenswerten liegt typischerweise vor, wenn Kunden diese bei traditionellen Finanzintermediären erwerben, wie etwa Banken und Wertpapierhäuser⁶⁸⁷, FinTech-Unternehmen⁶⁸⁸ und Zahlungsdienstleister⁶⁸⁹. Diese Institute verwahren die Kryptovermögenswerte ihrer Kunden in aller Regel in Hosted Wallets, die ähnlich wie Sammelkonten funktionieren. Die Kryptovermögenswerte können dabei regelmäßig nur innerhalb eines geschlossenen Systems übertragen werden.⁶⁹⁰ Ferner können Anleger Kryptovermögenswerte erwerben durch den Kauf von Anteilen an kollektiven Kapitalanlagen,⁶⁹¹ strukturierten Produkte oder sonstigen Forderungsrechten bzw. Schuldverschreibungen mit derivativer Komponente⁶⁹².

Während in den meisten Fällen die Finanzintermediäre die Kryptovermögenswerte tatsächlich erwerben und in ihren eigenen Wallets verwahren (lassen), partizipieren ihre Kunden in aller Regel lediglich an der wirtschaftlichen Entwicklung der Basiswerte. Sie tragen mit anderen Worten die mit der traditionellen Intermediation verbundenen Gegenparteirisiken.⁶⁹³ ANDREAS M. ANTONOPOULOS hat diese Form der Reintermediation als «infrastructure inversion» bezeichnet. Danach operiert neue Technologie vorübergehend auf bestehender Infrastruktur, bevor, und dies muss sich im Falle von Blockchains erst noch realisieren, alte Technologie auf neuer Infrastruktur ausgeführt wird.⁶⁹⁴

Ein Spezialfall treuhänderischer Reintermediation ist *MicroStrategy Incorporated*: Das am NASDAQ öffentlich gehandelte Softwareunternehmen hat im Jahr 2020 damit begonnen, mehrere Milliarden US-Dollar seiner Liquiditätsreserven in Bitcoin zu investieren und zu diesem Zweck sogar Schuldverschreibungen am Markt zu platzieren.⁶⁹⁵ Weitere Beispiele, die in diese Kategorie

⁶⁸⁷ Siehe bspw. Swissquote, Crypto-assets, *passim*.

⁶⁸⁸ Siehe bspw. Robinhood, Crypto, *passim*.

⁶⁸⁹ Siehe bspw. Revolut, Crypto, *passim*, und PayPal, Cryptocurrency, *passim*.

⁶⁹⁰ Siehe für weitere Informationen zum PayPal-Angebot Shin, PayPal and Stablecoin, *Unchained Podcast*, *passim*.

⁶⁹¹ Siehe bspw. den *Grayscale Digital Large Cap Fund* mit Domizil auf den Kaimaninseln, *Grayscale, Digital Large Cap Fund*, *passim*.

⁶⁹² Siehe bspw. die börsengehandelten Tracker-Zertifikate auf Bitcoin und andere Kryptowährungen von *Vontobel*, *Tracker Certificates*, *passim*; ferner die *Exchange Traded Products (ETPs)* von *21Shares*, *Digital Asset ETPs*, *passim*, oder von *Bitcoin Capital*, *Active Crypto ETP*, *passim*.

⁶⁹³ Siehe hierzu unten, [IV.5.1c](#).

⁶⁹⁴ Siehe Antonopoulos, *Internet of Money*, Bd. 1, 62.

⁶⁹⁵ Siehe die Pressemitteilungen des Unternehmens: *MicroStrategy, Bitcoin Purchase*, *passim*; *MicroStrategy, Convertible Senior Notes*, *passim*.

von Reintermediation gehören, sind die beiden US-amerikanischen Unternehmen *Square, Inc.*⁶⁹⁶ und *Tesla, Inc.*⁶⁹⁷.

Der ultimative Reintermediationseffekt ist zu erwarten, wenn Zentralbanken und Nationalstaaten vermehrt zwecks Bildung von Währungsreserven Kryptowährungen erwerben. *El Salvador* etwa hat diesen Weg im Sommer 2021 eingeschlagen.⁶⁹⁸

Nach gut zehnjähriger Wartezeit sind schliesslich Anfang 2024 auch die Bitcoin ETFs von der SEC genehmigt worden. Die grossen Anbieter, wie etwa BlackRock bzw. iShares, werden voraussichtlich einen beachtlichen Reintermediationseffekt mit sich bringen.⁶⁹⁹

Die Überlappung von traditionellen Finanzintermediären und den Kryptomärkten wird v.a. unter dem Gesichtspunkt der Finanzstabilität kritisch analysiert: Im Wesentlichen geht die Befürchtung dahin, dass sich die Risiken von Kryptovermögenswerten und dezentralen Applikationen in den traditionellen Märkten verbreiten.⁷⁰⁰ Der Vorschlag prohibitiver Kapitalanforderungen des Basler Ausschusses für Banken und Wertpapierhäuser ist stellvertretend für die Haltung.⁷⁰¹ Demgegenüber ist die Reintermediation von dezentralen Systemen in regulatorischer Hinsicht gerade oftmals erwünscht.⁷⁰²

6.5 Ursachen und Kritik

Es kann festgehalten werden, dass die erwähnten Reintermediationseffekte eine Gegenbewegung zur netzwerkbasierten Intermediation dezentraler Systeme darstellen. Die Reintermediation wird je nach Ebene durch unterschiedliche Faktoren bestimmt:

Trotz insgesamt sinkender Transaktionskosten scheinen alte und neue Intermediäre zu einem gewissen Grad weiterhin einen Mehrwert für ihre Kunden zu schaffen.⁷⁰³ Die Reintermediation scheint einerseits darin begründet zu

⁶⁹⁶ Siehe Square, Bitcoin, *passim*.

⁶⁹⁷ Siehe Tesla, Form 10-K, 23.

⁶⁹⁸ Siehe Busch, *El Salvador*, NZZ, *passim*.

⁶⁹⁹ In diesem Sinne auch Crenshaw, Dissenting Statement, *passim*.

⁷⁰⁰ Siehe OECD, Institutionalisation, 34–47.

⁷⁰¹ Siehe hierzu unten, [VI.4.3c.vi](#).

⁷⁰² So etwa in unverkennbarer Weise IOSCO, Final Report DeFi 2023, 21–25 (Recommendation 2).

⁷⁰³ Siehe hinsichtlich der ähnlichen Entwicklung im Bereich von E-Commerce Giaglis/Klein/O'Keefe, Information Systems Journal 2002, 232, 239–240, 244 m.w.N.

sein, dass die Inhaber von Kryptovermögenswerten oftmals nicht bereit sind, die mit der Verwahrung und Verwaltung ihrer Vermögenswerte verbundenen Risiken selbst zu tragen.⁷⁰⁴ Die erwähnten Formen der Intermediation bieten für Retail- und institutionelle Investoren denn auch gewisse Vorteile, namentlich eine Kompromisslösung zwischen Verfügbarkeit und Sicherheit, die Einsparung von Kosten, die mit der Einrichtung eigener Sicherheitsmassnahmen verbunden wären, die einfache Anbindung an das traditionelle Finanzsystem, Rechtssicherheit aufgrund etablierter Marktlösungen oder ganz einfach das Vorhandensein nützlicher Expertise.

Andererseits kann die Irreversibilität von Transaktionen beim Kauf von Gütern über das Internet den Einsatz von *Escrow-Anbietern* erfordern, sofern sich die Vertragsparteien nicht vertrauen. Escrow-Anbieter stellen sicher, dass der Verkäufer die Zahlung erst erhält, nachdem die Ware an den Käufer geliefert wurde.⁷⁰⁵ Ähnliche Mechanismen, die jedoch auf Smart Contracts zurückgreifen, finden sich in dezentralen Handelsplattformen wieder.⁷⁰⁶

Sodann sind Reintermediationseffekte zu einem gewissen Grad auch den *technischen Eigenschaften* dezentraler Systeme geschuldet: Die Protokolle hinter Bitcoin und Ethereum sehen Obergrenzen der Datenverarbeitung vor, weshalb die Anzahl Transaktionen pro Zeiteinheit beschränkt ist.⁷⁰⁷ Infolge der künstlichen Verknappung steigen zudem die Transaktionsgebühren, was die Übertragung kleiner Beträge wenig attraktiv macht.⁷⁰⁸ Die Nutzer konkurrieren mit anderen Worten um die Aufnahme ihrer Daten in die Blockchain. Die Funktion der Überlastung macht aus einem dezentralen System eine Art *Clubgut* im Sinne der ökonomischen Theorie.⁷⁰⁹ Aufgrund der beschränkten Skalierbarkeit solcher Protokolle kommt es zur Herausbildung von intermediären Prozessen und Strukturen an der Peripherie der Systeme, welche die begrenzte Verarbeitungskapazität der Netzwerke für die Marktteilnehmer rationalisieren.⁷¹⁰ Dazu gehören namentlich auch zentrale Handelsplattformen, welche im Vergleich

⁷⁰⁴ So auch Böhme et al., *Journal of Economic Perspectives* 2015, 220–221; Geva, in: Brummer, *Evolution*, 37; Janczuk-Gorywoda, in: Hacker et al., *Re-Intermediation*, 268.

⁷⁰⁵ Siehe auch Janczuk-Gorywoda, in: Hacker et al., *Re-Intermediation*, 271–272.

⁷⁰⁶ Siehe unten, [IV.3.4](#).

⁷⁰⁷ Siehe zur sog. *Block Size* unten, [III.3.3b](#).

⁷⁰⁸ Vgl. zur Funktionsweise von Transaktionsgebühren Antonopoulos, *Mastering Bitcoin*, 126–128; Berentsen/Schär, *Bitcoin*, 215–216, 245–250, Böhme et al., *Journal of Economic Perspectives* 2015, 218.

⁷⁰⁹ G.L.M. Chiu/Koepl, *The Review of Financial Studies* 2019, 1718–1719, 1750. Vgl. ferner zum *Clubgut* oben, [II.5.2b](#).

⁷¹⁰ So bereits Bonneau et al., *Proceedings 2015 IEEE Symposium on Security and Privacy*, 114.

zu Transaktionen, die unmittelbar auf dem dezentralen Netzwerk stattfinden, eine in vielen Fällen deutlich kostengünstigere Abwicklung des Handels über die eigene Datenbank erlauben.⁷¹¹

Die in dezentralen Systemen vorherrschenden *kryptoökonomischen Anreizmechanismen* scheinen ebenfalls gewisse Zentralisierungseffekte – zumindest in gewissen Bereichen des Netzwerks – als Nebenerscheinung zu produzieren.⁷¹²

In der Literatur wird insb. ein Schwerpunkt auf die Evolution von Mining Pools in Bitcoin gelegt, wobei die Analysen zu sehr unterschiedlichen Schlussfolgerungen kommen: Für viele Beobachter ist die Konzentration von Rechenkapazität Ausdruck einer systemwidrigen Zentralisierung.⁷¹³ Andere anerkennen die Realität von Mining Pools, gehen aber davon aus, (i) dass die Konzentration von Rechenkapazität eine natürliche Obergrenze kenne, nach deren Erreichen ein Mining Pool wieder schrumpft, indem einzelne Miner zu einem anderen Pool wechseln, (ii) dass letztlich spieltheoretische Erwägungen verhindern, dass einflussreiche Mining Pools ihre Macht zulasten der übrigen Netzwerkteilnehmer und Nutzer ausüben oder aber (iii) dass eine gewisse Zentralisierung im Mining-Bereich nicht automatisch ein Problem für das gesamte dezentrale System darstellen müsse, können die übrigen Netzwerkteilnehmer doch einem Machtmissbrauch mit geeigneten Massnahmen entgegenwirken.⁷¹⁴

In Bezug auf den letzten Punkt ist an die realpolitische Dimension dezentraler Governance zu erinnern. Diese sorgt in vielen Fällen für ein Gleichgewicht der an einem dezentralen System beteiligten Interessengruppen: Weder die Gemeinschaft der Entwickler noch ein Mining-Pool noch sonst eine Person verfügen über die Autorität, unilateral die Regeln des Systems zu ändern.⁷¹⁵

⁷¹¹ Siehe unten, [IV.2.4](#).

⁷¹² Die Zentralisierung des Kapitals u.a. als Folge der Akkumulation und Konzentration von Kapital wurde von Karl Marx als Zwangsläufigkeit des kapitalistischen Systems beschrieben; vgl. Marx, Kapital, 654–656.

⁷¹³ Siehe etwa Berentsen/Schär, Bitcoin, 110, 224–225; Böhme et al., Journal of Economic Perspectives 2015, 219–220, 222; Eyal/Gün Sirer, in: Christin/Safavi-Naini, Bitcoin Mining, insb. 438, 448; Lianos, in: Hacker et al., Blockchain and Competition, 341, 343–344; Ma/Gans/Tourky, Rotman School of Management Working Paper Nr. 3103104, 28. Juni 2019, 7; wohl zu pessimistisch Eich, in: Hacker et al., Politics of Bitcoin, 94; hinsichtlich PoS-Protokollen Fanti et al., in: Goldberg/Moore, Compounding of Wealth, 43; ferner He/Tang/Wang, Staking Pool Centralization, 2.

⁷¹⁴ Siehe etwa Cong/He/Li, The Review of Financial Studies 2020, 4–5, 35 m.w.N.; Antonopoulos, Mastering Bitcoin, 270–271, 272–273; hinsichtlich PoS-Protokollen Roşu/Saleh, Management Science 2020, 1–2.

⁷¹⁵ Siehe etwa Ammous, Bitcoin Standard, 224–225. Vgl. hierzu ferner unten, [IV.5.2e.iii](#).

Ein gewisser innerer Widerspruch zum Dezentralitätsparadigma ist ferner auch darin zu finden, dass sich viele Nutzer dezentraler Systeme weiterhin auf *intermediatisierte Dienstleistungen* verlassen, wie etwa von Hosted Wallet-Anbietern und Betreibern zentraler Kryptohandelsplattformen.⁷¹⁶ Demgegenüber kann dieser Entwicklung durch die Nutzung dezentraler Handelsplattformen bis zu einem gewissen Grad Abhilfe geschaffen werden. Schliesslich finden sich auch kritische Stimmen am verbreiteten *treuhänderischen Modell*, wonach Investoren mithilfe von traditionellen Marktteilnehmern in Kryptovermögenswerte investieren, was offensichtlich dem Prinzip der Self-Custody widerspricht.⁷¹⁷

Diese Entwicklungen stellen ohne Zweifel ein Spannungsverhältnis zur netzwerkbasierten Intermediation her. Doch beschränken sich *eindeutige* intermediäre Prozesse und Strukturen heute v.a. auf die Peripherie eines dezentralen Systems, d.h. insb. auf Hosted Wallet-Anbieter und zentrale Handelsplattformen, und nicht etwa auf das System selbst. In den Bereichen der sicheren Verwahrung von Kryptovermögenswerten sowie der Anlageberatung und Vermögensverwaltung können Intermediäre für ihre Kunden regelmässig weiterhin einen Mehrwert schaffen.⁷¹⁸ Aber selbst in diesen Bereichen, wie die Evolution dezentraler Handelsplattformen zeigt, kann es früher oder später zu weiteren Ablöseprozessen kommen.⁷¹⁹

Von den peripheren Dienstleistern zu unterscheiden sind demgegenüber die Teilnehmer dezentraler Netzwerke. Für diesen Bereich ist davon auszugehen, dass Reintermediationseffekte zwar vorhanden, aber insgesamt zu schwach ausgeprägt sind oder aber durch gegenläufige Effekte ausgeglichen werden, um das Aufkommen und den Fortbestand netzwerkbasierter Intermediation zu behindern.

⁷¹⁶ Siehe Lianos, in: Hacker et al., *Blockchain and Competition*, 342–343; Catalini/Gans, *Communications of the ACM* 2020, 88; Gyr, *Blockchain and Smart Contracts*, N 41, 44, welche aufgrund dieser Entwicklung den zentralen Aspekt der Blockchain-Technologie bereits «ad absurdum» geführt sieht; Benos/Garratt/Gurrola-Perez, *Ledger* 2019, 146, deren Aussagen sich wohl einzig auf private, permissioned Blockchains beziehen; ferner Dimitropoulos, in: Hacker et al., *Global Currencies*, 133; Neyer/Geva, *Journal of Payments Strategy and Systems* 2017, *passim*.

⁷¹⁷ Siehe Antonopoulos, *Cargo Class Bitcoin*, Youtube, *passim*.

⁷¹⁸ Vgl. Zamani/Giaglis, *Industrial Management & Data Systems* 2018, 641–642, 643; kritisch demgegenüber insb. wegen der intransparenten Preisgestaltung in der mediatisierten Wertpapierverwahrung Micheler/von der Heyde, *Butterworths Journal of International Banking and Financial Law* 2016, 655.

⁷¹⁹ Vgl. hierzu unten, [IV.2.4](#).

7. Zusammenfassung Kapitel II

Das zweite Kapitel befasst sich aus unterschiedlichen Blickwinkeln mit den Themen der Intermediation, Finanzintermediation, Disintermediation und Reintermediation:

Die Arbeit zeigt im *ersten* Abschnitt auf, wie gesellschaftlich ubiquitär Intermediation und Disintermediation sind. Es werden in diesem Zusammenhang soziale, religiös-spirituelle, politische und wirtschaftliche Intermediation unterschieden. Zu letzterer Form der Intermediation gehört auch die Finanzintermediation. Ihnen allen gemeinsam ist, dass einer Person oder einer Gruppe von Personen, die miteinander verbunden sind, eine zentrale Rolle im Hinblick auf die intermediäre Aktivität zukommt. Dieser Umstand wird als *personale* bzw. *institutionelle* Intermediation bezeichnet. Sie stellt in der Geschichte eine historische Konstante dar. Mit der personalen und institutionellen Intermediation ist schliesslich die logische Zentralisierung von Entscheidungsgewalt und Kontrolle verbunden.

Im *zweiten* Teil des Kapitels werden der Begriff und die volkswirtschaftliche Bedeutung der Finanzintermediation nachgezeichnet. Unter der Finanzintermediation wird vorliegend die Organisation der Produktion und des Austausches von Finanzkontrakten durch die Marktteilnehmer verstanden. Der Begriff umfasst somit inhaltlich sowohl Finanzintermediäre als auch Handelsplätze und deren Nachhandelsinfrastrukturen. Finanzintermediation kann aus ökonomischer Sicht eine im Vergleich zu reinen Markttransaktionen effizientere Organisation von Austauschgeschäften darstellen. Allerdings bringt die Finanzintermediation ihrerseits neue Verhaltensrisiken mit sich, welche vorliegend als Kontroll- und Vertrauensrisiken bezeichnet werden. Letztlich können diese Risiken auf das zugrundeliegende Prinzipal-Agent-Verhältnis zwischen dem Kunden und Anleger auf der einen Seite und dem Finanzintermediär auf der anderen Seite zurückgeführt werden.

Der *dritte* Abschnitt geht auf das Konzept der Disintermediation ein. Darunter wird vorliegend die vollständige Eliminierung von Zwischengliedern aus bestehenden finanzintermediären Prozessen und Strukturen verstanden, so dass Anbieter und Nachfrager von Finanzkontrakten in einer unmittelbaren Produktions- und Austauschbeziehung stehen, die nur noch von Computer- und Informationstechnologie abhängig ist (zum Begriff der netzwerkbasierten Intermediation siehe unten). Als Beispiele teilweiser Disintermediation im heu-

tigen Finanzsektor können etwa die Asset Securitization, das Crowdfunding, DLT-Handelssysteme sowie CBDCs angeführt werden. Die technologischen Innovationen der letzten Jahrzehnte sind massgeblich für allfällige Disintermediationseffekte verantwortlich, die gemeinhin unter dem Begriff der Fin-Tech zusammengefasst werden. Es wird generell erkennbar, dass traditionelle Finanzintermediäre in der Digital Economy an Bedeutung verloren haben. An ihre Stelle sind in vielen Fällen auf Märkten basierende Austauschbeziehungen getreten.⁷²⁰ Auffällig ist allerdings, dass erst mit Bitcoin und Ethereum eine vollständige Eliminierung von intermediären Strukturen und Prozessen möglich wurde.

Im vierten Abschnitt des Kapitels wird die neue Bewegung mit der Bezeichnung Decentralized Finance bzw. DeFi vorgestellt und in die bisherigen Ausführungen eingeordnet. Dabei sind gerade die historischen Vorläufer zentral für das Verständnis dieser neuen Bewegung in der Finanzwelt. DeFi ist nach vorliegender Definition die dezentrale Replikation traditioneller finanzintermediärer Aktivitäten mittels offener und interoperabler Computerprotokolle. Dezentrale Handelsplattformen nehmen dabei eine zentrale Rolle in DeFi ein.

Der fünfte Teil befasst sich sodann mit den ökonomischen und soziotechnischen Eigenschaften der netzwerkbasierten Intermediation als ein neues Phänomen. In DeFi wird die personale und institutionelle Intermediation aufgrund der mit dezentralen Systemen verbundenen Disintermediationseffekte aufgelöst. Es kommt in der Folge zur Herausbildung einer neuartigen Form der Intermediation: der netzwerkbasierten Intermediation. Die netzwerkbasierte Intermediation ist anders als ihre Vorläufer nicht mehr auf den Einsatz von personalen oder institutionellen Intermediären angewiesen, sondern lediglich noch auf Computercode, der von einem Netzwerk von Computern ausgeführt wird. Die heute von Finanzintermediären ausgeübten Funktionen werden mit anderen Worten verteilt;⁷²¹ die Funktionen verschwinden aber nicht.⁷²² Die dadurch ausgelösten Veränderungen haben Auswirkungen auf die Märkte und die Marktteilnehmer, die Prozesse und Instrumente sowie die Spielregeln.

Allerdings zeigen jüngere Entwicklungen, wie der letzte Abschnitt des Kapitels ausführt, dass die netzwerkbasierte Intermediation in der Praxis von Gegenbewegungen der Reintermediation begleitet werden kann. Dabei werden übersichtshalber drei Ebenen unterschieden, welche typischerweise von

⁷²⁰ Siehe Bernet, Finanzintermediation, 161–162, 164.

⁷²¹ Zu diesem Begriff siehe unten, [III.1](#).

⁷²² ANGELA WALCH spricht in ähnlicher Weise von der *Fragmentierung* der Intermediationsfunktion; vgl. Simons Institute, Blockchain Intermediation, Youtube, *passim*.

Reintermediationseffekten betroffen sind: periphere Dienstleister, dezentrale Netzwerke und die traditionelle Finanzintermediation. Die teilweise Rückführung von Entscheidungsgewalt und Kontrolle in zentralisierte Strukturen scheint einen gewissen logischen Widerspruch zum Dezentralitätsparadigma netzwerkbasierter Intermediation zu erzeugen. Allerdings werfen diese Entwicklungen das Konzept der netzwerkbasierten Intermediation nicht gleich wieder vollständig über Bord. Dezentrale Systeme sind ein reales Phänomen, wie die Ausführungen zu dezentralen Handelsplattformen in dieser Arbeit noch aufzeigen werden.⁷²³

⁷²³ Siehe insb. unten, [IV](#).

III. Technische Grundlagen

*If you don't believe me or don't get it,
I don't have time to try to convince you, sorry.*

– Satoshi Nakamoto⁷²⁴

1. Begriffliches: dezentral vs. verteilt

In der Literatur werden Bitcoin, Ethereum und andere Blockchains regelmäßig als dezentrale Systeme oder dezentrale Netzwerke beschrieben. Sodann werden Anwendungen, die auf solchen Netzwerken zur Ausführung gelangen, typischerweise als dezentrale Applikationen bezeichnet. Die Begriffe werden in Abgrenzung zu zentralen Modellen verwendet.

In der Literatur findet sich sodann auch eine leicht abweichende Unterscheidung: Demnach seien zentrale und dezentrale von verteilten Systemen abzugrenzen.⁷²⁵ Diese Unterscheidung hat insofern etwas für sich, als dass sie mit dem Begriff der Dezentralität die *Unmittelbarkeit* eines Austauschgeschäfts bzw. einer Transaktion zwischen zwei Personen betont, wohingegen sie mit dem Begriff der Verteiltheit ein System meint, das die Verarbeitungslasten eines Austauschgeschäfts *mehreren* Personen aufbürdet. Nach dieser Ansicht können Bargeldtransaktionen als dezentral beschrieben werden. Demgegenüber sind solche in Kryptowährungen verteilt, da ein Netzwerk von Computern in die Übertragung, Abrechnung und Abwicklung der Transaktionen involviert ist.⁷²⁶ In diesem Sinne wurde vorliegend festgehalten, dass Übertragungen von Kryptowährungen nicht vollständig frei von Intermediären, sondern auf dem Model der netzwerkbasierten Intermediation beruhen.⁷²⁷

⁷²⁴ Nakamoto, Scalability and transaction rate, BitcoinTalk, *passim*.

⁷²⁵ Siehe Luther/Stein Smith, Journal of Institutional Economics 2020, 434–438.

⁷²⁶ Siehe Luther/Stein Smith, Journal of Institutional Economics 2020, 436–439 («We maintain that bitcoin is neither a centralized nor a decentralized payment mechanism. Since it relies on the network of users to process transactions, it is best classified as a distributed payment mechanism.»).

⁷²⁷ Siehe oben, [II.5](#).

In informationstechnischer Hinsicht sind jedoch die Unmittelbarkeit der Kommunikation und die Verteilung von Aufgaben und Funktionen auf mehrere Computer bzw. Nodes in Peer-to-Peer-Netzwerken eng ineinander verwoben, sodass in aller Regel nicht strikt zwischen der Dezentralität und der Verteiltheit eines Netzwerks unterschieden wird.⁷²⁸

Im zweiten Kapitel dieser Arbeit wurde *Dezentralisierung* als die Verteilung der Entscheidungsgewalt und der Kontrolle über ein System auf mehrere voneinander unabhängige Personen definiert.⁷²⁹ Dabei bilden die Disintermediation, d.h. der vollständige Verzicht auf traditionelle intermediäre Prozesse und Strukturen, und somit die Unmittelbarkeit von Austauschgeschäften keine absolut notwendige Bedingung der Dezentralisierung, wie dies anhand des neu eingeführten Begriffs der netzwerkbasierten Intermediation aufgezeigt wurde.⁷³⁰ Der Begriff der Dezentralisierung enthält somit nach vorliegender Auffassung bereits das Element der Verteiltheit. Demgegenüber stellt er nicht (primär) auf die Unmittelbarkeit eines Austauschgeschäfts ab.

In dieser Arbeit kommt in erster Linie der Begriff der Dezentralisierung bzw. Dezentralität zur Anwendung. Nachfolgend ist darum von dezentralen Systemen, dezentralen Netzwerken und dezentralen Applikationen die Rede. Das in Kapitel VII erarbeitete Rechtsprinzip knüpft ebenfalls an das Konzept der Dezentralität an.⁷³¹

Um im Einzelfall die *Unmittelbarkeit* eines Vorgangs zu betonen, kann die eingangs erwähnte Abgrenzung zwischen Dezentralität und Verteiltheit dennoch ausnahmsweise sinnvoll sein:

In Fällen, in denen die Unmittelbarkeit einer Transaktion, eines Austauschgeschäfts oder der Abwicklung im Vordergrund steht, soll darum auch der Begriff der Dezentralität verwendet werden. Das Begriffsverständnis der *dezentralen* Handelsplattform steht dem nicht grundsätzlich entgegen.⁷³² Wohingegen die Involvierung mehrerer voneinander unabhängiger Personen im Vordergrund steht, soll von Verteiltheit gesprochen werden. So wird etwa das *verteilte* Register von einem *verteilten* Netzwerk von Computern unterhalten. Die terminologische Unterscheidung soll darüber hinaus auch in rechtlicher Hinsicht Beachtung finden: *Geldwäschereirechtlich* geht es in erster Linie um den Grad

⁷²⁸ Siehe etwa Wu/Savoie, in: Bidgoli, Peer-to-Peer Network Architecture, 132, 149; ferner ausführlich Özsü/Valduriez, Distributed Database Systems, 4. Aufl., 395–408, 436–438.

⁷²⁹ Siehe oben, [II.1.5](#).

⁷³⁰ Siehe oben, [II.5.4](#).

⁷³¹ Siehe unten, [VII](#).

⁷³² Zu den unterschiedlichen Plattformkategorien unten, [IV.3](#).

der Dezentralität einer Handelsplattform, da die Aktivität der Übertragung von Vermögenswerten regulatorisch im Vordergrund steht. *Finanzmarktinfrastrukturechtlich* bietet sich hingegen der Begriff der Verteiltheit an, da in der Regel Handel, Abrechnung und Abwicklung von Transaktionen durch ein verteiltes Computernetzwerk den Gegenstand der juristischen Analyse bilden.

Dabei ist selbstverständlich zu beachten, dass bei einer solchen Abgrenzung, soweit ihr wie vorliegend bedingt gefolgt wird, nicht mehr alleine die Frage der Verteilung der Entscheidungsgewalt und der Kontrolle hinsichtlich einer Aktivität im Vordergrund steht.

2. Dezentrale Systeme

2.1 Einleitung

Dezentrale Systeme setzen in technischer Hinsicht *drei Eigenschaften* voraus: (i) die verteilte, gemeinschaftliche Verwaltung, (ii) die Offenheit und Interoperabilität der zugrundeliegenden Protokolle und (iii) kryptografische Mechanismen zur Absicherung der Vermögenswerte.

Dezentrale Systeme werden sodann unterteilt in dezentrale Netzwerke und dezentrale Applikationen. Während dezentrale Netzwerke die Abwicklungsebene bilden, stellen dezentrale Applikationen die Anwendungsebene dezentraler Systeme dar.

2.2 Verteilte, gemeinschaftliche Verwaltung

Die Haupttrugenschaft dezentraler Systeme liegt im Verzicht auf eine zentrale Autorität. Die Fähigkeit, für das System Entscheidungen zu treffen, ist mit anderen Worten weder bei einer Einzelperson noch bei einer Gruppe von Personen, die miteinander wirtschaftlich oder rechtlich verbunden sind, angesiedelt.

Freilich müssen wie in allen soziotechnischen Institutionen, die von Menschen unterhalten werden, auch in dezentralen Systemen Entscheidungen getroffen werden. Einerseits ist etwa zu entscheiden, wem wie viele Kryptovermögenswerte gehören. Andererseits sind Entscheidungen darüber zu treffen, wie sich das Netzwerk entwickeln soll. Daraus folgt, dass die Verteilung von Entscheidungsgewalt und Kontrolle in einem dezentralen System in irgendeiner Form geregelt werden muss. Es liegt auf der Hand, Entscheidungen gemeinsam zu treffen. Diese Eigenschaft wurde im ersten Kapitel als Dezentralisierung, d.h. die Verteilung von Entscheidungsgewalt und Kontrolle auf mehrere Personen, bezeichnet.⁷³³

Diese Form der Dezentralisierung kann am besten mit *gemeinschaftlicher Verwaltung* des Systems beschrieben werden. Eine wesentliche Eigenschaft dezentraler Systeme liegt also darin, dass sie gemeinschaftlich verwaltet wer-

⁷³³ Siehe oben, [II.1.5](#).

den.⁷³⁴ Vor diesem Hintergrund bilden die Teilnehmer solcher Systeme eine Zweckgemeinschaft, deren Funktionsweise jedoch nicht als demokratisch im politikwissenschaftlichen Sinne zu verstehen ist.⁷³⁵ Das Vorliegen einer solchen Zweckgemeinschaft bedeutet nicht zwingend, dass die Teilnehmer über gleichgerichtete Interessen und Ziele verfügen müssen, woraus ein Unterordnungswille unter einen gemeinsamen Zweck abgeleitet werden könnte.⁷³⁶ Offen ist ausserdem, ob überhaupt Rechtsansprüche zwischen den Beteiligten bestehen.⁷³⁷ Auf jeden Fall liegt ein faktisches Gebilde aufgrund gemeinschaftlicher Verwaltung nach dem Bottom-up-Modell vor: Die Teilnehmer sind frei, zur Verwaltung des Systems beizutragen oder aber ihren Beitrag jederzeit wieder aufzugeben. Niemand kann gegen seinen Willen gezwungen werden, sich an der gemeinschaftlichen Verwaltung zu beteiligen.⁷³⁸ Entsprechend handelt es sich um eine *verteilte*, gemeinschaftliche Verwaltung, die jedem Beteiligten eine gewisse Entscheidungsautonomie belässt.⁷³⁹ Hierin besteht eine klare Parallele zu den Idealen der Cypherpunks und der von ihnen propagierten Open-Source-Kultur. Diese Bottom-up-Produktion von öffentlichen Gütern wird in der soziologischen Literatur als Infrastrukturmutualismus bezeichnet.⁷⁴⁰

⁷³⁴ Siehe auch Berentsen/Schär, Bitcoin, 69; ferner Enyi/Dang Yen Le, Butterworths Journal of International Banking and Finance Law 2017, 496 («maintained and policed collaboratively»).

⁷³⁵ So aber Berentsen/Schär, Bitcoin, 72.

⁷³⁶ Siehe hinsichtlich der Voraussetzungen an das Zustandekommen einer *einfachen Gesellschaft* BGer 4A_533/2014 vom 29. April 2015, E. 2.2.3, wonach die Gesellschafter willens sein müssen, «[...] die eigene Rechtsstellung einem gemeinsamen Zweck unterzuordnen, um auf diese Weise einen Beitrag an die Gemeinschaft zu leisten [...]»; ferner BGer 4C.195/2006 vom 12. Oktober 2007, E. 2.4.1; ausführlich Meier-Hayoz/Forstmoser, Schweizerisches Gesellschaftsrecht, § 12 N 23–30.

⁷³⁷ Für die Teilnehmer eines dezentralen Systems grundsätzlich *bejahend* von der Crone/Kessler/Angstmann, SJZ 2018, 340–341, die von einer «Systemvereinbarung», welche zwischen allen Systemteilnehmern zustande kommt, sprechen; a.A. demgegenüber Bärtschi/Meisser, in: Weber/Thouvenin, Virtuelle Währungen, 142; Eggen, AJP 2018, 561; Müller/Reutlinger/Kaiser, EuZ 2018, 87, wonach der Umstand, ob obligatorische Rechte in Bezug auf virtuelle Währungen bestehen, massgeblich von der Ausprägung des «Dezentralisierungselementes» abhängt; Jacquemart, Offene Blockchainsysteme, Rz. 331, 431; Meyer, Crypto Tokens, N 216–220, 224–228; Omlor, ZHR 2019, 308–309, wonach weder eine Forderungsbeziehung noch ein Rechtsbindungswille der Beteiligten bestehe (ferner 328, wo von «reiner Fiktion» des Rechtsbindungswillens die Rede ist).

⁷³⁸ Siehe Berentsen/Schär, Bitcoin, 73 m.Verw. auf sog. Forks.

⁷³⁹ Vgl. in diesem Zusammenhang Bose/Dong/Simpson, Financial Ecosystem, 283–310, 397, die einen besonderen Fokus auf die dezentralisierte gemeinschaftliche Entscheidungsfindung im Finanzbereich legen.

⁷⁴⁰ So etwa Swartz, Cultural Studies 2018, 632–634.

Das Fundament dieser Zweckgemeinschaften bilden Computerprotokolle (siehe hierzu sogleich unten). Diese legen fest, welche Aufgaben und Rollen von den Teilnehmern ausgeübt werden können und nach welchen Regeln Entscheidungen getroffen werden. Wie noch zu sehen sein wird, betrifft das Prinzip der verteilten, gemeinschaftlichen Verwaltung zwar in erster Linie die Abwicklungsebene, d.h. dezentrale Netzwerke; sie kann sich jedoch darüber hinaus auch auf die Applikationsebene, d.h. dezentrale Applikationen, wie etwa eine dezentrale Handelsplattform, beziehen.⁷⁴¹

Die verteilte, gemeinschaftliche Verwaltung eines dezentralen Systems führt im Vergleich zum zentralisierten Modell zu einer deutlichen Erschwerung der Koordination der involvierten Personen. Ausserdem ist die Koordination angesichts der heterogenen Interessenlage in globalen Systemen alles anderes als trivial. Die in Computerprotokollen eingebetteten Regeln sind darum als eine neuartige Form von Regelungs- und Handlungsstrukturen zu begreifen,⁷⁴² wobei sie, wie bereits ausgeführt wurde, nicht die einzigen Governance-Mechanismen in dezentralen Systemen ausmachen.⁷⁴³

2.3 Offene, interoperable Protokolle

In den Computerwissenschaften beschreibt der Begriff des *Protokolls* ein Regelwerk der Datenübertragung zwischen elektronischen Geräten. Damit Computer effektiv miteinander kommunizieren können, bedarf es vorab der Einigung auf standardisierte Regeln und Verfahren. Dies erfolgt durch ein Protokoll.⁷⁴⁴

Als Internetprotokolle gelten etwa TCP/IP, HTTP(S), SMTP und DNS. Die Kommunikation über das Internet stützt sich in erster Linie auf das Transmission Control Protocol (TCP) und das Internet Protocol (IP).⁷⁴⁵ Die TCP/IP-Protokolle definieren die Standards und Regeln für den Informationsaustausch zwischen Geräten, die mit dem Internet verbunden sind, und legen fest, wie Daten paketierte, adressiert, übertragen, weitergeleitet und empfangen werden sollen.⁷⁴⁶

⁷⁴¹ Siehe unten, [III.4](#).

⁷⁴² Siehe oben, [II.5.2](#).

⁷⁴³ Siehe oben, [II.5.3](#).

⁷⁴⁴ Siehe Butterfield/Ekembe Ngondi, Protocol, *passim*; ferner Özsü/Valduriez, Distributed Database Systems, 3. Aufl., 67; Mertens et al., Grundzüge der Wirtschaftsinformatik, 19.

⁷⁴⁵ Siehe Özsü/Valduriez, Distributed Database Systems, 3. Aufl., 67.

⁷⁴⁶ Siehe DeNardis, Global War for Internet Governance, 65, 67; Özsü/Valduriez, Distributed Database Systems, 3. Aufl., 67–69.

Ähnlich wie das OSI-Referenzmodell, das zur Beschreibung offener Kommunikationssysteme verwendet wird und zwischen Datentransport- und Anwendungsdiensten unterscheidet,⁷⁴⁷ wird vorliegend zwischen dezentralen Netzwerken und dezentralen Applikationen unterschieden. Es handelt sich auch bei dezentralen Systemen, zumal sie auf den Internetprotokollen TCP/IP basieren, um Mehrebenensysteme.⁷⁴⁸

Dezentrale Netzwerke, wie etwa Bitcoin und Ethereum, beruhen ihrerseits auf eigenen Protokollen. Diese Protokolle legen die grundlegende Funktionsweise des Netzwerks u.a. in Form von Konsensregeln fest.⁷⁴⁹ Darüber hinaus können auch dezentrale Applikationen auf eigenen Protokollen beruhen, was aber nicht immer der Fall sein muss. Auch diese Protokolle legen gemeinsame Standards fest, die von anderen Protokollen und Applikationen verwendet werden können.⁷⁵⁰

Eine zentrale Eigenschaft dezentraler Systeme ist deren generelle Offenheit.⁷⁵¹ Diese wird in der Literatur oft mit den Begriffen «permissionless» und «non-permissioned» beschrieben. Die Offenheit bezieht sich auf mehrere Komponenten des Systems: Dezentrale Systeme sind *nutzungs-, teilnahme- und entwicklungsoffen*.⁷⁵² Mit anderen Worten kann jede interessierte Person das dezentrale System nutzen; vorausgesetzt werden lediglich ein Wallet sowie eine Internetverbindung. Ferner kann grundsätzlich jede Person an der Durchsetzung der Protokollregeln teilnehmen, indem sie einen Client des Protokolls auf ihrem Computer ausführt. Schliesslich steht es jeder genügend versierten Person offen, zur technischen Weiterentwicklung eines Protokolls beizutragen, ist doch der Quellcode des Protokolls Open Source.

⁷⁴⁷ Sog. *Open Systems Interconnection-Modell* (OSI), das von der ISO als Standard anerkannt ist; vgl. die Darstellung in ISO, *Information technology*, 28; ausführlich hierzu Alpar et al., *Wirtschaftsinformatik*, 454–455; sehr hilfreich ist auch die Darstellung bei Kleine, *OSI-Referenzmodell*, *passim*.

⁷⁴⁸ Ähnlich auch Cambridge Centre for Alternative Finance, *Distributed Ledger Technology*, 33–39, wo zwischen Protocol Layer, Network Layer und Data Layer unterschieden wird. Vgl. zu den unterschiedlichen Ebenen des Internets und Webs Özsü/Valduriez, *Distributed Database Systems*, 3. Aufl., 67–70.

⁷⁴⁹ Siehe Antonopoulos, *Mastering Bitcoin*, 1–2; Antonopoulos/Wood, *Mastering Ethereum*, 2; Bonneau et al., *Proceedings 2015 IEEE Symposium on Security and Privacy*, 106–107, 108–109; Narayanan et al., *Bitcoin*, 168–170; Berentsen/Schär, *Bitcoin*, 97–98, 111–112, 205–207.

⁷⁵⁰ Siehe Schär, *Federal Reserve Bank of St. Louis Review* 2021, 156.

⁷⁵¹ Siehe Schär, *Federal Reserve Bank of St. Louis Review* 2021, 169.

⁷⁵² Siehe auch Jacquemart, *Offene Blockchainsysteme*, Rz. 161–167, der allerdings von «technischer Offenheit» spricht.

Mit der Nutzungs- und Entwicklungsoffenheit dezentraler Systeme verbunden ist deren *Interoperabilität*. Die Interoperabilität betrifft sowohl die Netzwerk- als auch die Applikationsebene solcher Systeme. Die verwendeten Protokolle weisen Schnittstellen auf, die es Entwicklern erlauben, mit eigenen Protokollen und Applikationen an das bestehende System anzuknüpfen. Diese Schnittstellen werden u.a. in sog. *Standards* definiert.⁷⁵³ Ein Beispiel in Ethereum ist der ERC-20-Standard für fungible Token.⁷⁵⁴ Im DeFi-Bereich wird diese Eigenschaft von Protokollen und Applikationen auch mit den Konzepten der *Composability* und «Legoartigkeit» der Anwendungen umschrieben.⁷⁵⁵ Nach diesem Prinzip können Entwickler verschiedene Anwendungen nach Belieben miteinander verbinden, woraus unter Umständen neuartige Dienstleistungen und Geschäftsmodelle entstehen können.

Im Ergebnis können dadurch einzelne dezentrale Applikationen aufeinander aufbauen. Namentlich können Nutzer bspw. über die dezentrale Handelsplattform Kyber Network die Liquidität der dezentralen Handelsplattform Uniswap anzapfen.⁷⁵⁶ Konkret ist dies möglich, weil einzelne Smart Contracts miteinander kommunizieren können: So kann ein von einem Nutzer angerufener Smart Contract eine Aktion eines zweiten Smart Contracts auslösen, welcher wiederum mit einem dritten Smart Contract interagieren kann. Solange der Nutzer die Netzwerkteilnehmer für die entsprechenden Rechenkosten entschädigt, kann somit eine Vielzahl von computerbasierten Aktionen miteinander verbunden werden.

2.4 Kryptografisch abgesicherte Vermögenswerte

a. Kryptografische Absicherung

An dieser Stelle soll der in dieser Arbeit bereits mehrfach verwendete Begriff des Kryptovermögenswerts definiert werden:

Bei *Kryptovermögenswerten* handelt es sich um kryptografisch abgesicherte Vermögenswerte. Technisch betrachtet sind diese Vermögenswerte rein fiktiver Natur. Allerdings wird die Verfügungsmacht über die Vermögenswerte in einer Datenstruktur abgebildet, die im verteilten Register des Netzwerks ab-

⁷⁵³ Siehe Harvey/Ramachandran/Santoro, DeFi, 23, 32, 66.

⁷⁵⁴ Siehe hierzu unten, [III.2.4c](#).

⁷⁵⁵ Siehe Schär, Federal Reserve Bank of St. Louis Review 2021, 169.

⁷⁵⁶ Siehe zu diesen Plattformen unten, [IV.3.6](#) und [IV.3.7](#).

gespeichert ist. An der fiktiven Natur ändert sich selbst dann nichts, wenn die Rechtsordnung die Datenstrukturen als solche anerkennen und ihnen Rechtswirkungen zusprechen.

In der Praxis treten diese Datenstrukturen in aller Regel in Form von Transaktionsketten (sog. *Unspent Transaction Outputs*, UTXOs) oder als Kontostrukturen (Accounts) auf. Transaktionen nach dem UTXO-Modell setzen sich aus Inputs zusammen, über welche in Form von Outputs verfügt werden kann. Dabei geht einem Output in aller Regel wenigstens ein Input voraus. Eine Ausnahme bilden sog. Coinbase-Transaktionen, welche als Teil eines neuberechneten Blocks Vermögenswerte *ex nihilo* schaffen.⁷⁵⁷ Das Bitcoin Protokoll basiert auf UTXOs; Ethereum ist hingegen kontenbasiert (sog. *Externally Owned Accounts*, EOAs)⁷⁵⁸. In beiden Systemen spielen Transaktionen eine bedeutende Rolle, indem sie zu Zustandsübergängen in den verteilten Registern führen; die in solchen Registern abgespeicherten Datenstrukturen sind allerdings abhängig von den konkreten Funktionalitäten des jeweiligen dezentralen Systems.⁷⁵⁹

Die *kryptografische Absicherung* bezieht sich nicht etwa auf die Datenstrukturen an sich, sondern auf die Verfügungsmacht über die Datenstrukturen. Mit anderen Worten besteht eine wesentliche Neuartigkeit dezentraler Systeme in der Anwendung kryptografischer Zugangsverfahren, welche es einer Vielzahl von Personen erlauben, in einmaliger und eindeutiger Weise über Vermögenswerte zu verfügen, ohne dass es zu diesem Zweck einer einzigen buchführenden Autorität bedarf.⁷⁶⁰

Gemeinhin werden Kryptowährungen bzw. Coins und Token unterschieden.⁷⁶¹

b. Kryptowährungen (bzw. Coins)

Kryptowährungen sind das native Transaktionsmedium eines dezentralen Netzwerks (so z.B. bitcoins und ethers bzw. BTC und ETH). Ihre Existenz und Emission sind bereits im Protokoll des Netzwerks angelegt.

⁷⁵⁷ Vgl. hierzu Antonopoulos, *Mastering Bitcoin*, 119–121.

⁷⁵⁸ Vgl. zu EOAs Antonopoulos/Wood, *Mastering Ethereum*, 26.

⁷⁵⁹ Vgl. Antonopoulos/Wood, *Mastering Ethereum*, 6.

⁷⁶⁰ Der Bundesrat spricht von einem «kryptobasierten Zugangsverfahren», welcher dem Inhaber eines Private Keys in ausschliesslicher Weise die Verfügungsmacht über die betreffenden Vermögenswerte vermittelt; vgl. hierzu Botschaft DLT 2019, 292, ferner 279.

⁷⁶¹ Siehe Schär, *Federal Reserve Bank of St. Louis Review* 2021, 156, 157.

BTC und ETH werden dafür gebraucht, die Netzwerkteilnehmer für ihre Rechenkosten zu entschädigen. Die Rede ist von Transaktionsgebühren bzw., in Ethereum, von sog. Gas. Token sind demgegenüber Abstraktionen, welche nach der Logik eines bestehenden dezentralen Netzwerks und der darauf basierenden dezentralen Applikationen herausgegeben und kontrolliert werden können.⁷⁶² Token haben mit anderen Worten keine eigene Blockchain. Während ETH einen Teil der Protokollebene von Ethereum darstellt, ist ein Token das Ergebnis eines entsprechend programmierten Smart Contracts auf der Ethereum Blockchain.⁷⁶³

c. Token

Informationstheoretisch ist ein Token ein Objekt, das die Möglichkeit zur Ausführung von Operationen innerhalb eines Computersystems oder Computernetzwerks darstellt.⁷⁶⁴ Mit Blick auf dezentrale Systeme wird unter einem Token die in einem verteilten Register abgespeicherte informationelle Repräsentation eines digitalen oder realen Gutes sowie in aller Regel das regelgebundene Programm oder Mittel zur Verfügung über ein solches Gut verstanden. Token können je nach Programmierung unterschiedliche Vermögenswerte, Rechte oder Datenstrukturen repräsentieren.⁷⁶⁵

Die von der FINMA angestossene und international nunmehr verbreitete *Dreiteilung* von Token in Zahlungs-Token (bzw. Kryptowährungen), Nutzungs-Token und Anlage-Token stellt dabei eine erste Orientierungshilfe dar.⁷⁶⁶ Relativiert wird diese Klassifizierung aufgrund der enormen praktischen Bedeutung von hybriden Token, d.h. Token, welche Elemente der vorerwähnten Kate-

⁷⁶² Siehe Antonopoulos/Wood, *Mastering Ethereum*, 221.

⁷⁶³ Siehe Antonopoulos/Wood, *Mastering Ethereum*, 227 («*In order to create a new token on Ethereum, you must create a new smart contract*»), sodann 242–243; Werner et al., *Decentralized Finance*, 2; ferner di Angelo/Salzer, in: Xu et al., *Tokens*, 1, 2–3.

⁷⁶⁴ Siehe Butterfield/Ekembe Ngondi, *Token*, *passim*.

⁷⁶⁵ Siehe Werner et al., *Decentralized Finance*, 2 m.w.N.; *grundlegend* aus einer juristischen Perspektive Eggen, *AJP* 2018, 561–565.

⁷⁶⁶ Siehe FINMA, *Wegleitung ICOs*, 2–3; ähnlich BaFin, *Krypto-Token*, 5–6; ausführlich zu unterschiedlichen Taxonomien Oliveira et al., *Blockchain Tokens*, in: *International Conference of Information Systems 2018*, 6–7; in den USA steht aufsichtsrechtlich demgegenüber die Einordnung als *Security* bzw. *Investment Contract* unter dem Securities Act von 1933 im Vordergrund, wobei die Einordnung typischerweise basierend auf dem *Howey-Test* des US-amerikanischen Supreme Courts vorgenommen wird; vgl. hierzu Van Valkenburgh, *Framework for Securities Regulation*, *passim*.

gorien miteinander kombinieren.⁷⁶⁷ Token können ausserdem herausgegeben werden, um etwa mitgliedschaftsbezogene Rechte in einer DAO auszuüben (sog. Governance Token), Zugriffsmöglichkeiten auf Onlinere Ressourcen zu gewähren oder Teilnehmern eines Systems einen Anreiz für erwünschte Aktivitäten zu setzen (so z.B. die Funktion von Pooltoken als Vergütung für die Zurverfügungstellung von Liquidität gegenüber einer dezentralen Handelsplattform)⁷⁶⁸. Token können sodann auch als digitales Identifikationsmittel eingesetzt werden.⁷⁶⁹ Schliesslich werden Token auch zwecks Realisierung von Stablecoins emittiert.⁷⁷⁰

Wie der ICO-Boom von 2017-18 gezeigt hat, kann der Erwerb eines Tokens einerseits Investitions-, ja sogar Spekulationscharakter aufweisen. Andererseits kann die Motivation, einen Token zu verwenden, auch darin bestehen, eine Gemeinschaft oder ein Ökosystem um eine dezentrale Applikation herum aufzubauen oder den Tokeninhabern ganz einfach die Nutzung einer solchen Anwendung zu ermöglichen. Dass Token aus verschiedenen Blickwinkeln analysiert werden können,⁷⁷¹ ist vorliegend nicht weiter zu vertiefen.

In technischer Hinsicht können Token ferner über ihre *Fungibilität* charakterisiert werden. Während Token, einmal abgesehen von ihrem digitalen Spuren im verteilten Register eines Netzwerks,⁷⁷² typischerweise fungibel sind, besteht auch die Möglichkeit, nichtfungible Token herauszugeben und zu besitzen. Diese kommen etwa dort zum Einsatz, wo der Token einen einmaligen Vermögenswert, wie z.B. ein Sammlerstück, eine Parzelle Land oder eine spezifische Schuld einer Person, verkörpern soll.⁷⁷³

⁷⁶⁷ Siehe für eine Kritik Kuhn, in: Weber/Kuhn, *Taxonomie*, Rz. 9–10; ebenfalls kritisch aus Gründen der potenziell innovationshemmenden Wirkung einer solchen starren Kategorisierung Fußwinkel/Kreiterling, *BaFin Perspektiven* 1/2018, 54.

⁷⁶⁸ Siehe zu dieser Funktion etwa unten, [IV.3.7c](#).

⁷⁶⁹ Siehe die Liste bei Antonopoulos/Wood, *Mastering Ethereum*, 222; Ethereum Community, *Token Systems*, *passim*; ferner Schär, *Federal Reserve Bank of St. Louis Review* 2021, 160; ausführlich Oliveira et al., *Blockchain Tokens*, in: *International Conference of Information Systems* 2018, 4–5 m.w.N.

⁷⁷⁰ Vgl. FINMA, *Ergänzung Wegleitung ICOs*, *passim*; siehe auch Schär, *Federal Reserve Bank of St. Louis Review* 2021, 158–159.

⁷⁷¹ Siehe diesbezüglich die Übersicht über die Literatur sowie die eigenständige Parametrisierung in Oliveira et al., *Blockchain Tokens*, in: *International Conference of Information Systems* 2018, 6–7 m.w.N., 8–9.

⁷⁷² Siehe hierzu Antonopoulos/Wood, *Mastering Ethereum*, 223.

⁷⁷³ Der wohl bekannteste NFT verschafft seinem Besitzer gewisse Rechte am digitalen Bild «Everydays: the First 5000 Days» des Künstlers Beeple; siehe diesbezüglich Wikipedia, *Everydays: the First 5000 Days*, Wikipedia, *passim*.

*CryptoKitties*⁷⁷⁴ stellen etwa solche Objekte dar, wobei jede digitale Katze nachweislich einmalig und nach Ansicht der Marktteilnehmer entsprechend unterschiedlich wertvoll ist.⁷⁷⁵ Die Einmaligkeit des Tokens wird durch eine eindeutige Kennung gewährleistet.⁷⁷⁶

Schliesslich können Token sowohl *extrinsische* (z.B. ein Goldbarren oder Grundstück) als auch *intrinsische* Vermögenswerte (z.B. ein CryptoKitty) repräsentieren. Aus ursprünglich extrinsischen und allenfalls intermediatisierten Vermögenswerten kann durch den Vorgang der Tokenisierung ein intrinsischer Werte geschaffen werden. Dies kann nunmehr an den neu geschaffenen Registerwertrechten beobachtet werden, welche etwa an die Stelle unverurkundeter Rechte, physischer Wertpapiere oder intermediatisierter Bucheffekten treten können.⁷⁷⁷

Der heute verbreitetste Standard für fungible Token in Ethereum ist ERC-20.⁷⁷⁸ Für nichtfungible Token wird demgegenüber der ERC-721-Standard angewendet.⁷⁷⁹ Jeder ERC-721-Token hat seine eigene Identifikationsnummer, welche mit weiteren Metadaten verknüpft werden kann.⁷⁸⁰ Der ERC-20-Standard schafft eine gemeinsame Schnittstelle, damit Smart Contracts mit unterschiedlichen ERC-20-Token umgehen können.⁷⁸¹ Diese und andere Standards dienen dazu, die Interoperabilität zwischen Smart Contracts, Wallets und grafischen Benutzeroberflächen (*Graphic User Interfaces*, GUIs) sicherzustellen.⁷⁸² In diesem Sinne haben sie die faktische Wirkung von Protokollen, ohne als solche zu qualifizieren. Die Standards können in entsprechenden Implementierungen mit weiteren Funktionalitäten versehen werden (z.B. OpenZeppelin).⁷⁸³

⁷⁷⁴ <https://www.cryptokitties.co/>.

⁷⁷⁵ Siehe *CryptoKitties*, Collectible and Breedable Cats, 8.

⁷⁷⁶ Siehe Antonopoulos/Wood, *Mastering Ethereum*, 223, 247.

⁷⁷⁷ Vgl. etwa Botschaft DLT 2019, 284.

⁷⁷⁸ Siehe Ethereum, EIP-20, GitHub, *passim*.

⁷⁷⁹ Siehe Ethereum, EIP-721, GitHub, *passim*.

⁷⁸⁰ Siehe Harvey/Ramachandran/Santoro, *DeFi*, 37.

⁷⁸¹ Ausführlich hierzu Antonopoulos/Wood, *Mastering Ethereum*, 227–231.

⁷⁸² Siehe Antonopoulos/Wood, *Mastering Ethereum*, 249; di Angelo/Salzer, in: Xu et al., *Tokens*, 3.

⁷⁸³ Siehe Antonopoulos/Wood, *Mastering Ethereum*, 250–251.

3. Dezentrale Netzwerke (sog. Abwicklungsebene)

3.1 Aufbau und Struktur

a. Bitcoin

Das erste und bis heute bedeutendste dezentrale Netzwerk ist die *Bitcoin Blockchain*. Bitcoin ist in erster Linie als Zahlungsnetzwerk konzipiert, dessen Hauptfunktion in der Speicherung und Übertragung von digitalen Vermögenswerten liegt, ohne dafür auf einen Intermediär zurückgreifen zu müssen.⁷⁸⁴ Die Bitcoin Blockchain beruht im Wesentlichen auf den folgenden Komponenten:

- einem *verteilten Peer-to-Peer (P2P)-Netzwerk* bestehend aus einer Vielzahl von Teilnehmern, die direkt miteinander kommunizieren und in diesem Rahmen Informationen zu Transaktionen und Blöcken austauschen können;
- einem öffentlich einsehbaren, für die Teilnehmer massgeblichen verteilten Register aller Transaktionen, deren Eintragungen in Form von Blöcken erfolgt (Blockchain i.e.S.);
- Konsensregeln, die bestimmen, was als gültige Transaktionen und Blöcke gilt, und durch entsprechende kryptoökonomische Anreizmechanismen den verteilten Konsens des Systems sicherstellen;
- einem auf Rechenleistung basierenden verteilten Konsensalgorithmus, der die Transaktionen zu Blöcken bündelt (sog. *Proof-of-Work, PoW*);
- kryptografischen Verfahren zur Prüfung der Integrität von Adressen und Transaktionen;
- einer (nativen) Kryptowährung (bitcoin, BTC), die einerseits den Transaktionszweck des Systems erfüllt und andererseits Bestandteil der Anreizmechanismen ist; und
- einer Open-Source-Software, welche die oben erwähnten Punkte implementiert (sog. *Client*).⁷⁸⁵

⁷⁸⁴ Siehe statt vieler Nakamoto, Bitcoin, 1; Antonopoulos, Mastering Bitcoin, 1–3.

⁷⁸⁵ Siehe Antonopoulos, Mastering Bitcoin, 2; Bonneau et al., Proceedings 2015 IEEE Symposium on Security and Privacy, 105–109; Antonopoulos/Wood, Mastering Ethereum, 1–2;

In terminologischer Hinsicht ist auf Folgendes hinzuweisen: Technisch gesehen besteht die Blockchain lediglich aus der Komponente des verteilten Registers. Scheinbar aus Marketinggründen hat sich im öffentlichen Diskurs der Blockchain-Begriff für das gesamte Netzwerk durchgesetzt. Vorliegend wird der Klarheit halber von dezentralen Netzwerken gesprochen, wenn das gesamte Netzwerk gemeint ist.

b. Ethereum

Ein weiteres Beispiel für ein dezentrales Netzwerk ist die *Ethereum Blockchain*, die derzeit das zweitgrösste Projekt dieser Art darstellt. Die oben erwähnten Komponenten des Bitcoin Netzwerks treffen im Wesentlichen auch auf Ethereum zu.⁷⁸⁶

Ethereum weist jedoch auch wesentliche Unterschiede zu Bitcoin auf: Ethereum erlaubt die Ausführung von *Turing-vollständigen* Computerprogrammen.⁷⁸⁷ Damit kann Code (konkret: Bytecode) von arbiträrer Komplexität ausgeführt werden. Solcher Code dient als Grundlage für die Programmierung von Smart Contracts, die wiederum die Ausführung von dezentralen Applikationen, die auf der Ethereum Blockchain operieren, möglich macht.⁷⁸⁸

Die Umgebung, in welchem solche Smart Contracts ablaufen, ist die *Ethereum Virtual Machine* (EVM). Turing-Vollständigkeit bedeutet, dass die EVM theoretisch unendliche viele Rechenschritte zulässt. Um Endlosschleifen (*Loops*) entgegenzuwirken, sieht das Ethereum Protokoll einen Gebührenmechanismus vor, deren Einheiten (sog. Gas) nach einer gewissen Anzahl Rechenschritte aufgebraucht sind. Dadurch soll verhindert werden, dass unbegrenzt laufende Rechenzyklen dezentraler Applikationen das dezentrale Netzwerk in die Knie zwingen.⁷⁸⁹

ferner Berentsen/Schär, Bitcoin, 53–64, die in intuitiv einleuchtender Weise zwischen Transaktionsfähigkeit, Transaktionslegitimität und Transaktionskonsens unterscheiden; siehe auch Wright/De Filippi, Rise of Lex Cryptographia, 25. Juli 2017, 4–5 m.w.H.

⁷⁸⁶ Siehe Antonopoulos/Wood, Mastering Ethereum, 6–7.

⁷⁸⁷ Das Konzept einer universellen Rechenmaschine geht auf den britischen Mathematiker und Computerwissenschaftler Alan M. Turing zurück; vgl. etwa Turing, Proceedings of the London Mathematical Society 1936, *passim*; ferner Patt/Patel, computing systems, 9–12; ausführlich Antonopoulos/Wood, Mastering Ethereum, 8–9, die u.a. auch das für Turing-Maschinen relevante *Halting Problem* besprechen.

⁷⁸⁸ Siehe Ethereum, Computation And Turing-Completeness, *passim*; ferner Ethereum Homestead, What is Ethereum?, *passim*.

⁷⁸⁹ Siehe Wood, Ethereum Yellow Paper, 7, 11; ausführlich Antonopoulos/Wood, Mastering Ethereum, 9, 105–107, 314–317.

Ethereum wird aufgrund der oben beschriebenen Eigenschaften oftmals als «the world computer» oder als eine «general-purpose blockchain» beschrieben, die anders als das Bitcoin Netzwerk nicht nur die Speicherung und Übertragung von Kryptowährungen bezweckt, sondern innerhalb der EVM komplexe Datenstrukturen abbilden kann.⁷⁹⁰ Diese Fähigkeit dezentraler Netzwerke ist insofern relevant für die vorliegende Arbeit, als dass die meisten dezentralen Handelsplattformen den Einsatz von Smart Contracts voraussetzen.

Allerdings ist an dieser Stelle zu erwähnen, dass auch Bitcoin trotz Turing-Unvollständigkeit simple Formen von Smart Contracts, wie etwa Multisig und Hash Time Locked Contracts (HTLC), unterstützt.⁷⁹¹ Vorliegend ist der Einfachheit halber auch in diesen Fällen in aller Regel von Smart Contracts die Rede.

3.2 Beteiligte Personen

Bitcoin und Ethereum gelten als nutzungs- und teilnahmeoffene Netzwerke. Die Nutzung der Netzwerke für Transaktionen steht jedermann offen. Ausserdem können interessierte Personen als Teilnehmer an der Durchsetzung der Konsensregeln partizipieren. Solche Netzwerke werden in der Literatur als *permissionless* bzw. öffentlich bezeichnet.⁷⁹² Ihre Nutzungs- und Teilnahmeoffenheit unterscheidet dezentrale Netzwerke von *permissioned* und privaten Blockchains. Im Wesentlichen beinhalten solche Netzwerke Intermediations- und Vertrauenselemente, weshalb sie nicht als Grundlage für dezentrale Handelsplattformen infrage kommen. Auf *permissioned* bzw. *private* Blockchains wird vorliegend aus Platzgründen nicht weiter eingegangen.⁷⁹³

Eine Schwierigkeit dezentraler Systeme liegt darin, traditionelle Identitätssysteme mit der offenen Natur dezentraler Netzwerke in Einklang zu bringen, ohne gleichzeitig auf neue Autoritäten zurückgreifen zu müssen.⁷⁹⁴

⁷⁹⁰ Vgl. etwa Antonopoulos/Wood, *Mastering Ethereum*, 1, 6.

⁷⁹¹ Siehe Antonopoulos, *Mastering Bitcoin*, 149–184, 291, 293, 312–313; sodann Ethereum, *Scripting*, *passim*.

⁷⁹² Siehe etwa Buterin, *Public and Private Blockchains*, *passim*.

⁷⁹³ Siehe für weitere Informationen zu diesen Blockchain-Typen Miller, in: Shetty/Kamhoua/Njilla, *Permissioned and Permissionless Blockchains*, 193–196; Buterin, *Public and Private Blockchains*, *passim*; Government Office for Science, *Distributed Ledger Technology*, 17; BIS/CPMI, *Distributed ledger technology*, 5; Kaulartz, CR 2016, 475; Cambridge Centre for Alternative Finance, *Distributed Ledger Technology*, *passim*; Pilkington, in: Ollerros/Zhegu, *Blockchain technology*, *passim*.

⁷⁹⁴ Vgl. Bacon et al., *Richmond Journal of Law & Technology* 2018, 1–106, 45.

In dezentralen Systemen existieren demgegenüber zwei Formen von Identitäten: Einerseits dient die Public-Key-Kryptografie als Grundlage für die Nutzung des Systems;⁷⁹⁵ andererseits werden für die Teilnahme am System Identitäten durch quantifizierbare Faktoren substituiert, welche von allen Teilnehmern überprüft werden können, wie insb. Rechenkapazitäten und Vermögenswerte.⁷⁹⁶ Die Funktion von bürgerlichen Identitäten wird durch diese Proxy-Identitäten substituiert, die je nach anwendbarem Konsensalgorithmus unterschiedlich ausfallen können. In Netzwerken mit PoW, wie etwa Bitcoin und derzeit noch Ethereum, erfolgt die «Identifikation» der Teilnehmer über die zur Verfügung gestellte Rechenleistung (Mining). In PoS-Netzwerken beruht die Legitimierung der Teilnahme demgegenüber auf dem hinterlegten Kapital (Staking). Dezentrale Netzwerke beruhen mit anderen Worten auf dem Prinzip der Selbstauswahl der Teilnehmer, wobei diese kryptoökonomisch *Skin in the Game* haben müssen.⁷⁹⁷

Im Hinblick auf dezentrale Netzwerke können vereinfacht die folgenden Rollen unterschieden werden, wobei in der Praxis eine Person durchaus mehrere Rollen ausüben kann:⁷⁹⁸

- Eine erste Gruppe von Teilnehmern sind sog. *Full Nodes*. Diese tragen zum System bei, indem sie die Konsensregeln eines Protokolls autonom durchsetzen. Full Nodes verfügen zudem über eine vollständige Kopie aller Zustände (Transaktionen, Smart Contracts usw.) und sind somit in Bezug auf die Verifizierung von Daten von den übrigen Teilnehmern unabhängig.
- Eine zweite Gruppe von Teilnehmern sind je nach Konsensprotokoll Miners bzw. Stakers. Diese werden auch als sog. *Consensus Nodes* bezeichnet. Sie tragen ebenfalls zum System bei, indem sie Transaktionen sammeln und durch das Aufbringen von Ressourcen (Rechenkapazitäten, Kapital usw.) zu Blöcken verarbeiten. Consensus Nodes betreiben den Konsensmechanismus des dezentralen Netzwerks.⁷⁹⁹

⁷⁹⁵ Siehe hierzu oben, [II.4.1b.i](#).

⁷⁹⁶ Ausführlich Narayanan/Clark, *acmqueue* 2017, 14, 17, 17–19.

⁷⁹⁷ Siehe Miller, in: Shetty/Kamhoua/Njilla, *Permissioned and Permissionless Blockchains*, 193–194.

⁷⁹⁸ Eine vergleichbare Rolleneinteilung in Bitcoin findet sich bei Antonopoulos, *Mastering Bitcoin*, 188–189, 196–197; Berentsen/Schär, *Bitcoin*, 97–98; ferner Antonopoulos/Wood, *Mastering Ethereum*, 42–44.

⁷⁹⁹ Siehe sogleich unten, [III.3.3](#).

- *Nutzer* nutzen die Funktionalitäten des Systems, z.B. durch die Übertragung von Kryptowährung oder die Ausführung der Logik eines Smart Contracts. Sie verlassen sich in diesem Rahmen in aller Regel auf andere Netzwerkteilnehmer (z.B. Wallet-Anbieter mit eigenem Full Node), von denen sie dadurch zu einem gewissen Grad abhängig sind.
- Schliesslich können auch die *Entwickler*, die durch ihre Mitarbeit zur technischen Entwicklung und Unterhaltung der zugrundeliegenden Protokolle und Software Clients beitragen, zu den Beteiligten eines dezentralen Netzwerks gezählt werden.

Nicht zum dezentralen Netzwerk gehören demgegenüber Dienstleister bzw. Intermediäre, welche lediglich an der Peripherie des Netzwerks aktiv sind (insb. Wallet-Anbieter, zentrale Handelsplattformen, Verwahrer von Kryptovermögenswerten). Sie gehören zum Ökosystem dezentraler Systeme. Viele dieser *peripheren Dienstleister* betreiben allerdings aus technischen oder ökonomischen Gründen zumindest einen eigenen Full Node. Für einen funktionierenden Infrastrukturmutualismus ist es nicht nur wichtig, dass das Netzwerk frei von Restriktionen ist, sondern auch, dass möglichst viele Personen effektiv dazu beitragen.

3.3 Konsensmechanismus

a. Konsensalgorithmus

Das Protokoll bestimmt, wie ein dezentrales Netzwerk zu einer einheitlichen Auffassung darüber gelangt, welche Transaktionen gültig sind und somit in das verteilte Register aufgenommen werden. Zu diesem Zweck werden die Transaktionen von den Consensus Nodes gesammelt und für einen Block vorgeschlagen. Consensus Nodes führen sodann einen Algorithmus aus, um autoritativ zu *entscheiden*, welcher der vorgeschlagenen Blöcke als nächster an die bereits bestehende Kette von Blöcken angehängt wird. Diese neuartige Möglichkeit, in dezentraler Weise eine Einigung zu finden, wurde erstmals in Bitcoin durch den *Nakamoto-Konsens* umgesetzt.⁸⁰⁰

⁸⁰⁰ Siehe hierzu oben, [II.4.1b.i.](#)

Die derzeit bedeutendsten Konsensalgorithmen sind *Proof-of-Work (PoW)*, *Proof-of-Stake (PoS)* und *Delegated Proof-of-Stake (DPoS)*. Im Falle von PoW ist von Minern bzw. Mining die Rede, bei PoS handelt es sich um Staker bzw. Staking und in DPoS-Systemen sind typischerweise Validatoren tätig. Die Terminologie kann allerdings von Protokoll zu Protokoll variieren.

Der wesentliche Unterschied der verschiedenen Konsensalgorithmen besteht in der aufzubringenden Ressource: Während Consensus Nodes bei PoW dem Netzwerk Rechenkapazitäten und somit letztlich Energie zur Verfügung stellen,⁸⁰¹ hinterlegen Consensus Nodes in PoS- und DPoS-Systemen einen bestimmten Betrag der jeweiligen Kryptowährung als Sicherheit (sog. *Stake*), die für den Fall eines Manipulationsversuchs eines Consensus Nodes eingezogen und vernichtet werden kann.⁸⁰² Erst durch die Bereitstellung der entsprechenden Ressourcen können Consensus Nodes in der Entscheidungsfunktion tätig werden. Es bestehen darüber hinaus weitere Konsensalgorithmen, auf die vorliegend allerdings nicht weiter eingegangen werden kann.⁸⁰³

b. Ablauf am Beispiel des «Nakamoto-Konsens»

Der Algorithmus hinter dem «Nakamoto-Konsens» wird von den Netzwerkteilnehmern so lange ausgeführt, bis sie nach den Regeln des Protokolls einen gültigen Block finden. Sobald ein Consensus Node einen gültigen Block gefunden hat, teilt er ihn umgehend den übrigen Netzwerkteilnehmern mit. Mit anderen Worten befinden sich Consensus Nodes bezüglich der Produktion eines gültigen Blocks in einem kompetitiven Rennen.⁸⁰⁴

Diese Wettbewerbssituation kann ausnahmsweise auch zu einer vorübergehenden Pattsituation führen, die dadurch entsteht, dass mehrere Consensus Nodes mehr oder minder zur gleichen Zeit jeweils einen gültigen Block finden. In diesem Fall kommt es zu einer temporären Aufspaltung der Blockchain in

⁸⁰¹ Ausführlich zum PoW-Berechnungsvorgang Antonopoulos, *Mastering Bitcoin*, 244–254; Berentsen/Schär, *Bitcoin*, 207–210; ferner Bonneau et al., *Proceedings 2015 IEEE Symposium on Security and Privacy*, 107–108.

⁸⁰² Siehe Antonopoulos/Wood, *Mastering Ethereum*, 320–321.

⁸⁰³ Vgl. zu einigen dieser alternativen Konsensmechanismen die Übersicht bei Bonneau et al., *Proceedings 2015 IEEE Symposium on Security and Privacy*, 116 m.w.H.

⁸⁰⁴ Siehe Bonneau et al., *Proceedings 2015 IEEE Symposium on Security and Privacy*, 107; Antonopoulos, *Mastering Bitcoin*, 235–236, 264.

unterschiedliche Versionen (sog. *Fork*).⁸⁰⁵ Dieser Typ einer Blockchain Fork ist von *bewusst* herbeigeführten Forks, die als eine Form der Governance zu betrachten sind, zu unterscheiden.⁸⁰⁶

Für das Protokoll ist letztlich diejenige Version massgeblich, die am meisten Rechenkapazität auf sich vereint.⁸⁰⁷ In einem dezentralen System, das nicht auf PoW beruht, werden demgegenüber alternative Entscheidungsverfahren verwendet. In einem PoS-System halten Consensus Nodes typischerweise eine Abstimmung über den nächsten Block ab, wobei ein dem Mehrheitsprinzip nachgebildetes Verfahren basierend auf der Höhe der hinterlegten Vermögenswerte zur Anwendung gelangt.⁸⁰⁸ In diesem Fall wird auch von «virtuellem Mining» gesprochen, da die Aufwendung von Energie nicht mehr im Vordergrund steht.⁸⁰⁹

Consensus Nodes erstellen Blöcke in einem bestimmten Zeitintervall, das als Blockzeit (sog. *Block Time*) bezeichnet wird. In Bitcoin wird im Durchschnitt alle 10 Minuten ein neuer Block gefunden.⁸¹⁰ In Ethereum betragen die Blockzeiten durchschnittlich 15 Sekunden.⁸¹¹ Andere dezentrale Systeme haben unter Umständen noch kürzere Blockzeiten (z.B. Solana oder Avalanche). Sobald eine Transaktion in einen Block aufgenommen wurde, gilt die Transaktion als durch den betreffenden Block bestätigt (sog. *Confirmation*). Mit jedem weiteren Block, der an den ersten Block mit der betreffenden Transaktion angehängt wird, nimmt die Anzahl der Bestätigungen zu.⁸¹² Die Rückabwicklung einmal bestätigter Blöcke wird mit jeder Bestätigung mathematisch unwahrscheinlicher.

Transaktionen, die noch nicht in einen Block aufgenommen worden sind, werden von den Teilnehmern vorübergehend bis zur Aufnahme in einem einsehbaren Transaktionspool (sog. *Mempool*) gesammelt.⁸¹³ Die dadurch entste-

⁸⁰⁵ Siehe Berentsen/Schär, Bitcoin, 228–230; Bonneau et al., Proceedings 2015 IEEE Symposium on Security and Privacy, 107; ausführlich Antonopoulos, Mastering Bitcoin, 211, 257–264.

⁸⁰⁶ Siehe hierzu, [II.5.3b.iv.](#)

⁸⁰⁷ Bonneau et al., Proceedings 2015 IEEE Symposium on Security and Privacy, 107; Berentsen/Schär, Bitcoin, 57–59, 216; Antonopoulos, Mastering Bitcoin, 255–256.

⁸⁰⁸ Siehe Antonopoulos/Wood, Mastering Ethereum, 321.

⁸⁰⁹ Ausführlich Narayanan et al., Bitcoin, 206–211.

⁸¹⁰ Siehe Berentsen/Schär, Bitcoin, 60; Bonneau et al., Proceedings 2015 IEEE Symposium on Security and Privacy, 108.

⁸¹¹ Siehe für aktuelle Statistiken <https://etherscan.io/chart/blocktime>.

⁸¹² Siehe Bonneau et al., Proceedings 2015 IEEE Symposium on Security and Privacy, 107.

⁸¹³ Siehe Antonopoulos, Mastering Bitcoin, 208–209, 235, 236.

hende «Warteschlange» ist in der oben erwähnten Blockzeit sowie an den begrenzten Speicherkapazitäten eines Blocks (sog. *Block Size*) begründet.⁸¹⁴ Bei Bitcoin beispielsweise ist die Blockgrösse derzeit auf maximal 4 Megabytes beschränkt, wobei die Blocks in der Praxis in aller Regel deutlich kleiner ausfallen.⁸¹⁵ In Ethereum ist die Blockgrösse dynamisch vom jeweiligen *Block Gas Limit* abhängig.⁸¹⁶

Aufgrund dieser bewussten technischen Begrenzungen hat der enorme Nachfrageanstieg sowohl in Bitcoin als auch Ethereum zu einem eigentlichen Markt für Transaktionsgebühren geführt, womit letztlich die Zahlungsbereitschaft der Nutzer darüber bestimmt, wie schnell ihre Transaktionen in einen Block integriert werden.⁸¹⁷

Das Protokoll überprüft in regelmässigen Zeitabständen den technischen Schwierigkeitsgrad der Blockproduktion, um zu verhindern, dass Blöcke schneller oder langsamer als die angestrebte Blockzeit produziert werden (sog. *Difficulty*). Wenn bspw. in Bitcoin die durchschnittlichen Blockzeiten zu lang oder zu kurz werden, passt das Protokoll den Schwierigkeitsgrad des Konsensalgorithmus nach 2'016 Blöcken automatisch an.⁸¹⁸ Dieser Anpassungsmechanismus ist notwendig, um die erwarteten Verbesserungen in der Hardwareentwicklung nach dem Moore'schen Gesetz und das variierende Interesse am Betrieb von Consensus Nodes im Laufe der Zeit auszugleichen.⁸¹⁹

In der Praxis existieren neben autonom handelnden Consensus Nodes in vielen Fällen sog. *Mining* bzw. *Staking Pools*. Diese Zusammenschlüsse einer Vielzahl von Consensus Nodes unter dem Dach eines gemeinsamen Protokolls oder ähnlichen Setups dient der wirtschaftlichen Planungssicherheit v.a. kleinerer Netzwerkteilnehmer.⁸²⁰ Damit verbunden ist allerdings in vielen Fällen

⁸¹⁴ Siehe hierzu Bonneau et al., Proceedings 2015 IEEE Symposium on Security and Privacy, 114; Narayanan et al., Bitcoin, 75; ausführlich Croman et al., in: Clark et al., Scaling Decentralized Blockchains, 106–110.

⁸¹⁵ Siehe Song, Understanding Segwit Block Size, Medium, *passim*.

⁸¹⁶ Siehe Antonopoulos/Wood, Mastering Ethereum, 317.

⁸¹⁷ Siehe zum Thema der Transaktionsgebühren sogleich unten, III.3.4.

⁸¹⁸ Ausführlich Berentsen/Schär, Bitcoin, 60–61, 211–213; Bonneau et al., Proceedings 2015 IEEE Symposium on Security and Privacy, 108; Narayanan et al., Bitcoin, 107–108.

⁸¹⁹ Siehe Nakamoto, Bitcoin, 3.

⁸²⁰ Siehe Bonneau et al., Proceedings 2015 IEEE Symposium on Security and Privacy, 108; Antonopoulos, Mastering Bitcoin, 267–269; Berentsen/Schär, Bitcoin, 222–225; ausführlich Narayanan et al., Bitcoin, 124–130.

eine gewisse Zentralisierung von Entscheidungsgewalt und Kontrolle beim Poolbetreiber.⁸²¹

Infolge der Ausführung des Konsensalgorithmus durch eine Mehrzahl von Consensus Nodes entsteht ein emergenter verteilter Konsens darüber, welche Transaktionen und Blöcke gültig sind. Der Konsensalgorithmus schafft mit anderen Worten eine einheitliche Sichtweise in einem verteilten Netzwerk, so dass keine weiteren Diskussionen darüber geführt werden müssen, wem was letztlich zusteht. Der Konsens erzeugt sodann als Nebeneffekt auch die Unveränderbarkeit des verteilten Registers (sog. *Immutability*).

3.4 Governance und die Rolle von Kryptowährungen

Im Whitepaper von Bitcoin ist der Begriff der Governance unerwähnt. Inzwischen handelt es sich um eines der meistdiskutierten Themen in der Literatur.⁸²² Governance in dezentralen Systemen hat sowohl eine ökonomische als auch eine soziotechnische Komponente. Das zweite Kapitel führte zu diesem Zweck den Begriff der dezentralen Governance ein.⁸²³

Wie an dortiger Stelle ausgeführt, kann dezentrale Governance in Governance i.e.S. und Governance i.w.S. unterteilt werden: *Governance i.e.S.* ist die Governance des Systems durch die systemeigenen, codierten Regeln. Hierzu gehört insb. die Ausführung des Konsensalgorithmus (siehe oben). *Governance i.w.S.* ist die Governance des Systems durch die Netzwerkteilnehmer, Nutzer, Entwickler und weitere interessierte Kreise des Ökosystems. Hinsichtlich letzterer Form der Governance kann ferner zwischen On-chain- und Off-chain-Governance differenziert werden: On-chain bedeutet, dass die Governance-Regeln im Netzwerkcode formalisiert werden; off-chain bedeutet demgegenüber, dass informellen Prozessen eine grössere Bedeutung als codierten Regeln zukommen soll. In diesem Fall ist oft auch von *Rough Consensus* die Rede, der typischerweise irgendwo zwischen einfacher Mehrheit und Einstimmigkeit der an einem Ergebnis interessierten Personen liegt.⁸²⁴

⁸²¹ Siehe hierzu oben, [II.6.3](#).

⁸²² Statt vieler Ehram, *Blockchain Governance*, Medium, *passim*.

⁸²³ Siehe oben, [II.5.3a](#).

⁸²⁴ Siehe zum Konzept ten Over/Moriarty, *The Tao of IETF*, *passim* («Another aspect of Working Groups that confounds many people is the fact that there is no formal voting. The general rule on disputed topics is that the Working Group has to come to 'rough consensus', meaning that a very large majority of those who care must agree.»).

Die Existenz von Kryptowährung ist *unabdingbar* für die Governance eines dezentralen Netzwerks. Namentlich besteht in offenen Systemen die Notwendigkeit kryptoökonomischer Anreize, damit Personen überhaupt partizipieren und sodann die Konsensregeln des Protokolls auch tatsächlich im Interesse des Systems ausführen.⁸²⁵ Anreize sind ferner dort zentral, wo die Teilnahme ökonomisch kostspielig ist, wie insb. im Fall des Minings.

Um die Bereitstellung der Blockproduktion zu incentivieren, erhalten Miner bzw. Staker frisch geschaffene Einheiten der Kryptowährung (sog *Block Subsidy*). Kumulativ oder alternativ erhalten Consensus Nodes typischerweise auch die Transaktionsgebühren oder wenigstens einen Teil davon als Entschädigung für ihren Beitrag zum Netzwerk.⁸²⁶ Die Summe neu geschaffener Kryptowährungseinheiten und Transaktionsgebühren wird als sog. *Block Reward* bezeichnet.⁸²⁷ Über den Schwierigkeitsmechanismus der Blockproduktion wird ökonomisch sichergestellt, dass sich nicht nur die Blockzeit, sondern darüber hinaus auch die Belohnungen in einem stabilen Gleichgewicht halten. Kryptowährungen dienen somit auch als Grundlage für die Koordination der Teilnehmer eines dezentralen Netzwerks.⁸²⁸

Demgegenüber ist die Emission eines nativen Tokens in permissioned Blockchains keine Notwendigkeit.⁸²⁹

⁸²⁵ Siehe Bonneau et al., Proceedings 2015 IEEE Symposium on Security and Privacy, 107; Böhme/Pesch, DuD 2017, 477; ferner Möser/Böhme, in: Brenner et al., 21.

⁸²⁶ Siehe etwa Narayanan et al., Bitcoin, 39–40, 97.

⁸²⁷ Siehe Ammous, Bitcoin Standard, 218.

⁸²⁸ So auch Davidson/De Filippi/Potts, Journal of Institutional Economics 2018, 649.

⁸²⁹ Siehe etwa Swanson, Consensus-as-a-service, 13.

4. Dezentrale Applikationen (sog. Applikationsebene)

4.1 Aufbau und Struktur

Dezentrale Applikationen (*Decentralized Applications*, DApps bzw. ÐApps) sind in aller Regel Blockchain-basierte Anwendungen, die sich typischerweise aus einem oder mehreren Smart Contracts sowie einer grafischen Benutzeroberfläche bzw. GUI zusammensetzen. Die GUI dient in erster Linie der Verbesserung der Bedienungsfreundlichkeit sowie der Verständlichkeit der von einer Anwendung generierten Outputs für den Nutzer. Sie ist in aller Regel über ein webbasiertes Frontend oder eine eigenständige Software erreichbar.⁸³⁰ Dezentrale Applikationen werden begrifflich regelmässig auch als Software oder Webapplikation bezeichnet, die allerdings in Abgrenzung zu herkömmlichen Anwendungen nicht auf einem zentralen Server gehostet, sondern auf einem dezentralen Netzwerk zur Ausführung gelangen.⁸³¹

Dezentrale Applikationen operieren auf einem dezentralen Netzwerk. Die Applikationsebene baut mit anderen Worten unmittelbar auf der Abwicklungsebene auf. Dies bedeutet, dass die Verfügbarkeit und Integrität dezentraler Applikationen vom besagten Netzwerk abhängig sind. Dezentrale Applikationen übernehmen somit das *Sicherheits- und Vertrauensmodell* des dezentralen Netzwerks. Aufgrund ihrer vertikalen und horizontalen Interoperabilität können dezentrale Applikationen nicht nur mit dem dezentralen Netzwerk, an welches sie anknüpfen, sondern auch mit anderen dezentralen Applikationen kommunizieren.

Dezentrale Applikationen basieren häufig auf Regeln und Verfahren, die in einem Protokoll festgelegt sind. Solche Protokolle legen etwa mithilfe von Smart Contracts fest, wie Teilnehmer kommunizieren oder wie Daten abgespeichert werden.⁸³² Ferner kann die Applikationsebene in weitere Ebenen unterteilt werden: Neben der Protokollebene können in DeFi etwa auch eine Anwen-

⁸³⁰ Siehe IOSCO, Public Report DeFi 2022, 7–8; Auer et al., BIS Working Papers Nr. 1066, Januar 2023, 5.

⁸³¹ Siehe Antonopoulos/Wood, *Mastering Ethereum*, 10; ferner Lin, *Stanford Journal of Blockchain Law & Policy* 2019, 59–60; Schär, *Federal Reserve Bank of St. Louis Review* 2021, 156; Gudgeon et al., *Proceedings Crypto Valley Conference on Blockchain Technology* 2020, 2.

⁸³² Siehe etwa Warren, *Difference between App Coins and Protocol Tokens*, *passim*.

dungs- und Aggregationsebene unterschieden werden.⁸³³ Im Falle von dezentralen Handelsplattformen weisen alle diese Ebenen eine gewisse Relevanz auf.⁸³⁴ An dieser Stelle ist bereits zu erwähnen, dass Smart Contracts darüber hinaus etwa auch die Durchsetzung von rechtlichen und regulatorischen Vorgaben sicherstellen können, was als weitere Ebene dezentraler Applikationen aufgefasst werden kann (sog. Compliance Layer).⁸³⁵

Dezentrale Applikationen wurden erstmals dank der Ethereum Blockchain bekannt und relevant: Unzufrieden mit den begrenzten technischen Möglichkeiten der Bitcoin Blockchain machte sich eine Gruppe von Entwicklern um Vitalik Buterin im Jahr 2013 daran, ein dezentrales Netzwerk bestehend aus Computern zu entwickeln, das wie ein einziger virtueller Supercomputer agieren soll.⁸³⁶

Dezentrale Applikationen können für eine Vielfalt von Anwendungen programmiert werden. Bekannte Anwendungen bestehen bspw. im Bereich dezentraler Kommunikation (z.B. Status⁸³⁷), dezentraler Bereitstellung von Computerleistung (z.B. Golem⁸³⁸) oder Speicherplatz (z.B. Filecoin⁸³⁹, Sia⁸⁴⁰ und Storj⁸⁴¹), dezentraler Prognosemärkte (z.B. Augur⁸⁴² und Gnosis⁸⁴³) und Werbemärkte (z.B.

⁸³³ Siehe hinsichtlich der unterschiedlichen Ebenen Schär, Federal Reserve Bank of St. Louis Review 2021, 156; ferner Hoffmann, Digital Finance Stack, Medium, *passim*.

⁸³⁴ Siehe hierzu oben, III.2.3.

⁸³⁵ Siehe etwa das Projekt C-Layer (<https://www.c-layer.org/>), das im Zusammenhang mit tokenisierten Vermögenswerten, wie etwa Aktien, das Einschieben einer Compliance-Ebene auf der Blockchain vorsieht. Die Mt Pelerin Group SA mit Sitz in Genf hat einen Compliance Layer mit der Bezeichnung «Bridge Protocol» bereits implementiert; vgl. Mt Pelerin Group SA, White Paper, 30. Ein erstes Beispiel einer regulatorischen Whitelist aus der Praxis findet sich in Peaster, First Security Token Arrives on Uniswap DEX, Blockchain, *passim*.

⁸³⁶ Siehe Ethereum, Ethereum Whitepaper, *passim* («The intent of Ethereum is to create an alternative protocol for building decentralized applications, providing a different set of trade-offs that we believe will be very useful for a large class of decentralized applications, with particular emphasis on situations where rapid development time, security for small and rarely used applications, and the ability of different applications to very efficiently interact, are important.»); ferner Wood, Ethereum Yellow Paper, 1, 18; ausführlich zum Hintergrund Russo, Infinite Machine, *passim*.

⁸³⁷ <https://status.im/>.

⁸³⁸ <https://golem.network/>.

⁸³⁹ <https://filecoin.io/>.

⁸⁴⁰ <https://sia.tech/>.

⁸⁴¹ <https://storj.io/>.

⁸⁴² <https://www.augur.net/>.

⁸⁴³ <https://gnosis.io/>.

Basic Attention Token⁸⁴⁴), dezentraler autonomer Organisationen (z.B. Aragon⁸⁴⁵) sowie des Handels mit virtuellen, nichtfungiblen Vermögenswerten (z.B. CryptoKitties⁸⁴⁶ und Decentraland⁸⁴⁷). In der vorliegenden Arbeit liegt der Fokus hingegen fast ausschliesslich auf Anwendungen aus dem Bereich von DeFi, im Besonderen auf dezentralen Handelsplattformen.

4.2 Beteiligte Personen

a. Im Allgemeinen

Im Gegensatz zu dezentralen Netzwerken werden dezentrale Applikationen nicht von einem eigenständigen Computernetzwerk unterhalten. Ihre Funktionalitäten basieren unmittelbar auf dem Netzwerk der Abwicklungsebene, dessen Sicherheits- und Vertrauensmodell sie übernehmen (siehe auch oben). Als beteiligte Personengruppen sind darum in erster Linie lediglich die *Nutzer* und *Entwickler* zu erwähnen. Dezentrale Applikationen sind im Grundsatz ebenso nutzungs- und entwicklungsoffen wie dezentrale Netzwerke.

In der Praxis können die Entwickler von Smart Contracts vorsehen, dass nur Personen mit privilegierten Zugriffsrechten Zugang zu bestimmten Funktionen der Anwendungen haben (sog. *Access Control-Funktionen*).⁸⁴⁸ In DeFi ist dies derzeit eine verbreitete Herangehensweise an die Entwicklung von Protokollen und Smart Contracts, nachdem diese auf einem dezentralen Netzwerk bereits in Ausführung gesetzt worden sind. Access Control-Funktionen erlauben etwa dem Entwicklerteam, gewisse Parameter einer Anwendung nachträglich abzuändern.⁸⁴⁹ Eine alternative dezentrale Herangehensweise an die Governance von dezentralen Applikationen ist die Herausgabe eines Governance Tokens im Zusammenhang mit einer DAO.

⁸⁴⁴ <https://basicattentiontoken.org/>.

⁸⁴⁵ <https://aragon.org/>.

⁸⁴⁶ <https://www.cryptokitties.co/>.

⁸⁴⁷ <https://decentraland.org/>.

⁸⁴⁸ Siehe ausführlich zu *Admin Key-Risiken* unten, [IV.5.2d.ii](#).

⁸⁴⁹ Siehe Werner et al., *Decentralized Finance*, 3.

b. DAOs im Besonderen

Dezentrale autonome Organisationen (sog. *Decentralized Autonomous Organizations*, DAOs) stellen Entitäten dar, die mithilfe von Smart Contracts, die auf einem dezentralen Netzwerk zur Ausführung gelangen, ein Regelwerk implementieren, das u.a. auf kryptoökonomischen Prinzipien beruht und es ihren Teilnehmern ermöglicht, einen gemeinsamen Zweck zu erreichen.⁸⁵⁰ BUTERIN definiert in der Folge eine DAO als «[...] *automation at the center, humans at the edges.*»⁸⁵¹ Die SEC spricht von einer «[...] *'virtual' organization embodied in computer code and executed on a distributed ledger or blockchain.*»⁸⁵²

Als Teil des Anreizsystems geben DAOs typischerweise *Governance Token* heraus, die im Wesentlichen der Koordination der dezentralen Entscheidungsfindung dienen. Darüber hinaus können einem Governance Token auch weitere Funktionen zukommen (z.B. ein Recht auf Gewinnbeteiligung). Die Zuteilung von Governance Token erfolgt oftmals auf Basis der an die Entwicklung oder Verwaltung einer Anwendung geleisteten Beiträge (z.B. Bereitstellung von Liquidität über eine dezentrale Handelsplattform); die Allokation kann aber auch über einen öffentlichen Verkauf der Token erfolgen.⁸⁵³ Die Smart Contracts von DAOs können schliesslich zur Finanzierung des von den Teilnehmern gemeinsam verfolgten Zwecks Kryptovermögenswerte annehmen, aufbewahren und ausbezahlen.⁸⁵⁴

Dezentrale Governance in Form von DAOs haben insb. für DeFi-Projekte grosse praktische Bedeutung erlangt. Die Protokolle *Compound* und *Maker* gehören zu den Vorreitern in diesem Bereich, aber mit *Uniswap* und weiteren Protokollen existieren auch DAOs im Bereich dezentraler Handelsplattformen. Die Kompetenzen einer DAO fallen dabei je nach dezentraler Applikation sehr unterschiedlich aus.⁸⁵⁵

⁸⁵⁰ Vgl. hinsichtlich der ursprünglichen Idee hinter der Ur-DAO, welche gemeinhin als *The DAO* bezeichnet wird, die letztlich aufgrund eines Hackerangriffs 2016 scheiterte, Jentzsch, *Decentralized Autonomous Organization*, 1; Tual, *A Primer to DAOs*; ferner Meier/Schuppli, in: Molin-Kränzlin/Schneuwly/Stojanovic, *The DAO*, 33 m.w.N.; zum Hack vom Juni 2016 siehe Antonopoulos/Wood, *Mastering Ethereum*, 325–327.

⁸⁵¹ Buterin, *DAOs and More*, *passim*.

⁸⁵² SEC, *The DAO Report*, 1.

⁸⁵³ Siehe Nadler/Schär, *Decentralized Finance*, 1.

⁸⁵⁴ Siehe Buterin, *DAOs and More*, *passim*; in Bezug auf die Token von *The DAO SEC*, *The DAO Report*, 5–6.

⁸⁵⁵ Vgl. Buterin, *Beyond coin voting governance*, *passim*, der einen Minimalansatz hinsichtlich der Kompetenzen solcher Governance postuliert.

DAOs sind nach vorliegender Auffassung *Grenzerscheinungen*, die der Dichotomie in dezentrale Netzwerke und dezentrale Applikationen nicht ohne Weiteres zugänglich sind: DAOs sind grundsätzlich der Applikationsebene zuzuordnen. Ihnen kommt grundsätzlich kein Abwicklungscharakter zu, denn die Abwicklung von Transaktionen bzw. Abstimmungen findet letztlich auf dem zugrundeliegenden dezentralen Netzwerk statt. Andererseits weisen DAOs aber Teilnehmer in Form der Inhaber der Governance Token auf, die Entscheidungen treffen, so dass eine gewisse Ähnlichkeit mit dezentralen Netzwerken nicht zum Vornherein zu verkennen ist.⁸⁵⁶ Dafür spricht auch das gemeinsame Regelwerk samt eigenständigen Anreizmechanismen, die der Koordination der Entscheidungen durch die Teilnehmer im Hinblick auf einen gemeinsamen Zweck dienen.⁸⁵⁷ Durch die Verteilung von Entscheidungsgewalt und Kontrolle können sie die Verwaltung einer dezentralen Applikation vergemeinschaften bzw. mutualisieren. Daraus entstehen tokenbasierte Regelungs- und Handlungsstrukturen, wobei die Governance der Anwendung von den Governance-Systemen des Netzwerks abhängig bleibt.⁸⁵⁸

In der jüngeren Vergangenheit haben sich bestehende rechtliche Strukturen dem Konzept einer DAO angenähert. Der US-Bundesstaat Wyoming hat etwa ein Gesetz erlassen, dass es DAOs ermöglicht, von der LLC-Rechtsform Gebrauch zu machen, um im Umgang mit der Aussenwelt grössere Rechtssicherheit zu erlangen.⁸⁵⁹

⁸⁵⁶ Vgl. auch Buterin, DAOs and More, *passim*, der bezüglich Bitcoin von einer DAO ausgeht; ferner die These vertretend, dass DAOs eine neue Erscheinungsform sind, die sich in die bestehenden gesellschaftsrechtlichen Strukturen nur schwer einordnen lassen, Brummer/Seira, Legal Wrappers, 3 («a radically different template for organizational behavior»).

⁸⁵⁷ Siehe z.B. das Projekt *Aragon*, das auf der Ethereum Blockchain und der *Aragon Chain* aufbaut und einerseits Smart Contracts für das Aufsetzen von DAOs entwickelt und andererseits mit *Aragon Network* eine eigene DAO u.a. als Streitbeilegungsmechanismus für andere DAOs anbietet; vgl. Aragon Wiki, *passim*; ferner Aragon Network, Whitepaper, *passim*.

⁸⁵⁸ Vgl. zu sog. *Nested Enterprises* Ostrom, Governing the Commons, 90, 101–102.

⁸⁵⁹ Siehe etwa Bull, Wyoming's DAO Law, Coindesk, *passim*.

5. Skalierungslösungen

5.1 Layer-1-Netzwerk und ihre Trade-offs

Wie eingangs erwähnt, sind die derzeit bekanntesten dezentralen Netzwerke Bitcoin und Ethereum. Bei ihnen handelt es sich um *Layer-1-Netzwerke*. Aufgrund ihrer stark angestiegenen Popularität sind die beiden Netzwerke in den letzten Jahren und Monaten vermehrt an ihre Kapazitätsgrenzen gestossen. Die begrenzten Speicherkapazitäten der Protokolle haben in der Folge die Transaktionsgebühren in die Höhe schnellen lassen.

Grundsätzlich ist in informationstechnischer Hinsicht davon auszugehen, dass ein dezentrales Netzwerk nicht vollständig dezentralisiert werden kann.⁸⁶⁰ Dies liegt daran, dass Dezentralität *technischen Trade-offs* unterliegt, die letztlich durch die physikalischen Gesetze bedingt und somit unumgänglich sind.⁸⁶¹ Untersuchungen zu verteilten Netzwerken haben etwa zur Formulierung des *CAP-Theorems* geführt: Nach diesem Theorem ist es für ein verteiltes Computernetzwerk bei nicht rechtzeitiger Erreichbarkeit aller Netzwerkteilnehmer (Partitioning) unmöglich, gleichzeitig Datenkonsistenz (Consistency) und Datenverfügbarkeit (Availability) zu gewährleisten.⁸⁶²

Nicht unähnlich stellt sich die Situation für dezentrale Systeme dar: Diese haben nach dem *DCS-Theorem* einen technischen Kompromiss zwischen Dezentralität (Decentralization), Konsens (Consensus) und Skalierbarkeit (Scalability) zu treffen. Das *DCS-Theorem* besagt, dass ein dezentrales System höchstens zwei der drei Eigenschaften aufweisen kann.⁸⁶³ Für ein *dezentrales System* be-

⁸⁶⁰ Siehe Buterin, Meaning of Decentralization, Medium, *passim*; Narayanan et al., Bitcoin, 28; ferner Laurie, Decentralised Currencies Probably Impossible, 3, 4, der selbst für das Bitcoin Netzwerk in dessen Anfängen die Einführung von «Checkpoints» durch die Entwickler festgestellt hat. Allerdings muss man sich bewusst sein, dass Netzwerkteilnehmer Checkpoints nach Belieben ignorieren können, wobei in diesem Fall für das Netzwerk das Risiko einer (Hard) Fork besteht. Checkpointing wurde bspw. als Massnahme gegen eine zehntätige *Chain Reorganisation Attack* auf die Bitcoin Gold Blockchain verwendet, mit dem Hinweis, dass «[t]he majority of honest pool hashpower continues to mine on the honest chain.»; vgl. diesbezüglich CryptoDJ, Emergency update, *passim*.

⁸⁶¹ Vgl. die Darstellung in Cambridge Centre for Alternative Finance, Distributed Ledger Technology, 45–46.

⁸⁶² Siehe hierzu Brewer, Computer 2012, *passim*; Özsu/Valduriez, Distributed Database Systems, 4. Aufl., 521.

⁸⁶³ Siehe Slepak/Petrova, DCS Theorem, 2; McConaghy, DCS Triangle, *passim*.

deutet dies, dass es die Wahl treffen muss zwischen einer konsistenten und für alle Netzwerkteilnehmer verfügbaren Darstellung der Zustände (Konsens bzw. Sicherheit) oder einer grossen Datenmenge, die das System pro Zeiteinheit verarbeiten kann (Skalierbarkeit).⁸⁶⁴ Mit anderen Worten beschlägt der Grad der Dezentralisierung entweder die Konsistenz und Verfügbarkeit der Daten oder die technische Effizienz des Netzwerks. Oder nochmals leicht anders formuliert: Es existiert ein Trade-off zwischen der erforderlichen Zeit, die Teilnehmer benötigen, um hinsichtlich Transaktionen endgültige Entscheidungen zu treffen (Finalität), und des Kommunikationsaufwands pro Zeiteinheit der an einem Netzwerk beteiligten Computer.⁸⁶⁵ Kurzum: «*Decentralization carries a performance cost.*»⁸⁶⁶

Um das Trilemma aufzulösen, werden im Prinzip zwei Lösungen vorgeschlagen: Einerseits kann die Skalierbarkeit des dezentralen Netzwerks selbst verbessert werden, was typischerweise durch entsprechende Anpassungen an den Protokollen und Implementierungen geschehen kann. Diese Optimierungen führen zu einer Verbesserung des Datendurchsatzes auf dem zugrundeliegenden dezentralen Netzwerk (*on-chain*). Jedoch gehen solche Anpassungen regelmässig zulasten der Dezentralität des Netzwerks. Andererseits können sog. Layer-2-Lösungen an ein bestehendes dezentrales Netzwerk anknüpfen, wobei die auf dem Layer 2 ausgeführten Transaktionen von den kryptografischen Verfahren des dezentralen Netzwerks Gebrauch machen (*off-chain*).⁸⁶⁷

Neue Protokolle sind inzwischen entwickelt worden, welche vorgeben, selbst grössere Umsätze über den Layer 1 abwickeln zu können.⁸⁶⁸ Da Bitcoin und Ethereum als die derzeit bedeutendsten dezentralen Netzwerke regelmässig an ihre Kapazitätsgrenzen stossen, sollen die nachfolgenden Ausführungen den Lesern einen kurzen Überblick über die wichtigsten Skalierungslösungen verschaffen.⁸⁶⁹

Vorliegend nicht weiter berücksichtigt wird hingegen die Skalierungslösung der Parallelisierung von Operationen in Ethereum (sog. *Sharding*). So ist es möglich, dass dezentrale Handelsplattformen künftig auf einer separaten Par-

⁸⁶⁴ Siehe Wüst/Gervais, in: 2018 Crypto Valley Conference on Blockchain Technology, Do you need a Blockchain?, 47.

⁸⁶⁵ Siehe Buterin, Parametrizing Casper, Medium, *passim*.

⁸⁶⁶ Croman et al., in: Clark et al., Scaling Decentralized Blockchains, 116, 117.

⁸⁶⁷ Siehe sogleich unten, III.5.2.

⁸⁶⁸ Eine unverbindliche Übersicht solcher Protokolle bzw. Netzwerke findet sich bspw. in <https://coinmarketcap.com/coins/>.

⁸⁶⁹ Siehe die unterschiedlichen Abschnitte der Entwicklungs-Roadmap von Ethereum in Ethereum, ETH2 Upgrades, *passim*.

tion der Ethereum Blockchain resp. einem Shard zur Ausführung gelangen. Die Shards würden sodann miteinander über eine Main Chain (sog. *Beacon Chain*) kommunizieren, um letztlich die Datenzustände wieder zu synchronisieren.⁸⁷⁰ Die konkreten Konsequenzen von Sharding auf dezentrale Handelsplattformen sind heute noch nicht absehbar.

5.2 Layer-2-Netzwerke

a. Einleitung

Netzwerke *zweiter Ordnung* (Layer 2) knüpfen an ein dezentrales Netzwerk erster Ordnung (Layer 1) an. Transaktionen und Operationen auf dem Layer 2 werden ausserhalb des dezentralen Netzwerks erster Ordnung (d.h. *off-chain*) ausgeführt.

Layer-2-Protokolle weisen ein ähnliches Sicherheits- und Vertrauensmodell wie das von ihnen angeknüpfte dezentrale Netzwerk erster Ordnung auf. Namentlich zeigt sich dies daran, dass die Nutzer eines Layer-2-Protokolls in Eigenregie auf das Layer-1-Netzwerk zurückgreifen können, um dort ihre Off-chain-Aktivitäten on-chain zu konsolidieren.⁸⁷¹ Layer-2-Protokolle können allerdings auch ein vom Layer 1 unterschiedliches Sicherheits- und Vertrauensmodell implementieren (so etwa Sidechains).

Die mit der Einführung von Layer-2-Netzwerken verfolgten Ziele können unterschiedlicher Natur sein. Hauptsächlich ist damit aber die Verbesserung der Skalierbarkeit des Layer-1-Netzwerks beabsichtigt. Dadurch, dass die Speicherung von Daten und die Berechnungen von Transaktionen und Operationen zu einem grossen Teil off-chain erfolgen, können die Rechenlasten des Layer 1 verringert werden.⁸⁷² Auch *dezentrale Handelsplattformen* können für einige ihrer Funktionen auf Layer-2-Netzwerke zurückgreifen.

Die Verknüpfung von mehreren Netzwerken erster und zweiter Ordnung ist möglich, weil die verwendeten Protokolle interoperabel sind.⁸⁷³ Künftig sind

⁸⁷⁰ Siehe für weitergehende Informationen Ethereum Wiki, On sharding blockchains FAQs, *passim*.

⁸⁷¹ Siehe Gudgeon et al., in: Bonneau/Heninger, Layer-Two Blockchain Protocols, 204; Stark, Making Sense of Layer 2, Youtube, *passim*.

⁸⁷² Siehe Gudgeon et al., in: Bonneau/Heninger, Layer-Two Blockchain Protocols, 202.

⁸⁷³ Siehe hierzu oben, [III.2.3](#).

auch dezentrale Netzwerke dritter Ordnung, vierter Ordnung usw. denkbar. Die Interoperabilität unterschiedlicher dezentraler Netzwerke ist hingegen nicht immer gewährleistet.⁸⁷⁴

Die Anknüpfung an das Netzwerk erster Ordnung kann in der Praxis auf unterschiedliche Weise erfolgen:

b. State Channels

State Channels ermöglichen, Zustandsänderungen off-chain abzubilden und bei Bedarf den Endzustand der *State Channels* im verteilten Register (on-chain) zu konsolidieren. *Payment Channels* sind eine Sonderform von *State Channels*, wobei ein «Kontostand» in Kryptowährungen die abgebildeten Zustände darstellen.⁸⁷⁵

Um ein bedeutendes Layer-2-Netzwerk handelt es sich etwa beim *Lightning Netzwerk*. Das *Lightning* Protokoll greift auf das Konzept der *State Channels* zurück, welche es zu *Payment Channels* weiterentwickelt. Die Zahlungskanäle knüpfen unmittelbar an die Bitcoin Blockchain als Layer 1 an. Sie werden technisch mithilfe von Multisig-Transaktionen und Smart Contracts erstellt, an denen jeweils zwei Personen beteiligt sind.⁸⁷⁶ Aufgrund der unmittelbaren Anknüpfung an die Bitcoin Blockchain erbt das *Lightning Netzwerk* überwiegend das Sicherheits- und Vertrauensmodell des Bitcoin Netzwerks. Zahlungen in *Lightning* gleichen darum kryptografisch abgesicherten Versprechungen, welche die an einem Kanal beteiligten Personen bei Bedarf on-chain einlösen können.⁸⁷⁷

Lightning ermöglicht ein globales Zahlungsnetzwerk, indem tausende Nodes untereinander Kanäle unterhalten.⁸⁷⁸ Im Gegensatz zur ursprünglichen Vision eines P2P-Zahlungsnetzwerks, das für alltägliche Ausgaben verwendet werden kann,⁸⁷⁹ tendiert die Bitcoin Community heute dazu, den Layer 1 in erster Linie als einen Abwicklungsmechanismus für grössere Beträge zu betrachten, wo-

⁸⁷⁴ Verschiedene Projekte, wie namentlich *Kosmos*, arbeiten an der Verbesserung der Interoperabilität unterschiedlicher Blockchains.

⁸⁷⁵ Siehe Antonopoulos, *Mastering Bitcoin*, 300–301; Gudgeon et al., in: Bonneau/Heninger, *Layer-Two Blockchain Protocols*, 205.

⁸⁷⁶ Ausführlich zu *Lightning* Antonopoulos, *Mastering Bitcoin*, 313–321; ferner Berentsen/Schär, *Bitcoin*, 254; Andreotti, Teil 1, *iusNet BR-KR 22.12.2022*, *passim*.

⁸⁷⁷ Siehe Coleman, *State Channels*, *passim*; Antonopoulos, *Mastering Bitcoin*, 300.

⁸⁷⁸ Siehe für eine Übersicht z.B. <https://1ml.com/>.

⁸⁷⁹ Siehe Nakamoto, *Bitcoin*, 1.

hingegen kleinere Beträge über die Zahlungskanäle des Lightning Netzwerks abgewickelt werden sollen.⁸⁸⁰ Das Bitcoin-Projekt in El Salvador etwa verwendet auch Lightning als technische Infrastruktur.

c. Sidechains

Sidechains (teilweise auch *Child Chains*) knüpfen ebenfalls an ein dezentrales Netzwerk erster Ordnung an. Der angeknüpfte Layer 1 wird in diesem Fall als sog. *Parent Chain* bezeichnet.⁸⁸¹ Sidechains sind anders als State Channels Netzwerke mit einem *eigenen* Sicherheits- und Vertrauensmodell, das in der Praxis deutlich von demjenigen der Parent Chain abweichen kann.⁸⁸² Entsprechend werden sie in der Literatur nur mit Vorbehalt als Layer 2 eingestuft.⁸⁸³ Dafür können Sidechains bspw. einen höheren Grad an Anonymität und schnellere Abwicklungszeiten als ihre Parent Chains gewährleisten.⁸⁸⁴ Sidechains qualifizieren bei zu grosser Zentralisierung gewisser Elemente nicht als dezentrale Netzwerke nach vorliegender Auffassung.

Beim *Liquid Network* handelt es sich namentlich um eine sog. Federated Sidechain. Sie wird somit von einem geschlossen Kreis von Teilnehmern unterhalten.⁸⁸⁵ Das Netzwerk knüpft an Bitcoin an und macht somit die Ausgabe von Token möglich, indem BTC in einer Multisig-Transaktion auf der Bitcoin Blockchain gesperrt und im Gegenzug neue Token (L-BTC) auf der Sidechain geschaffen werden. Die neu geschaffenen Token sind sodann nach den Regeln der Sidechain übertragbar. Durch die Umkehrung des Vorgangs können die Token bei Bedarf in die in der Multisig gesperrten bitcoins zurückgetauscht werden.⁸⁸⁶ Ferner lassen sich auch weitere tokenisierte Vermögenswerte, wie etwa Stablecoins, über Liquid herausgeben.⁸⁸⁷

⁸⁸⁰ Siehe etwa Poon/Dryja, Bitcoin Lightning Network, 3–4.

⁸⁸¹ Siehe Back et al., Sidechains, 6.

⁸⁸² Siehe Gudgeon et al., in: Bonneau/Heninger, Layer-Two Blockchain Protocols, 215; Stark, Making Sense of Layer 2, Youtube, *passim*; Back et al., Sidechains, 7, 14.

⁸⁸³ So etwa Gudgeon et al., in: Bonneau/Heninger, Layer-Two Blockchain Protocols, 204.

⁸⁸⁴ Siehe Nick/Poelstra/Sanders, Liquid, Abstract; Back et al., Sidechains, 4–5, 14–15; ferner Poon/Buterin, Plasma, 4.

⁸⁸⁵ Siehe Nick/Poelstra/Sanders, Liquid, 1–2, 3.

⁸⁸⁶ Siehe Nick/Poelstra/Sanders, Liquid, 3–5; Back et al., Sidechains, 9–10, 15; ferner Bonneau et al., Proceedings 2015 IEEE Symposium on Security and Privacy, 114.

⁸⁸⁷ Siehe Mow, Tether Lands on the Liquid Network, *passim*.

Ein weiteres Beispiel für eine Sidechain ist die *Plasma Chain*. Sie beruht auf Smart Contracts und sog. Merkle Trees, knüpft an die Ethereum Blockchain an und kann dabei eine oder mehrere eigenständige Sidechains begründen. Dabei kann die Plasma Chain auf einem Netzwerk oder einer Multisig basieren oder aber durch einen einzigen Operator ausgeführt werden.⁸⁸⁸ Der Grad an Dezentralität von Sidechains variiert mitunter stark. Die Nodes des Netzwerks, soweit ein solches vorgesehen ist, unterhalten die Sidechains grundsätzlich autonom von der Parent Chain. Sie publizieren in regelmässigen Abständen eine sog. Merkle Root der off-chain verarbeiteten Transaktionen im verteilten Register des Layer-1-Netzwerks.⁸⁸⁹ Die Nutzer haben ähnlich zu State Channels die Möglichkeit, ihre Aktivitäten in der Sidechain auf der Ethereum Blockchain zu konsolidieren.⁸⁹⁰ Typischerweise haben Nutzer für den Rückzug von Vermögenswerten ein Zeitfenster zu beachten, währenddem Dritte einen missbräuchlichen Rückzug anfechten können.⁸⁹¹

d. Rollups

Schliesslich haben sich in Ethereum *Rollups* als Layer-2-Protokolle etablieren können. Rollups erledigen einen Grossteil der Datenspeicherung und der Berechnungen off-chain, publizieren jedoch in regelmässigen Zeitabständen einen Hash aller Transaktionen und Operationen im verteilten Register des Layer-1-Netzwerks. Diese Daten sind somit Gegenstand der Konsensregeln des zugrundeliegenden dezentralen Netzwerks.⁸⁹² Anders als in State Channels und Plasma bedarf es keiner eindeutigen Zuordnung zwischen den gesperrten Vermögenswerten und den jeweiligen Inhabern mehr, woraus sich ein grösserer Anwendungsbereich für Rollups ergeben kann (insb. auch dezentrale Handelsplattformen).⁸⁹³

Rollups greifen auf einen Smart Contract zurück, der wie Plasma Merkle Trees verwendet, welche off-chain abgespeichert werden. Nutzer können in den Smart Contract einzahlen (deposit) oder Rückzüge daraus tätigen (withdrawal). Transaktionen innerhalb des Rollups werden in Batches on-chain abgewickelt,

⁸⁸⁸ Siehe Buterin, *Incomplete Guide to Rollups*, *passim*.

⁸⁸⁹ Vgl. Buterin, *Incomplete Guide to Rollups*, *passim*.

⁸⁹⁰ Siehe Poon/Buterin, *Plasma*, 2–7; ferner EthHub, *Plasma*, *passim*.

⁸⁹¹ Siehe EthHub, *Plasma*, *passim*; Buterin, *Incomplete Guide to Rollups*, *passim*.

⁸⁹² Siehe Buterin, *Incomplete Guide to Rollups*, *passim*.

⁸⁹³ Siehe Buterin, *Incomplete Guide to Rollups*, *passim*.

wobei jeweils auch ein sog. State Root enthalten ist. Dieser ermöglicht jeder interessierten Person, bei Bedarf den gesamten Merkle Tree wiederherzustellen und somit allfälliges Fehlverhalten der Rollup-Teilnehmer aufzudecken.⁸⁹⁴

Es gibt unterschiedliche Antworten auf die Frage, wer in einem Rollup die Batches zur Ausführung im verteilten Register bringen kann. Zu unterscheiden sind wie bei Sidechains zentrale (ein einziger Sequencer bzw. Operator) und verteilte Modelle (jeder Teilnehmer, Auktionsmodell usw.).⁸⁹⁵ Rollups sind selbst bei Existenz gewisser zentralisierter Funktionen vollständig non-custodial. So hat ein Sequencer grundsätzlich niemals Zugriff auf die im Smart Contract verwahrten Vermögenswerte.⁸⁹⁶

Rollups können in verschiedenen Ausprägungen auftreten. Im Wesentlichen werden Optimistic Rollups und ZK-Rollups unterschieden. Die beiden Typen sehen einen unterschiedlichen Prüfungsmechanismus für die on-chain-publizierten Transaktions-Batches vor.⁸⁹⁷

- *Optimistic Rollups* verwenden Betrugsnachweise (sog. Fraud Proofs): Der Smart Contract verfolgt die gesamte Historie der State Roots und den Hash jedes Batches. Wenn ein Teilnehmer oder Nutzer feststellt, dass ein Batch eine falsche State Root hat, kann er einen Beweis on-chain veröffentlichen. Der Smart Contract verifiziert den Beweis und macht den betreffenden Batch und alle darauffolgenden Batches rückgängig.
- *ZK-Rollups* verwenden demgegenüber Gültigkeitsnachweise (sog. Validity Proofs): Jeder Batch enthält einen kryptografischen Nachweis, der als ZK-SNARK bezeichnet wird und der beweist, dass der State Root das richtige Ergebnis der Ausführung des Batches ist. Unabhängig davon, wie gross die im Nachweis enthaltenen Berechnungen sind, kann der Nachweis sehr schnell on-chain überprüft werden.

Rollups werden in der Praxis oftmals für dezentrale Handelsplattformen verwendet, weshalb auf sie zu einem späteren Zeitpunkt nochmals zurückzukommen ist.⁸⁹⁸

⁸⁹⁴ Siehe Buterin, *Incomplete Guide to Rollups*, *passim*.

⁸⁹⁵ Siehe Buterin, *Incomplete Guide to Rollups*, *passim*.

⁸⁹⁶ Siehe Gudgeon et al., in: Bonneau/Heninger, *Layer-Two Blockchain Protocols*, 212.

⁸⁹⁷ Ausführlich hierzu Buterin, *Incomplete Guide to Rollups*, *passim*; ferner auch Gudgeon et al., in: Bonneau/Heninger, *Layer-Two Blockchain Protocols*, 211-214.

⁸⁹⁸ Siehe zu *Layer-2-Handelsplattformen* unten, [IV.3.9](#).

6. Zusammenfassung Kapitel III

Kapitel III verschafft den Lesern einen Überblick über die wesentlichen technischen Grundlagen dezentraler Systeme:

Das Kapitel geht zu *Beginn* auf die konzeptionellen Unterschieden zwischen Dezentralität und Verteiltheit ein. Es wird festgehalten, dass die vorliegende Arbeit grundsätzlich den Begriff der Dezentralisierung bzw. Dezentralität vorzieht, welcher bereits das Element der Verteiltheit enthält. Namentlich wird darunter die Verteilung der Entscheidungsgewalt und der Kontrolle hinsichtlich einer Aktivität auf mehrere Personen verstanden. Wenn der Schwerpunkt hingegen auf der Zahl der beteiligten Personen liegen soll, verwendet die Arbeit auch den Begriff der Verteiltheit (z.B. verteiltes Register).

Im *zweiten* Abschnitt des Kapitels werden die wesentlichen Eigenschaften dezentraler Systeme herausgearbeitet. Dabei handelt es sich namentlich um die verteilte, gemeinschaftliche Verwaltung, offene, interoperable Protokolle und kryptografisch abgesicherte Vermögenswerte bzw. Kryptovermögenswerte. Die verteilte, gemeinschaftliche Verwaltung weist auf den Bottom-up-Charakter dezentraler Systeme hin. Diese beruhen auf Computerprotokollen, welche offen und interoperabel sind. Mit Offenheit sind Nutzungs-, Teilnahme- und Entwicklungsoffenheit gemeint. Kryptovermögenswerte werden schliesslich in native Token (Kryptowährungen, Coins) und Smart Contract-basierte Token unterteilt.

Dezentrale Systeme werden sodann im *dritten* Abschnitt in ihre Einzelteile zerlegt: An erster Stelle steht das Fundament in Form eines dezentralen Netzwerks. Die Arbeit spricht auch von der Abwicklungsebene. Letztlich ist diese entscheidend dafür, auf welchem Sicherheits- und Vertrauensmodell das gesamte dezentrale System beruht. Die Einzelteile der Abwicklungsebene werden anhand der Bitcoin und Ethereum Blockchain genauer analysiert. Anschliessend werden die beteiligten Gruppen, namentlich Teilnehmer, Nutzer und Entwickler, sowie der Konsensalgorithmus näher betrachtet: Dabei zeigt sich, dass die beteiligten Personen unterschiedliche Rollen ausüben können, wobei gewisse Netzwerkteilnehmer in ihrer Funktion als Consensus Nodes (Miner bzw. Staker) für die Produktion neuer Blöcke zuständig sind. Schliesslich geht der Abschnitt auf die wesentlichen Züge der Governance in dezentralen Netzwerken ein. Hervorgehoben wird die Bedeutung der Kryptowährung als die Grundlage des Anreizmechanismus.

Der *vierte* Abschnitt widmet sich dezentralen Applikationen. Hierzu gehören u.a. dezentrale Handelsplattformen. Dezentrale Applikationen werden vereinfacht der Applikationsebene zugeordnet. Die Applikationsebene beruht auf der Abwicklungsebene und übernimmt darum deren Sicherheits- und Vertrauensmodell. Die Applikationsebene weist in aller Regel keine Netzwerkteilnehmer, sondern lediglich Nutzer und Entwickler auf. Eine besondere Erscheinungsform beteiligter Personen sind sodann DAOs. Ihnen kann im Zusammenhang mit der Governance einer dezentralen Applikation eine zentrale Bedeutung zukommen.

Der *letzte* Abschnitt des Kapitels untersucht verschiedene Skalierungslösungen. Skalierungslösungen sollen in erster Linie die beschränkten Verarbeitungskapazitäten dezentraler Netzwerke (Layer 1) überwinden. Grob unterschieden werden können einerseits Layer-2-Netzwerke, die direkt auf dem Sicherheits- und Vertrauensmodell des Layer-1-Netzwerks beruhen (State Channels und Rollups). Andererseits bestehen auch Layer-2-Netzwerke, die lediglich mit einem Layer-1-Netzwerk kommunizieren können, aber ihren eigenen Konsensalgorithmus implementieren (Sidechains). Für dezentrale Handelsplattformen kommen im Grundsatz alle Skalierungslösungen infrage.

IV. Dezentrale Handelsplattformen

History doesn't repeat itself but it often rhymes.

– Mark Twain⁸⁹⁹

1. Vorbemerkungen zur Begriffsverwendung

1.1 Generische Begriffsverwendung

Der Begriff der dezentralen Handelsplattform wird in der vorliegenden Arbeit als generische Bezeichnung für unterschiedliche Kategorien von dezentral und verteilt strukturierten Plattformen für den Handel mit Kryptovermögenswerten verwendet.

1.2 Abweichungen zu den Publikationen des Bundesrates

Das vorliegende Begriffsverständnis weicht von der Begriffsverwendung im Bericht des Bundesrates vom 7. Dezember 2018, im Erläuternden Bericht zur Vernehmlassungsvorlage des EFD vom 22. März 2019 und in der Botschaft des Bundesrates vom 27. November 2019 jeweils zu DLT und Blockchains ab.

Auf der obersten Ebene unterscheiden die Publikationen des Bundesrates zwischen «zentralen» bzw. «zentral geführten» Handelsplattformen und «dezentralen» bzw. «dezentral geführten» Handelsplattformen.⁹⁰⁰

⁸⁹⁹ Dieses Zitat wird in vorliegender oder ähnlicher Form dem US-amerikanischen Schriftsteller Mark Twain zugeschrieben, doch scheint dafür keine eindeutige Quellenlage zu bestehen.

⁹⁰⁰ Siehe als generelle Unterscheidung Bundesrat, DLT-Bericht 2018, 18–29; sodann im Kontext des GwG Bundesrat, DLT-Bericht 2018, 146–147 und Botschaft DLT 2019, 270–271; schliesslich im Kontext des FinfraG Bundesrat, DLT-Bericht 2018, 105–106.

- Hinsichtlich Anwendbarkeit des *Geldwäscherechts* auf dezentrale Handelsplattformen scheint sodann zwischen «dezentralen» und «vollständig dezentralen», «völlig dezentralen» bzw. «komplett dezentralen» Modellen unterschieden zu werden.⁹⁰¹
- Für die Qualifizierung dezentraler Handelsplattformen gemäss *Finanzmarktinfrastrekturrecht* scheint demgegenüber zwischen «dezentralen», «verteilten» bzw. «distributed» und «Peer-to-Peer» Plattformen differenziert zu werden. Zudem wird auch die zusammengesetzte Form «verteilte[n] Peer-to-Peer-Plattformen» verwendet.⁹⁰² Es wird ausserdem festgehalten, dass «vollständig dezentrale Finanzmarktinfrastrukturen» über keinen unmittelbaren und klar identifizierbaren Betreiber verfügen.⁹⁰³

Soweit ersichtlich, fehlt eine ausführliche Darstellung der unterschiedlichen Begriffe.⁹⁰⁴ Zudem wird scheinbar nicht konsequent zwischen Dezentralität und Verteiltheit unterschieden.⁹⁰⁵

Es scheint so, dass der Bundesrat bzw. das EFD eine bestimmte technologische Ausprägung vor Augen hatte, als er den Begriff der dezentralen Handelsplattform einführte.⁹⁰⁶ Vorliegend wird demgegenüber der Begriff der dezentralen Handelsplattform, wie eingangs erwähnt, als Sammelbezeichnung in generischer Weise verwendet. Inhaltlich liegt mutmasslich v.a. eine Übereinstimmung mit gewissen Typen von Escrow-basierten P2P-Handelsplattformen, Smart Contract-basierten P2P-Handelsplattformen sowie hybriden Handelsplattformen vor (siehe zu diesen Kategorien weiter unten).

1.3 Synopse

Im Folgenden findet sich eine Synopse der vom Bund verwendeten Begriffe mit dem Begriffsverständnis in der vorliegenden Arbeit:

⁹⁰¹ Siehe Bundesrat, DLT-Bericht 2018, 144, 147, 147 FN 803, 150; ferner EFD, Erläuternder Bericht DLT-Vernehmlassungsvorlage 2019, 25.

⁹⁰² Siehe Bundesrat, DLT-Bericht 2018, 105–106.

⁹⁰³ Siehe Botschaft DLT 2019, 273; ähnlich bereits EFD, Erläuternder Bericht DLT-Vernehmlassungsvorlage 2019, 26.

⁹⁰⁴ So auch SBF, Circular 2020/01, 9; MME, Stellungnahme, 27.

⁹⁰⁵ Siehe zu den Begriffen oben, [III.1](#).

⁹⁰⁶ Siehe insb. die Ausführungen in Bundesrat, DLT-Bericht 2018, 146–147, vgl. aber die Relativierungen in 29 («typischerweise», «beispielsweise» und «in der Regel»).

Publikationen des Bundes	Diese Arbeit
Zentrale Handelsplattformen	Zentrale / Custodial Handelsplattformen
Wechsel-Plattformen / Krypto-Broker	Zentrale / Custodial OTC-Handelsplattformen
Wechsel-Plattformen / Krypto-Broker	Non-custodial P2O-Handelsplattformen
Dezentrale Handelsplattformen	<i>Je nach Ausprägung:</i> – Escrow-basierte P2P-Handelsplattformen – Smart Contract-basierte P2P-Handelsplattformen – Hybride Handelsplattformen
Vollständig, völlig bzw. komplett dezentrale Handelsplattformen bzw. Distributed bzw. verteilte Plattformen bzw. Verteilte Peer-to-Peer Plattformen	<i>Je nach Ausprägung:</i> – Escrow-basierte P2P-Handelsplattformen – Atomic Swap-basierte P2P-Handelsplattformen – Smart Contract-basierte P2P-Handelsplattformen – Smart Contract-basierte Liquiditätspools – Layer-2-Handelsplattformen – On-chain-Handelsplattformen

2. Einleitung und kurzer historischer Rückblick

2.1 Dezentrale Handelsplattformen als dezentrale Applikationen

Dezentrale Handelsplattformen bilden eine Untergruppe dezentraler Applikationen.⁹⁰⁷ Sie treten somit neben andere dezentrale Applikationen, die je nach inhaltlicher Ausrichtung einen Teil von DeFi bilden.

2.2 Abriss über den Meinungsstand in der Literatur

Nach verbreiteter Auffassung werden unter dezentralen Handelsplattformen Blockchain-basierte Anwendungen verstanden, die es Nutzern erlauben, Kryptovermögenswerte miteinander zu handeln, ohne dafür auf einen Intermediär angewiesen zu sein.⁹⁰⁸ In dieselbe Richtung gehen Definitionen, die von Netzwerken für den P2P-Austausch von Kryptovermögenswerten⁹⁰⁹ oder von einem digitalen, teilweise sogar physischen P2P-Austausch solcher Vermögenswerte sprechen.⁹¹⁰

Allen Ansichten ist grundsätzlich gemeinsam, dass Nutzer dezentraler Handelsplattformen die Kontrolle über ihre Kryptovermögenswerte behalten. Dezentrale Handelsplattformen werden darum auch als *self-custodial* oder *non-custodial* bezeichnet.⁹¹¹

Einigkeit besteht sodann hinsichtlich Abrechnung und Abwicklung von Austauschgeschäften; diese haben *on-chain* über das verteilte Register eines de-

⁹⁰⁷ Vgl. zur Applikationsebene oben, III.4.

⁹⁰⁸ Siehe etwa Lin, Stanford Journal of Blockchain Law & Policy 2019, 58; ferner Werner et al., Decentralized Finance, 3.

⁹⁰⁹ Siehe Gensler, Blockchain and Money, 5.

⁹¹⁰ Siehe Van Valkenburgh, Electronic Cash, 5–6, 12–15.

⁹¹¹ Siehe Lin, Stanford Journal of Blockchain Law & Policy 2019, 59 («Users retain sole custody of their private keys throughout the transaction process.»); Schär, Federal Reserve Bank of St. Louis Review 2021, 160; Werner et al., Decentralized Finance, 3; Miller, Decentralized Exchanges, *passim*.

zentralen Netzwerks abzulaufen.⁹¹² Mit anderen Worten verwenden dezentrale Handelsplattformen für Abrechnung und Abwicklung keine traditionellen Mechanismen, sondern den Layer 1 des betreffenden dezentralen Systems.

Schliesslich sind dezentrale Handelsplattformen uneingeschränkt zugänglich, ohne dass es für die Nutzung oder Teilnahme auf das Dazwischenschalten eines Intermediärs ankommen würde.⁹¹³

	Verwahrung	Handel	Abrechnung und Abwicklung	Zugang
Ausgestaltung	Non-custodial	Je nach Kategorie	On-chain	Offen

Darüber hinaus besteht in der Literatur indessen wenig Einigkeit darüber, was unter einer dezentralen Handelsplattform zu verstehen ist. Auf die Formulierung einer Definition ist zu einem späteren Zeitpunkt zurückzukommen.⁹¹⁴

In der Tat existieren dezentrale Handelsplattformen innerhalb eines *Spektrums*, das eine Reihe unterschiedlicher Kategorien zulässt. Die wesentlichen funktionalen Unterschiede bestehen dabei insb. im Bereich der konkreten Ausgestaltung des Handels von Kryptovermögenswerten (im Gegensatz zur Verwahrung, Abrechnung und Abwicklung von Vermögenswerten sowie zur Zugänglichkeit der Plattform).

2.3 Protokoll und/oder Anwendung

Dezentrale Handelsplattformen sind, wie vorhin erwähnt, dezentrale Applikationen. In informationstheoretischer Hinsicht kann sodann zwischen der Protokoll- und der Anwendungsebene einer dezentralen Handelsplattform unterschieden werden:⁹¹⁵

⁹¹² Siehe Lin, Stanford Journal of Blockchain Law & Policy 2019, 72–73; Schär, Federal Reserve Bank of St. Louis Review 2021, 155–156, 161, 172; Werner et al., Decentralized Finance, 3; Cambridge Centre for Alternative Finance, Regulatory Landscape Study, 120.

⁹¹³ Siehe Schär, Federal Reserve Bank of St. Louis Review 2021, 153, 169; ferner Gensler, DC Fintech Week, *passim*.

⁹¹⁴ Siehe unten, [IV.6](#).

⁹¹⁵ Siehe etwa Ehram, Why Decentralized Exchange Protocols Matter, Medium, *passim*; leicht *abw.* Lin, Stanford Journal of Blockchain Law & Policy 2019, 59–60; ferner Antonopoulos/Wood, Mastering Ethereum, 10; Schär, Federal Reserve Bank of St. Louis Review 2021, 156. Mit *Anwendung* ist vorliegend entgegen dem herkömmlichen Verständnis nicht

- Typischerweise spezifiziert die *Protokollebene* die grundlegende Funktionsweise einer dezentralen Applikation. Darunter ist in erster Linie die Art und Weise der Kommunikation zwischen den Nutzern des Protokolls zu verstehen. Protokolle legen mit anderen Worten einen Kommunikationsstandard fest. In Bezug auf dezentrale Handelsplattformen entscheiden Protokolle etwa darüber, wie Aufträge zwischen den involvierten Computern geteilt und nach erfolgreichem Matching ausgeführt werden.
- Die *Anwendungsebene* beschäftigt sich andererseits mit einer konkreten Implementierung des betreffenden Protokolls, soweit ein solches existiert. Anwendungen können somit auf einem Protokoll aufbauen. Sie spezifizieren die Funktionalitäten der betreffenden Handelsplattform.

Weil ein Protokoll typischerweise nur die grundlegenden Bedingungen festlegt, können unterschiedliche Anwendungen mit einem Protokoll interagieren, solange sie dessen Bedingungen erfüllen. Entwickler von Anwendungen nutzen zu diesem Zweck die von einem Protokoll zur Verfügung gestellten Programmierschnittstellen bzw. APIs. Protokollteilnehmer, wozu auch Smart Contracts gehören können, können etwa über eine solche API mehreren dezentralen Handelsplattform gleichzeitig Liquidität zuführen. Nutzer einer Anwendung interagieren sodann mit dem Protokoll über eine Benutzeroberfläche, wie namentlich ein web- oder softwarebasiertes Frontend mit grafischen Elementen (GUI) oder direkt über einen entsprechenden Protokoll Client.

APIs und GUIs dienen in erster Linie der vereinfachten Ansteuerung der zugrundeliegenden Protokolle und Anwendungen durch die Nutzer einer dezentralen Applikation. Sodann fungieren sie für die Entwickler anderer Protokolle zu Interoperabilitätszwecken als offene Schnittstelle.

Ein Beispiel eines Protokolls, das in der Praxis von unzähligen Anwendungen verwendet wird, ist etwa Ox. Das Protokoll hinter Ox will einen gemeinsamen Plattformstandard etablieren, über welchen dezentrale Handelsplattformen (z.B. Matcha) miteinander kommunizieren und somit Liquidität teilen können. Das Ox-Protokoll kann von etlichen dezentralen Applikationen frei verwendet werden⁹¹⁶ Es ist demgegenüber nicht zwingend erforderlich, dass eine dezen-

nur eine nutzerorientierte Anwendungssoftware gemeint, denn dezentrale Applikationen können nicht nur eine Applikations-, sondern eben auch eine Protokollebene beinhalten; vgl. demgegenüber Alpar et al., Wirtschaftsinformatik, 433.

⁹¹⁶ Siehe Warren/Bandeali, Ox, 3 («Ox is an open protocol for decentralized exchange on the Ethereum blockchain. It is intended to serve as a basic building block that may be combined with other protocols to drive increasingly sophisticated dApps [...]. Ox uses a publicly accessible system of smart contracts that can act as shared infrastructure for a variety of dApps.»).

trale Handelsplattform auf einem Protokoll der oben beschriebenen Art beruht. So verfügt etwa EtherDelta über eigene Smart Contracts, die Nutzer direkt über eine entsprechende webbasierte GUI erreichen, sowie über ein eigenes Orderbuch, dessen Liquidität indessen nicht mit anderen Anwendungen geteilt wird (sog. *Walled Garden*-Applikation).

2.4 Dezentrale Handelsplattformen als Antwort auf die Mängel zentraler Handelsplattformen

Dezentrale Handelsplattformen sind eine Antwort des Ökosystems auf die Defizite zentraler Handelsplattformen.

Die Verwendung von Kryptobörsen für den Austausch von Kryptowährungen geht zeitlich weit zurück. Bereits im Frühjahr 2010 öffnete mit *Bitcoin Market* die erste zentrale Handelsplattform, auf welcher bitcoins gegen Fiatwährungen getauscht werden konnten.⁹¹⁷ Ebenso bald wurde die Zentralisierung von Märkten als ein «Fremdkörper» in einem Ökosystem wahrgenommen, das sich grundsätzlich die Verteilung von Kontrolle und Macht auf eine Vielzahl von Personen auf die Fahnen geschrieben hat. Erste Versuche, Kryptovermögenswerte ohne einen Intermediär auszutauschen, fanden allerdings erst Anfang 2014 statt.⁹¹⁸

Zentrale Handelsplattformen waren in der kurzen Geschichte von Blockchains und Kryptowährungen denn auch unzählige Male Opfer von Hackern. Dies ist hauptsächlich dem Umstand geschuldet, dass zentrale Kryptohandelsplattformen über die Daten ihrer Kunden verfügen und, weil es sich bei diesen Daten um Vermögenswerte handelt, darum attraktive Ziele für externe und interne Cyberangriffe darstellen.⁹¹⁹ Bei Kryptobörsen handelt es sich für Angreifer umgangssprachlich um «Honeypots».⁹²⁰ Da die Private Keys durch die Betreiber einer zentralen Handelsplattform verwahrt werden, sind auch die damit kontrollierbaren Kryptovermögenswerte einem permanentem Hacking-, Betrugs-

⁹¹⁷ Siehe den Thread auf BitcoinTalk *dwdollar*, *New Exchange* (Bitcoin Market), *BitconTalk*, *passim*.

⁹¹⁸ Ausführlich zu den Anfängen von dezentralen Handelsplattformen *The Blocknet Protocol*, *Evolution of Decentralized Exchange*, Medium, *passim*.

⁹¹⁹ Sog. *Security Holes*, vgl. Szabo, *Trusted Third Parties*, *passim*.

⁹²⁰ Vgl. auch Blocher, *AnwBl* 2016, 614.

oder Insolvenzrisiko ausgesetzt.⁹²¹ In der Kryptogemeinschaft wird diese Erkenntnis mit der Wendung *Not your keys, not your coins!* auf den Punkt gebracht.

Der bekannteste Vorfall ist und bleibt bis heute MtGox, bei welchem es zum Zusammenbruch der gleichnamigen japanischen Kryptobörse im Frühjahr 2014 kam. Mutmasslich hat ein Hacker rund 850'000 bitcoins entwendet; die genauen Umstände der Attacke scheinen aber bis heute ungeklärt.⁹²² Ein weiterer Vorfall, der neben unzähligen anderen⁹²³ erwähnt werden könnte, ist der Hack der Kryptobörse *Bitfinex* im August 2016. Dieser verursachte für die Kunden der Handelsplattform aus Hongkong einen Schaden im Gegenwert von rund 120'000 bitcoins.⁹²⁴ Im November 2022 hat schliesslich die Handelsplattform *FTX* in den USA und anderen Ländern aufgrund vermuteter betrügerischer Machenschaften Insolvenz anmelden müssen.⁹²⁵

Kunden von zentralen Handelsplattformen sind ausserdem wie in traditionellen Märkten den Interessenkonflikten des Plattformbetreibers ausgesetzt und potenziell Opfer marktmissbräuchlicher Geschäftsaktivitäten, wie etwa *Frontrunning* und *Wash Trading*.⁹²⁶ Die sich daraus ergebende politische Forderung ist auf die *Entflechtung* zentraler Handelsplattformen und die Separierung der von ihnen ausgeübten unterschiedlichen Funktionen und Rollen gerichtet.⁹²⁷

⁹²¹ Vgl. in diesem Zusammenhang die Studie in Moore/Christin, in: Sadeghi, *Beware the Middleman*, 26.

⁹²² Siehe Decker/Wattenhofer, in: Kutyłowski/Vaidya, *MtGox*, 325; Nilsson, *The missing Mt-Gox bitcoins*, *passim*.

⁹²³ Siehe für regelmässig nachgeführte Übersichten derartiger Hackerangriffe CryptoSec, *Timeline of Exchange Hacks*, *passim*; ferner IDEX Blog, *Complete List of Cryptocurrency Exchange Hacks*, *passim*.

⁹²⁴ Stan Higgins, *Bitfinex Bitcoin Hack*, *Coindesk*, *passim*.

⁹²⁵ Vgl. hierzu etwa U.S. District Court Southern District of New York, *SEC vs. Samuel Bankman-Fried*, *passim*.

⁹²⁶ Vgl. OAG, *Virtual Markets Integrity Initiative*, 5, 17–19, 21–22; Kokorin, *Capital Markets Law Journal* 2023, 24; vgl. ferner etwa den Vorwurf der SEC gegenüber Binance, wonach ein nahestehendes Unternehmen *Wash Trading* auf dem US-Ableger der Plattform betrieben haben soll; hierzu U.S. District Court for the District of Columbia, *SEC vs. Binance Holdings Limited et al.*, insb. 65–68; ferner zu möglichen Regulierungsansätzen zentraler Handelsplattformen Dell'Erba, *Michigan State Law Review* 2024, *passim*.

⁹²⁷ Siehe etwa IOSCO, *Final Report Crypto and Digital Asset Markets*, 16–18 (Recommendations 2 and 3); FSB, *Final Report Crypto-Asset Activities and Markets*, 11–12.

Ferner sind zentrale Handelsplattformen regelmässig Gegenstand strafrechtlicher und regulatorischer Untersuchungen. Die Tatsache, dass hinter den Betreibern solcher Plattformen in aller Regel eindeutig identifizierbare juristische und natürliche Personen stehen, macht sie zu relativ einfachen Zielen rechtlicher und regulatorischer Untersuchungen. Dies gilt insb. für die US-amerikanischen Aufsichts- und Strafbehörden (siehe z.B. die Untersuchungen betreffend BitMEX)^{928, 929}. Ausserdem kann dies wie etwa im Fall von OKEEx zu fast vollständigen Auszahlungsstopps führen, die letztlich auch die Kunden solcher Plattformen tangieren.⁹³⁰ Die Kunden zentraler Handelsplattformen können genauso wie die Plattformbetreiber selbst in ihren Aktivitäten eingeschränkt werden. Ob dies aus betrügerischen Absichten oder wegen finanzieller Schwierigkeiten der Plattform oder auf Druck einer Aufsichtsbehörde geschieht, ist für den Kunden letztlich sekundär.⁹³¹

Damit zusammenhängend kommt es im Zusammenhang mit zentralen Handelsplattformen regelmässig auch zur Verletzung der *Privatsphäre* und der Persönlichkeitsrecht von Kunden. Die Gewährleistung der Cybersicherheit von zentralen Datenbanken, welche infolge Umsetzung rechtlicher Vorgaben abertausende Kundendossiers umfassen können, stellt eine grosse Herausforderung dar, wie unzählige Vorfälle in der Vergangenheit gezeigt haben.⁹³²

Das technische Verdikt der Computerwissenschaften ist darum eindeutig: Zentrale Handelsplattformen sind in mehrerer Hinsicht SPoFs. Sie sind zudem, wie bereits erwähnt, Fremdkörper in einem Ökosystem, das sich primär aus dezentralen Netzwerken und Applikationen zusammensetzt.⁹³³ Dezentrale Handelsplattformen stellen eine Reaktion auf diese Erkenntnisse dar. Den mit zentralen Institutionen untrennbar verbundenen Schwächen werden darum Protokolle und Anwendungen für den dezentralen Austausch von Kryptovermögenswerten gegenübergestellt.

⁹²⁸ Siehe hinsichtlich *Aufsichtsverfahren* CFTC, BitMEX, *passim*; sodann hinsichtlich *Strafverfahren* DOJ, Off-Shore Cryptocurrency Derivatives Exchange, *passim*.

⁹²⁹ Eine Übersicht betreffend Verfahren der SEC, Cyber Enforcement Actions, *passim*. Allgemein und mit weiteren Hinweisen hierzu DOJ, Report of the Attorney General's Cyber Digital Task Force 2020, 14, 37–38, 52.

⁹³⁰ Siehe Voell/Pan, OKEEx Suspends Withdrawals, CoinDesk, *passim*.

⁹³¹ Siehe Singer, FUD or regulatory change, Cointelegraph, *passim*.

⁹³² Siehe z.B. Zhao/Biggs, Binance Customer Data Leaked, CoinDesk, *passim*.

⁹³³ Siehe Decker/Wattenhofer, in: Kutyłowski/Vaidya, MtGox, 313; Schär, Federal Reserve Bank of St. Louis Review 2021, 160; Szabo, Trusted Third Parties, *passim* («The best [Trusted Third Party] of all is one that does not exist, but the necessity for which has been eliminated by the protocol design, or which has been automated and distributed amongst the parties to a protocol.»).

2.5 Evolution dezentraler Handelsplattformen

Mit Blick auf die technologischen Entwicklungen dezentraler Handelsplattformen können bis dato die folgenden *Iterationen* unterschieden werden:

- Den Anfang machten Plattformen, über welche Nutzer sich direkt miteinander in Verbindung setzen konnten, um die Bedingungen eines Austausches von Kryptovermögenswerten individuell zu verhandeln (so insb. LocalBitcoins).
- Sodann entwickelten sich Plattformen, welche bestimmte, jedoch nicht zwingend alle Handelskomponenten mithilfe von Smart Contracts und ähnlichen Mechanismen automatisierten (so etwa Bisq, AtomicDEX und EtherDelta).
- Anschliessend bildete sich die Idee der Verwendung eines Protokolls heraus, das gemeinsame Standards aufstellt, damit unterschiedliche dezentrale Handelsplattformen miteinander Liquidität teilen können (so insb. 0x).
- Praktisch parallel dazu trat mit dem Automated Market Making (AMM)-Modell erstmals eine Alternative zum bis dahin vorherrschenden Orderbuchmodell in Erscheinung (insb. Uniswap).
- Als Reaktion auf die beschränkten Datenverarbeitungskapazitäten insb. der Ethereum Blockchain etablierten sich anschliessend Plattformen, die alle Handelsschritte auf ein dezentrales Netzwerk zweiter Ordnung (Layer 2) verlagern und das dezentrale Netzwerk erster Ordnung nur noch für die Abwicklung bzw. den Nachweis der Abwicklung verwenden (z.B. Loopring).
- Seit einiger Zeit werden dezentrale Netzwerke mit neuen Konsensalgorithmen entwickelt, welche es den darauf ausgeführten Plattformen erlauben, alle Handelsschritte vollständig auf dem Layer-1-Netzwerk abzubilden (so z.B. Serum).

Diese Evolution verlief keineswegs ausschliesslich und zeitlich linear, so dass die unterschiedlichen Plattfortmtypen heute nebeneinander bestehen und die bestimmenden Elemente der unterschiedlichen Iterationen kombiniert zur Anwendung gelangen können. Sodann ist kaum zu erwarten, dass es bei den aufgeführten Iterationen bleiben wird.

3. Plattformkategorien

3.1 Einleitung

Die nachfolgenden Ausführungen unterscheiden in konzeptioneller Hinsicht *neun* unterschiedliche Plattformkategorien.

Die Kategorien werden an Beispielen illustriert. Dabei ist zu beachten, dass einige der Plattformen kaum eine praktische Bedeutung erlangt oder eine solche bereits wieder eingebüsst haben. In wissenschaftlicher Hinsicht sind sie aber gleichwohl von Interesse. Des besseren Verständnisses wegen werden auch zentrale Modelle einbezogen, die offensichtlich nicht als dezentrale Handelsplattformen qualifizieren. Es ist zu erwähnen, dass in vielen Fällen keine trennscharfe Zuteilung zu einer Kategorie möglich ist. Dies ist insb. mit Blick auf hybride Plattformen der Fall. Zudem befinden sich viele der als Beispiele angeführten Handelsplattformen in ununterbrochenem Wandel, so dass die Einteilung in eine Kategorie lediglich als eine Momentaufnahme betrachtet werden sollte.⁹³⁴

3.2 Zentrale Handelsplattformen

a. Custodial Handelsplattformen

Custodial Handelsplattformen gehören zu den zentralen Handelsplattformtypen. Bekannte Vertreter sind etwa *Binance*⁹³⁵, *Bitfinex*⁹³⁶, *Bitstamp*⁹³⁷, *Coinbase*⁹³⁸, *Huobi*⁹³⁹ und *Kraken*⁹⁴⁰. Eine nahezu vollständige Liste sortiert nach Handelsvolumen findet sich auf CoinMarketCap.⁹⁴¹ Hinter jeder dieser Handelsplattformen steht eine i.d.R. gewinnorientierte Betreibergesellschaft.⁹⁴²

⁹³⁴ Vgl. für eine Übersicht dezentraler (und hybrider) Handelsplattformen, die allerdings nur unregelmässig aktualisiert wird, <https://github.com/distributed/index>.

⁹³⁵ <https://www.binance.com/>.

⁹³⁶ <https://www.bitfinex.com/>.

⁹³⁷ <https://www.bitstamp.net/>.

⁹³⁸ <https://www.coinbase.com/>.

⁹³⁹ <https://www.huobi.com/>.

⁹⁴⁰ <https://www.kraken.com/>.

⁹⁴¹ <https://coinmarketcap.com/rankings/exchanges/>.

⁹⁴² Vgl. hierzu und zu weiteren Punkten IOSCO, Public Report DeFi 2022, 16.

Wie der Name vermuten lässt, übernehmen die Plattformen das Custody bzw. die Verwahrung der Kryptovermögenswerte ihrer Kunden. Die Vermögenswerte bzw. die dazugehörigen Private Keys werden mit anderen Worten in den Datenbanken der Betreibergesellschaften verwahrt (*custodial*). Kunden dieser Plattformen geben damit vollständig die Kontrolle über die Vermögenswerte auf. Dies geschieht, indem Kunden Kryptovermögenswerte von ihren Wallets an eine von der Handelsplattform kontrollierte Wallet-Adresse senden.⁹⁴³

Custodial Handelsplattformen unterhalten aus IT-Sicherheitsgründen typischerweise die folgenden zwei Wallet-Typen: (1) Bei Hot Wallets handelt es sich um Online-Wallets, die permanent mit dem Internet bzw. einem dezentralen Netzwerk verbunden sind, um dem Betreiber der Plattform für Ein- und Auszahlungen im Tagesgeschäft rasch zur Verfügung zu stehen. (2) Cold Wallets, die auch als Cold Storage bezeichnet werden, erlauben demgegenüber die Verwahrung von Kryptovermögenswerten in der Offline-Datenbank der Betreibergesellschaft. Falls die in Cold Wallets verwahrten Kryptovermögenswerte für Rückzüge von Kunden benötigt werden, überträgt die Plattform die Kryptovermögenswerte i.d.R. zuerst an eines ihrer Hot Wallets und von dort aus anschliessend an das persönliche Wallet der Kunden.⁹⁴⁴

Trotz dieser Vorkehrungen sind die Datenbanken von Custodial Handelsplattformen, wie bereits erwähnt, wiederholt Opfer von Hackerangriffen und anderen Vorfällen geworden.⁹⁴⁵ Dies ist wenig überraschend, sind doch Custodial Wallets aufgrund der Grösse der von ihnen kontrollierten Vermögenswerte besonders attraktive Ziele für Hacker. Derzeit befinden sich bspw. in einem einzigen der Hot Wallets von Binance bitcoins im Gegenwert von einigen Milliarden US-Dollar.⁹⁴⁶ Aufgrund der Öffentlichkeit von Blockchains ist dies für jede Person sichtbar. Ausserdem ist auch Cold Storage nicht gegen jegliche Form von Hackerangriff gefeit, können sich doch bspw. auch Mitarbeiter einer Handelsplattform unbefugten Zugriff auf die Wallets des Betreibers verschaffen.

Neben der Verwahrung sind auch die übrigen Komponenten solcher Plattformen zentralisiert. Namentlich werden das Orderbuch und die Matching-Engine auf dem Server des Plattformbetreibers ausgeführt und aktualisiert.⁹⁴⁷ Mit

⁹⁴³ Siehe Warren, Decentralized Exchange, *passim*.

⁹⁴⁴ Vgl. IOSCO, Crypto-Asset Trading Platforms, 37,

⁹⁴⁵ Siehe für eine Übersicht möglicher Risiken zentralisierter Verwahrung IOSCO, Crypto-Asset Trading Platforms, 13.

⁹⁴⁶ <https://etherscan.io/address/0xbe0eb53f46cd790cd13851d5eff43d12404d33e8>.

⁹⁴⁷ Siehe IOSCO, Crypto-Asset Trading Platforms, 41; IOSCO, Public Report DeFi 2022, 16.

anderen Worten nimmt der Betreiber einer solchen Plattform die eingehenden Aufträge in das Orderbuch auf und führt Verkäufer und Käufer zusammen. Dabei findet der Handel in aller Regel nach dem Limit-Orderbuchmodell statt.⁹⁴⁸

Das *Limit-Orderbuchmodell* ist die in der traditionellen Finanzwelt verbreitetste Mechanik, um die Handelsinteressen unterschiedlicher Marktteilnehmer zu aggregieren und dadurch die Markttiefe abzubilden. Es erlaubt nach allgemeiner Auffassung, dass sich Verkäufer und Käufer eines Finanzkontrakts auf effiziente Art und Weise finden und miteinander ein Handelsgeschäft abschliessen können.⁹⁴⁹

Zentralisiert sind schliesslich auch die Abrechnung und Abwicklung von Austauschgeschäften in Kryptovermögenswerten. Über spezifische Infrastrukturen für Clearing und Settlement verfügen die Handelsplattformen grundsätzlich nicht.⁹⁵⁰ Der Eigentümerwechsel an einem Kryptovermögenswert wird konkret lediglich innerhalb der Datenbank des Betreibers verzeichnet (d.h. off-chain). Eine Aufzeichnung der Transaktion im verteilten Register eines dezentralen Netzwerks findet demgegenüber nicht statt. So wird der Austausch von BTC gegen ETH zwischen zwei Kunden von Coinbase auf keiner der beiden Blockchains verzeichnet. Von aussen betrachtet befinden sich die Vermögenswerte nach dem Handelsgeschäft immer noch in dem von Coinbase kontrollierten Wallet. Gehandelt werden damit lediglich IOUs über den Vertragsgegenstand. Der Kunde hat je nach Ausgestaltung des Rechtsverhältnisses einen vertraglichen Erfüllungsanspruch gegenüber dem Betreiber auf Auslieferung der erworbenen Kryptovermögenswerte.

Custodial Handelsplattformen sind typischerweise an das traditionelle Bankensystem angebunden. Dies ermöglicht den Kunden solcher Plattformen, mithilfe von Banküberweisungen oder Kreditkartentransaktionen Kryptovermögenswerte mit Fiatwährungen zu erwerben.⁹⁵¹

In der Schweiz gibt es inzwischen eine Reihe von Anbietern, die entweder den Handel mit Kryptovermögenswerten als Börse⁹⁵² oder als organisiertes Handelssystem (OHS) im Rahmen einer Bank- oder Wertpapierhausbewilligung er-

⁹⁴⁸ Siehe IOSCO, *Crypto-Asset Trading Platforms*, 37.

⁹⁴⁹ Vgl. zum *Limit-Orderbuchmodell* Glosen, *The Journal of Finance* 1994, *passim*; sodann Fox/Glosen/Rauterberg, *Duke Law Journal* 2015, 198–199.

⁹⁵⁰ Vgl. Siehe IOSCO, *Crypto-Asset Trading Platforms*, 37–38, 44.

⁹⁵¹ Siehe Warren, *Decentralized Exchange*, *passim*.

⁹⁵² So etwa die SDX Trading AG.

möglichen⁹⁵³ oder die 2021 eingeführte Bewilligung als Handelssystem für Distributed Ledger Technology-Effekten (DLT-Handelssystem) nach Art. 73a ff. FinfraG beantragt haben.⁹⁵⁴

b. Custodial OTC-Handelsplattformen

Bei *Over-the-Counter* (OTC)-Handelsplattformen handelt es sich ebenfalls um eine zentrale Handelsplattform. Typischerweise bringen OTC-tätige Finanzintermediäre verkaufs- und kaufwillige Marktteilnehmer zusammen, um grössere Volumina ausserhalb einer Custodial Handelsplattform zu handeln. Die meisten Custodial Handelsplattformen besitzen darum auch einen OTC-Desk. In der Schweiz bieten etwa Bitcoin Suisse⁹⁵⁵, Bity⁹⁵⁶ und Crypto Finance⁹⁵⁷ sowie die «Kryptobanken» SEBA⁹⁵⁸ und Sygnum⁹⁵⁹ solche Dienstleistungen an.

3.3 Non-custodial P2O-Handelsplattformen

a. Hintergrund

Prominente Vertreter dieser Handelsplattformkategorie sind derzeit etwa ShapeShift⁹⁶⁰ und Changelly. Bei Shapeshift handelt es sich um ein Unternehmen mit Hauptsitz in der Schweiz, das seit 2014 im Handel von Kryptowährungen aktiv ist.⁹⁶¹ Changelly wird von einem Unternehmen aus Hongkong betrieben, das seit 2015 den Handel mit Kryptovermögenswerten anbietet.⁹⁶²

⁹⁵³ So etwa das diskretionär betriebene OHS zum multilateralen Handel von Finanzinstrumenten oder Effekten in Form von Anlage-Token der Sygnum Bank AG («SygnEx») oder das OHS der Berner Kantonalbank AG («SME|X»). Demgegenüber scheint die Swissquote Bank AG mit der «SQX»-Plattform kein OHS zu betreiben, da die handelbaren Vermögenswerte nach Ansicht der Betreiberin weder Effekten noch Finanzinstrumente darstellen.

⁹⁵⁴ So etwa die BX Digital AG und die RULEMATCH AG. Vgl. zum Bewilligungsstand Ende 2022 FINMA, Jahresbericht 2022, 18–19.

⁹⁵⁵ <https://www.bitcoinsuisse.com/prime-brokerage>.

⁹⁵⁶ <https://bity.com/products/otc-trading>.

⁹⁵⁷ <https://www.cryptofinance.ch/brokerage/>.

⁹⁵⁸ <https://www.seba.swiss/trading-and-credit-solutions>.

⁹⁵⁹ <https://www.sygnum.com/solutions/brokerage/>.

⁹⁶⁰ <https://shapeshift.com/>.

⁹⁶¹ Siehe ShapeShift, What is ShapeShift?, *passim*.

⁹⁶² Siehe Changelly, About, *passim*.

Schliesslich ist auch die standardmässige Handelsfunktion des Schweizer Unternehmens Bity⁹⁶³ zu dieser Plattformkategorie zu zählen.

b. Funktionsweise am Beispiel von Shapeshift und Changelly

Dabei handelt es sich um Handelsplattformen, die – anders als Custodial und OTC-Handelsplattformen – keine Verfügungsmacht über die Kryptovermögenswerte ihrer Kunden haben (*non-custodial*).

So hatte ein Mitarbeiter von ShapeShift im März 2016 im Rahmen eines internen Hackerangriffs lediglich Zugriff auf die in einem Hot Wallet verwahrten bitcoins des Unternehmens. Die Vermögenswerte der Kunden konnte er in dessen nicht antasten.⁹⁶⁴

Nutzer erreichen die erwähnten Handelsplattformen über die Webseite oder Smartphone-Applikation des Betreibers. Sie haben typischerweise ein Konto auf der Plattform zu erstellen. Die Plattformen stellen aus Kundensicht ein Webinterface dar, das den Erwerb oder die Veräusserung von Kryptovermögenswerten im Austausch für Fiatwährungen sowie den direkten Austausch von Kryptovermögenswerten ermöglicht. Zu diesem Zweck geben Kunden ihre Wallet-Adresse an, auf welche bzw. von welcher die Kryptovermögenswerte zu übertragen sind.⁹⁶⁵

c. Beteiligte Parteien am Beispiel von Shapeshift und Changelly

Die Kunden bzw. ihre Finanzdienstleister, wie etwa ein Kreditkartenherausgeber, kontrahieren direkt mit dem Plattformbetreiber. Die Transaktionen erfolgen mit anderen Worten *peer-to-operator* (P2O). Ein öffentliches Orderbuch besteht grundsätzlich nicht. Um sich gegen Marktrisiken abzusichern, unterhalten die Plattformbetreiber auf unterschiedlichen zentralen Kryptohandelsplattformen im eigenen Namen Konten. Die aktuellen Kurse erhalten sie über

⁹⁶³ <https://bity.com/>.

⁹⁶⁴ Siehe hierzu Voorhees, Story of Sabotage at ShapeShift, Bitcoin.com, *passim* («The only comforting thought was that the loss was only our own money. With no customer accounts, neither customer funds nor personal information were at risk from the hack. That was by design from the beginning of ShapeShift; one of our tenets.»).

⁹⁶⁵ Siehe etwa Changelly, Frequently Asked Questions, Transactions, *passim*.

die jeweilige Plattform-API.⁹⁶⁶ Für ihre Dienstleistungen belasten die Betreiber ihren Kunden in aller Regel eine Gebühr.

Unzählige Wallet-Anbieter haben Non-custodial P2O-Handelsplattformen technisch in ihre Smartphone- und Desktop-Wallets integriert, so dass Nutzer direkt in den jeweiligen Applikationen Kryptovermögenswerte über diese Plattformen erwerben und veräußern können. Zu erwähnen sind bspw. Exodus⁹⁶⁷, Trust Wallet⁹⁶⁸, Atomic Wallet⁹⁶⁹ und Ledger⁹⁷⁰.

d. Weiterentwicklungen

ShapeShift hat im Januar 2021 bekanntgegeben, dass sie die Integration von Protokollen dezentraler Handelsplattformen (so insb. von 0x und THORChain) abgeschlossen haben. In diesem Rahmen bedarf die Nutzung der Plattform keines Kontos mehr. Zeitgleich hat ShapeShift angekündigt, dass sie das bisherige Geschäft, in dessen Rahmen das Unternehmen als Gegenpartei auftritt, nicht mehr weiterzuführen gedenkt.⁹⁷¹ Die Kundenregistrierungspflicht wurde erst im Herbst 2018 eingeführt, vermutlich auf Druck der Aufsichtsbehörde FinCEN.⁹⁷²

Im Juli 2021 folgte sodann der nächste Entwicklungsschritt, der wiederum aus primär regulatorischen Überlegungen erfolgt sein dürfte: Der CEO von ShapeShift, Erik Voorhees, beabsichtigte, die verschiedenen Unternehmen hinter der Plattform zu liquidieren und die Stakeholder, worunter neben den Eigentümern insb. die Mitarbeiter und Nutzer gehören, mit Governance Token der künftigen ShapeShift DAO auszustatten.⁹⁷³ Damit folgt ShapeShift dem Modell des Melon Protokolls (nun Enzyme), dessen Entwicklergesellschaft, die

⁹⁶⁶ Ausführlich Changelly, Best Exchange Rates, *passim* («When you select the coins you want to get, the system sends a rate request to the exchanges. After the exchanges receive the request, Changelly gets the answer showing up in the field. All this process is going in milliseconds. [...] Changelly is a link between you and the trading platforms.»).

⁹⁶⁷ <https://www.exodus.com/>.

⁹⁶⁸ <https://trustwallet.com/>.

⁹⁶⁹ <https://atomicwallet.io/>.

⁹⁷⁰ <https://www.ledger.com/>.

⁹⁷¹ Siehe Voorhees, No More KYC, Medium, *passim*.

⁹⁷² Siehe Voorhees, Introducing ShapeShift Membership, Web Archive, *passim*.

⁹⁷³ Siehe Voorhees, ShapeShift Decentralizes, Medium, *passim* («Fundamentally, ShapeShift is moving from a centralized, closed-source application with bank accounts, governed and owned by shareholders, to a decentralized, open-source application without bank accounts, governed and owned by holders of the FOX Token.»).

Melonport AG mit Sitz in Zug, bereits im Februar 2019 aufgelöst wurde,⁹⁷⁴ und seither für die Governance des Protokolls auf ein mehrköpfiges Council setzt.⁹⁷⁵

Am 5. März 2024 akzeptierte die SEC einen Vergleichsvorschlag der ShapeShift AG. Nach Auffassung der SEC ist die Betreiberin in der Zeit bis zur Auflösung der Plattform einer registrierungspflichtigen Wertpapierhändlerstätigkeit (*Dealer*) nachgegangen.⁹⁷⁶ Unklar ist, ob und welche der Kryptovermögenswerte als Securities i.S.d. Securities Exchange Act qualifizierten.⁹⁷⁷

3.4 Escrow-basierte P2P-Handelsplattformen

a. Hintergrund

Bekannte Handelsplattformen dieser Kategorie sind etwa *Bisq*⁹⁷⁸, *LocalBitcoins*⁹⁷⁹ und *Hodl Hodl*⁹⁸⁰.

LocalBitcoins wurde 2012 als P2P-Handelsplattform gegründet und wird von einem finnischen Unternehmen betrieben.⁹⁸¹ Seit November 2019 ist das Unternehmen bei der Finanzmarktaufsichtsbehörde des Landes als Virtual Currency Provider registriert.⁹⁸² *Hodl Hodl* wird sodann von einem Unternehmen mit Sitz auf den Marshallinseln betrieben.⁹⁸³ Demgegenüber steht hinter *Bisq* kein Unternehmen, sondern lediglich eine erstmals im April 2016 veröffentlichte Open-Source-Software sowie eine DAO mit eigenem Token.⁹⁸⁴

⁹⁷⁴ Siehe Butcher, Melonport dissolves, TechCrunch, *passim*.

⁹⁷⁵ Siehe Enzyme, Enzyme Protocol v2, Governance Overview, *passim*.

⁹⁷⁶ Siehe SEC, Order ShapeShift AG, 2.

⁹⁷⁷ Vgl. Peirce/Uyeda, Statement on ShapeShift AG, *passim*.

⁹⁷⁸ <https://bisq.network/>.

⁹⁷⁹ <https://localbitcoins.com/>.

⁹⁸⁰ <https://hodlhodl.com/>.

⁹⁸¹ Siehe LocalBitcoins, About, *passim*.

⁹⁸² Siehe LocalBitcoins, Virtual Currency Provider, *passim*.

⁹⁸³ Siehe Hodl Hodl, Terms and Conditions, Definitions, *passim*.

⁹⁸⁴ Siehe Surya, Bisq Network, *passim*; Bisq, The Bisq DAO, *passim*.

b. Funktionsweise am Beispiel von Bisq

Die wesentliche Gemeinsamkeit der oben erwähnten Handelsplattformen besteht in der Verwendung eines *Escrow- und Streitbeilegungsmechanismus*. Dabei werden die Kryptovermögenswerte des Veräusserers so lange in einem Escrow gehalten, bis der Erwerber der Vermögenswerte seine Gegenleistung erfüllt hat. Da es sich bei der Gegenleistung in aller Regel um die Überweisung von Fiatwährung handelt, ist der Escrow-Mechanismus die einzige Möglichkeit, einen einigermassen verlässlichen Austauschprozess über das Internet sicherzustellen.

Die Problematik besteht hauptsächlich darin, dass gewisse Zahlungsmethoden im traditionellen Finanzsektor, namentlich Kreditkarten und PayPal, mit einer geringen, aber praktisch nicht unbedeutenden Wahrscheinlichkeit reversibel und damit nicht final sind. Beim Tausch von Fiatwährung in Form von Bargeld gegen Kryptovermögenswerten stellt sich diese Problematik freilich nicht. Typischerweise machen Nutzer Angebote für Bitcoin, wobei unterschiedliche Zahlungsmethoden in Fiatwährung vereinbart werden können (z.B. eine SEPA-Überweisung).

Bei Einwänden einer Partei kommt ein Streitschlichtungsverfahren zur Anwendung, das in letzter Instanz unter Beizug einer Drittperson durchgeführt wird. Escrow-basierte P2P-Handelsplattformen skalieren im Ergebnis schlechter als dezentrale Handelsplattformen, die den Austausch von Fiatwährung gegen Kryptovermögenswerte nicht anbieten.

Bisq ist eine Escrow-basierte Handelsplattform, die im Wesentlichen nach den oben erwähnten Prinzipien funktioniert. In Bisq werden für das Escrow der Vermögenswerte konkret der sog. *Multisig*-Mechanismus des Bitcoin Protokolls verwendet.⁹⁸⁵ Multisig sind Adressen, die mehr als eine Signatur benötigen, um eine Transaktion auszuführen (*m-of-n-Signaturen*). Die Signaturen werden dabei in aller Regel von unterschiedlichen Personen geleistet und erfordern entsprechende Koordination zwischen den jeweiligen Inhabern der Private Keys.⁹⁸⁶ Nach Erbringung der Gegenleistung, welche in aller Regel in der Überweisung einer Fiatwährung auf das Bankkonto des Veräusserers der bitcoins besteht, können die Parteien gemeinsam die sich im Escrow befindlichen Vermögenswerte auslösen (2-of-2-Multisig). Mit anderen Worten verfügt die Multisig-Adresse über die zu tauschenden Kryptovermögenswerte nur so

⁹⁸⁵ Siehe Bisq, Frequently asked questions, Is Bisq safe?, *passim*.

⁹⁸⁶ Siehe Bitcoin Wiki, Multi-signature, *passim*.

lange, bis beide Parteien einvernehmlich die Transferierung der Kryptovermögenswerte an die Wallet-Adresse des Erwerbers bestimmen. Aus diesem Grund ist Bisq aus Nutzersicht vollständig non-custodial.⁹⁸⁷

Im Falle von Hodl Hodl handelt es sich demgegenüber um eine 2-of-3-Multisig, bei welcher der Plattformbetreiber selbst über einen Private Key verfügt.⁹⁸⁸ Er alleine besitzt allerdings keine Verfügungsmacht über die im Escrow gehaltenen Vermögenswerte. Anders verhält sich die Situation beim «traditionellen» Escrow von LocalBitcoins. LocalBitcoins hat im Prinzip jederzeit vollen Zugriff auf die Vermögenswerte, da kein Multisig eingesetzt wird.⁹⁸⁹

Darüber hinaus haben beide Parteien vor Ausführung des Geschäfts über Bisq in der erwähnten Multisig ein Sicherheitsdepot zu hinterlegen, das ihnen nach erfolgreicher Abwicklung des Geschäfts zurückerstattet wird. Diese Sicherheiten können im Fall einer Streitschlichtung als Sanktion der anderen Partei zugesprochen werden.⁹⁹⁰

Das Streitbeilegungsverfahren in Bisq sieht drei Stufen vor: (1) In einer ersten Phase haben die Parteien die Möglichkeit, ihren Konflikt autonom beizulegen (*Trader Chat*). (2) Sodann kann eine Partei einen Mediator wünschen, der einen Konfliktlösungsvorschlag zuhanden der Parteien macht (*Mediation*). Mediatoren sind Teilnehmer der Bisq DAO und haben im Vorfeld ein Sicherheitsdepot zu leisten, das bei Verstoß gegen die Schlichtungsregeln eingezogen werden kann. (3) Schliesslich kann eine mit dem Vorschlag des Mediators unzufriedene Partei eine im Smart Contract vorprogrammierte Transaktion auslösen, die alle im Escrow gehaltenen Vermögenswerte an eine Spenden-Wallet der DAO übertragen. Ferner hat diese Partei einen Schiedsrichter anrufen, der nach Anhörung der Parteien die Möglichkeit hat, eine der beiden Parteien aus dem DAO-Fonds zu entschädigen, bzw. künftig einen Entschädigungsvorschlag zuhanden der DAO-Teilnehmer machen kann (*Arbitration*).⁹⁹¹

Typischerweise weisen Escrow-basierte P2P-Handelsplattformen auch ein *Reputationssystem* auf, das es Nutzern erlaubt, die Integrität eines Handelspart-

⁹⁸⁷ Siehe Bisq, Frequently asked questions, How is collusion between mediators, arbitrators, and traders prevented?, *passim*.

⁹⁸⁸ Siehe Hodl Hodl, Help Topics, How does Hodl Hodl ensure security, Multisig escrow, undatiert, *passim*.

⁹⁸⁹ Siehe LocalBitcoins, Escrow, *passim*.

⁹⁹⁰ Siehe Bisq, Frequently asked questions, Why does Bisq require a security deposit in BTC?, *passim*.

⁹⁹¹ Ausführlich Bisq, Dispute Resolution, *passim*.

ners vor Ausführung des Geschäfts zu beurteilen.⁹⁹² Auf LocalBitcoins ist das Reputationssystem demgegenüber sekundär, da alle Nutzer über ein registriertes Konto verfügen müssen.⁹⁹³

c. Beteiligte Parteien am Beispiel von Bisq

Um Kryptovermögenswerte zu handeln, stellen Bisq-Nutzer entweder eigene Angebote in ein öffentliches Orderbuch ein oder sie akzeptieren die von anderen Nutzern erfassten Angebote. Der Matching-Prozess ist somit manuell. Der Pool an verfügbaren Angeboten wird von jedem Nutzer lokal abgespeichert. Jeder Nutzer verfügt insofern über eine lokale Kopie des Orderbuchs. Nach einer ähnlichen Logik funktioniert etwa Swap Online, deren Plattform aber direkt im Browser ausgeführt wird.⁹⁹⁴ Der Handel erfolgt sodann unmittelbar zwischen den einzelnen Nutzern (P2P). Ein allfälliger Plattformbetreiber ist nicht Gegenpartei des Geschäfts.⁹⁹⁵ Dies ist der wesentliche Unterschied zu den oben dargelegten Non-custodial P2O-Handelsplattformen.

Demgegenüber ist LocalBitcoins *direkt* in den Escrow-Prozess involviert. Es handelt sich also um einen *Custodial* Anbieter. Zwar kann der Verkäufer nach Erhalt von Fiatwährung die Auslösung der bitcoins aus dem Escrow verlangen,⁹⁹⁶ doch findet der eigentliche technische Auslösungsprozess innerhalb der Datenbank der Betreibergesellschaft statt. LocalBitcoins ist somit im Gegensatz zu Bisq und Hodl Hodl zentralisiert.

d. Weiterentwicklungen

Im Falle von Bisq besteht – anders als bei LocalBitcoins und Hodl Hodl – ein P2P-Kommunikationsnetzwerk, deren Open-Source-Software Nutzer zu verwenden haben, um auf die Plattform zugreifen zu können. Mit anderen Worten interagieren Nutzer von Bisq nicht über das webbasierte Interface bzw. den Server einer Drittperson. Konkret müssen die Nutzer eine Applikation auf ih-

⁹⁹² Siehe etwa Hodl Hodl, Help Topics, How does Hodl Hodl ensure security, Reputation system, *passim*; LocalBitcoins, Frequently Asked Questions, How does the feedback system work?, *passim*.

⁹⁹³ Siehe LocalBitcoins, Guide to Account Verification, *passim*.

⁹⁹⁴ Siehe Sopov, A libp2p-based Atomic Swaps Exchange Protocol, Medium, *passim*.

⁹⁹⁵ Siehe LocalBitcoins, Frequently Asked Questions, How am I protected from being scammed?, *passim*; ferner Hodl Hodl, FAQ, Are you holding my funds?, *passim*.

⁹⁹⁶ Siehe LocalBitcoins, Frequently Asked Questions, How am I protected from being scammed?, *passim*.

rem Computer installieren, welche sich sodann mit anderen Netzwerkteilnehmern unter Anwendung des Tor-Protokolls verbindet. Erst nach Herstellung dieser Verbindung können Nutzer Kryptovermögenswerte austauschen.⁹⁹⁷

Da es sich bei Bisq um Open-Source-Software handelt, kann der Code im Rahmen der anwendbaren Lizenz (d.h. GNU Affero General Public License 3.0⁹⁹⁸) weiterverwendet werden. Bei *Haveno* handelt es um eine solche Code Fork mit dem Ziel, die Funktionalitäten von Bisq verstärkt für den Privacy Coin Monero nutzbar zu machen.⁹⁹⁹

3.5 Atomic Swap-basierte P2P-Handelsplattformen

a. Hintergrund

Als Methode für den Austausch von Kryptovermögenswerten unterschiedlicher Blockchains (z.B. BTC für LTC) haben sich *Atomic Swaps* bzw. *Cross-chain Atomic Swaps* etabliert.¹⁰⁰⁰ Der Vorteil von Atomic Swaps gegenüber dem direkten Austausch von Kryptovermögenswerten unterschiedlicher dezentraler Netzwerke zwischen zwei Parteien liegt darin, dass die Partei, welche vorab leistet, nicht einfach darauf vertrauen muss, dass die Gegenpartei ebenfalls erfüllen wird. Andererseits ist auch kein Intermediär in den Atomic Swap involviert, welchem die Parteien zu vertrauen hätten.¹⁰⁰¹ Ferner können Parteien durch die Verwendung von Cross-chain Atomic Swaps auf zentrale Kryptohandelsplattformen verzichten.¹⁰⁰² Das ansonsten notwendig interpersonale Vertrauen wird mit anderen Worten mit dem Einsatz von Atomic Swaps durch Technologievertrauen substituiert.

Eine noch unvollständige Version von Atomic Swaps wurden erstmals in einem Beitrag auf dem Onlineforum [Bitcointalk.org](https://bitcointalk.org) von 2012 von SERGIO DEMIAN LERNER vorgeschlagen. Der Autor nannte den Mechanismus P2PTradeX.¹⁰⁰³

⁹⁹⁷ Siehe Bisq, Frequently asked questions, How is Bisq different from other decentralized exchanges?, *passim*.

⁹⁹⁸ Siehe Bisq, License, GitHub, *passim*.

⁹⁹⁹ Siehe Haveno, Why a new Platform?, GitHub, *passim*.

¹⁰⁰⁰ Siehe für mehr Informationen zu Atomic Swaps Narayanan et al., Bitcoin, 257–260.

¹⁰⁰¹ Siehe Miraz/Donald, Annals of Emerging Technologies in Computing 2019, 43.

¹⁰⁰² Siehe Xu/Ackerer/Dubovitskaya, Game-Theoretic Analysis, 1.

¹⁰⁰³ Siehe Lerner, P2P Trading between cryptocurrencies, BitcoinTalk, *passim*.

TIER NOLAN konzipierte sodann im gleichen Forum ein Jahr später die technischen Komponenten eines vollständigen Atomic Swaps.¹⁰⁰⁴

Dezentrale Handelsplattformen, die Atomic Swaps implementiert haben, sind bspw. AtomicDEX¹⁰⁰⁵ und DCRDEX¹⁰⁰⁶. Die erste Version des AtomicDEX-Protokolls wurde im August 2017 veröffentlicht.¹⁰⁰⁷ Eine Vorgängerversion dieses Protokolls war u.a. BarterDEX.¹⁰⁰⁸ Eine mit AtomicDEX vergleichbare Implementierung einer dezentralen Handelsplattform erlaubt ferner das Blocknet-Protokoll hinter der Plattform Block DX^{1009, 1010}. Der erste Atomic Swap zwischen den beiden Blockchains Decred und Litecoin fand sodann im September 2017 noch über eine Vorgängerversion von DCRDEX statt.¹⁰¹¹

Konzeptionell sind Atomic Swaps von Atomic Trades bzw. Atomic Transactions abzugrenzen. Letztere Konzepte besagen lediglich, dass eine Transaktion bzw. die beiden Seiten eines Austauschgeschäfts entweder vollständig oder gar nicht ausgeführt und abgewickelt werden.¹⁰¹² Die vorliegende Arbeit spricht im Falle von Austauschgeschäften auch von Atomic Settlement. Es handelt sich bei Atomic Swaps nach dem Gesagten um eine Teilmenge von Atomic Trades, welche sich ihrerseits aus zwei oder mehreren Atomic Transactions zusammensetzen.¹⁰¹³

b. Funktionsweise am Beispiel von AtomicDEX

AtomicDEX ist ein Protokoll, welches den Austausch von Kryptovermögenswerten mithilfe von Smart Contracts ermöglicht. Die Verwendung von Smart Contracts weist gewisse Parallelen mit den oben dargestellten Escrow-basierten P2P-Handelsplattformen auf. Diese greifen für den Erwerb von bitcoins auf den Multisig-Mechanismus des Bitcoin Protokolls zurück. Diese bitcoins werden in aller Regel mit Fiatwährung erworben.

¹⁰⁰⁴ Siehe Nolan, Alt chains and atomic transfers, BitcoinTalk, *passim*.

¹⁰⁰⁵ <https://komodoplatform.com/en/wallets.html>.

¹⁰⁰⁶ <https://dex.decred.org/>.

¹⁰⁰⁷ Siehe Komodo, Introduction to AtomicDEX, *passim*.

¹⁰⁰⁸ Siehe die Ausführungen in Komodo, Barterdex, *passim*.

¹⁰⁰⁹ <https://blockdx.com/>.

¹⁰¹⁰ Siehe Blocknet, Blocknet Protocol, GitHub, *passim*.

¹⁰¹¹ Siehe Yocom-Piatt, On-Chain Atomic Swaps, *passim*.

¹⁰¹² Siehe Antonopoulos, Mastering Bitcoin, 293; Antonopoulos/Wood, Mastering Ethereum, 129; ferner Miraz/Donald, Annals of Emerging Technologies in Computing 2019, 44 m.w.H.

¹⁰¹³ So auch Herlihy, Proceedings of the 2018 ACM Symposium on Principles of Distributed Computing 2018, 246 in fine.

Im Vergleich zu Escrow-basierten P2P-Handelsplattformen liegt der Schwerpunkt von Atomic Swap-basierten P2P-Handelsplattformen auf dem Austausch von Kryptovermögenswerten *unterschiedlicher* Blockchains. Hierfür werden die auf den unterschiedlichen dezentralen Netzwerken eingesetzten Smart Contracts technisch miteinander verknüpft.¹⁰¹⁴ Konkret: Auf UTXO-basierten Blockchains, wie etwa Bitcoin und Litecoin, verwendet das Protokoll Hash Time Locked Contracts (HTLC); auf kontobasierten Blockchains, namentlich Ethereum, kommt das entsprechende Smart Contract-Äquivalent zur Anwendung. Dies erlaubt den atomistischen Austausch von Kryptovermögenswerten unterschiedlicher Blockchains.¹⁰¹⁵ Dabei behalten die an einem Atomic Swap beteiligten Parteien bis zum effektiven Austausch jederzeit die volle Kontrolle über ihre eingebrachten Vermögenswerte.¹⁰¹⁶

c. Beteiligte Parteien am Beispiel von AtomicDEX

Die erfolgreiche Ausführung des Swap-Vorgangs über AtomicDEX erfordert insgesamt fünf On-chain-Transaktionen zwischen Maker und Taker.¹⁰¹⁷ Als *Maker* wird für den Rest dieser Arbeit diejenige Person bezeichnet, die ein Angebot macht, und als *Taker* gilt diejenige Person, welche das Angebot akzeptiert. Aufgrund der damit verbundenen Transaktionsgebühren kommen für derartige Atomic Swaps v.a. grössere Handelsgeschäfte infrage, bei denen zudem die Latenzzeit nicht im Vordergrund steht.¹⁰¹⁸ Im Ergebnis können Nutzer von Applikationen¹⁰¹⁹, die auf dem Protokoll basieren, unmittelbar miteinander Kryptovermögenswerte unterschiedlicher Blockchains tauschen, ohne dass ein Escrow-Intermediär die Vermögenswerte vorübergehend zu halten hat.¹⁰²⁰

Die Führung des öffentlichen Orderbuchs sowie die Zusammenführung der Parteien eines Austauschgeschäfts (Order Matching) erfolgen – ähnlich zu 0x (siehe hierzu unten) – durch ein separates P2P-Netzwerk. Dieses Relay-Netzwerk ist direkt mit den vom Protokoll unterstützten dezentralen Netzwerken

¹⁰¹⁴ Vgl. zur technischen Seite dieser Verknüpfung Narayanan et al., Bitcoin, 259.

¹⁰¹⁵ Eine grafische Übersicht des Ablaufs eines solchen Vorgangs findet sich in Decred, *decred/atomicswap*, GitHub, *passim*.

¹⁰¹⁶ Siehe etwa The Blocknet Protocol, Understanding a Decentralized Exchange, *passim*.

¹⁰¹⁷ Siehe Komodo, Atomic Swaps, *passim*.

¹⁰¹⁸ So auch Warren, Decentralized Exchange, *passim*.

¹⁰¹⁹ So z.B. über die Desktop- und Mobile-Applikation AtomicDEX (<https://atomicdex.io/>).

¹⁰²⁰ Siehe Komodo, Atomic Swaps, *passim* («An atomic swap is a technology that allows two users to trade cryptocurrencies across two separate blockchains without requiring an intermediary third party.»); ferner Miraz/Donald, Annals of Emerging Technologies in Computing 2019, 43–44.

verbunden und stellt dadurch die Einhaltung der Ausführungslogik von Atomic Swaps auf den jeweiligen Blockchains sicher.¹⁰²¹ Erst durch den Einsatz eines solchen verteilten P2P-Netzwerks werden die Funktionalitäten einer echten Handelsplattform, wie insb. Orderbuch und Order Matching, realisiert.¹⁰²²

d. Weiterentwicklungen

Als Weiterentwicklung von AtomicDEX kann das Protokoll hinter DCRDEX betrachtet werden. DCRDEX bezweckt in erster Linie den atomistischen Austausch von BTC oder LTC gegen DCR (Decred). Decred ist eine Kryptowährung mit eigenständiger Blockchain, deren Protokoll viele Anleihen bei Bitcoin macht, diese darüber hinaus allerdings mit einem neuartigen Konsensprotokoll verbindet.¹⁰²³ DCRDEX sieht ähnlich wie Bisq oder Block DX eine eigenständige Software vor, welche Nutzer zuerst herunterladen haben, bevor sie die Handelsplattform nutzen können. Während die Führung des Orderbuchs sowie das Matching über ein separates Client-Server-Netzwerk erfolgen, laufen alle übrigen Handelsschritte on-chain mithilfe von HTLCs ab. Ein Handelsgeschäft auf DCRDEX erfordert vier Transaktionen. Der eigentliche Handel ist vollständig gebührenfrei. Davon ausgenommen sind freilich die Transaktionsgebühren der in den Swap involvierten Blockchains. Vorab ist zudem eine einmalige Registrierungsgebühr zu bezahlen, die bei Protokollverstößen verfallen kann.¹⁰²⁴

AtomicDEX kündigte im Oktober 2020 an, dass regulatorische Veränderungen die Einführung von KYC für die offizielle Version der Plattform notwendig machen. Angeführt wird das Risiko, dass die Entwickler der Plattform und/oder die am Netzwerk teilnehmenden Liquiditätsgeber als Verantwortliche unter Gesichtspunkten der Geldwäschereiregulierung betrachtet werden könn-

¹⁰²¹ Siehe Komodo, Order Matching with Full-Relay and Non-Relay Nodes, *passim*; ferner Komodo, Dealing with Confirmations, *passim* («Since AtomicDEX is trading permanently on blockchains – as opposed to updating an internal database of vouchers – both sides of the trading pair need to wait and watch as miners on the respective blockchains calculate transaction confirmations.»).

¹⁰²² Gl.M. Miraz/Donald, Annals of Emerging Technologies in Computing 2019, 48.

¹⁰²³ Siehe Decred, What is Decred?, *passim*.

¹⁰²⁴ Siehe Decred, DCRDEX, GitHub, *passim*; ausführlich hierzu Yocom-Piatt, A New Kind of DEX, *passim*.

ten.¹⁰²⁵ Dies hindert selbstredend niemand daran, den Softwarecode zu forken und eine Alternative zu AtomicDEX aufzubauen.

3.6 Smart Contract-basierte P2P-Handelsplattform

a. Hintergrund

Smart Contract-basierte P2P-Handelsplattformen existieren seit dem Aufkommen von EtherEx¹⁰²⁶, OasisDEX¹⁰²⁷ und EtherDelta. Entwickelt wurden die Plattformen bereits in den Jahren 2015 und 2016. Ein ausgeprägtes Wachstum erlebten sie insb. im Rahmen des ICO-Booms zwischen Sommer 2017 und Frühjahr 2018.¹⁰²⁸

Erwähnenswert ist v.a. die Geschichte von EtherDelta. Die Plattform von ZACHARY COBURN ging im Juli 2016 live. Zeitweise war sie die meistbenutzte Applikation auf der Ethereum Blockchain.¹⁰²⁹ Gegen den Gründer reichte die US-amerikanische Börsenaufsicht SEC allerdings im November 2018 eine Klage wegen angeblichen Verstosses gegen die Registrierungspflicht von Wertpapierbörsen. Das Verfahren wurde letztlich durch einen Vergleich beigelegt.¹⁰³⁰ Die Argumentation der SEC ging – unter Berücksichtigung der von ihr im DAO-Bericht gemachten Erwägungen – dahin, dass eine gewisse Zahl der auf EtherDelta gehandelten Token Securities bzw. Investment Contracts im Sinne des US-amerikanischen Börsenrecht darstellten, was die Plattform zu einer Wertpapierbörse machte, weshalb sie sich bei der SEC hätte registrieren müssen.¹⁰³¹ Nutzer können die von EtherDelta verwendeten Smart Contracts

¹⁰²⁵ Siehe Komodo Team, The Regulation is Coming, *passim* («AtomicDEX is and remains a non-custodial decentralized exchange solution; however, its protocol process could be viewed as acting as a facilitator service enabling users to find and trade with others in an unregulated fashion. Although there is no central server connecting the actual trading partners, services, and nodes that handle trades require compliance. The exchange system, platform, or whichever party supports these activities is legally liable.»); ferner Komodo Team, Community Update on AtomicDEX & KYC/AML, *passim* («[...], parties that wish to participate in trading activities on the officially supported AtomicDEX liquidity network will need to complete a KYC process.»).

¹⁰²⁶ <https://github.com/etherex/etherex>.

¹⁰²⁷ <https://oasisdex.com/>; <https://oasis.app/trade/>.

¹⁰²⁸ Siehe Kiepuszewski, OasisDEX, Youtube, *passim*.

¹⁰²⁹ Siehe Coburn, EtherDelta, Youtube, *passim*.

¹⁰³⁰ Siehe SEC, SEC Charges EtherDelta Founder With Operating an Unregistered Exchange, *passim*.

¹⁰³¹ Siehe SEC, Order Coburn, 8–9.

aufgrund der Eigenschaft der Unveränderlichkeit dezentraler Netzwerke und Applikationen grundsätzlich immer noch verwenden.¹⁰³² Inzwischen existiert aber EtherDelta 2, welche die von COBURN begründete Plattform fortsetzt.¹⁰³³ Andere dezentrale Handelsplattformen haben zudem den Code von EtherDelta kopiert (so z.B. ForkDelta¹⁰³⁴).

Jüngere Vertreter dieser Handelsplattformkategorie mit teilweise wesentlichen Unterschieden zu EtherDelta und OasisDEX ist bspw. das Protokoll 0x¹⁰³⁵.

b. Funktionsweise am Beispiel von EtherDelta und OasisDEX

Smart Contract-basierte P2P-Handelsplattformen verwenden für wesentliche Funktionen des Handels mit Kryptovermögenswerten Smart Contracts (typischerweise auf der *Ethereum* Blockchain). Namentlich werden Smart Contracts etwa für die vorübergehende Verwahrung von Kryptovermögenswerten zwecks deren Bereitstellung für das Austauschgeschäft, die Führung des Orderbuchs und das Order Matching zwischen Verkäufern und Käufern verwendet. Die Abwicklung erfolgt sodann direkt auf dem dezentralen Netzwerk (on-chain).

Im Gegensatz zu zentralen Handelsplattformen, wie etwa Binance oder Coinbase, werden die Kryptovermögenswerte auf EtherDelta in einem Smart Contract deponiert. Dies ist auch darum erforderlich, weil der Smart Contract die Vermögenswerte für das Austauschgeschäft bereithalten muss. Lediglich die Person, welche einen Vermögenswert mithilfe ihres Private Keys im Smart Contract deponiert hat (*deposit*), kann ihn wieder auslösen (*withdraw*) oder einen Auftrag stornieren (*cancel*), es sei denn, ein anderer Nutzer hat das Angebot zum Austausch des Vermögenswerts bereits akzeptiert. Darüber hinaus kann der Nutzer bestimmen, für wie lange sein Auftrag im Orderbuch gültig sein soll, bevor der Vermögenswert automatisch an sein Wallet zurückübertragen wird. Jede Interaktion mit den Smart Contracts entspricht einer On-Chain-Transaktion. Eine Ausnahme bildet die Funktion *getBalance*, welche

¹⁰³² <https://etherscan.io/address/0x4aea7cf559f67cedcad07e12ae6bc00f07e8cf65>.

¹⁰³³ <https://etherdelta.com/>.

¹⁰³⁴ <https://forkdelta.app/>; siehe zum Hintergrund zu dieser Fork des EtherDelta Codes free-atnet, ForkDelta, Reddit, *passim*.

¹⁰³⁵ <https://0x.org/>.

es dem Nutzer erlaubt, den «Kontostand» seiner Vermögenswerte vom Smart Contract abzufragen. Sowohl ETH als auch ERC-20 Tokens können auf EtherDelta gehandelt werden.¹⁰³⁶

Die Handelsmechanik von EtherDelta richtet sich wie bei traditionellen Handelsplattformen nach dem Orderbuchmodell. Das Matching von Verkäufer und Käufer erfolgt in einem ersten Schritt jedoch manuell, indem der Taker denjenigen Maker-Auftrag im Orderbuch auswählt, den er annehmen möchte. Selbst wenn also überschneidende Angebot bestehen, findet kein automatisches Matching statt.¹⁰³⁷ Alle weiteren Schritte der Ausführung sowie die Abwicklung des Handelsgeschäfts erfolgen sodann automatisiert durch den Smart Contract und somit on-chain. Obschon Nutzer von EtherDelta ihre Kryptovermögenswerte im Vorfeld eines Austauschgeschäfts in einem Smart Contract deponieren müssen, weist EtherDelta ein *Off-chain*-Orderbuch auf. Konkret werden die Aufträge der Nutzer in einer Datenbank auf einem zentralen Server abgespeichert. Diese Datenbank kommuniziert sodann mit den Smart Contracts zwecks Handelsausführung und -abwicklung. Das Orderbuch wird aktualisiert, sobald das Handelsgeschäft erfolgreich auf dem dezentralen Netzwerk abgewickelt worden ist.¹⁰³⁸

Demgegenüber setzt das Protokoll OasisDEX auf ein *On-chain*-Orderbuch. Das heisst, dass Nutzer auch die einzelnen Aufträge an das verteilte Register eines dezentralen Netzwerks zu übermitteln haben.¹⁰³⁹ Ferner erfolgt auch das Order Matching des Protokolls vollständig on-chain und damit automatisiert.¹⁰⁴⁰ Indem auf OasisDEX alle Aktivitäten on-chain ausgeführt werden müssen, weist das Protokoll im Vergleich zu EtherDelta einen höheren Grad an Dezentralität auf.

Auf EtherDelta resultiert das Platzieren eines Auftrags anders als auf OasisDEX im Orderbuch weder in Gaskosten noch Handelsgebühren für den Maker. Allerdings zahlt der Taker eines Auftrags sowohl die Gaskosten der Ethereum Blockchain als auch eine Handelsgebühr von 0.3% des Transaktionsvolumens an die im Smart Contract spezifizierte Adresse. Im Falle von EtherDelta konnte

¹⁰³⁶ Siehe Coburn, EtherDelta, Youtube, *passim*; frenchhoudini, EtherDelta is a decentralized exchange, Reddit, *passim*; ausführlich zur Handelsmechanik von EtherDelta SEC, Order Coburn, 4–7.

¹⁰³⁷ Siehe Lin, Stanford Journal of Blockchain Law & Policy 2019, 71–72.

¹⁰³⁸ Siehe SEC, Order Coburn, 6–7; vgl. ferner zu den Details des Orderbuchs von EtherDelta Coburn, EtherDelta, Youtube, *passim*.

¹⁰³⁹ Siehe OasisDEX, Introduction to the OasisDEX Protocol, *passim*.

¹⁰⁴⁰ Siehe OasisDEX, OasisDEX Market Taker Guide, *passim*.

COBURN aufgrund seines Besitzes des Private Keys zu den Smart Contracts die Adresse und die Handelsgebühren festlegen und nachträglich ändern.¹⁰⁴¹ Alle weiteren Interaktionen mit den Smart Contracts von EtherDelta verursachen ebenfalls Transaktionsgebühren.¹⁰⁴²

Zentral für Smart Contract-basierte P2P-Handelsplattformen ist die Verwendung eines Orderbuchs. Von den bisher dargestellten Handelsplattformen unterscheidet sich dieser Plattfortmtyt darin, dass im Hinblick auf den Tausch von Kryptovermögenswerten ausschliesslich die Smart Contracts einer Blockchain (i.d.R. Ethereum) zur Anwendung gelangen.

c. Beteiligte Parteien am Beispiel von EtherDelta und OasisDEX

Nutzer von Smart Contract-basierten P2P-Handelsplattformen interagieren in aller Regel über ein Frontend mit den Smart Contracts (z.B. <https://oasis.app/trade/>).

Zwischen den an einem Handelsgeschäft beteiligten Parteien steht im Idealfall lediglich ein Smart Contract (so im Falle von OasisDEX). Handelsausführung und Handelsabwicklung erfolgen somit unmittelbar zwischen den Nutzern einer dezentralen Applikation, weshalb vorliegend von P2P-Handelsplattformen gesprochen wird.

Allerdings zeigt der Fall von EtherDelta auf, dass gewisse Elemente einer solchen Plattform durchaus organisatorisch zentralisiert sein können. In Fall von EtherDelta war es das Orderbuch, das der Gründer der Plattform auf einem zentralen Server ausführte. COBURN intervenierte allerdings weder direkt in die Handelsausführung noch in die Handelsabwicklung. Dies wäre für ihn in technischer Hinsicht auch gar nicht möglich gewesen.¹⁰⁴³ Nicht ausgeschlossen ist hingegen, dass auch ein Off-chain-Orderbuch *dezentral* bzw. verteilt geführt wird. Eine mögliche Herangehensweise ist diejenige des Protokolls 0x (siehe sogleich unten).

Eine weitere Möglichkeit ist die Verwendung des IPFS-Protokolls mitsamt P2P-Netzwerk für das Frontend des Orderbuchs. Dies führt dazu, dass das Orderbuch von einem verteilten Netzwerk von Computern gehostet wird. Ein

¹⁰⁴¹ Siehe hierzu SEC, Order Coburn, 4 FN 9.

¹⁰⁴² Siehe Coburn, EtherDelta, Youtube, *passim*; eine Übersicht findet sich bei frenchhoudini, How fees work, Reddit, *passim*.

¹⁰⁴³ Siehe SEC, Order Coburn, *passim*.

Beispiel ist die dezentrale Applikation Mesa, die auf dem Gnosis Protokoll¹⁰⁴⁴ basiert und deren Frontend über IPFS gehostet wird.¹⁰⁴⁵ Die Smart Contracts von Mesa sind für Nutzer sowohl über eine HTTPS-Domain (<https://mesa.eth.link/>) als auch eine IPFS-Domain (<ipfs://bafybeidxpifp3onk22bmijp733qucp4tsj2vpf4m6apszlhuc6ussrpaa>) erreichbar. Mesa kann damit als die derzeit wohl einer der dezentralsten Handelsplattformen auf Ethereum bezeichnet werden.¹⁰⁴⁶

d. Weiterentwicklungen

Als die grösste Schwäche von Smart Contract-basierten P2P-Handelsplattformen werden die zahlreichen Interaktionen mit der Blockchain betrachtet. Selbst auf der Plattform EtherDelta, die anders als das Protokoll OasisDEX kein On-chain-Orderbuch vorsieht, interagieren Nutzer für einen erfolgreichen Austausch von Vermögenswerten mindestens dreimal mit einem Smart Contract (deposit, trade und withdraw). In OasisDEX erzeugt bereits die Erstellung eines Auftrages im Orderbuch Gaskosten. Auf der Ethereum Blockchain können diese Kosten unter Umständen prohibitiv sein. Dies tangiert v.a. die Aktivitäten von Market Makern negativ, denn diese haben ihre Aufträge regelmässig den aktuellen Umständen anzupassen. Andernfalls geht ihr Geschäftsmodell nicht auf.¹⁰⁴⁷

Neuere Protokolle verzichten darum für die Führung des Orderbuchs gänzlich auf Smart Contracts, sie versuchen jedoch anders als EtherDelta die Dezentralität der Handelsplattform beizubehalten.¹⁰⁴⁸ Das Verzeichnis aller im Markt

¹⁰⁴⁴ Siehe hierzu Gnosis Protocol, Introduction to Gnosis Protocol, *passim*.

¹⁰⁴⁵ Siehe hierzu ausführlich Gnosis, Experience & Challenges of Building a Fully Decentralized Trading Protocol, Medium, *passim* («With the smart contracts deployed on Ethereum and the front-end package via IPFS, if any actor wanted to censor any aspect of the DEX, it would be technically necessary to take down every Ethereum and IPFS node, making the attempt highly unlikely.»).

¹⁰⁴⁶ Zu erwähnen ist, dass Mesa kein kontinuierliches Orderbuch aufweist, sondern ein Orderbuch basierend auf dem Frequent-Batch-Auction-Modell implementiert; siehe Kreutler, Announcing Gnosis Protocol, *passim* («Mesa is launched and maintained by the dxDAO, a community-owned and operated organization that develops, governs, and promotes DeFi protocols. Available through IPFS and ENS, the Mesa dapp is a general trading interface that supports simple market making strategies for stablecoins on Gnosis Protocol.»); vgl. in theoretischer Hinsicht Smith, Exchange Protocol for the Decentralized Web, 1-2.

¹⁰⁴⁷ Siehe Warren/Bandeali, 0x, 4; ferner Angeris et al., Cryptoeconomic Systems 2021, 3.

¹⁰⁴⁸ Kritisch Smith, Exchange Protocol for the Decentralized Web, 1-2; ebenfalls Angeris et al., Cryptoeconomic Systems 2021, 3.

verfügbaren Aufträge soll dabei vollständig ausserhalb von auf dem dezentralen Netzwerk abgelegten Smart Contracts geführt werden, wohingegen die Abwicklung des Handels weiterhin on-chain erfolgen soll.¹⁰⁴⁹

Das Protokoll 0x etwa – ein Protokoll, das aus dem ICO-Boom im August 2017 hervorging – sieht Orderbücher vor, die von sog. *Relayers* off-chain geführt werden. Relayers treten als Drittparteien zwischen Makers und Takers einer Transaktion. Vereinfacht gesagt, empfangen, veröffentlichen und übermitteln Relayers die von den Nutzern des 0x Protokolls erzeugten Mitteilungen.¹⁰⁵⁰ Die Relayers können dabei entweder direkt über eine gemeinsame API oder über ein verteiltes Netzwerk (0x Mesh) miteinander kommunizieren.¹⁰⁵¹ Aus den von Nutzern (*Makers*) empfangenen Kaufs- und Verkaufsinteressen erstellen Relayers ein Orderbuch. Andere Nutzer des Protokolls (*Takers*) können sodann die von den Relayers übermittelten Aufträge manuell akzeptieren, indem sie diese zur Ausführung auf der Ethereum Blockchain bringen. Erst die Ausführung greift somit auf einen Smart Contract zurück (*Exchange Contract*), alles andere geschieht off-chain. Die Kryptovermögenswerte verbleiben mit anderen Worten bis zur Ausführung des Geschäfts in den Wallets der Parteien. Damit Relayers ihre Dienste anbieten, werden die von den Makers und/oder Takers bezahlten Transaktionsgebühren mithilfe des Exchange Contracts an die Relayers ausbezahlt. Dies geschieht, sobald ein Auftrag erfolgreich von einem Taker akzeptiert und ausgeführt wurde.¹⁰⁵² Als Zahlungsmittel für Transaktionsgebühren dient der Nutzungs-Token ZRX des 0x Protokolls.¹⁰⁵³

Die Ausführung des Austauschgeschäfts erfolgt aufgrund der Verwendung von Smart Contracts atomistisch, d.h., es werden entweder beide Seiten des Geschäfts oder keine ausgeführt.¹⁰⁵⁴ Zwar ist die Off-chain-Orderbuch von Relayers zentral für diesen Plattfortmtypus, doch ist der Einfluss von Relayers auf das Handelsgeschäft *beschränkt*: Namentlich haben Relayers zu keinem Zeitpunkt Zugriff auf die Vermögenswerte der an einem Austausch beteiligten Par-

¹⁰⁴⁹ Siehe Warren/Bandeali, 0x, 4 («A hybrid implementation, which we refer to as 'off-chain order relay with on-chain settlement,' combines the efficiency of state channels with the near instant settlement of on-chain order books.»).

¹⁰⁵⁰ Siehe 0x, Core Concepts, Off-chain relay, on-chain settlement, *passim* («A 'relayer' is any entity that helps traders create, find and fill 0x orders.»); ferner von einem digitalen Anschlagbrett sprechend Warren, Decentralized Exchange, *passim*.

¹⁰⁵¹ Siehe 0x, Core Concepts, Networked liquidity, *passim*; ferner 0x, Market-making on 0x, *passim*.

¹⁰⁵² Siehe Warren/Bandeali, 0x, 7.

¹⁰⁵³ Siehe 0x, ZRX Portal FAQ, How are liquidity rewards calculated?, *passim*.

¹⁰⁵⁴ Siehe 0x, Core Concepts, Off-chain relay, on-chain settlement, *passim*.

teien. Ferner sind Relayers auch nicht in den Matching-Prozess eingebunden. Ob ein Angebot ausgeführt wird, wird, wie oben erwähnt, allein vom Taker bestimmt.¹⁰⁵⁵

Die von ihnen akzeptierten Aufträge und somit auch die Transaktionsgebühren können Relayer selbst bestimmen, wobei Maker letztlich entscheiden, welchen Relayer sie für ihren Auftrag nutzen. Taker haben schliesslich die Wahl zwischen den Orderbüchern unterschiedlicher Relayers.¹⁰⁵⁶ Die Konsequenz ist, dass die Orderbücher unterschiedlicher Relayers in 0x nicht identisch aussehen müssen. Hinzukommt, dass Relayers «geschlossene» Liquiditätspools vorsehen können, deren Liquidität nur von bestimmten Wallet-Adressen geöffnet werden können sowie nur solchen zum Handel zur Verfügung stehen.¹⁰⁵⁷ Denkbar ist auch, dass die Liquiditätspools ähnlich zu Dark Pools im traditionellen Finanzsystem für Aussenstehende nicht einsehbare Orderbücher aufweisen.¹⁰⁵⁸

Die in 0x verwendeten Smart Contracts weisen Handelsfunktionalitäten auf, die mit traditionellen Handelsplattformen vergleichbar sind: Maker können namentlich einen Auftrag zurückziehen oder dessen zeitliche Gültigkeit beschränken; Taker können sodann Aufträge nur partiell ausführen.¹⁰⁵⁹ Anstelle der Verwendung von Relayers können Nutzer des Protokolls Aufträge auch unmittelbar einander übermitteln (z.B. per E-Mail oder über Reddit¹⁰⁶⁰) und akzeptieren.¹⁰⁶¹ Damit weist das 0x Protokoll Ähnlichkeiten mit einem traditionellen OTC-Trading Desk auf.

Schliesslich können Protokolle und Anwendungen sodann mit 0x verbunden werden, indem diese entweder auf 0x aufbauen oder 0x deren Protokolle integriert. Dies erlaubt u.a. die Aggregierung der auf anderen dezentralen Handelsplattformen verfügbaren Liquidität. Als Maker können bspw. auch Smart Contract-basierte Liquiditätspools, wie etwa Uniswap, oder professionelle Market Maker fungieren. Nutzer können sodann bspw. auf einer anderen dezentralen Handelsplattform (so z.B. Matcha) diese Liquidität als Taker nachfragen.¹⁰⁶² Freilich können Projekte den Open-Source-Code von 0x auch für ihre

¹⁰⁵⁵ Siehe Schär, Federal Reserve Bank of St. Louis Review 2021, 161.

¹⁰⁵⁶ Siehe Warren/Bandeali, 0x, 8.

¹⁰⁵⁷ Siehe Warren, Compliant peer-to-peer trading, *passim*.

¹⁰⁵⁸ Vgl. das Projekt RenEx, das allerdings derzeit nicht weiterverfolgt wird; siehe hierzu Ren, Privacy preserving virtual machine, 13–14.

¹⁰⁵⁹ Siehe Warren/Bandeali, 0x, 9–10.

¹⁰⁶⁰ Z.B. TokenTrade, Marketplace for Ethereum ERC20 Tokens, Reddit, *passim*.

¹⁰⁶¹ Siehe 0x, Core Concepts, Off-chain relay, on-chain settlement, *passim*.

¹⁰⁶² Vgl. für eine Übersicht Oshiro, Exploring the 0x DeFi Ecosystem, *passim*.

eigene dezentrale Handelsplattform verwenden. Nachdem die Entwickler von DDEX¹⁰⁶³ anfänglich auf dem 0x Protokoll aufgebaut hatten, entschlossen sie sich Ende 2018, den Code des Protokolls zu forken, um ein eigenes Protokoll für eine dezentrale Handelsplattform zu entwickeln.¹⁰⁶⁴

3.7 Smart Contract-basierte Liquiditätspools

a. Hintergrund

Smart Contract-basierte Liquiditätspools (*Liquidity Pools*) gehören derzeit zu den beliebtesten dezentralen Handelsplattformen. Bekannte Vertreter sind bspw. die Protokolle Bancor¹⁰⁶⁵, Uniswap¹⁰⁶⁶, Curve¹⁰⁶⁷ und Kyber Network¹⁰⁶⁸.

Die Idee hinter Smart Contract-basierten Liquiditätspools geht zurück auf einen Reddit-Beitrag von VITALIK BUTERIN vom Oktober 2016.¹⁰⁶⁹ ALAN LU vertiefte sodann die Idee in einem Blogpost vom März 2017.¹⁰⁷⁰ Motiviert waren die beiden Beiträge von der Erkenntnis, dass der damalige Handel auf dezentralen Handelsplattformen, wie namentlich EtherDelta und OasisDEX, relativ ineffizient war. Es mangelte insb. an ausreichender Liquidität, da es an professionellen Market Makern fehlte. Dies lag daran, dass effizientes Market Making aufgrund der Kosten von On-Chain-Transaktionen praktisch unmöglich war und sich somit nicht etablieren konnte.¹⁰⁷¹ Wie oben ausgeführt, erfordert der Handel auf EtherDelta zahlreiche On-Chain-Transaktionen, welche jeweils Gebühren für die Nutzer verursachen.¹⁰⁷² Es bewahrheitete sich also einmal mehr, dass der Mangel an Liquidität die Achillesferse einer jeden Handelsplattform ist. Ausserdem sind gerade illiquide Vermögenswerte (sog. Long-Tail-Assets) grundsätzlich ungeeignet für Orderbücher, sodass auch hier Bedarf für neue Modelle existierte.¹⁰⁷³

¹⁰⁶³ <https://ddex.io/>.

¹⁰⁶⁴ Siehe Li, Why we are forking 0x, Medium, *passim*.

¹⁰⁶⁵ <https://bancor.network/>.

¹⁰⁶⁶ <https://uniswap.org/>.

¹⁰⁶⁷ <https://curve.fi/>.

¹⁰⁶⁸ <https://kyber.network/>.

¹⁰⁶⁹ Siehe Buterin, On-chain decentralized exchanges, Reddit, *passim*.

¹⁰⁷⁰ Siehe Lu, Building a Decentralized Exchange, *passim*.

¹⁰⁷¹ So Buterin, On-chain decentralized exchanges, Reddit, *passim* («The main challenge that I see with the MKR market, etherdelta and other markets right now is the high spreads, often 10% or even higher.»).

¹⁰⁷² Siehe hierzu oben, IV.3.6b.

¹⁰⁷³ Siehe Werner et al., Decentralized Finance, 4; Weisenthal/Alloway, Hayden Adams Explains Uniswap, Odd Lots Podcast, *passim*.

Im Unterschied zu Smart Contract-basierten P2P-Handelsplattformen verzichten Smart Contract-basierte Liquiditätspools auf die Führung eines Orderbuchs. An dessen Stelle treten Liquiditätspools, welche in automatisierter Weise kontinuierlich Liquidität für den Handel mit Kryptovermögenswerten bereitstellen.

b. Funktionsweise am Beispiel von Uniswap

Das Konzept des Liquiditätspools wurde erstmals 2017 durch das Protokoll *Bancor* eingeführt.¹⁰⁷⁴ Das Bancor Protokoll sieht anders als jüngere Plattformen noch vor, dass der Handel gegen den eigenen sog. Smart Token BNT erfolgen muss, dessen Angebot algorithmisch von einem Smart Contract in Abhängigkeit des Handelsvolumens gesteuert wird.¹⁰⁷⁵ Erst aber das Protokoll *Uniswap*, das im November 2018 auf Ethereum startete, hat das Konzept aufgrund des simplen Konzepts und der Bedienungsfreundlichkeit der dezentralen Applikation zu einer der beliebtesten DeFi-Anwendungen überhaupt gemacht.

Anders als die bisher vorgestellten Kategorien dezentraler Handelsplattformen weist Uniswap kein Orderbuch mehr auf, in welchem Käufer und Verkäufer zusammengeführt werden. Um ausserhalb von Orderbüchern Liquidität zur gewährleisten, werden stattdessen Liquiditätspools für Kryptovermögenswerte geschaffen. Dafür werden Handelspaare gebildet (z.B. ETH-DAL), wobei für jeden Vermögenswert jeweils ein Pool erstellt werden muss. Als Grundlage dieser Pools dient ein Smart Contract (Exchange Contract), der auf einem dezentralen Netzwerk (hier: Ethereum Blockchain) abgelegt und ausgeführt wird. Damit ist der Handel von Kryptovermögenswerten vollständig on-chain.¹⁰⁷⁶ Seit der zweiten Version können unterschiedliche ERC-20-Tokens sodann direkt gegeneinander getauscht werden, ohne dass noch jeweils der Umweg über ETH gemacht werden muss.¹⁰⁷⁷

¹⁰⁷⁴ Siehe Bancor Network, Introduction, *passim*.

¹⁰⁷⁵ Siehe Hertzog/Benartzi/Benartzi, Bancor Protocol. Continuous Liquidity for Cryptographic Tokens, 4–6.

¹⁰⁷⁶ Siehe Adams, Uniswap Whitepaper, *passim*.

¹⁰⁷⁷ Siehe Adams/Zinsmeister/Robinson, Uniswap v2, 2.

Die Pools erfüllen die Funktion eines Market Makers, der den einzelnen Märkten für Handelspaare Liquidität zur Verfügung stellt.¹⁰⁷⁸ Entsprechend wird das Konzept – in Anlehnung an bestehende Modelle in CeFi – als *Automated Market Maker* (AMM) bezeichnet.¹⁰⁷⁹ Da kein Market Maker im traditionellen Sinne involviert ist, ist es allerdings präziser, von automatisiertem oder algorithmischem Market Making zu sprechen. Letztlich werden die Aufträge gegen die Pools und somit nicht gegen andere Nutzer des Protokolls ausgeführt. Es findet mit anderen Worten kein Matching von Käufern und Verkäufern statt.¹⁰⁸⁰ Aufgrund dieser Peer-to-Pool-Methode werden AMMs vorliegend nicht den P2P-Handelsplattformen zugeordnet. Am ehesten lassen sich Smart Contract-basierte Liquiditätspools als eine dezentrale Version von ShapeShift oder Changelly beschreiben. Die Suche nach Gegenparteien erübrigt sich im Vergleich zu diesen P2O-Plattformen, denn das automatisierte Market Making erfolgt ohne Unterbruch; es gibt weder zeitlich Einschränkungen noch solche aufgrund erhöhter Volatilität oder Preisdrucks.¹⁰⁸¹

Neben der Automatisierung des Market Makings ist die *Preisstellung* eine weitere Besonderheit von Liquiditätspools. Preise werden ebenfalls automatisiert gestellt, indem sie einer mathematischen Formel folgen. In der einfachsten Ausprägung gilt $\text{Token A}_{\text{Pool}} \cdot \text{Token B}_{\text{Pool}} = k$ oder verkürzt $A \cdot B = k$.¹⁰⁸² k gilt dabei als Konstante, gemäss welcher der Preis einer Einheit eines Kryptovermögenswerts negativ mit den im Pool verfügbaren Einheiten korreliert. Dies bedeutet, dass der Preis eines Vermögenswerts desto höher ausfällt, je kleiner dessen Menge im Liquiditätspool im Verhältnis zum anderen Liquiditätspool

¹⁰⁷⁸ Ausführlich zu dieser Funktion Othman, *Automated Market Making*, 1. AMMs haben ihren Ursprung in der Forschung zu Prediction Markets, vgl. hierzu insb. Hanson, *The Journal of Prediction Markets* 2007, 7–8.

¹⁰⁷⁹ Siehe Buterin, *On-chain decentralized exchanges*, Reddit, *passim*; Lu, *Building a Decentralized Exchange*, *passim*; Hertzog/Benartzi/Benartzi, *Bancor Protocol. Continuous Liquidity for Cryptographic Tokens*, 5–6.

¹⁰⁸⁰ Siehe Adams, *Uniswap Whitepaper*, *passim*; ausführlich Xu et al., *SoK: DEX with AMM protocols*, 2, 7.

¹⁰⁸¹ Siehe Xu et al., *SoK: DEX with AMM protocols*, 2; Lin, *Stanford Journal of Blockchain Law & Policy* 2019, 69; teils kritisch Qureshi, *Unbundling Uniswap*, Medium, *passim* («You can imagine a variation of Uniswap that reads in historic volatility [or receives a proof of historic volatility], and refuses to execute trades when volatility spikes. Or alternatively, a variation of Uniswap that refuses to trade after receiving order flow that's too one-sided. After all, one-sided flow is usually a sign that new information is moving the market, and that information needs to be digested by the market before the market maker can profitably quote again. Or, simplest yet, pool LPs could decide via governance to turn off the pool when they believe it no longer makes sense to keep quoting.»).

¹⁰⁸² Siehe Adams, *Uniswap Whitepaper*, *passim*; ein gutes Beispiel der Funktionsweise findet sich bei Aramonte/Huang/Schrimpf, *BIS Quarterly Review* Dezember 2021, 34–35.

ist. Der Preis wird also in der Menge des Kryptovermögenswerts eines zweiten Pools ausgedrückt (d.h. ETH in DAI und DAI in ETH). Dabei ist sichergestellt, dass ein preisgewichtetes, relatives Gleichgewicht zwischen den beiden Pools besteht. Der Handel selbst hat in Einklang mit der oben erwähnten Formel keinen Einfluss auf die Konstante.¹⁰⁸³ Dasselbe gilt für poolexterne Faktoren, im Besonderen die Bedingungen an anderen Märkten.¹⁰⁸⁴ Allerdings hat die Grösse des Pools einen Einfluss auf den Preiseffekt eines Geschäfts.¹⁰⁸⁵

Grafisch¹⁰⁸⁶ kann die mathematische Formel anhand einer Preiskurve (sog. Bonding Curve) dargestellt werden. Die Kurve weist mit abnehmender Menge an Kryptovermögenswerten einen asymptotischen Verlauf auf. Damit kostet die letzte Einheit eines Pools theoretisch eine unendliche Menge an Vermögenswerten des anderen Pools.¹⁰⁸⁷ Diese Herangehensweise ist allerdings kapitalineffizient, muss doch für jeden einzelnen Preispunkt auf der Kurve Liquidität aufgebracht werden. Dieses Problem wurde mit der dritten Version von Uniswap adressiert. Nunmehr können Liquiditätsgeber ihre Liquidität auf einen bestimmten Kurvenbereich konzentrieren, was sich insb. für preisstabile Vermögenswerte, wie etwa Stablecoins, anbietet.¹⁰⁸⁸ Damit nähert sich Uniswap in Version 3 wieder dem traditionellen Orderbuchmodell an.

Die Kryptovermögenswerte befinden sich bis zum Austauschgeschäft im jeweiligen Pool des Exchange Contracts. Zum Austausch von Vermögenswerten kommt es, wenn ein Nutzer des Protokolls entsprechende Funktionen des Smart Contracts aufruft: Ein Nutzer, der bspw. den Stablecoin DAI gegen WETH tauschen möchte, schickt WETH an die entsprechende Pool-Adresse des Smart Contracts; zeitgleich fordert er den Smart Contract auf, das wertmässige Äquivalent von DAI abzüglich einer Handelsgebühr an ihn zu übermitteln. Die beiden Transaktionen werden dabei technisch so konstruiert, dass entweder beide ausgeführt werden oder keine der beiden. Es handelt sich namentlich um eine Atomic Transaction.

¹⁰⁸³ Siehe Adams, Uniswap Whitepaper, *passim*; ausführlich Angeris et al., *Cryptoeconomic Systems* 2021, 3–4 m.w.H.

¹⁰⁸⁴ Siehe Nguyen/Luu/Ng, *Dynamic Automated Market Making*, 3.

¹⁰⁸⁵ Dies wird typischerweise als *Slippage* bezeichnet, wobei damit die Differenz zwischen Spotpreis bei Auftragserteilung und tatsächlich realisiertem Preis gemeint ist; vgl. Xu et al., *SoK: DEX with AMM protocols*, 7; Harvey/Ramachandran/Santoro, *DeFi*, 96–98.

¹⁰⁸⁶ Siehe für eine gute Darstellung der Preisfunktion etwa Qureshi, *What explains the rise of AMMs?*, Medium, *passim*.

¹⁰⁸⁷ Siehe Schär, *Federal Reserve Bank of St. Louis Review* 2021, 161–162.

¹⁰⁸⁸ Siehe Adams et al., *Uniswap v3*, 1–3.

Den Nutzern stehen technisch gesehen sowohl Swaps als auch Transaktionen zur Verfügung: Im ersteren Fall erhält die Absender-Adresse den Token, im letzteren Fall werden die erworbenen Token an eine neue Adresse übertragen.¹⁰⁸⁹

c. Beteiligte Parteien am Beispiel von Uniswap

Die Nutzung von Uniswap erfolgt über ein Frontend, welches das Wallet des Nutzers direkt mit den Smart Contracts der Applikation kommunizieren lässt. Das Frontend ist für jedermann zugänglich (z.B. <https://app.uniswap.org/>). Es werden keine Plattformnutzungsgebühren oder Ähnliches erhoben. Daneben bestehen zahlreiche Alternativen, wie Nutzer mit den Smart Contracts von Uniswap direkt oder über Frontends Dritter (z.B. über Etherscan¹⁰⁹⁰ oder ein Mobile Wallet¹⁰⁹¹) interagieren können.¹⁰⁹²

Personen, welche den Pools aufgrund ihrer geringen Zeitpräferenz Kryptovermögenswerte beisteuern, werden Liquiditätsgeber (*Liquidity Provider*) genannt. Die Zurverfügungstellung von Vermögenswerten erfolgt ebenfalls über ein Frontend, das mit den Smart Contracts verbunden ist (z.B. <https://app.uniswap.org/#/pool>) und somit jedermann offensteht. Dabei haben Liquiditätsgeber grundsätzlich immer Vermögenswerte beider Pools in einem bestimmten Verhältnis einzubringen. In Uniswap gilt etwa, dass Liquiditätsgeber in beide Pools wertmässig gleich viele Kryptovermögenswerte einzubringen haben. Das anfängliche Austauschverhältnis bestimmt dabei der Liquiditätsgeber, welcher die Pools durch die Erstellung des Exchange Contracts ins Leben ruft.¹⁰⁹³

Das Preisfindungsmodell von AMMs beruht auf der impliziten Annahme, dass Arbitrageure Abweichungen von Marktpreisen auf anderen – zentralen und dezentralen – Handelsplattformen ausnützen.¹⁰⁹⁴ Indem sie dem aus ihrer Sicht überbewerteten Pool Liquidität beisteuern, erhalten sie Vermögenswerte des unterbewerteten Pools. Auch sie steuern aus Sicht der Nutzer ein öffentli-

¹⁰⁸⁹ Siehe Adams, Uniswap Whitepaper, *passim*.

¹⁰⁹⁰ <https://etherscan.io/address/0x7a250d5630b4cf539739df2c5dadb4c659f2488d> (danach auf «Contract» und sodann je nach Funktion «Read Contract» oder «Write Contract»).

¹⁰⁹¹ Ein Beispiel ist das Bridge Wallet von Mt Pelerin Group AG mit Sitz in Genf.

¹⁰⁹² Siehe für eine Übersicht Zinsmeister, Overview of Uniswap, GitHub, *passim*.

¹⁰⁹³ Siehe Adams, Uniswap Whitepaper, *passim*; detailliert zu den unterschiedlichen Rollen Xu et al., SoK: DEX with AMM protocols, 3–4.

¹⁰⁹⁴ Siehe Uniswap, How Uniswap works, *passim*; Adams, Uniswap Whitepaper, *passim*; Xu et al., SoK: DEX with AMM protocols, 4; Werner et al., Decentralized Finance, 4.

ches Gut bei, denn AMMs sind für die Preisbildung auf externe Handelsquellen angewiesen. In der Praxis handelt es sich bei Arbitrageuren in aller Regel um Computerprogramme, die auf mehreren Märkten gleichzeitig ein Inventar an Kryptovermögenswerten bewirtschaften. Diese Programme werden auch als Bots bezeichnet werden.¹⁰⁹⁵

Liquiditätsgeber in Uniswap erhalten für den Aufbau von Poolreserven Liquiditätstoken (*Liquidity Token* bzw. *Pool Token*). Diese werden von einem Smart Contract erzeugt (mint), um die von den Liquiditätsgebern eingebrachte Liquidität abzubilden. Liquiditätsgeber können jederzeit ihre Kryptovermögenswerte wieder auszulösen, indem sie ihre Liquiditätstoken zerstören (burn). Dabei kommt das Austauschverhältnis zum jeweiligen Zeitpunkt zur Anwendung.¹⁰⁹⁶ Das Beisteuern von Liquidität stellt aus Sicht der Nutzer ein öffentliches Gut dar.¹⁰⁹⁷ Allerdings erfolgt dieser mit gewissen Verlustrisiken verbundene Vorgang nicht entschädigungslos.¹⁰⁹⁸ Die Liquiditätsgeber erhalten einen proportionalen Anteil an den vereinnahmten Handelsgebühren, die den Nutzern im Rahmen des Austauschs von Kryptovermögenswerten belastet werden (derzeit 0.3% des Transaktionsvolumens).¹⁰⁹⁹ Seit Version 3 des Uniswap Protokolls können Liquiditätsgeber zwischen Pools mit unterschiedlichen Handelsgebühren wählen.¹¹⁰⁰

Um Marktteilnehmern einen zusätzlichen Anreiz zu bieten, Liquiditätspools für bestimmte Handelspaare zu schaffen, sehen gewisse Protokolle vor, Token an die Liquiditätsgeber auszuschütten. Dies wird gemeinhin als *Liquidity Mining* bzw. *Liquidity Farming* bezeichnet.¹¹⁰¹ Ein Beispiel unter vielen ist das Protokoll Ampleforth, dass die Liquiditätsgeber der Pools AMPL/ETH mit seinem eigenen Token belohnt.¹¹⁰² Dieselbe Anreizstruktur ist u.U. auch in der

¹⁰⁹⁵ Eine in der Praxis beliebte Open-Source-Software für Arbitrage und Market Making ist *Hummingbot* (<https://hummingbot.io/>).

¹⁰⁹⁶ Siehe Adams, Uniswap Whitepaper, *passim*.

¹⁰⁹⁷ Vgl. Buterin, Path Independence, *passim*; ferner Xu et al., SoK: DEX with AMM protocols, 5.

¹⁰⁹⁸ Das Verlustrisiko im Vergleich zum blossen Halten der Vermögenswerte wird üblicherweise als *Divergence* bzw. *Impermanent Loss* bezeichnet. Dabei handelt es sich um nicht-realisierten Verlust, der allerdings beim Verlassen des Pools in einen realisierten Verlust resultieren kann; vgl. etwa Xu et al., SoK: DEX with AMM protocols, 7–8.

¹⁰⁹⁹ Siehe Uniswap, Ecosystem Participants, *passim*.

¹¹⁰⁰ Siehe Adams et al., Uniswap v3, 3.

¹¹⁰¹ Siehe Qureshi, What explains the rise of AMMs?, Medium, *passim*; Xu et al., SoK: DEX with AMM protocols, 4; ausführlich zu Yield Farming, wozu auch Liquidity Mining gehört, Coussaert/Xu/Matsui, SoK: Yield Aggregators in DeFi, 2–3.

¹¹⁰² Siehe Ampleforth, Geysers, *passim*.

Emission von Governance Token durch das jeweilige Protokoll wiederzuerkennen.¹¹⁰³ Dass Liquidität bzw. ein Mangel davon einmal mehr das «Kryptonit» von Handelsplattformen darstellen kann, wurde somit auch für das AMM-Modell erkannt.¹¹⁰⁴

d. Weiterentwicklungen

Das AMM-Modell, das von Uniswap popularisiert wurde, ist in der Folge mehrfach für spezifische Anwendungsfälle adaptiert worden:

*Curve*¹¹⁰⁵ hat sich etwa auf Liquiditätspools bestehend aus unterschiedlichen Stablecoins und ähnlich bewerteten Vermögenswerten spezialisiert. Davon ausgehend, dass Stablecoins eine vergleichsweise tiefe Volatilität aufweisen und Preisdifferenzen zueinander gering ausfallen, gelangt in *Curve* eine modifizierte Preiskurve zur Anwendung.¹¹⁰⁶ Ausserdem sind die Handelsgebühren im Vergleich zu Uniswap standardmässig tiefer (0.04%), wobei sie ansteigen können, wenn die Preisdifferenz zwischen zwei Stablecoins mit gleichem Referenzwert zunimmt.¹¹⁰⁷

Das Protokoll von *Balancer*¹¹⁰⁸ sieht sodann Liquiditätspools vor, die sich anders als bei Uniswap nicht nur aus zwei, sondern aus mehreren Kryptovermögenswerten mit unterschiedlicher Gewichtung zusammensetzen können.¹¹⁰⁹ Dies erlaubt – vergleichbar mit Index Funds – den Handel ganzer Portfolios von Vermögenswerten gegeneinander.¹¹¹⁰ Unterschiedliche Gebühren sind ebenso möglich. Schliesslich erlaubt *Balancer* auch die Bildung privater Pools, deren Liquidität von einem eingeschränkten Kreis an Liquiditätsgebern eingebracht wird. Nutzer können demgegenüber ihre Kryptovermögenswerte typischerweise ohne Einschränkung auch gegen private Pools handeln.¹¹¹¹

¹¹⁰³ Siehe Xu et al., SoK: DEX with AMM protocols, 6.

¹¹⁰⁴ Siehe etwa El Isa, What will it take to scale DEX liquidity?, Medium, *passim*.

¹¹⁰⁵ <https://curve.fi/>.

¹¹⁰⁶ Siehe Curve Finance, Understanding Curve, *passim*; ferner Egorov, StableSwap, *passim*.

¹¹⁰⁷ Siehe Angeris/Chitra, AFT '20: Proceedings of the Second ACM Conference on Advances in Financial Technologies 2020, 81.

¹¹⁰⁸ <https://balancer.finance/>.

¹¹⁰⁹ Siehe Balancer, FAQ, Basics, What is the Balancer Protocol?, *passim*; ausführlich Martinielli/Mushegian, A non-custodial portfolio manager, liquidity provider, and price sensor, *passim*.

¹¹¹⁰ Siehe Angeris/Chitra, AFT '20: Proceedings of the Second ACM Conference on Advances in Financial Technologies 2020, 81.

¹¹¹¹ Siehe Balancer, Shared Pool, *passim*.

DODO¹¹¹² führt schliesslich anstelle der in Uniswap vorgesehenen deterministischen Kurve für die Preisstellung zwischen den Pools ein arbiträres, flexibles Modell ein. Das Protokoll hält die Preise nahe am Marktpreis, indem ein Preisorakel eingesetzt wird.¹¹¹³ Ähnlich funktioniert das Protokoll Kyber Dynamic Market Making (DMM)¹¹¹⁴, das auf virtuelle anstelle echter Reserven setzt.¹¹¹⁵ In beiden Fällen soll dadurch im Ergebnis möglichst die Funktionsweise eines Orderbuchs imitiert werden.

Auch in anderen dezentralen Systemen oder als Layer-2-Protokolle hat sich das AMM-Modell bereits etablieren können.¹¹¹⁶

Zu den verfügbaren Liquiditätspools gehören inzwischen auch private Market Maker, die den Marktteilnehmern *eigene* Kurse stellen.¹¹¹⁷ Im Kyber Network etwa können professionelle Market Maker das Risikoprofil ihrer Handelsaktivitäten nach eigenem Ermessen anpassen, indem sie auf ihre Reserven das als Fed Price Reserve (FPR) bezeichnete Modell anwenden. Dabei ist es für FPR-Market Makers anders als im reinen AMM-Modell nicht erforderlich, ihre Liquidität vorab in Smart Contracts zu platzieren.¹¹¹⁸ Nutzer von solchen dezentralen Netzwerken (darunter auch 0x) verwenden stattdessen ein Request for Quote (RFQ)-basiertes Handelssystem, um mit den aus ihrer Sicht günstigsten Liquiditätspools zu handeln.¹¹¹⁹ Dadurch lassen sich die Handelsmechanik von Orderbuch-basierten Handelsplattformen und eines OTC-Trading Desks bzw. Dark Pools in das AMM-Modell integrieren.

¹¹¹² <https://dodoex.io/>.

¹¹¹³ Siehe DODO, DODO V2 docs, GitHub, *passim*.

¹¹¹⁴ <https://dmm.exchange>.

¹¹¹⁵ Siehe Nguyen/Luu/Ng, Dynamic Automated Market Making, 8.

¹¹¹⁶ Siehe etwa Pangolin auf der Avalanche Blockchain, <https://pangolin.exchange/>, oder Loopring auf Ethereum, <https://exchange.loopring.io/>. Vgl. hierzu unten, IV.3.9.

¹¹¹⁷ Siehe hierzu Qureshi, Unbundling Uniswap, Medium, *passim*; Schär, Federal Reserve Bank of St. Louis Review 2021, 163.

¹¹¹⁸ Siehe Kyber Network, Kyber Fed Price Reserve (FPR), *passim* («The FPR architecture allows professional MMs to either manually or build bots to operate their own unique algorithms, customize their trading strategy, and adjust their desired risk exposure.»); ferner bereits Kyber Network, On-Chain Liquidity Protocol, 7.

¹¹¹⁹ Siehe Kyber Network, On-Chain Liquidity Protocol, 7–8; Henderson, Growing DeFi with the help of professional market makers, *passim* («The user [...] simply sends in a request for liquidity and receives back a response with an optimally routed order. The magic happens behind the scenes where a large group of professional market makers are able to respond to the user's request and compete against on-chain liquidity to offer the user the best possible price.»).

Schliesslich kann auch die Derivateplattform *Synthetic*¹¹²⁰ als Smart Contract-basierten Liquiditätspools betrachtet werden. Synthetic erlaubt Nutzern, sowohl Short- als auch Long-Positionen in unterschiedlichen Vermögenswerten, wie etwa Fiatwährungen, Rohstoffe und Kryptowährungen, einzugehen. Die Abbildung erfolgt rein synthetisch (*Synths*). Für die Preisbestimmung werden Off-chain-Orakel verwendet.¹¹²¹ Der Smart Contract hält zwar anders als bei Uniswap keine Reserven der gehandelten Vermögenswerte, aber die auf der Plattform offenen Positionen werden durch den protokolleigenen Token SNX, die durch ein Netzwerk von Stakers in einem Smart Contract hinterlegt werden, überbesichert. Die Plattform verwendet weder Orderbuch noch Order Matching.¹¹²² Alle Handelsgeschäfte werden gegen einen Smart Contract ausgeführt: Dafür müssen Stakers in einem ersten Schritt entsprechende Synths (z.B. sUSD) gegen Überbesicherung schaffen. Dies führt zu einem Ansteigen des Debt Pools des Systems. Ein Handelsgeschäft führt sodann zur Vernichtung (*burn*) des bereits geschaffenen Tokens (hier sUSD) und im Gegenzug zur Produktion (*mint*) des zu erwerbenden Tokens (z.B. sBTC). Der Debt Pool bleibt durch eine solche Transaktion unverändert.¹¹²³ Die neu geschaffenen Tokens können sodann über andere Handelsplattformen (z.B. Kwenta¹¹²⁴) gehandelt werden.

Ähnlich funktioniert auch die Derivatehandelsplattform *Hegic*¹¹²⁵. Einerseits existieren Liquiditätsgeber, welche ETH und WBTC in Liquiditätspools einbringen, um entsprechende Call- oder Put-Optionen schreiben zu können, und andererseits Nutzer, welche die so geschriebenen Optionskontrakte erwerben. Sobald ein Kontrakt «in the Money» ist, kann er vom Erwerber ausgeübt werden. Die Ausführung und Abwicklung der Kontrakte erfolgt on-chain mittels Smart Contracts.¹¹²⁶ Hegic-Optionen können sodann auf der Handelsplattform Hetoro¹¹²⁷ gehandelt werden.

¹¹²⁰ <https://syntheticx.io/> bzw. <https://syntheticx.exchange/>.

¹¹²¹ Siehe Synthetic, System Architecture, *passim*.

¹¹²² Siehe Synthetic, Synthetic.Exchange, *passim*; ferner Synthetic Community, Project Overview, *passim* («Traders trade against pooled community collateral and not any specific counterparty.»).

¹¹²³ Siehe Synthetic, System Architecture, *passim*; ferner Synthetic Community, Staking Overview, *passim*.

¹¹²⁴ <https://kwenta.io/>.

¹¹²⁵ <https://www.hegic.co/>.

¹¹²⁶ Siehe Wintermute, On-chain Options Trading Protocol on Ethereum, 1, 5–6.

¹¹²⁷ <https://hetoro.com/h2m>.

3.8 Smart Contract-basierte Aggregatoren (Exkurs)

Ähnlichkeiten mit der Plattformkategorie der Smart Contract-basierten Liquiditätspools weisen sodann Protokolle auf, die aufgrund der Interoperabilität von DeFi-Protokollen die Liquidität mehrerer AMMs zusammenführen. Es wird in diesem Zusammenhang von *Aggregatoren* gesprochen.

Im Falle von *linch*¹¹²⁸ und *Matcha*¹¹²⁹ etwa können Nutzer über dessen Protokoll dutzende andere AMMs ansteuern. Dies ist möglich, weil AMMs nicht von der Verfügbarkeit einer Gegenpartei abhängig sind und somit jederzeit einen Preis stellen können.¹¹³⁰ Zu diesem Zweck sammeln Aggregatoren insb. Preisinformationen betreffend die ansteuerbaren Liquiditätspools. Aggregatoren sorgen sodann mithilfe von Smart-Order-Routing dafür, dass ein Auftrag möglichst effizient, allenfalls über mehrere Pools verteilt, ausgeführt wird. Die Ausführung des Auftrags erfolgt mithilfe von Smart Contracts in einer einzigen atomistischen Transaktion.¹¹³¹ Teilweise verwenden Aggregatoren auch Off-chain-Elemente im Rahmen der Handelsausführung, um die Effizienz der Preisaggregation oder des Order-Routings zu erhöhen.¹¹³²

3.9 Layer-2-Handelsplattformen

a. Hintergrund

Dezentrale Handelsplattformen, die über Layer-2-Protokolle oder Sidechains implementiert werden, sind als eigenständige Plattformkategorie zu betrachten. Sie stellen Skalierungslösungen zu Smart Contract-basierten Handelsplattformen dar, die unmittelbar auf einem dezentralen Netzwerk und somit auf dem Layer 1 zur Ausführung gelangen.

Als Beispiele von dezentralen Handelsplattformen, die auf dem Layer 2 von Ethereum zur Ausführung gelangen, sind etwa *Loopring*¹¹³³, *DeversiFi*¹¹³⁴ und

¹¹²⁸ <https://linch.exchange/>.

¹¹²⁹ <https://matcha.xyz/>.

¹¹³⁰ Siehe Harvey/Ramachandran/Santoro, DeFi, 52.

¹¹³¹ Siehe für *Matcha* Taylor, How Matcha finds the best prices, *passim*; ausführlich Forman, Ox API's Smart Order Routing, *passim*.

¹¹³² Vgl. etwa *linch*, *linch API*, *passim*; siehe hierzu Rai, Decentralized Exchanges, *passim*.

¹¹³³ <https://loopring.org/>.

¹¹³⁴ <https://www.deversifi.com/>.

*dYdX*¹¹³⁵ zu erwähnen. Diese Plattformen basieren im Wesentlichen auf dem Rollup-Modell. Die Merkmale unterschiedlicher Rollups sind Gegenstand von Ausführungen in Kapitel III.

Auch das Bitcoin Netzwerk bietet sodann mit dem Lightning Netzwerk eine Grundlage für dezentrale Layer-2-Handelsplattformen (siehe *Boltz*¹¹³⁶, *Open-DEX*¹¹³⁷, *StakenetDEX*¹¹³⁸).

b. Funktionsweise am Beispiel von Loopring

Loopring ist einerseits ein Layer-2-Protokoll für Ethereum und andere dezentrale Netzwerke. Die Fundamente des Protokolls bilden Smart Contracts und *Zero-Knowledge Proofs* (ZKP).¹¹³⁹ Loopring ist andererseits auch der Name der dezentralen Handelsplattform, welche sowohl ein Orderbuch- als auch ein AMM-Modell implementiert hat.¹¹⁴⁰ Die Technologie hinter dem Loopring-Protokoll wurde u.a. von BUTERIN entwickelt, um die Skalierbarkeit von Ethereum zu verbessern.¹¹⁴¹

Konkret handelt es sich bei den verwendeten ZKP um sog. *zk-SNARKs* bzw. *Zero-Knowledge Succinct Non-Interactive Arguments of Knowledge*. *zk-SNARK* ist eine kryptographische Methode, die es einer Person erlaubt, den Besitz einer bestimmten Information nachzuweisen, ohne dass die Person dem Gegenüber die Information offenzulegen und, abgesehen von einer einmaligen einseitigen Kommunikation, im Rahmen der Nachweiserbringung mit dem Gegenüber zu interagieren hat.¹¹⁴² Diese Methode wird bspw. auch für Transaktionen des Privacy Coins Zcash verwendet.¹¹⁴³

Eine vereinfachte Darstellung des Protokolls unterscheidet zwischen zwei Rollen: Relayers, die auch als Operators bezeichnet werden, und gewöhnliche Nutzer. *Relayers* sammeln die Layer-2-Transaktionen der Nutzer des Protokolls, produzieren sodann einen *zk-SNARK* der Transaktionsdaten und übermitteln in

¹¹³⁵ <https://dydx.exchange/>.

¹¹³⁶ <https://boltz.exchange/>.

¹¹³⁷ <https://opendex.network/>.

¹¹³⁸ <https://stakenet.io/>.

¹¹³⁹ Siehe Wang et al., Loopring, 2–3; Loopring, Loopring 3, *passim*.

¹¹⁴⁰ <https://exchange.loopring.io>.

¹¹⁴¹ Siehe Buterin, On-chain scaling, *passim*.

¹¹⁴² Siehe etwa Zcash, What are zk-SNARKs?, *passim*; ferner Wu/Wang, The Scientific World Journal 2014, 1.

¹¹⁴³ Siehe zu Zcash unten, IV.5.2c.ii.

regelmässigen Zeitabständen das Ergebnis in einer On-chain-Transaktion an die Ethereum Blockchain (Layer 1).¹¹⁴⁴ Aufgrund der Bündelung unzähliger Layer-2-Transaktionen in einer einzigen Layer-1-Transaktion wird die Loopring-Handelsplattform als *Rollup* bezeichnet.¹¹⁴⁵ Mithilfe von ZK-Rollups erreicht die Ethereum Blockchain ein Vielfaches ihrer bisherigen Transaktionskapazitäten, wodurch auch die Gaskosten pro Transaktion massiv sinken.¹¹⁴⁶

Um Loopring zu verwenden, haben Nutzer über eine webbasierte GUI oder API Kryptovermögenswerte in einem Smart Contract der Plattform zu deponieren (deposit).¹¹⁴⁷ Der jeweilige «Kontostand» eines Nutzers wird off-chain in einem sog. *Merkle Tree* abgebildet. Eine Layer-2-Transaktion führt lediglich zu einer Aktualisierung des betreffenden Merkle Tree. Die Transaktion als solche wird mit anderen Worten vorläufig nicht im verteilten Register des dezentralen Netzwerks verzeichnet. Die Aktualisierung des Merkle Tree erfolgt unverzüglich, so dass die betreffenden Vermögenswerte dem Nutzer sofort wieder zur Verfügung stehen. Erst die anschliessende Publikation der zk-SNARKs auf der Blockchain ist indessen als Abwicklung und somit als relevanter Zeitpunkt für die Finalität eines Handelsgeschäfts zu betrachten.¹¹⁴⁸

Es ist wichtig zu erwähnen, dass Nutzer ihre Kryptovermögenswerte aus dem Loopring-Smart Contract zurückziehen können (*force withdraw*). Somit haben Nutzer jederzeit und einseitig die Möglichkeit, ihren aktuellen «Layer-2-Kontostand» im verteilten Register des Layer 1 abzubilden.¹¹⁴⁹ Dies ist etwa dann relevant, wenn der Relayer unerwartet offline ist.¹¹⁵⁰ Allerdings kann die Rücküberweisung abhängig von den Gaskosten oder dem verwendeten Layer-2 eine gewisse Zeit in Anspruch nehmen.¹¹⁵¹

¹¹⁴⁴ Ausführlich Loopring, Loopring 3, *passim*; ferner DeversiFi, StarkWare Settlement Layer, *passim*.

¹¹⁴⁵ Siehe Loopring, Loopring 3, *passim*.

¹¹⁴⁶ Siehe Buterin, On-chain scaling, *passim*.

¹¹⁴⁷ Siehe Loopring, Loopring 3, *passim*.

¹¹⁴⁸ Siehe Loopring, Loopring 3, *passim* («A DEX can settle a ring off-chain and immediately show the final results to the user without waiting for the on-chain settlement confirmation. Using on-chain balances, users can modify their balances/allowances directly by interfacing with the blockchain. Therefore finality is only achieved when the ring settlement is confirmed on-chain.»); Wang et al., Loopring, 4–5; vgl. ferner auch Gudgeon et al., in: Bonneau/Heninger, Layer-Two Blockchain Protocols, 212 («eventual transaction finality»).

¹¹⁴⁹ Siehe Loopring, Loopring 3, *passim*.

¹¹⁵⁰ Siehe etwa betreffend Ausfalls des sog. *Sequencers* in Arbitrum (ein Optimistic Rollup) Off-chain Labs, Arbitrum One Outage Report, Medium, *passim*.

¹¹⁵¹ Siehe Loopring, How to use the L2 Loopring Exchange, *passim*; DeversiFi, Withdrawing Tokens *passim*.

Die Layer-1-Blockchain dient im Ergebnis für ZK-Rollups nur noch als Datenspeicher der Ergebnisse von Ereignissen, die sich off-chain über die Handelsplattform abspielen.¹¹⁵²

Relayers haben im Rahmen ihrer Aktivitäten niemals Zugriff auf die in den Smart Contracts aufbewahrten Kryptovermögenswerte der Nutzer, weshalb das Loopring-Protokoll als *non-custodial* bezeichnet werden kann.¹¹⁵³

c. Beteiligte Parteien am Beispiel von Loopring

Das Loopring-Protokoll sieht in erster Linie die bereits erwähnten Nutzer und Relayers (bzw. Operators) vor. Relayers unterhalten off-chain ein Orderbuch sowie die Transaktionshistorie der Nutzer. Als Ring Mining wird sodann die Funktion des Order Matching bezeichnet. Relayers können auch diese Off-chain-Funktion ausüben.¹¹⁵⁴ In der konkreten Ausgestaltung von Orderbuch und Matching-Engine sind Relayers frei.¹¹⁵⁵ Darüber hinaus sieht das Loopring-Protokoll ein Netzwerk von Computern vor, die Liquidität in Form von Aufträgen untereinander teilen. Auch diese Funktion, deren konkrete Ausgestaltung den Relayers überlassen ist, wird in aller Regel von Relayers ausgeübt.¹¹⁵⁶ Die Rolle des Relayers steht grundsätzlich jedermann offen. Voraussetzung dafür ist allerdings eine technische Infrastruktur mit hoher Leistungsfähigkeit und Verfügbarkeit. Selbst wenn die dezentrale Handelsplattform nicht mehr erreichbar wäre, könnten Nutzer ihre Vermögenswerte mithilfe der Relayers zurück auf den Layer 1 übertragen.¹¹⁵⁷

Anders als Loopring und die Derivateplattform dYdX, die ausschliesslich das ZK-Rollup-Modell implementieren, wählt die dezentrale Handelsplattform DeversiFi den sog. Validium-Modus von StarkEx. Infolge Nutzung dieses Protokolls sind nochmals deutlich weniger Transaktionsdaten on-chain zu publizieren.¹¹⁵⁸ Demgegenüber übernehmen Relayers die Funktion der Datenspeicherung off-chain.

¹¹⁵² Siehe Buterin, Scalable blockchains, Youtube, *passim*.

¹¹⁵³ Siehe Wang et al., Loopring, 4 («A set of public and free smart contracts that [...] trustlessly settles and transfers tokens on behalf of users, [...]»); hinsichtlich DeversiFi siehe DeversiFi, What is DeversiFi, *passim*; vgl. ferner Gudgeon et al., in: Bonneau/Heninger, Layer-Two Blockchain Protocols, 212.

¹¹⁵⁴ Siehe Wang et al., Loopring, 4.

¹¹⁵⁵ Siehe Wang et al., Loopring, 5.

¹¹⁵⁶ Siehe Wang et al., Loopring, 3–4, 5.

¹¹⁵⁷ Siehe Wang, Withdraw from Loopring 3.1, *passim*; sodann Loopring, Loopring 3, *passim*; ferner DeversiFi, What is the purpose of the Data Availability Committee?, *passim*.

¹¹⁵⁸ Siehe StarkEx Docs V2, Data Availability Modes, *passim*.

Relayers in DiversiFi setzen sich aus einer geschlossenen Gruppe von bekannten Unternehmen zusammen. Diese Gruppe wird auch als Data Availability Committee bezeichnet.¹¹⁵⁹ Diese Plattform scheint in dieser Hinsicht zentralisierter als Loopring und dYdX zu sein.

Die Loopring-Handelsplattform sieht einen eigenen Utility-Token vor. Auf Ethereum hat der Token das Kürzel «LRC».¹¹⁶⁰ Der LRC-Token wird auf der Plattform insb. dazu gebraucht, um Gebühren zu bezahlen. Es werden im Wesentlichen zwei Gebührentypen unterschieden: Taker zahlen einerseits Handelsgebühren an die Liquiditätspools (AMM-Modell) bzw. Maker (Orderbuchmodell) im Zusammenhang mit einem Handelsgeschäft und andererseits Transaktionsgebühren an die Relayers für die von ihnen erbrachten Dienstleistungen. Von den Transaktionsgebühren ist ein bestimmter Prozentsatz als Protokollgebühren für Liquiditätsgeber, einen Versicherungsfonds für allfällige Schäden aufgrund von Programmierfehlern in Smart Contract und DAO-Teilnehmer für deren Beteiligung an der Fortentwicklung der Plattform reserviert.¹¹⁶¹

AMM-Liquiditätsgeber und Market Makers werden zusätzlich durch Liquidity Mining-Programme bzw. Rabatte dazu incentiviert, Liquidität auf die Handelsplattform zu bringen.¹¹⁶² Einmal mehr zeigt sich, dass die Liquiditätsfrage im Zentrum der von einem Protokoll eingesetzten Anreizmechanismen steht. Angesichts der Vielzahl von Layer-2-Plattformen ist die Frage berechtigt, ob dadurch nicht eine Fragmentierung der vorhandenen Liquidität verursacht wird.

d. Weiterentwicklungen

Vergleichbare Skalierungspotenziale sind auch mit Optimistic Rollups realisierbar.¹¹⁶³ Uniswap V3 etwa hat im Sommer 2021 ihr Layer-1-AMM-Modell auf den Layer-2-Rollups *Optimism*¹¹⁶⁴ und *Arbitrum*¹¹⁶⁵ implementiert.¹¹⁶⁶ Ähnliches gilt für die Derivateplattform Synthetix.¹¹⁶⁷ Es sei darauf hingewiesen,

¹¹⁵⁹ Siehe DeversiFi, What is the purpose of the Data Availability Committee?, *passim*.

¹¹⁶⁰ Siehe Wang et al., Loopring, 8.

¹¹⁶¹ Siehe Finestone, LRC Tokenomics, Medium, *passim*.

¹¹⁶² Siehe für weitere Hinweise Loopring, How to use the L2 Loopring Exchange, *passim*.

¹¹⁶³ Siehe zu Optimistic Rollups oben, [III.5.2d](#).

¹¹⁶⁴ <https://optimism.io/>.

¹¹⁶⁵ <https://arbitrum.io/>.

¹¹⁶⁶ Siehe Uniswap, Introducing Uniswap V3, *passim*; Uniswap, Uniswap on Optimism, *passim*; Uniswap, Uniswap on Arbitrum, *passim*.

¹¹⁶⁷ Siehe für eine Übersicht der Entwicklungen Synthetix Community, Layer 2, *passim*.

dass auch Optimistic Rollups über die Funktion «Force Withdraw» verfügen, welche den Nutzern die Möglichkeit gibt, einseitig die Vermögenswerte aus dem Layer-2-Protokoll zurückzuziehen.¹¹⁶⁸

Eine Layer-2-Handelsplattform, die Ähnlichkeiten mit den bereits erwähnten Atomic Swap-basierten P2P-Plattformen aufweist, ist Boltz. Boltz ist ein Protokoll, das es erlaubt, bitcoins, die sich in Layer-2-Kanälen des Lightning Netzwerks befinden (LN-BTC), gegen Layer-1-bitcoins (BTC) zu tauschen. Der umgekehrte Vorgang ist ebenso möglich. Dasselbe gilt derzeit für litecoins und ethers bzw. gewisse ERC-20 Tokens.¹¹⁶⁹

Anders als Atomic Swap-basierte P2P-Handelsplattformen handelt es sich bei Boltz um On-chain-off-chain bzw. Off-chain-on-chain Atomic Swaps (z.B. BTC zu LN-BTC). Hinzukommen kann eine Cross-chain-Komponente. Damit sind selbst Cross-chain Atomic Swaps von Vermögenswerten verschiedener Layers der involvierten Blockchains möglich (z.B. LN-BTC zu LTC).¹¹⁷⁰ Diese Form von Semi-on-chain Atomic Swaps werden auch *Submarine Swaps* genannt.¹¹⁷¹

Soweit es sich darüber hinaus um ein Handelsgeschäft ausschliesslich über das Bitcoin Lightning Netzwerk handelt (d.h. Off-chain-off-chain Atomic Swap), ist der Austausch von Kryptovermögenswerten zwischen zwei Parteien unverzüglich. Auch hier ist es möglich, Cross-chain Atomic Swaps durchzuführen (z.B. LN-BTC zu LN-LTC).¹¹⁷²

Sparkswap ist eine Open-Source-Software, welche eine Handelsplattform nach dem Orderbuchmodell für Off-chain Cross-chain Atomic Swaps möglich macht.¹¹⁷³ Dasselbe gilt für die Plattform OpenDEX, die neben dem Lightning Netzwerk auf dem Ethereum-Layer-2-Netzwerk Connex aufbaut.¹¹⁷⁴

¹¹⁶⁸ Siehe Optimism, Optimistic Sequencing, *passim*.

¹¹⁶⁹ Siehe Boltz, Frequently Asked Questions, *passim*.

¹¹⁷⁰ Siehe hierzu auch die Ausführungen bei Miraz/Donald, ICISDM 2019: Proceedings of the 2019 3rd International Conference on Information System and Data Mining 2019, 187 («This feature of [Lightning Network] not only enables off-chain atomic cross-chain swaps [...], but also materialises the notion of decentralised exchanges, as each [Lightning Network] node having channels linked to multiple blockchain networks can act as a decentralised exchange.»); ferner zur Unterscheidung zwischen On-chain und Off-chain Atomic Swaps Miraz/Donald, Annals of Emerging Technologies in Computing 2019, 45–46.

¹¹⁷¹ Siehe michael1011, Submarine Swaps, Medium, *passim*.

¹¹⁷² Siehe Fromknecht, Connecting Blockchains, *passim*; ferner hierzu Miraz/Donald, Annals of Emerging Technologies in Computing 2019, 46.

¹¹⁷³ Siehe Griffith, sparkswap, Medium, *passim*; ferner Harper, Sparkswap, Bitcoin Magazine, *passim*.

¹¹⁷⁴ Siehe OpenDEX, OpenDEX Features, *passim*.

Schliesslich bieten auch andere dezentrale Netzwerke ihren Nutzern Zugang zu Layer-2-Handelsplattformen. Im Falle der Polkadot Blockchain ist namentlich *Polkadex Orderbook*¹¹⁷⁵ zu erwähnen. Es handelt sich um eine auf dem Polkadex Netzwerk ausgeführte dezentrale Handelsplattform nach dem Orderbuchmodell.¹¹⁷⁶

3.10 On-chain-Handelsplattformen

a. Hintergrund

Die meisten DeFi-Anwendungen laufen derzeit auf der Ethereum Blockchain. Ethereum befindet sich allerdings in einer Phase grundlegenden technologischen Wandels. Um höheren Transaktionslasten Rechnung tragen zu können, soll der Konsensalgorithmus der Netzwerkteilnehmer von derzeit PoW auf künftig PoS umgestellt werden. Hinzukommt, dass Ethereum 2.0 sich künftig nicht aus einer, sondern mehreren Shards zusammensetzen soll, die über eine gemeinsame Main Chain miteinander kommunizieren.¹¹⁷⁷

Dezentrale Handelsplattformen auf Ethereum erben unglücklicherweise nicht nur die positiven Sicherheitseigenschaften des Netzwerks, sondern auch dessen begrenzten Datenverarbeitungskapazitäten. Die beschränkten Datenverarbeitungskapazitäten von Ethereum haben insb. im Bereich dezentraler Handelsplattformen einen Entwicklungsschub auf anderen Blockchains ausgelöst. Dazu gehören etwa die Blockchains von *Polkadot*¹¹⁷⁸, *Solana*¹¹⁷⁹ und *Avalanche*¹¹⁸⁰. Diese jüngeren dezentralen Netzwerke gelten als skalierungsfähiger als Ethereum.

In der Folge werden alle Handelsschritte dezentraler Handelsplattformen wieder vollständig on-chain programmiert. Angetrieben wird dies v.a. durch das Bedürfnis, wirtschaftlich effizientere dezentrale Handelsplattformen zu realisieren. Das beliebte AMM-Modell auf Ethereum hat diesem Bedürfnis bisher

¹¹⁷⁵ <https://www.polkadex.trade/>.

¹¹⁷⁶ Siehe Polkadex, *Polkadex Orderbook*, *passim*.

¹¹⁷⁷ Siehe hierzu oben, III.5.1.

¹¹⁷⁸ <https://polkadot.network/>.

¹¹⁷⁹ <https://solana.com/>.

¹¹⁸⁰ <https://www.avalabs.org/>.

nicht vollständig gerecht werden können. Das Orderbuchmodell gilt darum weiterhin als die allokativ effizienteste Form des Handels mit Vermögenswerten.¹¹⁸¹

Frühe Vertreter dieser Plattformkategorie sind insb. *BitShares DEX*¹¹⁸², *NewDEX*¹¹⁸³, das *Stellar DEX Protokoll*¹¹⁸⁴ und *Binance DEX*¹¹⁸⁵. Aufgrund der beschränkten Dezentralität der zugrundeliegenden Netzwerke (d.h. BitShares, EOS¹¹⁸⁶, Stellar¹¹⁸⁷ und Binance [Smart] Chain¹¹⁸⁸) werden diese Plattformen vorliegend jedoch den hybriden Handelsplattformen zugeordnet (siehe unten).

b. Funktionsweise am Beispiel von Serum

Alle Handelsschritte einer On-chain-Handelsplattform, d.h. von der Führung des Orderbuchs über die Matching-Engine bis hin zur Abwicklung der Transaktionen, laufen vollständig auf der Blockchain ab. Sie werden mit anderen Worten direkt innerhalb des dezentralen Netzwerks ausgeführt. Insofern könnte auch von einer technischen Weiterentwicklung von Smart Contract-basierten Plattformen, wie etwa OasisDEX oder Uniswap, gesprochen werden. Allerdings werden On-chain-Handelsplattformen aus den oben erwähnten Gründen derzeit nicht auf Ethereum entwickelt, weshalb vorliegend von einer grundsätzlich neuen Plattformkategorie ausgegangen wird.

Vonseiten des Netzwerks setzen On-chain-Handelsplattformen rasche Abwicklungszeiten voraus. Das Open-Source-Projekt *Serum*¹¹⁸⁹ wird entsprechend auf der *Solana Blockchain* entwickelt, die ein Vielfaches der Transak-

¹¹⁸¹ So etwa Qureshi, Unbundling Uniswap, Medium, *passim*.

¹¹⁸² <https://wallet.bitshares.org/>; siehe für mehr Informationen zur Handelsplattform BitShares, Decentralized Exchange, *passim*.

¹¹⁸³ <https://newdex.io/>.

¹¹⁸⁴ Z.B. <https://www.stellarx.com/>, <https://stellarterm.com/> und <https://stellarport.io/>.

¹¹⁸⁵ <https://www.binance.org/>.

¹¹⁸⁶ Siehe hinsichtlich der EOS Blockchain O'Neal, Decentralization Is Not Its Priority, Cointelegraph, *passim*; ebenfalls kritisch hinsichtlich der Verwendung von DPoS Schrepel, Harvard Journal of Law & Technology 2019, 138; ferner Werbach, New Architecture of Trust, 57.

¹¹⁸⁷ Siehe hinsichtlich der Stellar Blockchain O'Neal, Stellar's Blockchain Briefly Goes Offline, Cointelegraph, *passim* m.w.H.

¹¹⁸⁸ Changpeng «CZ» Zhao, CEO von Binance, bezeichnet die Binance Blockchains angesichts der beschränkten Dezentralität als CeDeFi, ein Kofferwort aus Centralized Finance und Decentralized Finance, vgl. Shen, Binance's CZ Views, Coindesk, *passim*; ferner, wobei in erster Linie die Webseite <https://www.binance.org> betroffen ist, Zmudzinski, Binance DEX Website Will Geoblock Users From 29 Countries, Cointelegraph, *passim*.

¹¹⁸⁹ <https://projectserum.com/>.

tionen pro Zeiteinheit der Ethereum Blockchain verarbeiten kann, ohne dafür angeblich grössere Einbussen bei der Dezentralität des Netzwerks in Kauf zu nehmen.¹¹⁹⁰

Vereinfacht gesagt, ist die dezentrale Handelsplattform Serum ein Smart Contract bzw. ein *Programm*, das auf Solana ausgeführt wird.¹¹⁹¹ Um Kryptovermögenswerte zu handeln, übertragen Nutzer aus ihrem Wallet Vermögenswerte in ihr «Handelskonto» (*Intermediary Account*). Anschliessend platzieren sie eine Order im Orderbuch, die mit einer passenden Gegenorder zusammengeführt wird. Abschliessend können Nutzer die Vermögenswerte aus ihrem Handelskonto auf ihr persönliches Wallet zurückübertragen (*Settlement*). Nutzer können ausserdem Orders, die nicht mehr ihren initialen Präferenzen entsprechen, löschen.¹¹⁹² Orderbuch und Matching erfolgen automatisiert innerhalb des auf der Solana Blockchain abgelegten Programms. Im Gegensatz zum AMM-Modell können Nutzer ihre Orders etwa hinsichtlich Menge, Preis und Auftragsart frei bestimmen.¹¹⁹³

Schliesslich erlaubt Serum auch die Implementierung von AMMs (z.B. *BonfidaSwap*¹¹⁹⁴) und von Cross-chain Atomic Swaps zwischen unterschiedlichen Blockchains.¹¹⁹⁵ In ähnlicher Weise weisen die Blockchains Avalanche und Polkadot ebenfalls dezentrale Handelsplattformen nach dem AMM-Modell auf.¹¹⁹⁶

c. Beteiligte Parteien am Beispiel von Serum

An einem Austauschgeschäft auf Serum sind lediglich die beiden Parteien des betreffenden Geschäfts beteiligt. Alle übrigen Komponenten der dezentralen Handelsplattform laufen deterministisch innerhalb des Programms ab. Davon ausgenommen ist lediglich die unregelmässige Aktualisierung der Matching-Engine, die systembedingt einer Instruktion bedarf, da Computercode nicht von selbst ausgeführt wird. Dafür sind die Serum-Netzwerkteilnehmer verant-

¹¹⁹⁰ Siehe hierzu Yakovenko, Solana, *passim*.

¹¹⁹¹ Siehe Serum, Technical introduction to the Serum DEX, 1, 3.

¹¹⁹² Ausführlich Serum, Technical introduction to the Serum DEX, 4–9.

¹¹⁹³ Siehe Serum Foundation, White Paper, 5, 9.

¹¹⁹⁴ <https://swap.bonfida.com>.

¹¹⁹⁵ Siehe Serum Foundation, White Paper, 7–9.

¹¹⁹⁶ Siehe für Avalanche z.B. <https://pangolin.exchange/>; für Polkadot z.B. <https://polkaswap.io/>.

wortlich.¹¹⁹⁷ Ein Frontend zu Serum wird von mehreren Webseiten¹¹⁹⁸ angeboten.¹¹⁹⁹ Ein GUI zum Serum-Programm auf der Solana Blockchain kann ausserdem von jedermann aufgesetzt werden.¹²⁰⁰

Im Zusammenhang mit Austauschgeschäften auf Serum fallen neben Transaktions- auch Handelsgebühren an.¹²⁰¹ Während die Transaktionsgebühren an die Netzwerkteilnehmer der Solana Blockchain gehen, fallen die Handelsgebühren je nach Verteilungsschlüssel den Netzwerkteilnehmern, GUI-Betreibern sowie einer Community-Wallet zu, deren Gebühren derzeit allerdings mehrheitlich vernichtet werden.¹²⁰²

d. Weiterentwicklungen

THORSwap¹²⁰³ ist ein Protokoll, das wie Cross-chain Atomic Swaps den effektiven Austausch von Kryptovermögenswerten unterschiedlicher Blockchains möglich macht. Das Protokoll implementiert zu diesem Zweck ein dezentrales Netzwerk mit eigenständigem Konsensalgorithmus namens THORChain.¹²⁰⁴ Wenn ein Nutzer etwa BTC zu USDT tauschen möchte, stellen die Netzwerkteilnehmer durch Beobachtung bestimmter Adressen auf den involvierten Blockchains (sog. *Vault Addresses*) sicher, dass die Ausgangstransaktion in USDT erst ausgelöst wird, nachdem die Eingangstransaktion in BTC erfolgt ist.¹²⁰⁵ Die Vermögenswerte für die Vaults werden durch Liquiditätsgeber, die dafür entschädigt werden, zur Verfügung gestellt.¹²⁰⁶ Es besteht insofern eine Ähnlichkeit zu Smart Contract-basierten Liquiditätspools.

¹¹⁹⁷ Siehe Serum, Technical introduction to the Serum DEX, 6–7; vgl. in allgemeiner Hinsicht zu dieser *Keeper*-Funktion Werner et al., *Decentralized Finance*, 3; in Ethereum Harvey/Ramachandran/Santoro, *DeFi*, 48–49, 55–56, 59.

¹¹⁹⁸ So z.B. über <https://dex.projectserum.com>, <https://bonfida.com/dex>, <https://dex.raydium.io> oder <https://trade.mango.markets/>.

¹¹⁹⁹ Siehe Serum Academy, Serum DEX List, *passim*.

¹²⁰⁰ Siehe Project Serum, Serum DEX UI, GitHub, *passim*.

¹²⁰¹ Siehe Serum Foundation, White Paper, 9.

¹²⁰² Siehe Serum Foundation, White Paper, 6; Serum, Technical introduction to the Serum DEX, 14; für eine aktuelle Übersicht des Verteilungsschlüssels siehe Project Serum, Fees, *passim*.

¹²⁰³ <https://thorswap.finance/>.

¹²⁰⁴ Siehe THORSwap, What is THORSwap, *passim*; ausführlich thorchain.org, THORChain TSS, *passim*.

¹²⁰⁵ Siehe für Details eines Swaps THORChain, Technology, *passim*.

¹²⁰⁶ Siehe THORChain, Continuous Liquidity Pools, *passim*.

3.11 Hybride Handelsplattformen

a. Hintergrund

Die wohl älteste und bekannteste hybride Handelsplattform ist IDEX¹²⁰⁷. Bereits im September 2017 ging die Plattform live. Dabei nahmen die Entwickler einige wesentliche Änderungen gegenüber den Wegbereitern EtherDelta und OasisDEX vor.¹²⁰⁸ Motiviert waren die Entwickler von den bereits erwähnten Schwächen dieser Smart Contract-basierten P2P-Handelsplattformen.¹²⁰⁹ Konkret war beabsichtigt, dass *neu* nicht nur das Orderbuch, sondern auch die Handelsausführung vollständig off-chain ablaufen sollen.¹²¹⁰

b. Funktionsweise am Beispiel von IDEX

Erwähnenswert am IDEX-Modell ist die Tatsache, dass das Orderbuch und die Handelsausführung zentralisiert sind. Alle Handelsschritte bis zur Handelsabwicklung erfolgen somit *direkt* auf den Servern des Plattformbetreibers bzw. über einen Smart Contract, welcher in beschränktem Ausmass vom Plattformbetreiber kontrolliert wird.¹²¹¹ Erst die Abwicklung der Geschäfte erfolgt auf dem dezentralen Netzwerk. Der Hauptvorteil von IDEX gegenüber anderen dezentralen Handelsplattformen ist die Reduktion der Anzahl an On-Chain-Transaktionen, was letztlich den Nutzern Gaskosten einspart.¹²¹² Damit bestehen deutliche Ähnlichkeiten zwischen IDEX und zentralen Kryptohandelsplattformen bzw. traditionellen Handelsplattformen.¹²¹³ So werden Aufträge innert Bruchteilen einer Sekunde über das Orderbuch zusammen- und ausgeführt, deren Abwicklung auf der Blockchain erfolgt allerdings erst zu einem späteren Zeitpunkt.¹²¹⁴

¹²⁰⁷ <https://index.io/>.

¹²⁰⁸ Siehe hierzu Kiepuszewski, OasisDEX, Youtube, *passim*.

¹²⁰⁹ Siehe Aurora Labs, IDEX, 2.

¹²¹⁰ Siehe IDEX, History of DEXs: Phase 3, *passim*.

¹²¹¹ Siehe Aurora Labs, IDEX, 2; ferner Bearle, Why IDEX is centralized, Medium, *passim*.

¹²¹² Siehe Aurora Labs, IDEX, 3–4.

¹²¹³ Siehe IDEX, IDEX 2.0, 6.

¹²¹⁴ Siehe IDEX, IDEX 2.0, 6.

Die Derivateplattform *dYdX*¹²¹⁵ nutzt ebenfalls zentralisierte Komponenten (Orderbuch und Order Matching), um die Handelsausführung zu beschleunigen.¹²¹⁶ Insofern könnte die Plattform auch den hybriden Plattformen zugeordnet werden.

Der wesentliche Unterschied zum zentralen Handelsplattformmodell besteht darin, dass die Nutzer von IDEX vor Auftragserteilung die Vermögenwerte in einem Smart Contract zu deponieren haben, der bis zur Abwicklung die Funktion eines Escrows übernimmt.¹²¹⁷ Die von den Nutzern autorisierten und erfolgreich im Orderbuch zusammengeführten Aufträge werden sodann zwecks Abwicklung auf der Blockchain in eine Warteschleife gestellt. IDEX autorisiert schliesslich in bestimmten Zeitintervallen über ihr *Arbiter*-Protokoll die Abwicklung der Handelsgeschäfte auf dem dezentralen Netzwerk.¹²¹⁸ Zu erwähnen ist, dass IDEX nur diejenigen Handelsgeschäfte zwecks Abwicklung an das dezentrale Netzwerk senden kann, welche von den Nutzern mittels ihres Private Keys autorisiert worden sind.¹²¹⁹ Nutzer können zudem ihre Vermögenwerte aus dem Smart Contract erst zurückziehen, nachdem alle Geschäfte abgewickelt worden sind.¹²²⁰ Sollten die Server von IDEX für eine längere Zeit nicht mehr erreichbar sein, haben Nutzer die Möglichkeit, einseitig die Vermögenwerte aus den Smart Contracts nach Ablauf einer Frist zurückzuziehen.¹²²¹

Eine weitere hybride Handelsplattform ist nach vorliegender Auffassung sodann *AirSwap*¹²²². Im Gegensatz zu IDEX erlaubt das zugrundeliegende Protokoll aber für deutlich dezentralere Implementierungen. AirSwap verbindet Elemente einer Escrow-basierten P2P-Handelsplattform mit denjenigen einer Smart Contract-basierten P2P-Handelsplattform, verzichtet dabei jedoch auf ein klassisches Orderbuch. AirSwap sieht anstelle eines automatisierten Orderbuchs ein Request for Quote (RFQ)-System vor. Konkret können Nutzer (Maker) über die Plattform ihre blossen *Handelsabsicht* bekunden. Interessierte Marktteilnehmer (Taker) können sodann in konkrete Verhandlungen mit ei-

¹²¹⁵ Vgl. hierzu auch oben, IV.3.9c.

¹²¹⁶ Siehe Juliano, *dYdX*, 4; sodann Howard, *Decentralized Exchanges*, Cointelegraph, *passim*; ferner hinsichtlich der Layer-2-Lösung *dYdX*, General, *passim*.

¹²¹⁷ Vgl. hinsichtlich des von IDEX verwendeten Smart Contracts die folgende Adresse <https://etherscan.io/address/0x2a0c0dbecc7e4d658f48e01e3fa353f44050c208>.

¹²¹⁸ Ausführlich IDEX, *IDEX 2.0*, 7–8.

¹²¹⁹ Siehe IDEX, *IDEX 2.0*, 8.

¹²²⁰ Siehe Aurora Labs, *IDEX*, 4.

¹²²¹ Siehe Dunning_Krugerrands, *Reddit*, *passim*.

¹²²² <https://www.airswap.io/>, <https://trader.airswap.io/>.

nem Maker treten. Die Details eines Handelsgeschäfts werden zwischen den Parteien off-chain mithilfe eines separaten Kommunikations- und Matching-Protokolls (*Indexer*) manuell verhandelt. Sobald eine Einigung vorliegt, kann der Taker einen für den Maker verbindlichen Auftrag an den Smart Contract senden. Anschliessend erfolgt die Abwicklung des Auftrages on-chain mithilfe des bereits angerufenen Smart Contracts.¹²²³

c. Beteiligte Parteien am Beispiel von IDEX

Im Zentrum der IDEX-Plattform steht die Betreiberin Aurora Labs S.A. Die zentralen Komponenten der IDEX-Plattform haben vermutlich die Betreiberin dazu bewogen, bereits im November 2018 zu beschliessen, eine KYC-Policy einzuführen.¹²²⁴ Dass das SEC-Verfahren gegen COBURN in Sachen EtherDelta eine Rolle dabei gespielt hat, kann nicht ausgeschlossen werden.

Seit Einführung der KYC-Policy bedarf die Nutzung von IDEX eines Nutzerkontos.¹²²⁵ Bewohner gewisser Nationen und Regionen sind gänzlich von der Nutzung der Plattform ausgeschlossen.¹²²⁶

d. Weiterentwicklungen

Eine hybride Plattform, welche ebenfalls auf Smart Contracts setzt, allerdings AMM-Pools à la Balancer vorsieht, ist *Swarm Markets*.¹²²⁷ Swarm Markets wird von Swarm Capital GmbH mit Sitz in Deutschland betrieben. Nutzer haben grundsätzlich vollständige Kontrolle über ihre Vermögenswerte. Die Plattform hat allerdings einen Compliance-Layer implementiert. Hierzu gehören KYC und die Möglichkeit der Betreibergesellschaft, bei Bedarf einzelne Nutzer bzw. deren Vermögenswerte in den Smart Contracts zu blockieren.¹²²⁸

¹²²³ Siehe Oved/Mosites, Swap, 4–8; ferner AirSwap, FAQ, How does trading on AirSwap work?, *passim*; sodann Schär, Federal Reserve Bank of St. Louis Review 2021, 163.

¹²²⁴ Siehe Wearn, Pragmatic Decentralization, *passim*.

¹²²⁵ Siehe IDEX, Terms of Service and Privacy, 3. Identity Verification, *passim* («When you access the Services or create an Account, we will ask for your name, physical address, mailing address, date of birth, and other information that will allow us to identify you.»).

¹²²⁶ Siehe IDEX, Terms of Service and Privacy, 7. Restricted Jurisdictions, *passim*.

¹²²⁷ <https://swarm.markets/>.

¹²²⁸ Siehe Swarm Markets, FAQ, *passim*; ferner Morris, DeFi Is Like Nothing Regulators Have Seen Before, Coindesk, *passim*.

Die IDEX-Plattform setzt ihr Modell künftig über eine Layer-2-Lösung um. Damit lässt sich die Zahl der heute notwendigen On-chain-Transaktionen weiter senken. Ähnlich einer zentralen Kryptohandelsplattform sollen nur noch die Einzahlung (*deposit*) und der Rückzug (*withdrawal*) von Kryptovermögenswerten on-chain ausgeführt werden müssen. Demgegenüber sollen die einzelnen Vermögensstände der Wallet-Adressen nicht mehr im Smart Contract selbst, sondern in einem Off-chain-Register abgespeichert werden. Im Ergebnis sollen nur noch die Proofs der einzelnen Layer-2-Transaktionen an das dezentrale Netzwerk übertragen werden.¹²²⁹

Weitere Beispiele von hybriden Handelsplattformen sind etwa Plattformen, die über *Sidechains* implementiert werden. Sidechains sind Layer-2-Netzwerke, die anders als Rollups den Konsensalgorithmus und somit die Sicherheit des dezentralen Netzwerks erster Ordnung nicht übernehmen.¹²³⁰ Aufgrund des eigenständigen Risiko- und Vertrauensmodells werden Sidechain-basierte Plattformen vorliegend den hybriden Handelsplattformen zugerechnet. Zu solchen Plattformen gehören z.B. TDEX¹²³¹, die auf Bitcoins Liquid Netzwerk¹²³² beruht, und Demex¹²³³, welche eine multi-chain-fähige Handelsplattform auf der Sidechain Switchero TradeHub¹²³⁴ darstellt.

Aus vergleichbaren Überlegungen werden auch beschränkt dezentralisierte On-chain-Handelsplattformen vorliegend als hybride Handelsplattformen eingestuft.¹²³⁵

3.12 Übersicht der Plattformkategorien

Die nachfolgende Tabelle stellt eine vereinfachende Übersicht über die wichtigsten Differenzierungsmerkmale der unterschiedlichen Handelsplattformen dar:

¹²²⁹ Ausführlich IDEX, IDEX 2.0, 12–13.

¹²³⁰ Siehe hierzu oben, III.5.2c.

¹²³¹ <https://specs.tdex.network/>.

¹²³² <https://liquid.net/>.

¹²³³ <https://dem.exchange/>.

¹²³⁴ Siehe hierzu Switchero TradeHub, Introduction, *passim*.

¹²³⁵ Siehe für einige Beispiele oben, IV.3.9a.

	Verwahrung	Handel	Abrechnung und Abwicklung	Zugang
Custodial HP	Custodial	Off-chain	Off-chain	Eingeschränkt
Custodial OTC-HP	Custodial	Off-chain	Off-chain	Eingeschränkt
Non-custodial P2O-HP	Non-custodial	Off-chain	On-chain	Eingeschränkt*
Escrow-basierte P2P-HP	Non-custodial	Off-/On-chain	On-chain	Offen*
Atomic Swap-basierte P2P-HP	Non-custodial	Off-/On-chain	On-chain	Offen*
Smart Contract-basierte P2P-HP	Non-custodial	Off-/On-chain	On-chain	Offen
Smart Contract-basierte Liquiditätspools	Non-custodial	On-chain	On-chain	Offen
Smart Contract-basierte Aggregatoren	Non-custodial	Off-/On-chain	On-chain	Offen
Layer-2-HP	Non-custodial	Off-chain (Layer 2)	Off-chain (Layer 2)/ On-chain	Offen
On-chain-HP	Non-custodial	On-chain	On-chain	Offen
Hybride HP	Non-custodial	Off-/On-chain	On-chain	Eingeschränkt*

* = Regelfall

4. Gemeinsamkeiten und Unterschiede dezentraler Handelsplattformen

4.1 Gemeinsamkeiten

a. Kontrolle über Kryptovermögenswerte

Eine zentrale Gemeinsamkeit aller dezentralen Handelsplattformen ist die Tatsache, dass Nutzer die Verfügungsmacht über ihre Kryptovermögenswerte behalten. Dies gilt so lange, als dass ein Nutzer Zugriff auf das Wallet hat, in welchem Private Keys gespeichert abgespeichert sind. In diesem Zusammenhang wird von *Non-Custodial*-Applikationen gesprochen. Die Wallets selbst werden in der vorliegenden Arbeit als Self-Hosted Wallets bezeichnet. Sie unterscheiden sich von einem Konto, welches etwa auf der Grundlage personenbezogener Informationen erstellt wird.

Der Grundsatz der Kontrolle ist dort zu relativieren, wo ein Nutzer im Rahmen der Handelsausführung Kryptovermögenswerte vorübergehend in einem Smart Contract zu hinterlegen hat (so z.B. EtherDelta, AtomicDEX, IDEX, Uniswap). In diesem Fall unterliegen die Vermögenswerte der codierten Ausführungslogik des eingesetzten Smart Contracts. Falls jedoch ausschliesslich der Hinterleger über die im Smart Contract gehaltenen Vermögenswerte verfügen kann, ist die Kontrolle weiterhin gewährleistet.

Für gewisse Plattformkategorien, wie etwa Escrow-basierte P2P-Handelsplattformen, ist aufgrund der Umstände im Einzelfall zu entscheiden, ob der Nutzer effektiv die Kontrolle über die Vermögenswerte behält.

b. On-chain-Handelsabwicklung

Eine weitere zentrale Gemeinsamkeit aller dezentralen Handelsplattformen ist die Tatsache, dass die Handelsabwicklung bzw. das Settlement on-chain erfolgt. Dezentrale Handelsplattformen müssen ein On-chain-Settlement der Transaktionen vorsehen, weil andernfalls die Vermögenswerte beim bisherigen Besitzer verbleiben würden. Ein Austauschgeschäft kann als abgeschlossen bezeichnet werden, wenn die Übertragung eines Kryptovermögenswerts nach der Logik eines dezentralen Netzwerks innerhalb dessen verteilten Re-

gisters aufgezeichnet wurde. Dadurch erhält der Inhaber des Private Keys der Empfängeradresse die ausschliesslich Verfügungsmacht über die Vermögenswerte.

Dabei kann die Aufzeichnung die einzelne Transaktion an sich beinhalten oder aber wie im Falle von Layer-2-Handelsplattformen (z.B. Loopring) lediglich einen Nachweis einer Transaktion. Für dezentrale Handelsplattformen, die auf Layer-2-Netzwerken (z.B. Loopring, Bitcoin Lightning) aufbauen oder mithilfe von Sidechains implementiert werden, genügt es nach vorliegender Ansicht, dass Nutzer lediglich die Möglichkeit zur On-chain-Handelsabwicklung aufweisen. Solche dezentralen Handelsplattformen wickeln Austauschgeschäfte in erster Linie off-chain ab, Nutzer können aber bei Bedarf eine On-chain-Transaktion auslösen.

c. Handelbare Vermögenswerte

Auf allen dezentralen Handelsplattformen werden *Kryptovermögenswerte* gehandelt, wobei je nach Plattform eine sehr unterschiedliche Auswahl bestehen kann. Am einfachsten ist der Handel von Kryptovermögenswerten *derselben* Blockchain.¹²³⁶ Alle Transaktionen finden somit innerhalb desselben verteilten Registers statt. So können typischerweise auf Ethereum-basierten dezentralen Handelsplattformen (z.B. EtherDelta und Uniswap) lediglich ETH und ERC-20 Tokens gehandelt werden.

Die Handelbarkeit von Kryptovermögenswerten *anderer* dezentraler Netzwerke auf Ethereum (z.B. BTC) bedarf demgegenüber separater Lösungen. Hierzu gehören etwa die Tokenisierung bzw. das Wrapping solcher Vermögenswerte in einem Token (so z.B. WBTC) oder die Verwendung von Smart Contracts bzw. sog. Bridges, welche die beiden dezentralen Netzwerke miteinander verbinden. Gewisse dezentrale Handelsplattformen erlauben den Austausch von Kryptovermögenswerten unterschiedlicher dezentraler Netzwerke mithilfe von Atomic Swaps (z.B. AtomicDEX), eigenständigen dezentralen Netzwerken mit doppelseitigen Asset Pegs (z.B. Liquid, RenBridge¹²³⁷, tBTC¹²³⁸) oder mit einseitigen Asset Pegs (z.B. THORSwap). Zu erwähnen ist, dass bei all diesen Lösungen die Kryptovermögenswerte die jeweiligen Blockchains nicht verlassen. Sie werden lediglich dort in einem Smart Contract oder einem ähnlichen Mechanismus «parkiert» (*locked*). Umbuchungen innerhalb unter-

¹²³⁶ Siehe auch Lin, Stanford Journal of Blockchain Law & Policy 2019, 60.

¹²³⁷ <https://bridge.renproject.io/>.

¹²³⁸ <https://tbtc.network/>.

schiedlicher verteilter Register sind demnach nicht möglich. Beim Wrapping werden zudem auf der zweiten Blockchain neue Kryptovermögenswerte geschaffen (mint). Ein Nutzer des Protokolls kann schliesslich die hinterlegten Vermögenswerte wieder auslösen, indem er die Kryptovermögenswerte der zweiten Blockchain vernichtet (burn).¹²³⁹

Interoperabilitäts-Lösungen sind nicht in jedem Fall gänzlich frei von Intermediären, wie etwa die Beispiele von WBTC und Liquid zeigen.¹²⁴⁰ Allerdings sind jeweils eine Mehrzahl von Personen involviert.¹²⁴¹ Lösungen, wie etwa Ren-Bridge und tBTC, greifen demgegenüber auf dezentrale Netzwerke zurück, in welchen die Teilnehmer einen bestimmten Betrag als Sicherheit hinterlegen müssen. Bei Verstoß gegen die Protokollregeln des Netzwerks wird die Sicherheit vom Netzwerk beschlagnahmt.¹²⁴² Die verwendeten Smart Contracts können sodann aus Nutzersicht Admin Key-Risiken einführen.¹²⁴³ Aufgrund der derzeitigen Entwicklungen ist es absehbar, dass die Interoperabilität unterschiedlicher Blockchains und somit die Verfügbarkeit von Kryptovermögenswerten über mehrere dezentrale Netzwerke hinweg künftig noch stark optimiert werden.

Grundsätzlich ausgeschlossen vom Handel sind demgegenüber *Fiatwährungen*. Der dezentrale Handel von Fiatwährungen, die in digitaler Form immer eine Schuld des jeweiligen Emittenten darstellen, ist aus technischen Gründen nicht möglich. Die buchmässige Erfassung von Fiatwährungen erfolgt letztlich zentral beim Emittenten, sodass für ein reibungsloses Zusammenspiel ein Intermediär ins dezentrale System eingeführt werden müsste.¹²⁴⁴ Dies ist ein wesentlicher Unterschied zu zentralisierten Kryptohandelsplattformen, so dass ein Grossteil von Nutzern anfänglich über einen Intermediär die ersten Kryptovermögenswerte erwirbt. Eine Ausnahme bilden Escrow-basierte P2P-Handelsplattformen, deren Handelsausführung überwiegend off-chain erfolgt (so z.B. Bisq).

¹²³⁹ Siehe MakerDAO Blog, What Are Blockchain Bridges, *passim*.

¹²⁴⁰ Siehe Kyber Network/BitGo Inc/Republic Protocol, Wrapped Tokens, 2, 13; ferner Tran, What is WBTC?, Decrypt, *passim* («Since there is still a gap between Bitcoin and Ethereum – the chains can't natively talk to each other – trust in people is required. Compared to BTC, Wrapped BTC will never have the same level of security or trustlessness as the original because it relies on people and organizations to manage the system instead of pure code.»).

¹²⁴¹ Vgl. hinsichtlich wBTC Harvey/Ramachandran/Santoro, DeFi, 128–129.

¹²⁴² Siehe RenProject, Darknodes, GitHub, *passim*; ferner tBTC, Security Model, *passim*.

¹²⁴³ Siehe zu Admin Key-Risiken ausführlich unten, [IV.5.2d.ii](#).

¹²⁴⁴ Siehe Warren, Decentralized Exchange, *passim*.

Fiatwährungen sind aber insoweit Bestandteil des Universums dezentraler Handelsplattformen, als dass *Stablecoins* Fiatwährungen als Referenzwert verwenden. Im Falle von *Stablecoins*, die mit Fiatwährung hinterlegt sind (z.B. USDT und USDC), hat dem Handel dieser Tokens die Tokenisierung der Fiatwährung vorauszugehen. Vorstellbar wäre schliesslich, dass Intermediäre künftig eine Fiat-Anbindung an dezentrale Handelsplattformen anbieten, indem sie für ihre Kunden Wallets führen.

Grundsätzlich keine Voraussetzung von dezentralen Handelsplattformen ist die Fungibilität der zugrundeliegenden Vermögenswerte. So können auch NFTs über eine dezentrale Handelsplattform getauscht werden, soweit die Plattform einen solchen Standard unterstützt. Typischerweise werden NFTs über spezialisierte Auktionsplattformen versteigert.¹²⁴⁵

4.2 Unterschiede

a. Orderbuch vs. Liquiditätspools

Der Hauptunterschied zwischen dezentralen Handelsplattformen besteht in erster Linie in der Frage, ob eine dezentrale Handelsplattform ein Orderbuch unterhält oder Liquiditätspools vorsieht. Damit zusammenhängend wird differenziert danach, ob eine Transaktion Peer-to-Peer oder Peer-to-Pool ausgeführt wird. In der Literatur wird terminologisch auch zwischen «Exchange» und «Swap» unterschieden.¹²⁴⁶ Diese rein begriffliche Unterscheidung wird vorliegend nicht benutzt, denn in beiden Fällen findet der Austausch bzw. Swap von Token statt.¹²⁴⁷

Im Fall von *Peer-to-Peer*-Plattformen werden die Aufträge zweier Nutzer unmittelbar zusammengeführt. Es handelt sich dabei in aller Regel um Handelsplattformen, die ein Orderbuchmodell aufweisen (so etwa Bisq, AtomicDEX, EtherDelta, Ox, Serum, Loopring und IDEX).

Bei *Peer-to-Pool*-Plattformen werden die Aufträge von Nutzern gegen einen Pool von Vermögenswerten ausgeführt. Diese Vermögenswerte befinden sich typischerweise in einem Smart Contract. Solche Smart Contracts bilden Liquiditätspools, indem sie zwecks *automatisiertem* Market Making (AMM) Kryp-

¹²⁴⁵ Vgl. für eine Übersicht Wang et al., Non-Fungible Token, 21.

¹²⁴⁶ Siehe Delphi Digital, Decentralized Finance, 5.

¹²⁴⁷ Vgl. Harvey/Ramachandran/Santoro, DeFi, 50.

tovermögenswerte halten. Es existiert mit anderen Worten kein Orderbuch. Zu diesem Plattfortmtyp gehören bspw. Uniswap, Bancor, Balancer, Kyber Network und THORSwap. In Uniswap V3 können Liquiditätsgeber jedoch aufgrund der Möglichkeit, Kapital innerhalb einer bestimmten Preisspanne konzentriert anzubieten, Market Making-Strategien betreiben, die für Handelsplattformen mit Orderbuch typisch sind. Handelstechnisch gesehen ist somit eine teilweise Annäherung an das als effizient geltende (Limit-)Orderbuchmodell festzustellen.¹²⁴⁸

Zwar spielt Preisarbitrage in beiden Modellen eine zentrale Rolle, doch ist sie für die Funktionsfähigkeit von Liquiditätspools unerlässlich. Dies setzt voraus, dass immer auch alternative Plattformen existieren, auf deren Preisbildung sich AMMs verlassen können.

b. On-chain- vs. Off-chain-Orderbuch

Dezentrale Handelsplattformen, die ein Orderbuch vorsehen, unterscheiden sich sodann anhand der Frage, ob das Orderbuch on-chain oder off-chain geführt wird. Während On-chain-Orderbücher direkt auf dem verteilten Register des dezentralen Netzwerks gehostet werden, bestehen für off-chain geführte Orderbücher unterschiedliche Modelle.¹²⁴⁹ Um die Transaktionsgebühren möglichst tief zu halten, folgen die meisten dezentralen Handelsplattformen in Ethereum heute einem Off-chain-Orderbuchmodell (so etwa EtherDelta, 0x, IDEX). Vorläufer, wie bspw. OasisDEX, sehen noch On-Chain-Orderbücher vor.

In Bezug auf Handelsplattformen für Bitcoin handelt es sich grundsätzlich immer um Off-chain-Orderbücher (so z.B. im Falle von Bisq und AtomicDEX).

Dezentrale Handelsplattformen, die auf Blockchains mit hohen Transaktionsdurchsätzen beruhen (z.B. Solana), basieren demgegenüber auf On-Chain-Orderbüchern (so z.B. Serum). Dasselbe gilt grundsätzlich für Layer-2-Protokolle, die sich auf Ethereum und andere dezentrale Netzwerke stützen (z.B. Loopring).

Der Vollständigkeit halber sei erwähnt, dass AMM-Handelsplattformen gänzlich auf ein Orderbuch verzichten. AMMs sind grundsätzlich immer on-chain, wobei sie bei Layer-2-Plattformen systembedingt off-chain geführt werden.

¹²⁴⁸ Siehe Harvey/Ramachandran/Santoro, DeFi, 103.

¹²⁴⁹ Siehe hierzu ausführlich Lin, Stanford Journal of Blockchain Law & Policy 2019, 62–66.

c. Matching-Modelle

Auf dezentralen Handelsplattformen kommen vergleichbar mit traditionellen Märkten eine Vielfalt von Matching-Modellen zur Anwendung:

- Am häufigsten anzutreffen ist das klassische *Limit-Orderbuch* (LOB)-Modell, welches nach dem Prinzip der doppelten Auktion funktioniert.¹²⁵⁰ Marktteilnehmer machen gleichzeitig Kauf- (Bids) und Verkaufsangebote (Offers bzw. Asks), die für ein Handelspaar im jeweiligen Verzeichnis – dem Orderbuch – registriert und sodann entweder manuell durch Takers oder automatisch (d.h. durch einen Smart Contract oder die Software des Plattformbetreibers) zusammengeführt werden. Hohe Kauf- und tiefe Verkaufsangebote werden dabei mit einer höheren Wahrscheinlichkeit zusammengeführt und sodann ausgeführt (Preispriorität). Die Handelsteilnehmer sind in diesem Modell die unmittelbar an einem Austausch beteiligten Gegenparteien.¹²⁵¹ Bisq, AtomicDEX, EtherDelta, 0x, IDEX, Serum und Loopring folgen bspw. dem Limit-Orderbuch-Modell.
- Ferner verwenden gewisse dezentrale Handelsplattformen auch eine Ausprägung des *Dealer- Market-Maker*-Modells. In diesem Modell ist die Rolle von Nutzern darauf beschränkt, die von spezialisierten Marktteilnehmern angebotenen Geld- und Briefkurse (Bid und Ask) entweder anzunehmen oder abzulehnen. Diese Dealer und Market Maker handeln dabei auf eigene Rechnung und somit auf eigenes Risiko. In diesem Modell besteht grundsätzlich keine Preispriorität.¹²⁵² Dezentrale Handelsplattformen mit einem RFQ-Mechanismus, wie namentlich Kyber Network oder AirSwap, weisen eine mit dem Dealer- bzw. Market-Maker-Modell vergleichbare Funktionsweise auf.
- Eine Neuheit im Vergleich zu traditionellen Handelsplattformen ist das AMM- *Bonding-Curve*-Modell. Die Verwendung dieses Modells führt dazu, dass ein Auftrag stets eine «Gegenpartei» aufweist (vergleichbar mit Market Orders im LOB-Modell). Entsprechend erübrigt sich die Suche nach einer Gegenpartei. Ferner existiert kein Matching im technischen Sinne, da die Aufträge gegen Liquiditätspools bzw. Reserven ausgeführt werden. Hierzu gehören etwa Uniswap, Balancer und Curve.

¹²⁵⁰ Siehe Smullen/Hand, Dictionary of Finance, 121; Banks, Dictionary of Finance, 164; ferner in *experimenteller* Hinsicht zur doppelten Auktion Smith, in: Smith, *Experimental Methods in the Political Economy of Exchange*, 243; bahnbrechend bereits Smith, *The Journal of Political Economy* 1962, *passim*.

¹²⁵¹ Siehe Foucault/Pagano/Röell, *Market Liquidity*, 16, 17, 17–23.

¹²⁵² Siehe Foucault/Pagano/Röell, *Market Liquidity*, 16, 17, 23–27.

- Ein Matching-Modell, das in traditionellen Finanzmärkten eher selten Anwendung findet, ist das *Niederländische Auktionsmodell*. Eine solche Rückwärtsauktion beginnt anders als traditionelle bieterseitige Auktionen mit einem aus Verkäufersicht zu hohem Angebotspreis, der so lange gesenkt wird, bis ein an der Auktion teilnehmender Käufer das betreffende Gut kauft. Der Verkäufer kann dabei einen Mindestpreis vorsehen, unter welchem er nicht bereit ist, zu verkaufen.¹²⁵³ Mit anderen Worten wird auf einer dezentralen Handelsplattform, welche dieses Modell vorsieht, der Preis einer bestimmten Menge an Kryptovermögenswerten stetig gesenkt, bis die letzte angebotene Einheit durch einen Käufer erworben wird. Der für diese marginale Einheit realisierte Preis ist sodann massgeblich für alle anderen Käufer, vorausgesetzt, sie haben mindestens zu diesem Preis offeriert. Eine solche Auktion läuft in der Praxis typischerweise über einen längeren Zeitraum, um den Käufern genügend Zeit für das Stellen von Kaufangeboten zu gewähren.¹²⁵⁴ Eine dezentrale Handelsplattform mit diesem Matching-Modell ist bspw. DutchX.
- Vergleichbar mit dem Marktdesign des Niederländischen Auktionsmodells ist das *Frequent-Batch-Auction-Modell*.¹²⁵⁵ In der Finanzmarktp Praxis wird dieses Modell regelmässig im Zusammenhang mit der Regulierung des Hochfrequenzhandels diskutiert und vereinzelt auch bereits eingesetzt.¹²⁵⁶ Der Angebotspreis wird hier im Gegensatz zur Rückwärtsauktion nicht ständig gesenkt, sondern die Auktion weist eine bestimmte Laufzeit (Millisekunden, Sekunden, Minuten, ...) auf, während welcher Verkäufer und Käufer Angebote einstellen. Auch hier gilt für alle Marktteilnehmer letztlich der Markträumungspreis, wiederum vorausgesetzt, dass ihr Preisangebot darüber liegt.¹²⁵⁷ Dezentrale Handelsplattformen, welche dieses Batching-Modell implementieren, sind etwa Mesa und Gnosis Auction¹²⁵⁸.

¹²⁵³ Siehe etwa Smullen/Hand, Dictionary of Finance, 24; Banks, Dictionary of Finance, 170; Dictionary of Banking and Finance, 112.

¹²⁵⁴ Siehe DutchX, *passim*; ausführlich Gnosis, Gnosis Whitepaper, 16–18.

¹²⁵⁵ Vgl. zu den Unterschieden Rafa, Batch vs Dutch auctions, *passim*.

¹²⁵⁶ Siehe etwa die statistischen Ausführungen in ESMA, Report Periodic Auctions, 4–6; ferner Budish/Cramton/Shim, The Quarterly Journal of Economics 2015, 1549, 1555–1557; Fox/Glostén/Rauterberg, Duke Law Journal 2015, 269 m.w.H.; schliesslich im Zusammenhang mit dem Absturz von Aktienkursen Jagannathan, Journal of Financial Econometrics 2020, 2.

¹²⁵⁷ Vgl. zur Keeper-Funktion in Gnosis Auction Werner et al., Decentralized Finance, 4.

¹²⁵⁸ <https://ido-ux.dev.gnosisdev.com/>.

- Schliesslich bestehen *hybride* Matching-Modelle, welche Elemente der oben erwähnten Modelle kombinieren. So sehen gewisse dezentrale Handelsplattformen Matching-Mechanismen vor, welche nicht bloss zwei Gegenparteien nach dem LOB-Modell oder eine Gegenpartei mit den Reserven eines Pools zusammenführen, sondern einen «Ringhandel» zwischen mehreren an einem Austausch beteiligten Parteien herstellen können. In einem Ringhandel werden z.B. Token A mit Token B, Token B mit Token C und Token C mit Token A zusammengeführt.¹²⁵⁹ dezentrale Handelsplattformen basierend auf dem Frequent-Batch-Auction-Modell eignen sich für einen solchen Ringhandel (so etwa Mesa¹²⁶⁰).

d. Kassa- vs. Termingeschäfte

Das Angebot handelbarer Produkte und einsetzbarer Handelstechniken auf dezentralen Handelsplattformen lässt sich mit denjenigen traditioneller Handelsplattformen grundsätzlich vergleichen. So ist namentlich der Handel von Kryptovermögenswerten sowohl in Form von Kassa- bzw. Spotgeschäften als auch in Form von Termin- bzw. Derivatgeschäften möglich.¹²⁶¹

Zwar sind die Terminmärkte für den Handel von Optionen und anderen Derivaten im Vergleich zu ihren zentralisierten Pendanten noch stark unterentwickelt. Der aktuelle Marktführer für Termingeschäfte ist BitMEX¹²⁶² – eine zentralisierte Handelsplattform, die neben klassischen Futures sog. Perpetual Swaps anbietet.¹²⁶³ Allerdings finden sich zunehmend dezentrale Handelsplattformen, die sich auf den Handel mit Optionen, Futures und Swaps spezialisieren.¹²⁶⁴

Dezentrale Handelsplattformen für *Termingeschäfte* sind aufgrund der rein synthetischen Abbildung der Handelspaare in den Kontrakten auf die Preisbildung an *externen* Märkten angewiesen. Zudem wird in aller Regel der Preis ei-

¹²⁵⁹ Siehe Smith, Exchange Protocol for the Decentralized Web, 1–2; Gnosis Protocol, Trades, *passim*.

¹²⁶⁰ Siehe Mesa, What advantages do ring trades bring?, *passim*.

¹²⁶¹ Zu den Begriffen siehe Zobl/Kramer, Kapitalmarktrecht, Rz. 10; ferner Boemle et al., Kassamarkt, 644; sodann Boemle et al., Termingeschäft, 1026.

¹²⁶² <https://www.bitmex.com>.

¹²⁶³ Siehe BitMEX, Trading on BitMEX, *passim*.

¹²⁶⁴ Siehe etwa die dezentralen Handelsplattformen Synthetix (<https://www.synthetix.io/>), dYdX (<https://dydx.exchange/>), MCDEX (<https://mcdex.io/>) und DerivaDEX (<https://derivadex.com/>).

nes Stablecoins als Referenzwert für Termingeschäfte verwendet, um das Volatilitätsrisiko für Käufer zu begrenzen. Zu diesem Zweck greifen dezentrale Handelsplattformen bspw. auf die Orakel von Maker¹²⁶⁵ und Chainlink¹²⁶⁶ zurück.

Als Beispiel soll der *Perpetual Swap* BTC-USDC dienen, mit welchem Nutzer auf der dezentralen Handelsplattform dYdX entweder eine gehebelte Long- oder Short-Position auf BTC eingehen können.¹²⁶⁷ Zur Preisermittlung von BTC und USDC werden Orakel eingesetzt, die einen Durchschnittspreis von BTC und USDC auf Grundlage der Marktpreise an einer Vielzahl von zentralen und dezentralen Handelsplattformen berechnen. Um zu verhindern, dass die Orakel einen SPoF für dezentrale Systeme darstellen,¹²⁶⁸ sehen die Orakel-Protokolle typischerweise eine Vielzahl voneinander unabhängiger Preisermittler vor, die als Nodes eines separaten Relay-Netzwerks die Preise der unterschiedlichen Handelsplattformen an die Orakel-Smart Contracts des betreffenden dezentralen Netzwerks übermitteln.¹²⁶⁹ Im Ergebnis wird dadurch auch für Orakel eine dezentrale, nicht intermediatisierte Struktur eingeführt.

e. Weitere Unterschiede

Die vorgestellten Plattformkategorien können schliesslich anhand weiterer Kriterien miteinander verglichen werden.

Grössere Unterschiede bestehen etwa in der Höhe der beim Handel anfallenden Netzwerkgebühren. Die Nutzung von Layer-1-Plattformen ist typischerweise mit höheren Gebühren als die Nutzung von Layer-2-Plattformen verbunden. Ferner können die Nutzungs- und Handelsgebühren der einzelnen Handelsplattformen in der Praxis sehr stark divergieren. Die ausgeprägte Anzahl der Plattformen sollte allerdings für einen entsprechenden Preisdruck sorgen. Eine Kommodifizierung ist auch aufgrund der Verwendung von Aggregatoren zu erwarten, welche durch ein entsprechendes Order-Routing den bestmöglichen Preis an einer Vielzahl von Plattformen sicherstellen können. Schliesslich können dezentrale Handelsplattformen auch aufgrund der abweichenden Abwicklungsfinalität von Geschäften untersucht werden. Aus-

¹²⁶⁵ <https://makerdao.com/en/feeds/>.

¹²⁶⁶ <https://data.chain.link/>.

¹²⁶⁷ Siehe zur Mechanik eines Perpetual Contracts Juliano, dYdX Launches BTC Perpetual Contract Market, Medium, *passim*.

¹²⁶⁸ Vgl. Werner et al., Decentralized Finance, 11.

¹²⁶⁹ Vgl. etwa MakerDAO, Maker Protocol, 10–11; ausführlich MakerDAO, Oracles, *passim*; ferner Ellis/Juels/Nazarov, ChainLink, 3, 6–7, 26–27; Breidenbach et al., Chainlink 2.0, 16, 20, 65.

tauschgeschäfte über Layer-2-Protokolle weisen in aller Regel lediglich eine verzögerte Finalität der Transaktionen auf, während die Abwicklung von Handelsgeschäften über Layer-1-Plattformen unmittelbar im verteilten Register abgebildet werden.¹²⁷⁰

¹²⁷⁰ Siehe zu den Unterschieden zwischen Layer 1 und Layer 2 oben, [III.5](#).

5. Chancen und Risiken

5.1 Chancen

a. Einleitung

Dezentrale Handelsplattformen können unterschiedliche Chancen mit sich bringen: (i) Dezentrale Handelsplattformen sind grundsätzlich frei zugänglich, weshalb auch Retailanleger und Personen, die bisher keinen Zugang zu den Finanzmärkten haben, Kryptovermögenswerte über sie handeln können. (ii) Ferner sind mit der Nutzung dezentraler Handelsplattformen keine traditionellen Gegenpartei- und Systemrisiken verbunden. (iii) Sie erlauben zudem einen Gleichlauf zwischen den Verfügungsrechten an den Vermögenswerten und deren faktischen Kontrolle. (iv) Dezentrale Handelsplattformen ermöglichen sodann globale Liquiditätsnetzwerke in einer transparenten Umgebung. (v) Ihr Einsatz kann schliesslich in Ermangelung eines Intermediärs Risiken im Bereich des Rent Seekings reduzieren.

b. Freie Zugänglichkeit

i. Beschränkter Zugang für Retailanleger

Traditionelle Finanzmarktinfrastrukturen stehen gewöhnlichen Anlegern grundsätzlich nicht offen. Diese sind vielmehr auf die Dienstleistungen direkter oder indirekter Teilnehmer solcher Finanzmarktinfrastrukturen angewiesen.¹²⁷¹

Dies ist auch für den Handel von Finanzinstrumenten von Relevanz, von welchem Retailanleger historisch aus Effizienz- sowie Anleger- und Funktionsschutzgründen ausgeschlossen worden sind.¹²⁷² So hält Art. 18 Abs. 2 FinfraG

¹²⁷¹ Vgl. zu den dahinterstehenden regulatorischen Prinzipien BIS-CPSS/IOSCO, Principles for financial market infrastructures, 101–108, wobei anzumerken sei, dass diese nicht direkt auf Handelsplätze und -systeme zur Anwendung gelangen (vgl. 5 FN 2).

¹²⁷² Siehe Portmann, Best execution, N 6 m.w.N.; hinsichtlich des BEHG Botschaft BEHG 1993, 1382, 1386, 1401–1402; ferner Hertig/Schuppisser, in: Hertig et al., Kommentar BEHG, Art. 2b N 46; Zobl/Kramer, Kapitalmarktrecht, Rz. 26; Watter, in: Walder/Jaag/Zobl, Handel in Wertschriften, 185.

fest, dass der Zugang zu einer Finanzmarktinfrastuktur beschränkt werden kann, sofern dadurch die Sicherheit oder die Effizienz gesteigert wird und diese Wirkung durch andere Massnahmen nicht erreicht werden kann oder aber die Eigenschaften des möglichen Teilnehmers den Geschäftsbetrieb der Finanzmarktinfrastuktur oder ihrer Teilnehmer gefährden könnten. Art. 34 FinfraG enthält sodann spezifische Regeln für Handelsplätze. Der Teilnehmerkreis an einem Handelsplatz ist demnach auf Finanzintermediäre beschränkt. Eine solche Regelung stellt einerseits die oben erwähnten Ziele sicher, begründet aber letztlich auch die Existenz der Kontroll- und Vertrauensrisiken von Retailanlegern in Finanzmärkten.¹²⁷³

Eine Änderung ergibt sich allerdings für DLT-Handelssysteme, die nunmehr auch natürlichen und juristischen Personen, die nicht Finanzintermediäre sind, unmittelbar offenstehen.¹²⁷⁴

ii. Dezentrale Handelsplattformen

Dezentrale Handelsplattformen sind demgegenüber grundsätzlich für jedermann frei zugänglich (sog. Disintermediated Access). Die einzige Bedingung ist die Einrichtung eines Self-Hosted Wallets. Dies gilt nicht nur für Anleger, sondern selbst für Emittenten von Finanzinstrumenten.

Das folgende Beispiel mag dies veranschaulichen: Der Emittent tokenisierter Aktien kann etwa die Plattform *Uniswap* dazu verwenden, seine eigenen Anteile handelbar zu machen. Er erstellt zu diesem Zweck einen Smart Contract, den er anschliessend mit seinen tokenisierten Aktien und einem Gegenwert, wie z.B. einen Stablecoin, ausstattet. Anleger können schliesslich über *Uniswap* den Stablecoin gegen die Aktien tauschen, indem sie neue Einheiten des Stablecoins an den Smart Contract senden.¹²⁷⁵

Dabei muss die Person, welche Kryptovermögenswerte zum Handel an einer dezentralen Handelsplattform zuführt, selbst nicht notwendigerweise die Emittentin der Vermögenswerte sein. Jedermann kann mit anderen Worten Kryptovermögenswerte auf solchen Plattformen dem Handel zuführen.

¹²⁷³ So auch Fox/Glosten/Rauterberg, *Duke Law Journal* 2015, 206.

¹²⁷⁴ Art. 73c Abs. 1 lit. e FinfraG; ausführlich zu den Überlegungen hinter der Öffnung von DLT-Handelssystemen gegenüber Retailkunden Bundesrat, DLT-Bericht 2018, 109–111.

¹²⁷⁵ Vgl. für eine rechtliche Einordnung dieser Aktivität unten, [V](#).

Die Hürden des Marktzugangs, wie sie in traditionellen Märkten bestehen, sind in dezentralen Handelsplattformen überwiegend abgebaut. Die Kontroll- und Vertrauensrisiken des traditionellen Handels von Vermögenswerten sind mangels Finanzintermediäre obsolet. Da Anleger nicht auf Dritte angewiesen sind bzw. von deren Tätigwerden abhängig sind, erhalten sie einen einfachen Zugang zu DeFi-Protokollen.¹²⁷⁶ Selbstverständlich bedeutet die unmittelbare Zugänglichkeit von dezentralen Handelsplattformen nicht notwendigerweise, dass die Nutzung frei von Risiken ist.¹²⁷⁷

c. Verringerung von traditionellen Gegenparti- und Systemrisiken

i. Ubiquität von Gegenpartierisiken

In modernen Finanzmärkten ist Geld grundsätzlich ein Schuldtitel.¹²⁷⁸ Daraus folgt, dass letztlich allen Zahlungsströmen Verbindlichkeiten zugrunde liegen. Am deutlichsten wird dies anhand der Passivseite der Bilanzen von Zentral- und Geschäftsbanken ersichtlich: Diese erhöhen die Geldmenge einer Volkswirtschaft, indem sie durch entsprechende Buchungen Verbindlichkeiten sozusagen «aus dem Nichts» erschaffen.¹²⁷⁹ Diese Fähigkeit ist letztlich auf den vorherrschenden Papiergeldstandard und somit die endgültige Aufhebung der Deckung durch und Einlösungspflicht in Gold in den 1970er Jahren zurückzuführen.¹²⁸⁰ Mit Ausnahme der von Zentralbanken in Verkehr gesetzten Bank-

¹²⁷⁶ Vgl. auch FSB, Decentralised financial technologies, 2, wobei «permissionless distributed ledgers» – nach vorliegender Auffassung zu Unrecht – gerade nicht mit «financial inclusion» in Verbindung gebracht werden.

¹²⁷⁷ Siehe unten, [IV.5.2.](#)

¹²⁷⁸ Siehe Coggan, Paper Promises, Introduction («Modern money is debt and debt is money.»); ferner Mayer, Neue Ordnung des Geldes, 25–26, der von «Passivgeld» spricht.

¹²⁷⁹ Siehe bereits von Mises, Theorie des Geldes, 266–275, der zwischen «Sachkredit» und «Zirkulationskredit» unterscheidet, wobei lediglich letzterer die Geldmenge erweitert; Rothbard, Mystery of Banking, 94–98, 161–170; ferner Turner, Between Debt and Devil, 57–60, der von «debt contracts» spricht; Ryan-Collins et al., Where Does Money Come From?, 16–18.

¹²⁸⁰ Siehe Friedman, Money Mischief, 15, 249 («[...] a world monetary system has emerged that has no historical precedent: a system in which every major currency in the world is, directly or indirectly, on an irredeemable paper money standard [...]. The ultimate consequences of this development are shrouded in uncertainty.»).

noten¹²⁸¹ und der von ihnen herausgegebenen Sichtguthaben steht hinter jeder Geldeinheit letztlich eine Forderung eines Marktteilnehmers gegen den jeweiligen Emittenten.¹²⁸² «*From the point of view of the system as a whole, every liability is someone else's asset.*»¹²⁸³ Der betriebswirtschaftliche Hauptunterschied zwischen einer Zentralbank- und Geschäftsbankbilanz liegt darin, dass Zentralbanken ihre «Verbindlichkeiten» *fortwährend* bedienen können.¹²⁸⁴

Weil praktisch alles Geld seit dem Ende von Bretton Woods in den 1970er Jahren und somit der Auflösung der Goldbindung des US-Dollars schuldbasiert ist, haben die Schulden des öffentlichen und privaten Sektors die höchsten Stände seit dem Zweiten Weltkrieg erreicht.¹²⁸⁵ Namentlich Banken werden für ihren hohen Verschuldungsgrad, den sog. *Leverage*, kritisiert.¹²⁸⁶ Exzessives Schuldenmachen im öffentlichen und Finanzsektor hat historisch betrachtet regelmässig zum Staatsbankrott geführt.¹²⁸⁷ Entsprechend nimmt die Verschuldung von Privathaushalten ebenfalls eine bedeutende Rolle ein.¹²⁸⁸

Diese Ausführungen verdeutlichen, dass unser heutiges Finanzsystem ungeachtet der Existenz anderer Verträge, etwa Derivatgeschäfte, bereits in den Grundstrukturen eine Unzahl von Gegenparteirisiken beinhaltet. Gegenparteirisiken sind mit anderen Worten endemisch.¹²⁸⁹ Wir leben in einer Welt des Kredits und der Verschuldung. In aggregierter Form stellen Gegenparteirisiken ausserdem ein systemisches Risiko für den Finanzsektor im Besonderen und die Wirtschaft im Allgemeinen dar.¹²⁹⁰

¹²⁸¹ Vgl. Art. 7 Abs. 2 WZG: «[Die Nationalbank] nimmt die nicht benötigten Noten unbeschränkt gegen Vergütung des Nennwerts zurück.»; vgl. ferner Art. 988 OR, wonach das Kraftloserklärungsverfahren des Wertpapierrechts nicht auf Banknoten zur Anwendung gelangt.

¹²⁸² Vgl. hinsichtlich der besonderen Natur des Fremdkapitals der Schweizerischen Nationalbank Jordan, Braucht die Schweizerische Nationalbank Eigenkapital?, 5–6.

¹²⁸³ Mehrling, in: Taylor/Rezai/Michl, *Hierarchy of money*, 397.

¹²⁸⁴ Siehe Jordan, Braucht die Schweizerische Nationalbank Eigenkapital?, 7.

¹²⁸⁵ Siehe Kose et al., *Global Waves of Debt*, 5–6; ferner Credit Suisse, *Assessing Global Debt*, 4, 11–19.

¹²⁸⁶ Siehe etwa Admati/Hellwig, *The Bankers' New Clothes*, 17–31.

¹²⁸⁷ Vgl. in *empirischer* Hinsicht Reinhart/Rogoff, *This Time is Different*, xxvi–xxvii, xxxiii, 51–67; ferner Polleit/von Prollius, *Geldreform*, 151–161.

¹²⁸⁸ Siehe etwa Mian/Sufi, *House of Debt*, 12–13.

¹²⁸⁹ Eine *wirtschaftsethische* Einschätzung dieser Situation findet sich bei Hülsmann, *Ethics of Money Production*, 182–185.

¹²⁹⁰ Siehe aus netzwerk- und systemtheoretischer Sicht Schweitzer et al., *Science* 2009, 425; Haldane, in: Jansen/Schröter/Steher, *Rethinking*, 253–254; Hautsch/Schaumburg/Schienle, *Review of Finance* 2015, 689; vgl. ferner die Beiträge in Arner et al., *Systemic Risk in the Financial Sector*, *passim*.

ii. Erfüllungs-, Wiederbeschaffungs- und Liquiditätsrisiken

In traditionellen Effektenabwicklungssystemen bestehen mehrere Typen von Gegenpartei Risiken bzw. Risiken, die auf die Beziehung mit einer Gegenpartei zurückzuführen sind. Dies führte bereits früh zur Erkenntnis, dass Effektenabwicklungssysteme so zu konzipieren sind, dass die bekannten Risiken möglichst minimiert werden.¹²⁹¹

Die Bank for International Settlements (BIS) unterscheidet zwischen Wiederbeschaffungsrisiko, Erfüllungsrisiko und Liquiditätsrisiko. Diese Risikotypen werden gemeinhin unter dem Oberbegriff des Kreditrisikos (*Credit Risk*) zusammengefasst.¹²⁹² In abwicklungschronologischer Reihenfolge treten die erwähnten Kreditrisiken wie folgt auf:

- Unter dem sog. *Wiederbeschaffungsrisiko* (Replacement Cost Risk) wird das Risiko verstanden, dass ein Handelsgeschäft nach Abschluss des Vertrages, aber noch vor der Abwicklung scheitert und deswegen durch ein neues Geschäft ersetzt werden muss, dieses aber lediglich zu ungünstigeren (Preis-)Bedingungen abgeschlossen werden kann.¹²⁹³ Dieses Risiko wird auch als sog. Pre-Settlement Risk bezeichnet.¹²⁹⁴
- Als sog. *Erfüllungsrisiko* (Principal Risk) wird sodann das Risiko bezeichnet, dass der Verkäufer von Effekten diese unwiderruflich an den Käufer liefert, dieser allerdings seine Zahlungsverpflichtung gegenüber dem Verkäufer nicht erfüllt bzw. dass der Käufer von Effekten bereits unwiderruflich Zahlung an den Verkäufer leistet, dieser allerdings die Effekten an den Käufer nicht liefert.¹²⁹⁵ Bei Zahlungsunfähigkeit der Gegenpartei wird dieses Risiko auch als sog. Settlement Risk bezeichnet.¹²⁹⁶
- Schliesslich wird unter dem sog. *Liquiditätsrisiko* (Liquidity Risk) verstanden, dass eine Partei ihre Verpflichtung nicht bei Fälligkeit, sondern erst

¹²⁹¹ Vgl. Group of Thirty, Clearance and Settlement Systems, 1–2.

¹²⁹² Siehe BIS, Delivery versus Payment in Securities Settlement Systems, 12–14 m.w.H.; hinsichtlich Kreditrisiken bei der *Effektenabwicklung* Haene, SECOM, 6; hinsichtlich Kreditrisiken bei der *Zahlungsabwicklung* Mägerle/Oleschak, SIC, 6–7; demgegenüber *leicht abw.* BIS-CPSS/IOSCO, Recommendations for securities settlement systems, 39–41.

¹²⁹³ Siehe BIS, Delivery versus Payment in Securities Settlement Systems, 13; Bech et al., BIS Quarterly Review März 2020, 68.

¹²⁹⁴ Siehe BIS-CPSS/IOSCO, Recommendations for securities settlement systems, 39.

¹²⁹⁵ Siehe BIS, Delivery versus Payment in Securities Settlement Systems, 13.

¹²⁹⁶ Siehe Boemle et al., Settlement Risk, 955; ferner BIS, Delivery versus Payment in Securities Settlement Systems, 13, wobei der Begriff an dieser Stelle in erster Linie für Erfüllungsrisiken im Interbanken-Devisenhandel (sog. Herstatt-Risiko) verwendet wird.

zu einem späteren Zeitpunkt erfüllen kann. Die Ursache für das Liquiditätsrisiko liegt dabei nicht in der endgültigen Zahlungsunfähigkeit der Partei, sondern lediglich in deren vorübergehenden Zahlungsschwierigkeiten oder in technischen Problemen der Handelssysteme. Dieser Umstand kann die Gegenpartei dazu veranlassen, Effekten anderweitig zu beschaffen (z.B. durch eine Wertpapierleihe), Fremdkapital aufzunehmen oder ungeplante Effektenverkäufe zu tätigen. Dies wird als Liquiditätsrisiko bezeichnet, weil je nach Markt und Marktsituation Liquiditätsengpässe für die betroffene Gegenpartei sowie die übrigen Marktteilnehmer entstehen können.¹²⁹⁷

Kein eigentliches Gegenparteirisiko aus dem Effektenhandel, aber dennoch ein peripheres Risiko traditioneller Effektenabwicklungssysteme ist das Risiko, dass der Finanzintermediär, welcher die Effekten für den Verkäufer verwahrt bzw. das Zahlungsmittel dem Käufer zur Verfügung stellt, nach der Erfüllung der Zahlungsverpflichtung aber noch vor Lieferung der Effekten bzw. nach der Lieferung der Effekten, aber noch vor der Zahlung des Kaufpreises ausfällt.¹²⁹⁸ Typischerweise kann dieses Risiko zumindest für die Zahlungsseite durch die Verwendung von Zentralbankengeld vermieden werden.¹²⁹⁹

In der *grenzüberschreitenden* Abwicklung von Effektengeschäften können ferner spezifische Risiken bestehen, wie namentlich Rechts- und Fremdwährungsrisiken sowie Risiken im Zusammenhang mit dem Umstand, dass mehrere Finanzintermediäre und Abwicklungsregime tangiert sind.¹³⁰⁰

iii. Delivery versus Payment (DvP)

Alle diese Risiken können systemischer Natur sein. Besonders das Erfüllungsrisiko kann im Finanzsystem zu kaskadenartigen Ausfällen von Finanzintermediären und damit zu einem Vertrauensverlust der Marktteilnehmer in die Effektenabwicklungssysteme führen, weshalb es als wahrscheinlichste Quelle

¹²⁹⁷ BIS, Delivery versus Payment in Securities Settlement Systems, 13–14.

¹²⁹⁸ Siehe BIS, Delivery versus Payment in Securities Settlement Systems, 14, 15, spricht von dem sog. *Risk of Failure of a Settlement Bank, a Guarantor or a Custodian*.

¹²⁹⁹ Siehe BIS, Delivery versus Payment in Securities Settlement Systems, 14; BIS-CPSS/IOSCO, Recommendations for securities settlement systems, 16–17, 40; Mägerle/Oleschak, SIC, 3–4, 6; Haene, SECOM, 4, 6; vgl. ferner BIS-CPSS/IOSCO, Principles for financial market infrastructures, 67–68.

¹³⁰⁰ Siehe BIS-CPSS/IOSCO, Recommendations for securities settlement systems, 40–41, 43–44; zu den Risiken im Devisenbereich ausführlich BIS, Settlement Risk in Foreign Exchange Transactions, 4.

von Systemrisiken betrachtet wird.¹³⁰¹ Eine Möglichkeit, um insb. das Erfüllungsrisiko zu reduzieren, ist die Erfüllung der Lieferungsverpflichtung davon abhängig zu machen, ob die Zahlungsverpflichtung erfüllt wird. Die Verknüpfung der Wertpapierseite mit der Zahlungsseite wird als sog. *Delivery versus Payment* (DvP) bezeichnet.¹³⁰² Infolgedessen werden im Markt auch allfällige Liquiditätsrisiken verringert.¹³⁰³ In traditionellen Effektenabwicklungssystemen wird sodann das abrechnungsspezifische Wiederbeschaffungsrisiko durch den Einsatz von zentralen Gegenparteien (sog. Central Counterparty, CCP, oder Clearinghouse) verringert. Diese treten zwischen die beteiligten Parteien, indem sie als Käuferin gegenüber dem Verkäufer und als Verkäuferin gegenüber dem Käufer fungieren.¹³⁰⁴ Durch den Einsatz einer CCP kommt es unabhängig von der Zahlungsfähigkeit oder dem Zahlungswillen der Gegenpartei zur erfolgreichen Abrechnung von Effektengeschäften; ausserdem reduzieren CCPs die operationellen Risiken für Marktteilnehmer.¹³⁰⁵ Allerdings ist der Einsatz von CCPs seinerseits mit spezifischen Risiken verbunden, allen voran dem Risiko, dass die Gegenparteien einer CCP nicht oder nicht rechtzeitig erfüllen können.¹³⁰⁶ Die enorme technische und rechtliche Komplexität der heutigen Nachhandelsinfrastrukturen wird denn auch als wohlfahrtsökonomisch bedenklich eingestuft.¹³⁰⁷

Die BIS unterscheidet drei DvP-Modelle in der Effektenabwicklungspraxis: Im ersten Modell werden Effekten und Zahlungen auf einer Einzelhandelsbasis gleichzeitig abgewickelt (sog. Bruttomethode). Die Schweizer Systeme SIC für Zahlungen und SECOM für Effekten wickeln Transaktionen nach dem DvP-Modell 1 ab.¹³⁰⁸ Im zweiten Modell wird lediglich die Wertpapierseite brutto abgewickelt, während die Zahlungsseite zu einem bestimmten, späteren Zeit-

¹³⁰¹ Siehe BIS, *Delivery versus Payment in Securities Settlement Systems*, 14, 15; ferner BIS-CPSS/IOSCO, *Recommendations for securities settlement systems*, 41.

¹³⁰² Siehe BIS, *Delivery versus Payment in Securities Settlement Systems*, 15; Bech et al., *BIS Quarterly Review* März 2020, 71; Chiu/Koepl, *The Review of Financial Studies* 2019, 1716; in Bezug auf Aktientransaktionen Panisi/Buckley/Arner, *Stanford Journal of Blockchain Law & Policy* 2019, 196 m.w.N.

¹³⁰³ Siehe BIS, *Delivery versus Payment in Securities Settlement Systems*, 15.

¹³⁰⁴ Siehe Bech et al., *BIS Quarterly Review* März 2020, 68.

¹³⁰⁵ Siehe Milne, in: Diehl et al., *Central Securities Depositories and Securities Clearing and Settlement*, 342–344.

¹³⁰⁶ Siehe BIS-CPSS/IOSCO, *Recommendations for Central Counterparties*, 8–9 m.w.H.; ferner Hess, *AJP* 2004, 695.

¹³⁰⁷ Ausführlich hierzu Milne, in: Diehl et al., *Central Securities Depositories and Securities Clearing and Settlement*, 348, 350–352.

¹³⁰⁸ Siehe hierzu Mägerle/Oleschak, *SIC*, 3, 6; Haene, *SECOM*, 4, 6–8; ferner mit grafischer Darstellung BIS, *Real-Time Gross Settlement Systems*, 33–34.

punkt netto abgewickelt werden, d.h., ausstehende Verbindlichkeiten werden vor der Abwicklung miteinander verrechnet. Das *dritte* Modell sieht schliesslich sowohl für die Wertpapier- als auch die Zahlungsseite lediglich zu bestimmten Zeitpunkten eines Handelstages die gegenseitige Verrechnung mit anschliessender Abwicklung vor.¹³⁰⁹

In terminologischer Anlehnung an den DvP-Abwicklungsmechanismus werden ferner, je nachdem, ob es sich um reine Effektaustausch- oder Devisengeschäfte handelt, Delivery versus Delivery (DvD) und Payment versus Payment (PvP) unterschieden. Die Einrichtung eines dieser Mechanismen stellt einen internationalen Standard für Finanzmarktinfrastrukturen dar, der von Effektenabwicklungs- und Zahlungssystemen sowie zentrale Gegenparteien umgesetzt werden soll.¹³¹⁰

«Principle 12: Exchange-of-value settlement systems:

If an [Financial Market Infrastructure] settles transactions that involve the settlement of two linked obligations (for example, securities or foreign exchange transactions), it should eliminate principal risk by conditioning the final settlement of one obligation upon the final settlement of the other.»¹³¹¹

An diesen Standard anknüpfend können ferner die Dauer des Abwicklungszyklus, gemessen seit dem Zeitpunkt der Ausführung des Handelsgeschäfts, sowie die Ausgestaltung der rechtlichen Finalität eines Effektingeschäfts potenzielle Quellen von Gegenparti- und somit Systemrisiken darstellen.¹³¹²

iv. Dezentrale Handelsplattformen

Die oben erwähnten Gegenparteirisiken haben alle ihren Ursprung im traditionellen Finanzintermediationssystem.¹³¹³ Mangels intermediärer Prozesse und Strukturen weisen dezentrale Handelsplattformen demgegenüber keine traditionellen Gegenparteirisiken auf.¹³¹⁴ Hinzukommt, dass dezentrale Han-

¹³⁰⁹ Siehe BIS, Delivery versus Payment in Securities Settlement Systems, 16–24.

¹³¹⁰ Siehe BIS-CPSS/IOSCO, Principles for financial market infrastructures, 14, 76–77.

¹³¹¹ BIS-CPSS/IOSCO, Principles for financial market infrastructures, 76.

¹³¹² Siehe BIS-CPSS/IOSCO, Recommendations for securities settlement systems, 10, 14–15; BIS-CPSS/IOSCO, Principles for financial market infrastructures, 64–66, 142; ferner Mooney, University of Pennsylvania Journal of Business Law 2020, 405–406 m.w.N.

¹³¹³ So offenbar auch Mooney, University of Pennsylvania Journal of Business Law 2020, 404.

¹³¹⁴ Gl.M. Harvey/Ramachandran/Santoro, DeFi, 52, 130, 131, 142–144; ferner Amler et al., DeFinancing DeFi, 2; vgl. auch Ehrensam, Why Decentralized Exchange Protocols Matter, Medium, *passim*; ferner Lin, Stanford Journal of Blockchain Law & Policy 2019, 58, die allerdings lediglich von tieferen Gegenparteirisiken ausgeht.

delsplattformen definitionsgemäss grenzüberschreitend operieren, so dass spezifische grenzüberschreitende Risiken (z.B. Rechtsrisiken) nicht im herkömmlichen Sinne von Belang sind.

An einem Handelsgeschäft können zwar zwei konkrete Parteien beteiligt sein, doch ist die Erfüllung der von den Gegenparteien eingegangenen Verpflichtungen letztlich nicht von ihrer Leistungsfähigkeit oder ihrem Leistungswillen abhängig. Die Ausführung der beiden Transaktions-Legs (Delivery und Payment) wird auf dezentralen Handelsplattformen nämlich – in der Regel durch Smart Contracts – automatisiert. Dieses Element von dezentralen Handelsplattformen wird in Anlehnung an die Computerwissenschaften als «Atomic Settlement» bezeichnet. Atomic Settlement bedeutet, dass Smart Contracts *entweder* beide Legs erfolgreich abwickeln *oder* keines der beiden. Mit anderen Worten funktioniert Atomic Settlement nach dem Alles-oder-Nichts-Prinzip.¹³¹⁵ Demgegenüber ist es technisch ausgeschlossen, dass der Austausch von Kryptovermögenswerten lediglich teilweise ausgeführt wird.¹³¹⁶ Das *Erfüllungsrisiko* wird durch Atomic Settlement überwiegend eliminiert.¹³¹⁷

Atomic Settlements werden sodann unterschieden in solche, die innerhalb desselben dezentralen Netzwerks zur Ausführung gelangen (*Single-Chain* bzw. *Single-Ledger*), und solche, die über mehrere dezentrale Netzwerke hinweg stattfinden (*Cross-Chain* bzw. *Cross-Ledger*).¹³¹⁸ Ein Beispiel einer *Single-Chain*-Transaktion ist der Austausch von zwei unterschiedlichen ERC-20-Token auf der Ethereum Blockchain über Uniswap. Ein Beispiel für eine *Cross-Chain*-Transaktion ist etwa der Austausch von BTC gegen ETH, in welchem Fall zwei unterschiedliche Blockchains involviert sind (z.B. über THORChain).

Sowohl bei *Single-Chain* als auch bei *Cross-Chain* kommen in der Regel Smart Contracts zur Anwendung, wobei diese bei *Cross-Chain*-Transaktionen um die Funktion eines *Hash Time Locked Contracts* (HTLC) oder einen vergleichbaren

¹³¹⁵ Der Begriff stammt vom altgriechischen Wort *ἄτομος* bzw. *átomos*, was mit «unteilbar» übersetzt wird.

¹³¹⁶ Siehe Antonopoulos/Wood, *Mastering Ethereum*, 129; ferner Schär, *Federal Reserve Bank of St. Louis Review* 2021, 169; Lin, *Stanford Journal of Blockchain Law & Policy* 2019, 61 FN 13.

¹³¹⁷ So auch Chiu/Koepl, *The Review of Financial Studies* 2019, 1717; Weber/Baisch, *SZW* 2021, 693; ähnlich OECD, *Tokenisation and Implications for Financial Markets*, 32 («The distributed ledger can act as [...] a counterparty to all transacting parties [...]»); vgl. ferner ECB/BOJ, *STELLA*, 22, welche dies zumindest für «single-ledger DvP» feststellen; BIS/SIX/SNB, *Project Helvetia*, 11.

¹³¹⁸ Siehe zu den unterschiedlichen Konzepten ausführlich ECB/BOJ, *STELLA*, 5–7.

Mechanismus ergänzt werden.¹³¹⁹ Ein HTLC dient dazu, dass eine Partei den Empfang einer Transaktion vor Ablauf eines im Voraus bestimmten Zeitfensters kryptografisch zu bestätigen bzw. auszulösen hat, andernfalls der Vermögenswert vom Absender wieder ausgelöst werden kann.¹³²⁰ Mittels eines HTLC können somit zwei unterschiedliche dezentrale Netzwerke miteinander verbunden werden: Vereinfacht gesagt, werden bitcoins und ethers vorübergehend in je einem HTLC blockiert und das Auslösen des jeweiligen Vermögenswerts zeitlich davon abhängig gemacht, dass die jeweiligen HTLC-Transaktionen auf beiden Blockchains genügend tief im Ledger «vergraben» liegen (sog. Timelock). Die Transaktionen in den unterschiedlichen Registern werden ausserdem derart kryptografisch miteinander verknüpft, dass keine der am Handelsgeschäft beteiligten Parteien alleine über die Vermögenswerte verfügen kann. Sollte aber die eine Partei die von der Gegenpartei deponierten Vermögenswerte abrufen, d.h. digital signieren, was grundsätzlich ja von beiden Seiten intendiert ist, hat die Gegenpartei unmittelbar dieselbe Möglichkeit (sog. Hashlock).¹³²¹ Atomic Cross-Chain Settlement ist dabei nicht auf zwei Parteien beschränkt.¹³²² Neben dezentralen Netzwerken erster Ordnung (Layer 1) können auch dezentrale Netzwerke zweiter Ordnung (Layer 2) Atomic Settlement-Mechanismen aufweisen.¹³²³

HTLCs funktionieren letztlich wie Smart Contracts und erlauben somit für den Austausch von Kryptovermögenswerten ohne personale oder institutionelle Intermediation. Daraus folgt, dass die involvierten Parteien nicht mit traditionellen Gegenparteirisiken konfrontiert sind.¹³²⁴ Neben HTLCs bestehen weitere Möglichkeiten, Atomic Cross-Chain Swaps zu realisieren: *Relays*, die bspw. mittels Smart Contracts implementiert werden, können etwa dazu verwendet werden, die Daten eines anderen dezentralen Netzwerks auszulesen und zu verifizieren. Wenn die Verifikation erfolgreich ausfällt, kommt es zum

¹³¹⁹ Siehe Herlihy, Proceedings of the 2018 ACM Symposium on Principles of Distributed Computing 2018, 245; Xu/Ackerer/Dubovitskaya, Game-Theoretic Analysis, 1; Bech et al., BIS Quarterly Review März 2020, 76.

¹³²⁰ Siehe Antonopoulos, Mastering Bitcoin, 312–313; ausführlich Decker/Wattenhofer, in: Pelc/Schwarzmann, Duplex Micropayment Channels, 10–12.

¹³²¹ Ausführlich zu «Atomic Cross-Chain Swaps» Narayanan et al., Bitcoin, 257–260. Das Konzept geht zurück auf einen Forumsbeitrag von NOLAN, vgl. Nolan, Alt chains and atomic transfers, BitcoinTalk, *passim*.

¹³²² Siehe das Beispiel in Herlihy, Proceedings of the 2018 ACM Symposium on Principles of Distributed Computing 2018, 245.

¹³²³ Siehe Miraz/Donald, Annals of Emerging Technologies in Computing 2019, 46.

¹³²⁴ Siehe Miraz/Donald, Annals of Emerging Technologies in Computing 2019, 43–45, 47; vgl. ferner Narayanan et al., Bitcoin, 258; ECB/BOJ, STELLA, 6; Buterin, Chain Interoperability, 7.

Atomic Settlement.¹³²⁵ Ferner wird vorgeschlagen, ein separates dezentrales Netzwerk einzusetzen, das die jeweiligen Transaktionen «beobachtet» und den beteiligten Parteien erlaubt, den Austausch mithilfe eines gemeinsamen Smart Contracts zu koordinieren.¹³²⁶

Im Vergleich zu herkömmlichen DvP-Modellen handelt es sich bei Atomic Settlement auf dezentralen Handelsplattformen grundsätzlich um eine strenge Form von DvP: Die beiden Transaktionsseiten werden *notwendigerweise* zeitgleich ausgeführt. Atomic Settlement kann darum am ehesten als Weiterentwicklung des DvP-Modells 1 betrachtet werden, in welchem die Lieferung von Effekten und die Bezahlung des Kaufpreises zeitgleich auf einer Bruttobasis erfolgen.¹³²⁷ Allerdings weisen gewisse dezentrale und hybride Handelsplattformen auch Ähnlichkeiten zu Effektenabwicklungssystemen auf, die beide Legs am Ende eines Handelszyklus auf Nettobasis abwickeln (d.h. eine Mischung aus den DvP-Modellen 1 und 3). Die Handelsaufträge werden auf der Plattform zwar unmittelbar ausgeführt und gelten aus Nutzersicht als «abgeschlossen», die Abwicklung im dezentralen Netzwerk (d.h. on-chain) findet demgegenüber lediglich in bestimmten Zeitabständen – z.B. alle zehn Minuten, einmal stündlich oder einmal täglich – statt. Die Abwicklung findet i.d.R. allerdings anders als im DvP-Modell 3 auf Bruttobasis statt.

Kürzere Abwicklungszyklen tragen grundsätzlich zu einem Abbau von Gegenparteirisiken bei.¹³²⁸ Im Vergleich zu heutigen Nachhandelsinfrastrukturen ist mit einer – abhängig vom dezentralen System – moderaten bis massiven Beschleunigung der Abwicklungszeiten zu rechnen.¹³²⁹ Praktisch nähern sich gewisse dezentrale Handelsplattformen einer Echtzeit-Abwicklung von Transaktionen an.¹³³⁰

¹³²⁵ Siehe Buterin, Chain Interoperability, 7.

¹³²⁶ Siehe Zakhary/Agrawal/El Abbadi, Proceedings of the VLDB Endowment 2020, 1320, 1324–1325.

¹³²⁷ Siehe Bech et al., BIS Quarterly Review März 2020, 75, 76, 78; IOSCO, Fintech Report, 63; vgl. ferner BIS/SIX/SNB, Project Helvetia, 11.

¹³²⁸ Siehe ESMA, DLT Report, 5, 7; IOSCO, Fintech Report, 54–55; Casey et al., Impact of Blockchain Technology, 15, 17, 18, 20, 21; Buckley/Arner/Zetzsche, FinTech, 121.

¹³²⁹ Differenzierend nach verschiedenen Faktoren FINRA, Distributed Ledger Technology, 5–6; ebenso IOSCO, Fintech Report, 58, 59; vgl. ferner ECB/BOJ, STELLA, 20, 23–24, welche eine massive Verbesserung der Abwicklungsgeschwindigkeiten feststellten, wobei erwähnt werden muss, dass das Projekt auf den Permissioned Block- bzw. Sidechains Corda, Elements und Fabric basierte; vgl. hierzu die Übersicht in ECB/BOJ, STELLA, 20; BIS/SIX/SNB, Project Helvetia, 21–22 (auf Corda).

¹³³⁰ So auch Wall/Malm, Distributed Securities Depository, 38, 50, 54; Chiu/Koepl, The Review of Financial Studies 2019, 1717.

Mithilfe von Smart Contracts, welche in diesem Rahmen zu einem gewissen Grad die Rolle von zentralen Gegenparteien übernehmen, kann zudem das *Wiederbeschaffungsrisiko* verringert werden.¹³³¹ Zudem kann die Kapitaleffizienz erhöht werden, denn anders als im traditionellen Bereich müssen Nutzer dezentraler Handelsplattformen keine Sicherheiten bei einer CCP hinterlegen.¹³³² Sicherheiten, u.a. in Form von Ein- und Nachschüssen (Margins), sind in intermediatisierten Systemen primär aus Anreizgründen vorgesehen.¹³³³ Ein Restrisiko hinsichtlich Wiederbeschaffung bleibt allerdings dann übrig, wenn ein Handelsgeschäft abgeschlossen wird, dieses aber aufgrund der Kapazitätsgrenzen des dezentralen Netzwerks vorübergehend nicht in den Public Ledger aufgenommen werden kann und sich in der Zwischenzeit die Abschlussbedingungen für den Nutzer ungünstig entwickelt haben. Soweit solche abgegebenen Aufträge noch rechtzeitig gelöscht oder zurückgezogen werden können, haben die Nutzer von dezentralen Handelsplattformen immerhin die Möglichkeit, einen negativen Preiseffekt zu vermeiden. Cross-Chain-Transaktionen auf Basis von HTLC oder ähnlichen Mechanismen beinhalten schliesslich ebenfalls ein Wiederbeschaffungsrisiko für die beteiligten Parteien, das theoretisch proportional zum vorprogrammierten Zeitablauf ansteigt.¹³³⁴

Die massive Verringerung von traditionellen Gegenparteirisiken in dezentralen Handelsplattformen hat einen positiven Effekt auf das Systemrisiko.¹³³⁵ Es kommt aufgrund der Zusammenlegung von traditionellen Prozessen und Strukturen zur Reduktion der Gesamtkomplexität.¹³³⁶ Ungeachtet dessen lässt sich in dezentralen Handelsplattformen das *Liquiditätsrisiko* nicht ausschalten. Dies hat insb. damit zu tun, dass von den Marktteilnehmern ein ausgeprägtes Technologievertrauen erwartet wird. Technische Probleme, wie z.B. ein folgenreicher Softwarebug in einem Smart Contract, können dieses Vertrauen auf die Probe stellen. In der Folge kann das Liquiditätsrisiko der be-

¹³³¹ Siehe Bech et al., BIS Quarterly Review März 2020, 75; vgl. ferner BIS/SIX/SNB, Project Helvetia, 11.

¹³³² Vgl. Art. 49 FinfraG; ferner hierzu BIS-CPSS/IOSCO, Principles for financial market infrastructures, 9, 46–56.

¹³³³ Siehe etwa Bodie/Merton/Cleeton, Financial Economics, 33.

¹³³⁴ Siehe ECB/BOJ, STELLA, 22; ferner Buterin, Chain Interoperability, 7, 8, der darum von einer «free option» für die Gegenpartei spricht; ausführlich zu diesem, in vielen Fällen entschädigungslosen Optionsrecht Han/Lin/Yu, in: AFT '19 – Proceedings of the 1st ACM Conference on Advances in Financial Technologies 2019, *passim*.

¹³³⁵ Vgl. Avgouleas/Kiayias, European Business Organization Law Review 2019, 84–85, 106–107, die durch den Einsatz von permissioned DLT eine Verringerung der Systemrisiken in traditionellen Märkten mit CCPs als «warehouses of systemic risk» erwarten.

¹³³⁶ Vgl. Bech et al., BIS Quarterly Review März 2020, 74, 79.

troffenen Kryptovermögenswerte ansteigen. Ein besonderer Fall eines Liquiditätsrisikos liegt bspw. im Fall von Protokollen vor, die aufgrund einer marktbedingten Unterbesicherung Nachschusspflichten auslösen (z.B. *Maker-DAO*). Ohnehin lässt sich das marktbezogene Liquiditätsrisiko letztlich aufgrund seiner engen Beziehung zum allgemeinen Vertrauen in die Finanzintermediation bzw. die grundlegenden Mechanismen eines Marktes niemals vollständig eliminieren.¹³³⁷

v. Gegenparteirisiko bei Tokenisierung

Der Vollständigkeit halber sei erwähnt, dass der Handel mit Token, die einen Vermögenswert repräsentieren, der aus Sicht eines dezentralen Systems *extrinsisch* ist, wie z.B. Fiatwährungen, ein Wertpapier, eine Unze eines Edelmetalls oder ein Grundstück, weiterhin Gegenparteirisiken aufweisen können. Gegenparteirisiken bei tokenisierten Vermögenswerten bestehen bspw. aufgrund einer Rechtsbeziehung zum Emittenten des Wertpapiers (Beteiligungsrisiko) oder zum Verwahrer des Edelmetalls (Verwahrungsrisiko).¹³³⁸ Darüber hinaus können allenfalls Intermediäre zwischengeschaltet sein, welche reale Vermögenswerte mit der Digitalwelt einer Blockchain verknüpfen.¹³³⁹ Selbstredend besteht schliesslich auch ein Gegenparteirisiko im Rahmen der Verwahrung von Private Keys für einen Kunden.

d. Gleichlauf von Verfügungsrechten und faktischer Kontrolle

i. Intermediatisierte Wertpapierverwahrung

Die Funktion der Verwahrung und Verwaltung von kapitalmarktfähigen Papieren kommt in traditionellen Finanzmärkten nicht dem einzelnen Anleger zu. Mit Ausnahme der selten gewordenen Heim- und Emittentenverwahrung

¹³³⁷ Vgl. etwa Koppl, *From Crisis to Confidence*, 83 («*Confidence also influences the demand for money: when confidence rises, the demand for money falls; when confidence falls, the demand for money rises.*»).

¹³³⁸ Siehe Antonopoulos/Wood, *Mastering Ethereum*, 224.

¹³³⁹ So etwa OECD, *Tokenisation and Implications for Financial Markets*, 33–35; ferner Arruñada, *Minnesota Journal of Law, Science & Technology* 2018, insb. 82–83; vgl. auch etwa die Rolle des «physischen Validators» gemäss Art. 2 Abs. 1 lit. p des Gesetzes vom 3. Oktober 2019 über Token und VT-Dienstleister des Fürstentums Liechtenstein; siehe hierzu auch die Ausführungen in Fürstentum Liechtenstein, BuA TVTG 2019, 72–74, wo die «Scharnierfunktion» des physischen Validators hervorgehoben wird.

ist die Ausübung dieser Funktionen durch Finanzintermediäre heutzutage der absolute Regelfall. Die finanzintermediäre Verwahrung und Verwaltung von Wertpapieren wird als sog. *mediatisierte* bzw. *intermediatisierte Wertpapierverwahrung* bezeichnet.¹³⁴⁰

Intermediatisierte Verwahrungssysteme stellen einen bedeutenden Schritt in der historisch gewachsenen Immobilisierung und sodann De- bzw. Entmaterialisierung von Kapitalmarktpapieren dar.¹³⁴¹ Sie sind zudem im Gesamtkontext der Automatisierung und Virtualisierung des Börsenhandels seit den 1970er Jahren zu sehen.¹³⁴² Zusammen mit elektronischen Handels- und Effektenabwicklungssystemen erlauben intermediatisierte Verwahrungssysteme das sog. *Straight Through Processing (STP)* von Handelsaufträgen: Ein Börsenauftrag führt demnach automatisch zu den entsprechenden Umbuchungen in den Effektenkonten der involvierten Finanzintermediäre.¹³⁴³ Die Einführung der intermediatisierten Wertpapierverwahrung reduzierte nicht nur die Risiken des physischen Wertpapierhandels; sie erhöhte darüber hinaus die Effizienz und Stabilität der übrigen Finanzmarktinfrastrukturen.¹³⁴⁴

In rechtlicher Hinsicht gelten heute anstelle der früheren sachen- und obligationenrechtlichen Prinzipien die Bestimmungen des Bucheffektengesetzes vom 3. Oktober 2008 (BEG). Zwar wurden Kapitalmarktpapiere bereits vor dem BEG intermediatisiert verwahrt und verwaltet, der Erlass des BEG stellte das System allerdings auf ein vollständig neues Rechtsfundament.¹³⁴⁵ Das BEG regelt die Verwahrung von Wertpapieren und Wertrechten durch Verwahrungsstellen und deren Übertragung. Ferner gewährleistet es den Schutz der Eigentumsrechte der Anleger. Es trägt zur Rechtssicherheit im internationalen Verhältnis, zur effizienten Abwicklung von Effektengeschäften und zur Stabilität des Finanzsystems bei.¹³⁴⁶ Das BEG hat nach Auffassung des Gesetzgebers

¹³⁴⁰ Siehe Hess/Friedrich, GesKR 2008, 99, welche allerdings beide Begriffe scheinbar austauschbar verwenden; ferner Meier-Hayoz/von der Crone, Wertpapierrecht, N 1331, die lediglich von mediatisierten Wertpapierverwahrungssystemen sprechen.

¹³⁴¹ Ausführlich zu diesen Schritten Meier-Hayoz/von der Crone, Wertpapierrecht, N 1317–1330; Hess/Friedrich, GesKR 2008, 100–102; ferner Zobl/Lambert, SZW 1991, 125–131; betreffend SEGA-Sammelverwahrung Meier-Hayoz, ZBJV 1986, 391–396.

¹³⁴² Siehe oben, [II.1.4](#).

¹³⁴³ Siehe Hess/Friedrich, GesKR 2008, 117; Zobl/Kramer, Kapitalmarktrecht, N 1317; kritisch wegen den in der Praxis oft beobachtbaren «trade fails» bei grenzüberschreitenden oder mehrgliedrigen Verhältnissen Milne, in: Diehl et al., Central Securities Depositories and Securities Clearing and Settlement, 346–348.

¹³⁴⁴ Siehe Botschaft BEG 2006, 9321, 9322–9323; ferner Hess/Friedrich, GesKR 2008, 102.

¹³⁴⁵ Siehe von der Crone/Bilek, SZW 2008, 193–194.

¹³⁴⁶ Vgl. Art. 1 BEG.

ein Vermögensobjekt *sui generis* geschaffen. Die Bucheffekte weise demnach Merkmale sowohl einer schuldrechtlichen Forderung als auch einer Sache im Sinne der schweizerischen Privatrechtsordnung auf.¹³⁴⁷ Diese doppelte Rechtsnatur von Bucheffekten sei aufgrund ihrer relativen Natur gegenüber dem jeweiligen Emittenten des zugrundeliegenden Forderungs- oder Mitgliedschaftsrechts (bzw. allenfalls gegenüber der Verwahrungsstelle) sowie der ihnen von Gesetzes wegen zukommenden *erga omnes*-Rechtswirkungen gegenüber den Verwahrungsstellen und jedem Dritten zurückzuführen. Dieser Ansicht hat sich das Bundesgericht angeschlossen.¹³⁴⁸ In der Literatur ist die Rechtsnatur von Bucheffekten allerdings weiterhin umstritten.¹³⁴⁹

Die intermediatisierte Wertpapierverwahrung weist eine inhärente Zentralisierungstendenz auf.¹³⁵⁰ Die Wertpapiere eines Anlegers werden auf dessen Namen einem Effektenkonto bei einem Finanzintermediär gutgeschrieben. Dabei handelt es sich um die depotführende Bank oder das depotführende Wertpapierhaus des Anlegers. Der Finanzintermediär führt sodann in seiner Funktion als Verwahrungsstelle ein Effektenkonto bei einer Drittverwahrungsstelle, welche in der Schweiz in aller Regel die SIX SIS AG ist. Dieses Effektenkonto lautet auf den Namen des an die SIX SIS AG angeschlossenen Finanzintermediärs und stellt typischerweise ein Sammelkonto (Omnibus-Kunden-Konto) über die von seinen Kunden gehaltenen Effekten dar. Die SIX SIS AG fungiert ausserdem als Zentralverwahrerin gemäss FinfraG für die in der Schweiz immobilisierten und immaterialisierten Bucheffekten. Dies führt, bildlich gesprochen, zu einer nationalen Verwahrungspyramide.¹³⁵¹

¹³⁴⁷ Siehe Botschaft BEG 2006, 9339 m.w.H. auf verschiedene Meinungen in der Literatur.

¹³⁴⁸ Siehe BGE 138 II 137, E. 5.2.1 m.w.N.

¹³⁴⁹ Siehe etwa Meier-Hayoz/von der Crone, Wertpapierrecht, N 1339–1342, welche wie der Gesetzgeber und das Bundesgericht von einem Vermögensobjekt *sui generis* ausgehen; ähnlich Beeler, Bucheffekten, N 209–241, für welchen Bucheffekten Rechte gegenüber dem Emittenten darstellen, weshalb lediglich der Gutschrift eines Anlegers Bucheffektenqualität zukommen soll; a.M. Steiner, GesKR 2016, 338–340 m.w.H., der die Ansicht vertritt, dass eine Bucheffekte eine Repräsentation der zugrundeliegenden Rechte gegenüber dem Emittenten und somit lediglich eine «qualifizierte Buchung» darstellt, an welche aber die Rechtswirkungen des BEG anknüpfen.

¹³⁵⁰ So bereits BIS-CPSS/IOSCO, Recommendations for securities settlement systems, 13 («The costs and risks associated with owning and trading securities may be reduced considerably through immobilisation of physical securities, which involves concentrating the location of physical securities in a depository [or CSD].»).

¹³⁵¹ Siehe zur Pyramide der Wertpapierverwahrung Meier-Hayoz/von der Crone, Wertpapierrecht, N 1349–1354; Hess/Friedrich, GesKR 2008, 99–100.

Besonders im *grenzüberschreitenden* Verhältnis treten zu den obgenannten Verwahrungsstellen weitere hinzu: So sind die von einem Schweizer Anleger gehaltenen Aktien einer ausländischen Gesellschaft regelmässig im Ausland endverwahrt. Die Verwahrungspyramide kann darum ohne Weiteres vier, fünf oder mehr Ebenen umfassen, die aus weiteren Unterverwahrungsstellen und dem ausländischen Zentralverwahrer bestehen. Schliesslich kann auch ein internationaler Zentralverwahrer, wie namentlich *Clearstream* und *Euroclear*, Teil der Verwahrungskette bilden.¹³⁵² Wenig überraschend wird die Komplexität des heutigen Systems gemeinhin als sehr hoch eingestuft¹³⁵³ und die Rechtssicherheit als eher tief.¹³⁵⁴

ii. Direct Ownership- vs. Multi-Tiered Entitlement-Modell

Mehrgliedrige, grenzüberschreitende Verwahrungsketten beinhalten ferner auch vielfältige operationelle, namentlich rechtliche Risiken. Dabei bestehen Rechtsunsicherheiten nicht nur für den Anleger, sondern auch für die dazwischengeschalteten Finanzintermediäre und letztlich auch für den Emittenten von Wertpapieren.¹³⁵⁵

Hinsichtlich der Berechtigungen an den Bucheffekten in der intermediatisierten Wertpapierverwahrung werden zwei Grundmodelle unterschieden:¹³⁵⁶

- Im *Direct Ownership*-Modell, das in Kontinentaleuropa verbreitet ist und auch in der Schweiz¹³⁵⁷ gilt, bleibt der hinterlegende Anleger trotz der

¹³⁵² So Botschaft BEG 2006, 9321–9322.

¹³⁵³ Siehe Botschaft BEG 2006, 9321; Milne, in: Diehl et al., *Central Securities Depositories and Securities Clearing and Settlement*, 349–350, der darum auf systemische Risiken in Krisensituation hinweist; Hess/Friedrich, *GesKR* 2008, 99; Reiser, *SZW* 2017, 456; Mooney, *University of Pennsylvania Journal of Business Law* 2020, 388, 413–414, 441–442 m.w.H.; Group of Thirty, *Global Clearing and Settlement*, 23 («*Not surprisingly, the complexity of the clearing and settlement process is directly related to the number of actors involved. Of necessity, therefore, the level of complexity rises substantially as the process extends across borders.*»); DTCC, *Embracing Disruption*, 5 («*Unnecessarily Complex*»).

¹³⁵⁴ So etwa Paech, *Uniform Law Review* 2016, 614 («*considerable legal uncertainty*»), 625.

¹³⁵⁵ Ausführlich Thévenoz, *Stanford Journal of Law, Business and Finance* 2008, 389–401; ferner Chan et al., *ECB Occasional Paper Series* Nr. 68, August 2007, 33–34.

¹³⁵⁶ Eine sehr nützliche grafische Übersicht findet sich bei Hess/Friedrich, *GesKR* 2008, 106 m.w.H.; vgl. ferner Thévenoz, *Stanford Journal of Law, Business and Finance* 2008, 401–444; BIS-CPSS/IOSCO, *Recommendations for securities settlement systems*, 38, 46, 47, wobei zwischen «*direct holding systems*» und «*indirect holding systems*» unterschieden wird; weiterführend UNIDROIT, *Guide on Intermediated Securities*, 16–22.

¹³⁵⁷ Art. 13 Abs. 1 BEG; vgl. hierzu Botschaft BEG 2006, 9357; ferner Pfenninger, in: *Kommentar BEG*, Art. 13 N 2, der von den Bucheffekten und den wertpapierrechtlichen Urkunden als

Intermediarisierung der Bucheffekten an den durch sie repräsentierten Rechten unmittelbar berechtigt. Mit anderen Worten bleibt der Anleger Inhaber des Forderungs- oder Mitgliedschaftsrechts gegenüber dem Emittenten. Es besteht mit anderen Worten ein direktes Rechtsverhältnis zwischen Anleger und Emittenten. Der Anleger bleibt demgegenüber für die Ausübung seiner Rechte auf die Intermediäre angewiesen.¹³⁵⁸ In diesem Modell führen die involvierten Finanzintermediäre im Wesentlichen lediglich Buch über die Bestände des Endanlegers.¹³⁵⁹

- Demgegenüber weist das angelsächsische Modell der *Multi-Tiered Entitlements* (auch *Multi-Tiered Trusts*) lediglich derjenigen Partei eine Berechtigung an und aus den Wertpapieren zu, welche eine direkte rechtliche Beziehung zum Emittenten der Papiere aufweist. Der Anleger selbst ist aufgrund der Nominee-Beziehungen der involvierten Finanzintermediäre lediglich wirtschaftlich Berechtigter bzw. Beneficial Owner an den Aktien. Für die Ausübung seiner Rechte bleibt er ebenfalls auf die dazwischengeschalteten Intermediäre angewiesen.¹³⁶⁰

Die Konzentration von Wertpapieren in den Händen von Finanzintermediären wurde in der Literatur als «Agency Capitalism» bezeichnet.¹³⁶¹ Die Konsequenz dieser Entwicklung ist die *Verdopplung* der Kontroll- und Vertrauensrisiken, indem Investoren nunmehr sowohl den Emittenten der Wertpapiere als auch die dazwischengeschalteten Finanzintermediäre (und allenfalls institutionellen Investoren)¹³⁶² kontrollieren müssten, was neben Corporate Governance-Problemen insb. die besagten intermediärsspezifischen Risiken mit sich bringt.¹³⁶³ CHARLES W. MOONEY fasst diese Risiken unter dem Oberbegriff des Intermediärrisikos zusammen.¹³⁶⁴

«Hüllen» der zugrundeliegenden Rechte spricht; BSK Wertpapierrecht-Pulver/Meyer Bahar, Art. 13 BEG N 14, 16 m.w.N.; OFK FinfraG/BEG-Vogel/Heiz/Luthiger, Art. 13 BEG N 2–4.

¹³⁵⁸ Siehe hierzu BSK Wertpapierrecht-Pulver/Meyer Bahar, Art. 13 BEG N 22 («faktisch unentbehrlich»); Pfenninger, in: Kommentar BEG, Art. 13 N 5.

¹³⁵⁹ Siehe Thévenoz, Stanford Journal of Law, Business and Finance 2008, 404–406.

¹³⁶⁰ Siehe Thévenoz, Stanford Journal of Law, Business and Finance 2008, 406–408; ausführlich zur Situation in Grossbritannien Gullifer/Payne, Corporate Finance Law, 147, 553–555.

¹³⁶¹ Siehe Gilson/Gordon, Columbia Law Review 2013, 865.

¹³⁶² Siehe hierzu Bogle, Individual Stockholder, WSJ, *passim*, der in diesem Fall von «agency society» spricht; vgl. ferner Davis Evans, Virginia Law Review 2009, 1123–1124.

¹³⁶³ So Gilson/Gordon, Columbia Law Review 2013, 865–867; ferner Avgouleas/Kiayias, European Business Organization Law Review 2019, 83; hinsichtlich der Ausübung von Aktionärsrechten Mooney, University of Pennsylvania Journal of Business Law 2020, 413–414 m.w.N.

¹³⁶⁴ Siehe Mooney, Michigan Journal of International Law 2019, 532 («*Intermediary risk is a function of the structure of a particular holding system, including the holding infrastructure*

iii. Verwahrungsrisiken und Eigentümerintransparenz im Besonderen

Mit der Verwahrung von Wertpapieren durch Finanzintermediäre ist naturgemäß ein *Verwahrungsrisiko* (Custody Risk) verbunden. Hierzu gehört insb. das Risiko des Anlegers, vorübergehend oder dauerhaft die Verfügungsmöglichkeit über seine Wertpapiere zu verlieren. Dies kann auf unterschiedliche Sachverhalte zurückzuführen sein, wie etwa auf die Insolvenz einer der involvierten Verwahrstellen, wobei die verwahrten Papiere Teil der Konkursmasse bilden, auf die inkorrekte oder unvollständige Führung von Effektenkonten oder auf betrügerisches Verhalten einer Verwahrstelle, woraus den Anlegern jeweils ein Schaden entstehen kann.¹³⁶⁵ Beim Verwahrungsrisiko handelt es sich darum um ein spezifisches Gegenparteirisiko von Anlegern in intermediarisierten Verwahrungssystemen. Aufgrund der Vielzahl an der Verwahrungskette beteiligter Finanzintermediäre tritt das Verwahrungsrisiko für den einzelnen Anleger – v.a. im grenzüberschreitenden Verhältnis – in verschärfter Form auf.¹³⁶⁶

Im angelsächsischen Modell bestimmen sich die Rechte des Anlegers nach dem «kleinsten gemeinsamen Nenner» der rechtsgeschäftlichen Verwahrungskette: Eine vertragliche Bestimmung, welche die Rechte einer einzigen Verwahrungsstelle beschränkt, kann somit letztlich auch die Rechtsposition des Anlegers verschlechtern. Im Ergebnis bestimmen sich die Rechte des Anlegers nach den ungünstigsten Vertragsbedingungen der in der Verwahrungskette involvierten Parteien.¹³⁶⁷

Ein besonderes Verwahrungsrisiko stellt sodann die *Intransparenz* des heutigen Systems dar. Dabei werden grundsätzlich zwei Systeme unterschieden: In einem transparenten System sind die Anleger der Zentralverwahrerin und

and its relevant technology, the relevant private law of property and contract, legal and contractual duties that underpin the holding structure, the regulatory framework, and the relevant insolvency laws.»).

¹³⁶⁵ Zum Ganzen siehe BIS-CPSS/IOSCO, Recommendations for securities settlement systems, 18–19, 40; Haene, SECOM, 6; ausführlich Mooney, University of Pennsylvania Journal of Business Law 2020, 407–411.

¹³⁶⁶ Siehe BIS/CPSS, Cross-Border Securities Settlements, 20 («In a cross-border context, the involvement of multiple legal jurisdictions and multiple settlement intermediaries increases the importance of custody risks and greatly complicates their analysis.»); ferner BIS-CPSS/IOSCO, Recommendations for securities settlement systems, 19, 43; Mooney, University of Pennsylvania Journal of Business Law 2020, 411–413; Reiser, SZW 2017, 456; Avgouleas/Kiayias, European Business Organization Law Review 2019, 102–103.

¹³⁶⁷ Siehe Micheler, Cambridge Law Journal 2015, 510.

allen weiteren Intermediären bekannt; in einem intransparenten System halten Intermediäre alle Vermögenswerte in einem Sammelkonto bei der Zentralverwahrerin.¹³⁶⁸ Die USA und die grössten Märkte in Europa, inklusive die Schweiz, folgen letzterem Modell.

DAVID C. DONALD und MAHDI M. MIRAZ schreiben über die Transparenz in intermediatisierten Wertpapierverwahrungssystemen: «[...] *although fast and secure, it is unclear exactly what is being held and transferred with such speed in this indirect holding system.*»¹³⁶⁹ BECH et al. sprechen sodann von der Fragmentierung der Eigentümerinformationen in einem solchen mehrgliedrigen Verwahrungssystem.¹³⁷⁰ Die Undurchsichtigkeit mehrgliedriger Verwahrungssysteme führt dazu, dass die Verfügungs- und Handlungsrechte von Anlegern nachhaltig gefährdet sind.¹³⁷¹ Dies kann ähnlich zum Teilreservesystem von Geschäftsbanken im Geldwesen etwa durch die Überemission von Bucheffekten geschehen, welche als synthetische Verbriefung des Basiswerts, der im Zeitpunkt der Buchung noch nicht erworben worden ist,¹³⁷² betrachtet werden kann.¹³⁷³ Das Problem kann besonders akut bei Wertpapierleihen im Zusammenhang mit Leerverkäufen sein.¹³⁷⁴

Vorschläge für eine Verbesserung des heutigen Systems in Bezug auf eine Stärkung der Eigentümertransparenz bei tokenisierten Aktien und Anleihen liegen bereits einige vor: DONALD und MIRAZ fordern etwa die Nutzung von private bzw. permissioned DLTs zur eindeutigen Zuordnung der Mitglied-

¹³⁶⁸ Siehe Mooney, University of Pennsylvania Journal of Business Law 2020, 398 m.w.N.

¹³⁶⁹ Donald/Miraz, Fordham Journal of Corporate & Financial Law 2019, 111.

¹³⁷⁰ Siehe Bech et al., BIS Quarterly Review März 2020, 68; OECD, Tokenisation and Implications for Financial Markets, 32; ferner DTCC, Embracing Disruption, 5 («Multiple Versions of the Truth»).

¹³⁷¹ G.L.M. Donald/Miraz, Fordham Journal of Corporate & Financial Law 2019, 104, 114; Micheler/von der Heyde, Butterworths Journal of International Banking and Financial Law 2016, 652, 655; Schwarcz, Minnesota Law Review 2008, 395–396, 398; Mooney, University of Pennsylvania Journal of Business Law 2020, 414; FSB, Decentralised financial technologies, 14 FN 51; Yermack, Review of Finance 2017, 8 m.w.N.; ähnlich Paech, Uniform Law Review 2016, 628–629, der die Relativierung von *erga omnes*-Rechten in solchen Systemen hervorhebt; ausführlich hinsichtlich der Verfügungsrechte an Aktien in den USA Donald, Virginia Law & Business Review 2011, 45–46, 69–79.

¹³⁷² Vgl. hinsichtlich der Pflicht von Verwahrstellen zur unverzüglichen Eindeckung mit Bucheffekten bei Unterbestand Art. 11 Abs. 2 BEG.

¹³⁷³ So Donald/Miraz, Fordham Journal of Corporate & Financial Law 2019, 105, 114; hinsichtlich der Risiken im Zusammenhang mit Wertpapierfinanzierungsgeschäften Micheler, Cambridge Law Journal 2015, 521–523.

¹³⁷⁴ Siehe Mooney, in: Conac/Segna/Thévenoz, Shortfall of Intermediated Securities, 162–163, 174–175.

schafts- und Forderungsrechte, wobei die Emittenten selbst Nodes innerhalb des Netzwerks bilden würden und ausschliesslich verantwortlich für die Führung des Aktien- oder Anlehensregisters wären.¹³⁷⁵ Ähnlich schlägt MOONEY vor, ein «new platform system (NPS)» einzuführen, das Anleger und Emittenten direkt miteinander verbindet und Anlegern erlaubt, die Verfügungshoheit über ihre Rechte zu behalten. Das NPS könnte bspw. von bestehenden Finanzintermediären betrieben werden, ohne dass diese allerdings noch in die Transaktionen involviert wären. Es müsste nach Auffassung des Autors nicht zwingend auf DLT basieren.¹³⁷⁶ GEORGE S. GEIS vertritt schliesslich die Auffassung, dass Emittenten mithilfe von DLT «traceable shares» herausgeben können, was letztlich die Corporate Governance solcher Emittenten verbessern soll.¹³⁷⁷

Als Ergebnis kann festgehalten werden, dass intermediatisierte Wertpapierverwahrungssysteme aus Sicht der Anleger in mehrfacher Hinsicht Kontroll- und Vertrauensrisiken mit sich bringen, welche deren Stellung letztlich deutlich schwächen können.¹³⁷⁸

iv. Intermediatisierter Zahlungsverkehr

Nicht unähnlich zur Wertpapierverwahrung ist der Grad der Intermediation auf der Zahlungsseite eines Effektengeschäfts.¹³⁷⁹

Im Inlandzahlungsverkehr bieten einerseits Banken und andere Marktteilnehmer ihren Kunden Dienstleistungen des bargeldlosen Zahlungsverkehrs an.¹³⁸⁰ Andererseits dient das SIC-Zahlungssystem der Abrechnung und Abwicklung des bargeldlosen Interbanken-Zahlungsverkehrs in Schweizer Franken. Dieses Zahlungssystem wird durch die SIC AG im Auftrag der SNB betrieben. Zur Anbindung an das SIC-System führen Marktteilnehmer bei der

¹³⁷⁵ Siehe Donald/Miraz, *Fordham Journal of Corporate & Financial Law* 2019, 140–142.

¹³⁷⁶ Siehe Mooney, *University of Pennsylvania Journal of Business Law* 2020, 389, 393, 427–446.

¹³⁷⁷ Siehe Geis, *Northwestern University Law Review* 2018, 254–267; ähnlich auch Panisi/Buckley/Arner, *Stanford Journal of Blockchain Law & Policy* 2019, 211–213.

¹³⁷⁸ In empirischer Hinsicht siehe Droll/Podlich/Wedow, *Journal of Banking & Finance* 2016, 54 («[...] our empirical analysis highlights that better informed banks typically have shorter sub-custodian chains, which we interpret as evidence of agency problems in the custodian industry.»).

¹³⁷⁹ Vgl. etwa BIS-CPSS/IOSCO, *Recommendations for securities settlement systems*, 16–17, wo unterschiedliche Abwicklungsszenarien dargestellt werden; ferner BIS, *Real-Time Gross Settlement Systems*, 13–14.

¹³⁸⁰ Vgl. etwa hinsichtlich der Rolle der PostFinance AG Botschaft FinfraG 2014, 7516; ferner Botschaft NBG 2002, 6185; eine Übersicht findet sich sodann bei BIS/CPSS, *Red Book Switzerland*, 399–401.

SNB Girokonten, die Sichtguthaben als gesetzliches Zahlungsmittel halten.¹³⁸¹ Das Halten von Sichtguthaben bei der SNB steht in erster Linie Banken, Effektenhändlern, Versicherungen und Finanzmarktinfrastrukturen offen.¹³⁸² Wie bereits erwähnt, knüpft das SIC-Zahlungssystem sodann an das Effektenabwicklungssystem SECOM der Zentralverwahrerin SIX SIS AG an, was die DvP-Abwicklung von Effektengeschäften ermöglicht.¹³⁸³

Im Fremdwährungszahlungsverkehr ist die Intermediationspyramide nochmals komplexer. Dies liegt u.a. daran, dass der direkte Zugang zu ausländischem Zentralbankengeld regelmässig nur unter erschwerten Bedingungen möglich ist.¹³⁸⁴ Überweisungen im grenzüberschreitenden Bereich verlaufen regelmässig über Anweisungen innerhalb eines mehrstufigen Netzes von *Korrespondenzbanken*. Dabei werden die begleitenden Meldungen zwischen den einzelnen in den Zahlungsverkehr involvierten Banken über das standardisierte SWIFT¹³⁸⁵-Protokoll ausgeschaut.¹³⁸⁶ Neben solchen bilateralen und multilateralen Lösungen zwischen Schweizer Banken und ausländischen Instituten sticht zudem v.a. ein System zur Abwicklung von grenzüberschreitenden Devisengeschäften heraus. Dabei handelt es sich um die *Continuous Link Settlement (CLS) Bank International* mit Sitz in New York.¹³⁸⁷ Die CLS Bank ist selbst Teilnehmerin am SIC-System und unterhält damit ein Schweizer-Franken-Girokonto bei der SNB. Ähnliche Strukturen unterhält die CLS Bank mit ausgewählten ausländischen Zentralbanken.¹³⁸⁸ Dies erlaubt SIC-Teilnehmern Schweizer-Franken-Konten bei der CLS Bank zu führen und dadurch Geschäfte in achtzehn Fremdwährungen Zug-um-Zug abzuwickeln.¹³⁸⁹

Ein wesentlicher Unterschied zur intermediatisierten Wertpapierverwahrung besteht aus rechtlicher Sicht allerdings darin, dass Geld in modernen Zahlungssystemen ausschliesslich aus Verbindlichkeiten des jeweiligen Emittenten besteht.¹³⁹⁰ Damit weisen Zahlungssysteme systembedingt immer ein Ge-

¹³⁸¹ Siehe Mägerle/Oleschak, SIC, 3–4.

¹³⁸² Siehe SNB, Zugang zum SIC-System und zu Girokonten, 2–3.

¹³⁸³ Siehe Mägerle/Oleschak, SIC, 6; Haene, SECOM, 4, 6–8.

¹³⁸⁴ Siehe BIS-CPSS/IOSCO, Recommendations for securities settlement systems, 17.

¹³⁸⁵ SWIFT steht für «Society for Worldwide Interbank Financial Telecommunication».

¹³⁸⁶ Siehe etwa Abegg, in: Emmenegger, Grenzüberschreitender Zahlungsverkehr, 111–112; ferner Hess, in: Emmenegger, Euro-Zahlungen, 64–67.

¹³⁸⁷ <https://www.cls-group.com/>.

¹³⁸⁸ Siehe Schaller, Continuous Linked Settlement, 19, 71.

¹³⁸⁹ Siehe Mägerle/Oleschak, SIC, 6; im Detail Schaller, Continuous Linked Settlement, 76–84.

¹³⁹⁰ Siehe einleitend zu diesem Abschnitt oben, [IV.5.1c.i](#).

genparteirisiko auf, dass allerdings bei Verwendung von Zentralbankengeld erheblich reduziert ist.¹³⁹¹

Vergleichbar mit den internationalen Effektenverwahrungssystemen bestehen auch im grenzüberschreitenden Zahlungsverkehr verschiedenartige Rechtsunsicherheiten, welche letztlich aus Sicht der beteiligten Personen Kontroll- und Vertrauensrisiken darstellen.¹³⁹²

v. Dezentrale Handelsplattformen

Die Botschaft zum BEG erwähnte, dass «[d]ie Wertpapierverwahrung durch Verwahrungsstellen [...] wie alle Formen der Finanzintermediation auf dem Vertrauen der Anlegerinnen und Anleger [beruhe.]».¹³⁹³ Dieses Vertrauen ist eng verknüpft mit den oben erwähnten Verwahrungsrisiken intermediatisierter Systeme. Die zentrale Rolle von Intermediären in der Verwaltung und Verwahrung von Bucheffekten setzt letztlich ein Vertrauen seitens der Anleger voraus, das indessen mit hohen Transaktionskosten verbunden sein kann.¹³⁹⁴

Demgegenüber erlauben dezentrale Handelsplattformen für einen Gleichlauf zwischen Verfügungsberechtigung und Verfügungsmacht an Kryptovermögenswerten.¹³⁹⁵ Durch die Eliminierung aller intermediären Strukturen werden alle Zweifel am Letztbegünstigten ausgeräumt und dort, wo ein Emittent existiert, ein direktes bilaterales Verhältnis etabliert.¹³⁹⁶ Mit anderen Worten wird in DeFi das möglich, was in der ökonomischen Theorie unter *Property Rights* verstanden wird, nämlich die unmittelbare und ausschliessliche Kontrolle über die dazugehörigen vermögensmässigen und nichtvermögensmässigen Rechte, wie etwa das Stimmrecht.¹³⁹⁷ Mithilfe von Self-Hosted Wallets können

¹³⁹¹ Vgl. zu den Gegenparteirisiken BIS-CPSS/IOSCO, Principles for financial market infrastructures, 67–68.

¹³⁹² Vgl. mit Blick auf aufsichts- und strafrechtliche Risiken Abegg, in: Emmenegger, Grenzüberschreitender Zahlungsverkehr, 116.

¹³⁹³ Botschaft BEG 2006, 9342.

¹³⁹⁴ Siehe oben, [II.5.2c](#).

¹³⁹⁵ Vgl. Avgouleas/Kiayias, European Business Organization Law Review 2019, 105; ferner Benos/Garratt/Gurrola-Perez, Ledger 2019, 130; Mooney, University of Pennsylvania Journal of Business Law 2020, 427, 432, 445–446.

¹³⁹⁶ So auch Green/Snagg, in: Gullifer/Payne, Intermediated Securities, 344; vgl. Donald/Mirraz, Fordham Journal of Corporate & Financial Law 2019, 148; ESMA, DLT Report, 5; Paech, Uniform Law Review 2016, 631–632, 635.

¹³⁹⁷ Siehe Alchian, Il Politico 1965, 818, der die Bedeutung von «authority» hervorhebt; Furu-botn/Richter, New Institutional Economics, 82; vgl. ferner Douglas/McFarlane, in: Penner/Smith, Defining Property Rights, 223–232, 243, die zwischen einem «right to exclude»

die Inhaber von Kryptovermögenswerten selbst mit den Smart Contracts einer dezentralen Handelsplattform und somit direkt mit dem dezentralen Netzwerk interagieren. Sie sind mit Ausnahme der netzwerkbasierten Intermediation nicht auf Handlungen Dritter angewiesen, um Änderungen im verteilten Register des Systems zu veranlassen.¹³⁹⁸ Wie bereits im Rahmen der Ausführungen zu den Gegenparteirisiken erwähnt, macht die Verwendung dezentraler Netzwerke die direkte Übertragung von Kryptovermögenswerten zwischen den beteiligten Endbegünstigten möglich.¹³⁹⁹

Diese Neuerung wird insb. darum möglich, weil, wie oben gesehen, in dezentralen Handelsplattformen auch Intermediäre im Abrechnungs- und Abwicklungsbereich obsolet sind. Namentlich erlaubt die technische Integration des DvP-Mechanismus in den Computercode einer dezentralen Handelsplattform, dass Kryptovermögenswerte nicht mehr länger bei einer Drittperson verwahrt werden müssen.¹⁴⁰⁰

Damit wirken dezentrale Handelsplattformen letztlich zwei Problemen entgegen: Einerseits kann der Inhaber der Kryptovermögenswerte Dritte von einer unerwünschten Nutzung des Gutes ausschliessen bzw. ihn in der vereinbarten Nutzung des Gutes überwachen (*right to exclude*). Letzteres ist etwa dann der Fall, wenn der Inhaber verhindern will, dass seine Vermögenswerte Gegenstand einer übermässigen Wertpapierleihe sind.¹⁴⁰¹ Andererseits sind Koordinationsprobleme ausgeschlossen, da nur noch der Inhaber über eine Rechtsposition hinsichtlich des Gutes verfügt. Er alleine bestimmt, was mit den Kryptovermögenswerten geschieht (*right to use*). Letzterer Punkt kann in einem intermediatisierten Verwahrungssystem relevant sein, weil mehrere

und einem «right to use» unterscheiden, jedoch von Property Rights als «coherent whole» ausgehen; Lee, *Crypto-Finance*, 212–213 («qualitative aspect of securities»).

¹³⁹⁸ Siehe Amler et al., *DeFi-ning DeFi*, 2.

¹³⁹⁹ Dies bereits «antizipierend» für Wertpapierverwahrungssysteme Mooney, *Cardozo Law Review* 1990, 414 («[...] future innovations in technology and settlement systems might increase direct relationships between market participants and issuers and permit less reliance on intermediary control.»).

¹⁴⁰⁰ Vgl. Mooney, *University of Pennsylvania Journal of Business Law* 2020, 399–401, der darauf hinweist, dass sich die intermediatisierte Wertpapierverwahrung aufgrund der Bedürfnisse der Marktteilnehmer nach intermediatisierter Abrechnung und Abwicklung entwickelte.

¹⁴⁰¹ Vgl. IOSCO, *Fintech Report*, 56 («automate the enforcement»); ferner Buckley/Arner/Zetzsche, *FinTech*, 121, welche den Ausschluss einer mehrfachen Verwendung eines Vermögenswerts hervorheben. Die Anbahnung des *GameStop*-Vorfalls im Frühjahr 2021 hätte wohl dadurch verhindert werden können, indem nicht mehr Effekten als im Markt ausstehend weiterverliehen worden wären; vgl. zur *Short-Squeeze*-Problematik in der Vergangenheit Lamont, in: Fabozzi, *Short Sale*, 195 m.w.H.

Personen scheinbar gleichzeitig über identische oder ähnliche Rechte an einem Vermögenswert verfügen, diesen aber aufgrund von Koordinationskosten nicht effizient nutzen. In der Praxis kann es trotz Ausschlussmöglichkeit zur Nicht- oder Fahlallokation von Ressourcen kommen (so etwa von Stimmrechten an einer Aktiengesellschaft). Dieses Koordinationsproblem wird in der Literatur als die *Tragik der Anti-Allmende* bezeichnet.¹⁴⁰²

e. Globale Liquidität und Transparenz

i. Fragmentierter Handel

Der Handel an den globalen Finanzmärkten ist trotz der grundsätzlichen wirtschaftlichen, rechtlichen und technologischen Vernetzung weiterhin stark fragmentiert.¹⁴⁰³ Die Qualität des Handels am jeweiligen Markt ist abhängig von den lokalen Bedingungen, die durch unterschiedliche Faktoren bestimmt werden. Dazu gehören neben der Regulierung des Handels insb. auch dessen Liquidität und Transparenz. Von der Fragmentierung sind traditionelle Märkte und zentrale Kryptohandelsplattformen gleichermaßen betroffen.¹⁴⁰⁴

Vorliegend wird der Begriff der Fragmentierung wie folgt verstanden: Der Markt für einen Vermögenswert ist *fragmentiert*, wenn ein Vermögenswert an unterschiedlichen Handelsplätzen und -systemen gehandelt wird, weshalb es nicht zur Zusammenführung von Aufträgen über diesen Vermögenswert kommen kann.¹⁴⁰⁵ Infolge Fragmentierung können die Liquidität und die (Preis-)Transparenz für den betreffenden Vermögenswert leiden.

¹⁴⁰² Vgl. Heller, Harvard Law Review 1998, 624, 670–671, der darauf hinweist, dass die Tragik der Anti-Allmende zu Koordinationsproblemen und somit zur Unternutzung eines Gutes führen kann; ferner Buchanan/Yoon, The Journal of Law and Economics 2000, 3–4.

¹⁴⁰³ Siehe etwa FSB, Report on Market Fragmentation, 1; ferner Claessens, BIS Working Papers Nr. 815, Oktober 2019, 4. Siehe zu den unterschiedlichen technischen Möglichkeiten der Vernetzung von modernen Wertpapiermärkten Donald, in: Arner et al., Networked securities markets, 88–89.

¹⁴⁰⁴ Vgl. hinsichtlich Kryptomärkte FSB, Crypto-asset markets, 5.

¹⁴⁰⁵ Siehe FSB, Report on Market Fragmentation, 27; Claessens, BIS Working Papers Nr. 815, Oktober 2019, 5; Stoll, Financial Analysts Journal 2008, 20.

ii. Fragmentierte Liquidität

Preise, die aufgrund von Angebot und Nachfrage entstehen, sind ein zentrales Element des wirtschaftswissenschaftlichen Verständnisses eines Marktes.¹⁴⁰⁶ Ein Markt, in welchem eine Transaktion innert kurzer Zeit zu einem Preis ausgeführt werden kann, der möglichst nahe am gegenwärtigen Marktpreis liegt, gilt gemeinhin als ein *liquider* Markt. Dabei ist die Geld-Brief-Spanne (Bid-Ask-Spread) in der Regel ein guter Indikator für Liquidität bzw. Illiquidität.¹⁴⁰⁷ Liquidität ist derart zentral, dass Marktteilnehmer, wenn sie die Wahl haben, in aller Regel den liquiden Markt auswählen: Dies hat zur Folge, dass Liquidität grundsätzlich dazu tendiert, weitere Liquidität anzuziehen.¹⁴⁰⁸

Allerdings findet sich in der beobachtbaren Fragmentierung der Märkte ein gewisser Widerspruch zu diesem Prinzip: In traditionellen Märkten bestimmt sich die Liquidität eines Marktes nach dem lokal verfügbaren Angebot an Liquidität. Die Fragmentierung von Finanzmärkten hat daher in aller Regel auch die Fragmentierung der gesamthaft verfügbaren Liquidität zur Folge.¹⁴⁰⁹ Zudem haben in den letzten Jahren die technologischen Entwicklungen zu einer vertieften Fragmentierung des Handels an traditionellen Wertpapierbörsen beigetragen.¹⁴¹⁰ Ein fragmentierter Handel wird tendenziell als eher nachteilig für die Marktliquidität eingestuft.¹⁴¹¹

Immerhin erlauben moderne Handelssysteme die indirekte Verknüpfung unterschiedlicher elektronischer Handelsplattformen miteinander: Mithilfe von Smart-Order-Routing- oder ähnlichen Systemen können Marktteilnehmer ihre Aufträge an denjenigen Handelsplätzen und -systemen ausführen lassen, an denen die günstigsten Abschlussbedingungen, d.h. unter Berücksichtigung von Preis und Transaktionskosten, bestehen.¹⁴¹² Dadurch kann die vorherr-

¹⁴⁰⁶ Ausführlich hierzu Hodgson, in: *The New Palgrave Dictionary of Economics, Markets, passim*; ferner für eine *interdisziplinäre* Sicht des Marktes Cantor/Henry/Rayner, *Making Markets*, 2–6.

¹⁴⁰⁷ Siehe Foucault/Pagano/Röell, *Market Liquidity*, 2; ferner Schwartz/Francioni, *Equity Markets*, 60–61 m.w.H.

¹⁴⁰⁸ Siehe Foucault/Pagano/Röell, *Market Liquidity*, 254–255; Stoll, *Financial Analysts Journal* 2008, 15–16.

¹⁴⁰⁹ So auch Donald/Miraz, *Fordham Journal of Corporate & Financial Law* 2019, 102–103.

¹⁴¹⁰ Siehe oben, [II.3.3b](#).

¹⁴¹¹ Siehe Foucault/Pagano/Röell, *Market Liquidity*, 239; *offenlassend* IOSCO, *Transparency and Market Fragmentation*, 11; *sehr kritisch* Mattli, *Darkness by Design*, 18–19.

¹⁴¹² Siehe Monsch, *Hochfrequenzhandel*, 29–30; Foucault/Pagano/Röell, *Market Liquidity*, 39–40, 44, 239 m.w.N.; Stoll, *Financial Analysts Journal* 2008, 18, 20–21; ferner Abegglen/Andreotti, *GesKR* 2020, 50–51.

schende marktbedingte Liquiditätsfragmentierung zu einem gewissen Grad überwunden werden.¹⁴¹³

Es muss jedoch damit gerechnet werden, dass die unterschiedlichen nationalen Aufsichts- und Regulierungsregime weiterhin ein schwer überwindbares Hindernis auf dem Weg zur Erreichung globaler Liquidität in traditionellen Finanzmärkten darstellen.¹⁴¹⁴

iii. Fragmentierte Transparenz

Neben der Fragmentierung der Marktliquidität besteht in traditionellen Finanzmärkten eine ausgeprägte Fragmentierung der Markttransparenz.

Die Verteilung relevanter Informationen über unterschiedliche Handelsplätze und -systeme führt zu einer Verschlechterung der Informationslage der Marktteilnehmer. Davon ist insb. die Preistransparenz in Form von Vor- und Nachhandelsdaten betroffen.¹⁴¹⁵ DONALD und MIRAZ fordern daher die Verwendung von private bzw. permissioned DLT-Technologie zur Zusammenführung von Preisinformationen unterschiedlicher traditioneller Handelsplätze und -systeme *auf einer Plattform*.¹⁴¹⁶ DAVID YERMACK weist auf die Vor- und Nachteile gesteigerter Transparenz und Liquidität im Hinblick auf die Corporate Governance von Unternehmen bei Verwendung von permissionless Blockchains hin.¹⁴¹⁷

Allgemein ist festzustellen, dass sich die Markttransparenz in der traditionellen Finanzwelt aufgrund zunehmend längerer und somit fragmentierter Intermediationsketten verringert hat – z.B. im Bereich von Verbriefungen und Fund-of-Funds-Strukturen.¹⁴¹⁸ Zudem hängt die Informationsleistung der

¹⁴¹³ Siehe IOSCO, Changes in Market Structure, 22; kritisch Zimmermann, in: Strebel-Aerni, Umbruch, 131.

¹⁴¹⁴ Ähnlich Stoll, Financial Analysts Journal 2008, 24–25.

¹⁴¹⁵ Siehe Claessens, BIS Working Papers Nr. 815, Oktober 2019, 11–12; Donald/Miraz, Fordham Journal of Corporate & Financial Law 2019, 107.

¹⁴¹⁶ Siehe Donald/Miraz, Fordham Journal of Corporate & Financial Law 2019, 104, 109, 139–140.

¹⁴¹⁷ Siehe Yermack, Review of Finance 2017, 17–22.

¹⁴¹⁸ Siehe etwa Judge, Stanford Law Review 2012, 659–660, 690–697, welche zusätzliche intermediäre Prozesse und Strukturen im Bereich des Shadow Banking als «fragmentation nodes» bezeichnet; ferner Haldane, in: Jansen/Schröter/Steher, Rethinking, 253–254 («Counterparty risk is not just unknown; it is almost unknowable. And the higher the dimensionality of the network, the greater that uncertainty.»); ferner hinsichtlich der Nutzung von Fund of Funds-Strukturen Judge, The University of Chicago Law Review 2015, 608, 626–627.

Marktteilnehmer sowie deren Abhängigkeit von Finanzintermediären wesentlich von der Komplexität der vertriebenen Finanzprodukte ab.¹⁴¹⁹ Weil Transparenz die Entscheidungsunsicherheiten der Marktteilnehmer verringert, führt ein Mangel an Transparenz grundsätzlich zu einer Erhöhung mikro- und makroökonomischer Risiken.¹⁴²⁰ Andererseits ist darauf hinzuweisen, dass das Ziel grösstmöglicher Transparenz in komplexen Systemen die verhaltensbedingte Unsicherheit der Marktteilnehmer nicht zwangsläufig verringert, sondern unter Umständen sogar vergrössern kann.¹⁴²¹

Daraus kann geschlossen werden, dass eine eindimensionale Perspektive von Markttransparenz ungenügend ist, wenn gleichzeitig die Komplexität des heutigen Finanzsystems aufgrund von dessen Vernetzung und umfassenden Homogenität ausgeblendet wird. So sind etwa die konzentrierte, nichtmodulare Struktur des Finanzintermediationssystems und die mangelhafte Diversität im Risikoverhalten der Marktteilnehmer ebenfalls als wesentliche Treiber systemischer Risiken zu betrachten.¹⁴²²

iv. Dezentrale Handelsplattformen

«*Information wants to be free.*»¹⁴²³ Im Gegensatz zu diesem bekannten Diktum bilden die heute vorherrschenden Informationsintermediäre, namentlich Facebook, Google und Twitter, Informationssilos. Die Portabilität von Information aus solchen geschlossen Umgebungen ist nicht oder nur ungenügend gewährleistet. Dezentralisierung, verstanden als die Rückgabe der Entscheidungsgewalt und Kontrolle an den Nutzer von Internetplattformen, kann allerdings die bestehenden Informationssilos zunehmend auflösen.¹⁴²⁴ Wie im ers-

¹⁴¹⁹ Siehe Awrey, Harvard Business Law Review 2012, 238–239, 246–253, 267; Judge, The University of Chicago Law Review 2015, 615, 627–628.

¹⁴²⁰ Siehe Willke, in: Jansen/Schröter/Stehr, Transparency after the Financial Crisis, 64–69; Judge, Stanford Law Review 2012, 696–701.

¹⁴²¹ Siehe Tyrell/Böhme, in: Jansen/Schröter/Stehr, Resonanzkatastrophe, 293–294; Schwarcz, Washington University Law Review 2009, 245–246, der die potenziell negativen Feedbackmechanismen der Bilanzierung von Vermögenswerten zu Marktpreisen betont; aus allgemeiner Warte sodann Schwarcz, University of Illinois Law Review 2004, 16 («*In a world of complexity, disclosure alone will sometimes be insufficient to remedy the information asymmetry between the originator and its investors.*»).

¹⁴²² Siehe Haldane, Nature 2011, 355; Becker/Willke, in: Jansen/Schröter/Stehr, Information and Knowledge Asymmetries, 237–238 m.w.H.; ferner Schwarcz, Washington University Law Review 2009, 247–250, der als Antwort auf die Komplexität des Finanzsystems die Einführung eines «market liquidity provider» in Krisenfällen vorschlägt.

¹⁴²³ Siehe zum Ursprung dieses Ausspruchs Wagner, Columbia Law Review 2003, 999 FN 14.

¹⁴²⁴ So bereits Yeung et al., Future of Online Social Networking, *passim*.

ten Kapitel dieser Arbeit erwähnt, bildet die Rückgabe der Datenhoheit an den einzelnen Nutzer eines der Hauptziele des Web 3.0.¹⁴²⁵

Gleich verhält es sich mit der *Liquidität*, die in der Welt der Kryptovermögenswerte nunmehr ein rein informationelles Phänomen darstellt. Die Verfügbarkeit von Liquidität ist damit nicht mehr auf den jeweiligen Markt begrenzt oder etwa von den Betreibern von Smart-Order-Routing-Systemen abhängig. Aufgrund der Eigenschaft dezentraler Applikationen, offen und frei zugänglich zu sein, können dezentrale Handelsplattformen *globale* Orderbücher entwickeln, die eine im Vergleich zu traditionellen Handelsplattformen beispiellose Liquidität aufweisen.¹⁴²⁶

Marktteilnehmer sind fähig, über die interoperablen Schnittstellen der verwendeten Protokolle potenziell einen globalen Liquiditätspool anzusteuern.¹⁴²⁷ Die Literatur spricht darum von «networked liquidity».¹⁴²⁸ Dies wird im Bereich dezentraler Handelsplattformen besonders an Protokollen sichtbar, welche die Informationen aus unterschiedlichen Protokollen und somit unterschiedliche Liquiditätspools aggregieren. Konkret vergleichen Smart Contracts oder Relay Nodes die Bedingungen verschiedener Plattformen miteinander und wickeln – nicht unähnlich zu Smart-Order-Routing-Systemen – einen Auftrag unter Verwendung der entsprechenden Protokolle zu den für den Nutzer günstigsten Bedingungen ab.¹⁴²⁹ Dadurch kann in technischer Hinsicht die technische Best Execution des Auftrags gewährleistet werden. Dadurch wird eine Situation geschaffen, die mit der Konzentration von Liquidität vergleichbar ist, ohne dabei aber die Risiken bei einem Marktteilnehmer ansammeln zu müssen.¹⁴³⁰

Ausserdem muss die Liquidität nicht auf einzelne dezentrale Systeme beschränkt sein. So kann die Liquidität des gesamten Ökosystems, d.h. unterschiedlicher dezentraler Systeme, miteinander verbunden werden: Das derzeit wohl bekannteste Beispiel ist die Tokenisierung von bitcoins in Form von ERC-20 Token auf der Ethereum Blockchain – sog. *Wrapped bitcoins*, *wBTC*. Ein kleiner Anteil aller umlaufenden bitcoins werden dadurch auf Ethereum

¹⁴²⁵ Siehe oben, [II.4.3b](#).

¹⁴²⁶ Siehe Ehrsam, Why Decentralized Exchange Protocols Matter, Medium, *passim*; Chen/Bellavitis, Journal of Business Venturing Insights 2020, 3.

¹⁴²⁷ Gl.M. Zetzsche/Arner/Buckley, Journal of Financial Regulation 2020, 202.

¹⁴²⁸ Siehe Lin, Stanford Journal of Blockchain Law & Policy 2019, 74; Harvey/Ramachandran/Santoro, DeFi, 68; vgl. im Zusammenhang mit dem Relayer-Netzwerk von 0x, 0x, Core Concepts, Networked liquidity, *passim*.

¹⁴²⁹ Siehe Schär, Federal Reserve Bank of St. Louis Review 2021, 156, der vom «aggregation layer» spricht.

¹⁴³⁰ Ähnlich Donald/Miraz, Fordham Journal of Corporate & Financial Law 2019, 137.

verfügbar gemacht.¹⁴³¹ Diese Tokenisierung erhöht die im Ethereum Netzwerk zur Verfügung stehende Liquidität. Neben der noch intermediatisierten Lösung von WBTC existieren bereits disintermediatisierte Protokolle mit dem Ziel, die Interoperabilität unterschiedlicher dezentraler Systeme zu erhöhen und in diesem Rahmen etwa Cross-Chain Swaps zu ermöglichen.¹⁴³² Ferner bietet die dezentrale Handelsplattform Serum, die auf der Blockchain *Solana* operiert, eine Ethereum-Anbindung an, die es ihr erlaubt hat, von Beginn mit einer höheren Marktliquidität zu operieren, ohne dabei auf einen traditionellen Intermediär zurückgreifen zu müssen.¹⁴³³

Sodann kann in dezentralen Systemen durch die Eliminierung der Intermediationsketten die Komplexität der Prozesse und Strukturen deutlich verringert werden, was sich positiv auf die *Transparenz* der Funktionsweise der Märkte und dadurch voraussichtlich auch auf die Prävention systemischer Risiken auswirkt.¹⁴³⁴ Ferner erfolgt der Handel auf einer dezentralen Handelsplattform abhängig vom konkreten Modell vollständig transparent. Dadurch können etwa Aussenstehende die Preisbildung anhand der Transaktionsdetails nachvollziehen.¹⁴³⁵ Daneben sind auch die Informationen zu den an einer Transaktion beteiligten Adressen von Wallets bzw. Konten und Smart Contracts öffentlich einsehbar.¹⁴³⁶ An die Stelle der Datensilos traditioneller Finanzintermediation kann theoretisch ein globales Register über alle Transaktionen treten.¹⁴³⁷ Die dadurch erreichte Transaktionstransparenz erlaubt für sich alleine noch keine eindeutige Zuordnung der Wallet-Adressen zu den bürgerlichen Identitäten der betreffenden Inhaber der Vermögenswerte.¹⁴³⁸

¹⁴³¹ Siehe WBTC, Order Book, *passim*.

¹⁴³² Siehe etwa die Projekte Ren, Home, GitHub, *passim*, und THORChain, Introduction, *passim*, die beide als Weiterentwicklungen der Ideen hinter Atomic Swaps und tokenisierten Vermögenswerten betrachtet werden können.

¹⁴³³ Siehe Serum Foundation, White Paper, 7–9.

¹⁴³⁴ So wohl auch Avgouleas/Kiayias, European Business Organization Law Review 2019, 105, 106–107; vgl. hinsichtlich positiver Effekte durch die Verkürzung der Intermediationsketten bei *Finanzinnovationen* im Shadow Banking Judge, Stanford Law Review 2012, 713–720; ferner Chen/Bellavitis, Journal of Business Venturing Insights 2020, 3–4, die u.a. von «radical transparency» sprechen.

¹⁴³⁵ Vgl. Benos/Garratt/Gurrola-Perez, Ledger 2019, 130; ESMA, DLT Report, 5, 11–12, wobei allerdings auch auf das Spannungsverhältnis zwischen umfassender Datentransparenz und missbräuchlichen Verhaltensweisen in DLT hingewiesen wird.

¹⁴³⁶ Siehe Harvey/Ramachandran/Santoro, DeFi, 63–64.

¹⁴³⁷ Vgl. Euroclear/Slaughter and May, Blockchain Settlement, 7; DTCC, Embracing Disruption, 10.

¹⁴³⁸ Demgegenüber bestehen Vorschläge, DLT insb. zwecks Erreichung von Eigentümertransparenz zu verwenden; vgl. Nougayrède, Journal of Financial Regulation 2018, 305–306; ferner in Bezug auf KYC Euroclear/Oliver Wyman, Blockchain in Capital Markets, 12, 15.

Dezentrale Handelsplattformen machen aufgrund ihrer offenen und interoperablen Natur echte globale Märkte erst möglich: Diese virtuellen Märkte sind rund um die Uhr offen, mit wenigen Ausnahmen uneingeschränkt zugänglich und verfügen theoretisch über die gesamte Liquidität, die sich auf Kryptowährungen und tokenisierte Vermögenswerte zurückführen lässt.¹⁴³⁹ Zu erwähnen ist allerdings, dass die Geschwindigkeit der Kommunikation zwischen den Nutzern solcher Protokolle aufgrund der globalen Natur der Liquidität fast zwangsläufig tiefer als im traditionellen Bereich ausfallen muss. Das Problem, dass dezentrale Handelsplattformen im Vergleich zu zentralisierten Modellen eine höhere Latenz aufweisen, lässt sich aus physikalischen Gründen nur bedingt beheben.¹⁴⁴⁰

Gleichzeitig ist der Handel weitgehend transparent, sodass Preisinformationen sowie Informationen zu den beteiligten Wallets und Smart Contracts effizient verarbeitet werden können.

Im Gegensatz zu traditionellen Finanzmärkten haben schliesslich Rechtssysteme zumindest derzeit keinen oder einen nur sehr eingeschränkten Einfluss auf den Grad der Fragmentierung dezentraler Handelsplattformen.¹⁴⁴¹ Mit anderen Worten besteht grundsätzlich keine regulierungsbedingte geografische Fragmentierung von Märkten. Die Existenz von Fragmentierung in dezentralen Handelsplattformen ist demgegenüber vielmehr auf technologiebedingte Inkompatibilitäten zwischen den einzelnen Protokollen und einen Mangel an interoperablen Protokollen zurückzuführen.

Es kann zusammengefasst werden, dass der Einsatz dezentraler Handelsplattformen das Potenzial hat, die in traditionellen Märkten bestehende Fragmentierung von Liquidität und Transparenz zu verbessern.¹⁴⁴²

¹⁴³⁹ Siehe zu den Folgen der *Virtualisierung* des Handels bereits Bernet, Finanzintermediation, 170.

¹⁴⁴⁰ Siehe Messari Research, DEX v. EX, *passim*; ferner zur Latenzzeit von Blockchains Lin, Stanford Journal of Blockchain Law & Policy 2019, 73, 75; sodann bereits in Bezug auf die Netzwerkebene Buterin, On Settlement Finality, *passim*.

¹⁴⁴¹ Vgl. demgegenüber die Auswirkungen von Aufsicht und Regulierung auf die Fragmentierung von traditionellen Märkten FSB, Report on Market Fragmentation, 4–5; ferner Claessens, BIS Working Papers Nr. 815, Oktober 2019, 9–10.

¹⁴⁴² So auch, allerdings in Bezug auf private bzw. permissioned DLT Donald/Miraz, Fordham Journal of Corporate & Financial Law 2019, 139–140.

f. Reduktion von Rent Seeking

i. Rent Seeking und Regulatory Capture

Wie bereits ausgeführt, handeln Marktteilnehmer im Wirtschaftsgeschehen, wenn immer möglich, eigennützig und opportunistisch. Nach den Annahmen der ökonomischen Theorie der Politik (*Public Choice*) gilt dies allerdings auch für staatliche Akteure, wie etwa Politiker und Behördenvertretern.¹⁴⁴³ An die Stelle von Gütern und Dienstleistungen tritt in politischen Märkten der Austausch von Versprechungen und Stimmen.¹⁴⁴⁴ Als besondere Formen opportunistischer Verhaltensweisen in politischen Märkten sind Rent Seeking und Regulatory Capture zu verstehen:

Unter *Rent Seeking* wird in der politischen Ökonomie das institutionelle Verhalten von Marktteilnehmern verstanden, «politische Renten» etwa in Form von staatlichen Direktzahlungen, Preispolitik, Steuererleichterungen, Zöllen oder Marktregulierung zu erlangen. Infolge dieses Verhaltens erlangt der Marktteilnehmer wirtschaftliche Vorteile, ohne eine marktkonforme oder zumindest sozialadäquate Leistung zu erbringen.¹⁴⁴⁵ Die Erlangung solcher Vorteile, die in aller Regel dem eigenen wirtschaftlichen Fortkommen dienen, geht mit anderen Worten zulasten der übrigen Marktteilnehmer im Besonderen und der Gesellschaft im Allgemeinen. Dadurch grenzt sich Rent Seeking von dem in einer Marktwirtschaft erwünschten Profit Seeking ab.¹⁴⁴⁶ Sodann werden in der Literatur teils auch Urheber- und Patentrechte aufgrund ihres staatlich gewährten Monopolcharakters als politische Renten bezeichnet.¹⁴⁴⁷

¹⁴⁴³ Siehe bereits von Mises, *Bureaucracy*, 78–79; Downs, *Economic Theory of Democracy*, 27–31; Arrow, in: Haveman/Margolis, *Market Allocation*, 514–515; sodann grundlegend Buchanan/Tullock, in: *Liberty Fund, The Calculus of Consent*, 16–19; ferner Butler, *Public Choice*, 21–25; Tullock/Seldon/Brady, *Government Failure*, 5–6; eine ausführlich Übersicht findet sich auch bei Kirchgässner, *Homo Oeconomicus*, 102–134.

¹⁴⁴⁴ Siehe North Douglass C., *Journal of Theoretical Politics* 1990, 362.

¹⁴⁴⁵ Siehe Buchanan, in: *Liberty Fund, Rent Seeking and Profit Seeking*, 103–107; kritisch gegenüber dem Begriff Tullock/Seldon/Brady, *Government Failure*, 43–44 («If someone is observed receiving a rent or, for that matter, engaging in activities that might lead to the rent, the first thought should be to inquire whether society as a whole is better off as a result of the activity or product that generates the rent.»).

¹⁴⁴⁶ Siehe zum Konzept des Rent Seeking erstmals Tullock, *Western Economic Journal* 1967, *passim*; ferner zur Begriffsbegründung Krueger, *The American Economic Review* 1974, 291; sodann auch Stigler, *The Bell Journal of Economics and Management Science* 1971, 3–6, 10.

¹⁴⁴⁷ Siehe Boldrin/Levine, *Against Intellectual Monopoly*, 68–69, 76, 101–102, 171, 232, 260; Kinsella, *Against Intellectual Property*, 35; differenzierend Landes/Posner, *Intellectual Property Law*, 17–18, 21–24, 374, 406–419.

Rent Seeking tritt schliesslich auch in Form von *Rent Extraction* auf: In diesem Fall geht das Rent-Seeking-Verhalten vom Staat, namentlich von Angehörigen der Legislative oder Beamten, aus. Ein möglicher Anwendungsfall ist der Verzicht angedrohter Regulierungsmassnahmen im Austausch für politische Renten.¹⁴⁴⁸

Es ist davon auszugehen, dass Rent Seeking in einer «reinen» Marktwirtschaft aufgrund der beschränkten Rolle des Staates wohl marginal ausfiele.¹⁴⁴⁹ Das sozusagen notwendige Gegenstück zum Rent-Seeking-Verhalten Privater bildet deshalb das Konzept der *Regulatory Capture*.¹⁴⁵⁰ Diesem Ansatz liegt die Annahme zugrunde, dass staatliche Regeln nur ausnahmsweise das Ergebnis einer Abwägung von öffentlichen Interessen darstellen. Namentlich führt Rent Seeking dazu, dass der Gesetzgeber oder eine staatliche Behörde, welche im Auftrag des Gesetzgebers tätig ist, aufgrund des Einflusses von Marktteilnehmern wohlfahrtsökonomisch suboptimale Regeln erlässt und damit soziale Kosten für die Allgemeinheit erzeugt.¹⁴⁵¹ Demgegenüber kann der individuelle Nutzen von Rent Seeking für den einzelnen Marktteilnehmer die damit zusammenhängenden Kosten um ein Vielfaches übersteigen.¹⁴⁵² Der Nutzen fällt konzentriert aus, während die Kosten von allen getragen werden. Entsprechend kann auch erklärt werden, weshalb Industrieteilnehmer – im Unterschied zu Konsumenten – trotz der teils sehr unterschiedlichen Ziele kollektive Handlungsprobleme durch gemeinsames Lobbying überwinden können.¹⁴⁵³ Die Erkenntnis, dass staatliche Regeln kaum jemals neutral ausgestaltet werden, findet sich auch in der sozioökonomischen Forschung.¹⁴⁵⁴

¹⁴⁴⁸ Siehe hierzu McChesney, *Money for Nothing*, 22–23.

¹⁴⁴⁹ Teils kritisch Fischer, *Rent-Seeking, Institutions and Reforms*, 26–33 m.w.N.

¹⁴⁵⁰ G.L.M. wohl Lyons, *University of Michigan Journal of Law Reform* 2009, 277; in historischer Hinsicht für England sodann Capie, in: Mayes/Wood, *Historical perspective on financial regulation*, 84.

¹⁴⁵¹ So bereits der Wohlfahrtsökonom Pigou, *Economics of Welfare*, 296 («For we cannot expect that any State authority will attain, or will even whole-heartedly seek, that ideal. Such authorities are liable alike to ignorance, to sectional pressure and to personal corruption by private interest.»); ferner Stigler, *The Bell Journal of Economics and Management Science* 1971, 3 («A central thesis of this paper is that, as a rule, regulation is acquired by the industry and is designed and operated primarily for its benefit.»), 10; Peltzman, *The Journal of Law & Economics* 1976, 211–212; Laffont/Tirole, *The Quarterly Journal of Economics* 1991, 1089–1090.

¹⁴⁵² Siehe Tullock, *Western Economic Journal* 1967, 230; ausführlich Butler, *Public Choice*, 76–81.

¹⁴⁵³ Vgl. auch Olson, *Collective Action*, 141–148, der hinsichtlich Organisationsfähigkeit insb. auf die Grösse der organisierten Gruppe abstellt; ähnlich Riker, *Political Coalitions*, *passim*.

¹⁴⁵⁴ Vgl. Fligstein, *American Sociological Review* 1996, insb. 660–662.

Namentlich Wirtschaftssektoren, in dem ausgeprägte Informationsasymmetrien zwischen dem Staat als «Prinzipal» und den Marktteilnehmern als «Agenten» bestehen, gelten als besonders anfällig für Regulatory Capture.¹⁴⁵⁵ Genau genommen handelt es sich dabei allerdings um ein Kontroll- und Vertrauensproblem der Regierten gegenüber den Regierenden.¹⁴⁵⁶ Paradoerweise dienen Informationsasymmetrien damit nicht nur als Regulierungsanlass,¹⁴⁵⁷ sondern sie sind auch verantwortlich für Regulatory Capture.¹⁴⁵⁸ Es ist ferner davon auszugehen, dass insb. auch die Anzahl und Komplexität von Regeln das Rent-Seeking-Verhalten von Marktteilnehmern und infolgedessen die Auswirkungen eines allfälligen Regulatory Capture verstärken können.¹⁴⁵⁹ In derartigen Interventionsbereichen ist mit anderen Worten am ehesten mit Staats- und Regulierungsversagen zu rechnen.¹⁴⁶⁰

Beim Finanzsektor und dessen ausufernden (Über-)Regulierung¹⁴⁶¹ handelt es sich aufgrund der festgestellten Komplexitäten¹⁴⁶² sowie der Höhe der realisierbaren politischen Renten um einen besonders für Rent Seeking und Regulatory Capture anfälligen Wirtschaftszweig.¹⁴⁶³ Das Wettbewerbsniveau ist

¹⁴⁵⁵ Vgl. zu den theoretischen Grundlagen Laffont, *Econometrica* 1994, 508 («The framework is a principal-agent set up in which the principal is the State or the regulatory institution and the agent is the regulated firm. The principal maximizes social welfare under incentive constraints which result from the informational advantage of the agent and its strategic behavior.»); ferner Dal Bó, *Oxford Review of Economic Policy* 2006, 207–211.

¹⁴⁵⁶ Vgl. Levine/Forrence, *Journal of Law, Economics, & Organization* 1990, 170–171, 185.

¹⁴⁵⁷ Siehe etwa Ogus, *Regulation*, 38–41, 121; ferner Kahn, *Economics of Regulation*, 2.

¹⁴⁵⁸ Siehe Koopman/Mitchell/Thierer, *The Journal of Business, Entrepreneurship & the Law* 2015, 535.

¹⁴⁵⁹ So auch Buchanan, in: *Liberty Fund, Rent Seeking and Profit Seeking*, 108–109; ferner BRTF, *Imaginative Better Regulation*, 19.

¹⁴⁶⁰ Siehe Buchanan, in: *Liberty Fund, Politics without Romance*, 46–47; sodann bereits Coase, *Journal of Law and Economics* 1960, 28 («The kind of situation which economists are prone to consider as requiring corrective Government action is, in fact, often the result of Government action. Such action is not necessarily unwise. But there is a real danger that extensive Government intervention in the economic system may lead to the protection of those responsible for harmful effects being carried too far.»); weniger pessimistisch demgegenüber Stiglitz, in: Balleisen/Moss, *Government Failure vs. Market Failure*, 36 («So long as there is sufficient transparency and competition, there are corrective processes. Governments that fail will be replaced; they lose their credibility and legitimacy.»).

¹⁴⁶¹ Differenzierend in dieser Thematik Nobel, *SZW* 2014, 595–597, der in der Komplexität der Bankenregulierung, im internationalen Harmonisierungsdruck sowie im ideologischen Übereifer die Überregulierung des Finanzsektors begründet sieht; kritisch ferner Hettich, in: *SGK BV, Art. 98 N 11*.

¹⁴⁶² Siehe oben, [II.5.3c.iii](#).

¹⁴⁶³ Siehe etwa Arthur/Booth, *Does Britain Need a Financial Regulator?*, 125–148, 149 m.w.N.; ferner Bainbridge, *Minnesota Law Review* 2011, 1784–1788, 1815–1818; Ribstein, *Houston*

zudem im Vergleich zu anderen Industrien deutlich tiefer.¹⁴⁶⁴ Namentlich im Finanzmarktinfrastrukturbereich bestehen regelmässig natürliche Monopole,¹⁴⁶⁵ weshalb von dezentralen Ansätzen Verbesserungen erwartet werden können.¹⁴⁶⁶ Die Realisierbarkeit von politischen Renten hat sodann insb. auch mit dem in aller Regel weiten technischen Ermessen der Finanzmarktaufsichtsbehörden zu tun.¹⁴⁶⁷ Zudem verschärft auch die quantitativ substantielle Verschiebung der Normkompetenzen vom Gesetzgeber zur Exekutive die Problematik.¹⁴⁶⁸

Das mit der traditionellen Finanzintermediation verbundene Rent Seeking kann sich in Form von negativen Externalitäten bzw. Systemrisiken manifestieren: So wird mit überzeugenden Argumenten dargelegt, dass das ausgeprägte Rent-Seeking-Verhalten von Banken zu einer hohen Konzentration von Marktmacht und infolgedessen zu Marktverzerrungen und somit Fehlallokationen von Kapital und Risiken in der Finanzkrise 2007-08 geführt haben.¹⁴⁶⁹ Als Beispiele für die immense Machtkonzentration im Finanzsektor mögen auch die vielen Skandale und Krisen der letzten Jahre dienen. Erwähnt seien lediglich Lehman (2008), Madoff (2008), Libor (2011), Devisenhandel (2013), Gold- und Silberfixing (2014), Wirecard (2020) und die zahlreichen internationalen Geldwäschereiskandale der letzten Jahre. Bezeichnend – und politisch zumindest mitverursacht – ist sodann die Herausbildung systemrelevanter Fi-

Law Review 2003, 79; Romano, The Yale Law Journal 2005, 1526, 1591–1594, welche Politiker, die industriegetriebene Regulierungsvorschläge umsetzen, als «policy entrepreneurs» bezeichnet.

¹⁴⁶⁴ Siehe Weber, SZW 2009, 430.

¹⁴⁶⁵ Siehe etwa Mainelli/Milne, SWIFT Institute Working Paper Nr. 2015-007, 9. Mai 2016, 17.

¹⁴⁶⁶ Siehe FSB, Financial Stability Implications FinTech, 13, 16.

¹⁴⁶⁷ Vgl. hinsichtlich der EBK bzw. FINMA die konstante Rechtsprechung des Bundesgerichts: BGE 135 II 356, E. 3.1 («Die Frage, wie die EBK ihre Aufsichtsfunktion im Einzelnen erfüllt, ist weitgehend ihrem 'technischen Ermessen' anheimgestellt. Das Bundesgericht kann nur bei Rechtsverletzungen in die Beurteilung von dessen Handhabung durch das Bundesverwaltungsgericht korrigierend eingreifen [...]»); BGE 132 II 382, E. 4.1; BGE 131 II 306, E. 3.1.2; ferner BVGer B-488/2018 vom 17. Januar 2019, E. 4.3 («fachtechnischer Beurteilungsspielraum»); in empirischer Hinsicht sodann Zulauf/Gava, SZW 2019, 111; vgl. sodann hinsichtlich möglicher Auswirkungen des Begriffs der «financial institution» gemäss US-amerikanischem Geldwäschereirecht Van Valkenburgh, Bank Secrecy Act, insb. 4–6.

¹⁴⁶⁸ Siehe Nobel, BJM 2015, 151–153; allgemein aus US-amerikanischer Warte Hamburger, Administrative Law, *passim*.

¹⁴⁶⁹ Siehe Avgouleas, Global Financial Markets, 128–129, 146–149; ferner Khwaja/Mian, Annual Review of Economics 2011, 581, 594–595 m.w.N.; Zhang, Market Concentration and Rent Seeking, Harvard, John. M. Olin Center for Law, Economics, and Business, Fellows' Discussion Paper Series, Discussion Paper Nr. 72, 25. April 2017, 4.

nanzinstitute, die über eine implizite oder explizite Staatsgarantie verfügen.¹⁴⁷⁰ Dies alles verringert im Ergebnis den Wettbewerb im Finanzsektor und kann die Kosten für Anleger und Konsumenten sowie die Allgemeinheit in Form der Steuerzahler erhöhen.¹⁴⁷¹

ii. Dezentrale Handelsplattformen

Vorab zu erwähnen ist, dass zwischen (technologischer) Innovation sowie Rent Seeking und Regulatory Capture ein grundlegendes Spannungsverhältnis besteht: Innovation verringert einerseits opportunistisches Verhalten, indem es auf die etablierten Firmen einen fortwährenden Anpassungsdruck ausübt. Rent Seeking verringert andererseits Innovation, indem Marktherausforderer aufgrund von Markteintrittsbarrieren nur zu sehr hohen Kosten mit etablierten Firmen konkurrieren können.¹⁴⁷²

DeFi tangiert staatliche Regulierung sowohl im Finanzsektor als auch in Bezug auf das Internet. In beiden Bereichen sind Rent Seeking und Regulatory Capture ubiquitäre Probleme, die aus Sicht der Allgemeinheit nicht wünschenswert sind.¹⁴⁷³ Allerdings bewegt sich DeFi zu einem gewissen Grad *ausserhalb* des Einflussbereiches von Staaten und internationalen Organisationen. Der Verzicht auf Intermediäre hat in zweifacher Hinsicht positive Auswirkungen auf die Realisierbarkeit politischer Renten: Das Fehlen zentraler Anlaufstellen mit oder ohne staatlicher Zwangsbefugnis *reduziert* die Anfälligkeit dezentraler Systeme nicht nur für Rent Seeking durch die Teilnehmer eines Systems,

¹⁴⁷⁰ Siehe etwa die Untersuchung von Acharya/Anginer/Warburton, End of Market Discipline, 3–7 (*«Comparing financial firms to non-financial firms, we find that while a positive relation exists between risk and credit spreads for medium and small financial institutions, the risk-to-spread relation is significantly weaker for the largest institutions. [...] We find that passage of Dodd-Frank Act did not significantly alter investor expectations of future government support for large financial institutions.»*).

¹⁴⁷¹ Siehe etwa Zellweger-Gutknecht, Vernehmlassung BankG, 2–5, welche insb. kritisiert, dass der Public Liquidity Backstop (PLB), so wie ursprünglich geplant, zu einer Sozialisierung von Bankverlusten hätte führen können und somit ein ungemeines Risiko für die Steuerzahler dargestellt hätte; nunmehr einen Ex-ante-Finanzierungsmechanismu beinhaltend Botschaft BankG 2023, 19.

¹⁴⁷² Siehe hierzu Kidd, Chicago-Kent Law Review 2018, 175–177, aus dessen Sicht insb. die Geschwindigkeit von Innovation massgeblich für die praktischen Auswirkungen dieses Spannungsverhältnisses ist.

¹⁴⁷³ Siehe zu letzterem bereits Lee, Entangling the Web, New York Times, *passim* (*«The reason is simple: a regulated industry has a far larger stake in regulatory decisions than any other group in society. As a result, regulated companies spend lavishly on lobbyists and lawyers and, over time, turn the regulatory process to their advantage.»*).

sondern insb. auch für Regulatory Capture der Entscheidungsträger.¹⁴⁷⁴ Für vollständig dezentralisierte und somit staatlich unkontrollierbare Systeme ist sogar davon auszugehen, dass politische Renten unrealisierbar sind. In diesem Sinne stellt JEREMY KIDD richtigerweise fest: «*Power draws rent-seeking, not the other way around, and as government has grown increasingly powerful, the level of rent-seeking has assuredly grown with it.*»¹⁴⁷⁵ Selbst für den Fall, dass Teilnehmer eines dezentralen Netzwerks etwa in kartellierter Weise politische Renten in Form von staatlichen Sonderrechten anstreben würden, wären die Effekte in einem dezentralen System deutlich weniger ausgeprägt.

Theoretisch ist denkbar, dass die Willensbildung in einer DAO einer dezentralen Handelsplattform und in der Folge deren Governance durch besser informierte Teilnehmer zu deren Gunsten beeinflusst wird, doch wäre die Koordination solcher Anstrengungen aufgrund der Dezentralisierung von Entscheidungsgewalt und Kontrolle in DeFi-Projekten mit deutlich höheren Kosten als in der traditionellen Finanzmarktregulierung verbunden. Dort allerdings, wo ein Projekt weiterhin von einem überschaubaren Entwicklerteam kontrolliert wird,¹⁴⁷⁶ könnten sich Marktteilnehmer um vergleichbare politische Renten bemühen. Ein Beispiel wäre etwa die Erhöhung der Handelsgebühren aufgrund der Bemühungen einzelner einflussreicher Marktteilnehmer, die von einer solchen Protokolländerung direkt profitieren. Angesichts der tiefen Markteintrittshürden für neue Projekte im Bereich von DeFi müssten solche Anstrengungen aber in den meisten Fällen ohnehin relativ wirkungslos bleiben.¹⁴⁷⁷ Die negativen Auswirkungen allfälliger Rent-Seeking-Versuche auf den allgemeinen Wohlstand könnten wohl erheblich verringert werden.

¹⁴⁷⁴ Siehe insb. Kidd, Chicago-Kent Law Review 2018, 174–175, der sich allerdings auf FinTech im Allgemeinen bezieht; Davidson/De Filippi/Potts, Economics of Blockchain, 13–14; Yermack, Review of Finance 2017, 8; vgl. auch, aber scheinbar ausschliesslich hinsichtlich der nach Auffassung der Autoren heute übermässigen ökonomischen Renten von Finanzintermediären Avgouleas/Kiayias, European Business Organization Law Review 2019, 102, 107. Ähnlich De Filippi/Vieira, The Columbia Science & Technology Law Review 2014, 139, welche von einer Reduktion der Commodification von in dezentralen Gemeinschaften produzierten Gütern ausgehen.

¹⁴⁷⁵ Kidd, Chicago-Kent Law Review 2018, 174.

¹⁴⁷⁶ Siehe ferner zu den Risiken im Zusammenhang mit Admin Keys unten, [IV.5.2d.ii](#).

¹⁴⁷⁷ Siehe auch die wettbewerbsökonomischen Überlegungen, oben [II.5.2e](#). Vgl. zum Korrektiv tiefer Markteintrittshürden Buchanan, in: Liberty Fund, Rent Seeking and Profit Seeking, 104–107; hinsichtlich Angebote im Internet im Allgemeinen Koopman/Mitchell/Thierer, The Journal of Business, Entrepreneurship & the Law 2015, 540.

Abschliessend ist noch auf die Thematik von *Urheberrechten* an Software einzugehen: Derzeit wird der Code der allermeisten DeFi-Projekte unter freizügigen Lizenzen, wie namentlich Apache, Berkeley Software Distribution (BSD), GNU General Public License (GPL) oder Massachusetts Institute of Technology (MIT) veröffentlicht.¹⁴⁷⁸ Dies versteht sich nicht nur vor dem kulturellen Cypherpunk-Hintergrund von DeFi, sondern ist auch für die Sicherstellung der Interoperabilität unterschiedlicher Protokolle wichtig. Eine bemerkenswerte Ausnahme von diesem Grundsatz ist Uniswap Version 3. Der neue Code der beliebten dezentralen Handelsplattform wurde anders als noch Version 2 (GPL) neu unter der Business Source License (BSL) 1.1 veröffentlicht.¹⁴⁷⁹ Dies gibt den Entwicklern der Software für einen beschränkten Zeitraum (in diesem Fall maximal zwei Jahre) einen gewissen staatlichen Schutz vor kommerziellen Kopien, ohne jedoch anderweitige nichtkommerzielle Wiederverwendung einzuschränken.¹⁴⁸⁰ Der Lizenzwechsel scheint letztlich eine Reaktion von Uniswap auf Software Forks in der Vergangenheit gewesen zu sein, von denen es namentlich SushiSwap¹⁴⁸¹ und PancakeSwap¹⁴⁸² zu grosser Beliebtheit gebracht haben.¹⁴⁸³ Während die Lizenzierung von Uniswap V3 von den einen als klare Abwendung von den Prinzipien von Open-Source-Software betrachtet wird, finden andere, dass sie einem legitimen Bedürfnis der Entwicklergemeinschaft nach mehr Urheberrechtsschutz entspricht.¹⁴⁸⁴ Die Interoperabilität von Uniswap V3 scheint im Übrigen sichergestellt, da Drittprojekte weiterhin über offene Schnittstellen an die dezentrale Handelsplattform andocken können.¹⁴⁸⁵

¹⁴⁷⁸ Siehe für weitere Ausführungen zu den einzelnen Lizenzen Open Source Initiative, *Licenses & Standards*, *passim*.

¹⁴⁷⁹ Siehe Uniswap, *Introducing Uniswap V3, License*, *passim* («With this in mind, Uniswap v3 Core will launch under the Business Source License 1.1 – effectively a time-delayed GPL-2.0-or-later license. The license limits use of the v3 source code in a commercial or production setting for up to two years, at which point it will convert to a GPL license into perpetuity.»).

¹⁴⁸⁰ Siehe MariaDB, *Business Source License 1.1*, *passim*.

¹⁴⁸¹ <https://www.sushi.com/>.

¹⁴⁸² <https://pancakeswap.finance/>.

¹⁴⁸³ Zu diesem als Vampirattacke bezeichneten Vorgehen siehe jakub, *SushiSwap Saga Explained*, *passim*.

¹⁴⁸⁴ Siehe etwa Chervinsky, Twitter, *passim*. Allgemein zum Urheberrechtsregime bei Open-Source-Software Weber, *Success of Open Source*, 16–17, 209, 213.

¹⁴⁸⁵ Siehe Uniswap, *Introducing Uniswap V3, License*, *passim* («Note that the BUSL 1.1 license does not affect integrations. All code that may be needed for external integrations has been licensed under GPL or MIT, including math libraries, peripheral contracts, interfaces, and the developer sdk. Any wallet, interface, mobile app, protocol, or other project will be able to integrate with v3 as expected.»).

5.2 Risiken

a. Einleitung

Dezentrale Handelsplattformen können unterschiedliche Risiken aufweisen:¹⁴⁸⁶ (i) In erster Linie bringt das Halten von Kryptowährungen und Token Produktrisiken mit sich. (ii) Ferner bestehen aufgrund der Öffentlichkeit des verteilten Registers Transparenzrisiken für Nutzer. (iii) Sodann können sich Informationsrisiken aufgrund von Informationsasymmetrien zwischen den an einer dezentralen Handelsplattform beteiligten Parteien ergeben. (iv) Dezentrale Systeme weisen sodann Smart Contract- und Plattformrisiken auf. (v) Daraus können sich neuartige Systemrisiken ergeben. (vi) Dezentrale Systeme sind sodann mit kollektiven Handlungsproblemen insb. mit Blick auf die Governance solcher Systeme konfrontiert. (vii) Schliesslich bestehen potenziell rechtliche und regulatorische Risiken für dezentrale Handelsplattformen.

b. Produktrisiken

Mit Produktrisiken sind finanzwirtschaftliche Risiken gemeint, die mit dem dauerhaften oder vorübergehenden Halten von Kryptovermögenswerten verbunden sind. Zwar weisen Kryptovermögenswerte in aller Regel keine traditionellen Gegenparteirisiken und somit keine Kreditrisiken auf,¹⁴⁸⁷ doch sind sie selbstverständlich herkömmlichen Marktrisiken¹⁴⁸⁸ unterworfen. Typischerweise können Kryptowährungen und Token aufgrund eines allgemeinen oder produktspezifischen Rückgangs der Marktnachfrage an Wert verlieren. Ferner sind Kryptovermögenswerte sich ändernden Volatilitäten ausgesetzt,

¹⁴⁸⁶ Vgl. auch Weingärtner et al., Journal of Risk and Financial Management 2023, 12, welche die Risiken von DeFi in grafischer Weise («risk wheel») kategorisieren; ferner IOSCO, Public Report DeFi 2022, 36–42.

¹⁴⁸⁷ Siehe oben, IV.5.1c.iv.

¹⁴⁸⁸ Siehe für eine Definition von Marktrisiken Dowd, Measuring Market Risk, 1 («[...] market risk, or the risk of loss [or gain] arising from unexpected changes in market prices [e.g., such as security prices] or market rates [e.g., such as interest or exchange rates]. Market risks, in turn, can be classified into interest-rate risks, equity risks, exchange rate risks, commodity price risks, and so on, depending on whether the risk factor is an interest rate, a stock price, or another random variable. Market risks can also be distinguished from other forms of financial risk, particularly credit risk [or the risk of loss arising from the failure of a counterparty to make a promised payment] and operational risk [or the risk of loss arising from the failures of internal systems or the people who operate in them].»); ferner Skoglund/Chen, Financial Risk Management, 2.

die gerade in DeFi vergleichsweise hoch ausfallen können.¹⁴⁸⁹ Als Folge erhöhter Volatilitätsrisiken halten Nutzer vorübergehend Stablecoins, die allerdings je nach technischer und rechtlicher Ausgestaltung ein traditionelles Gegenpartearisiko aufweisen können (siehe sogleich). Schliesslich können tokenisierte Vermögenswerte entsprechende Marktrisiken ausweisen (z.B. das Beteiligungsrisiko bei tokenisierten Aktien).

Das produktspezifische Gegenpartearisiko von Stablecoins wird nachfolgend anhand des Beispiels von *Tether*¹⁴⁹⁰ dargestellt: USD-Tether (USDT) ist nach Aussage der Emittentin *Tether Limited* ein mit US-Dollar hinterlegter Stablecoin, wobei 1 USDT zu 1 US-Dollar am Markt handeln soll.¹⁴⁹¹ USDT gesteht den Tokeninhabern grundsätzlich die vertragliche Einlösbarkeit der Token gegen US-Dollar zu.¹⁴⁹² Obschon USDT seit Markteinführung fast immer zu *pari* mit dem US-Dollar handelt und der Stablecoin derzeit die grösste Marktkapitalisierung aller verfügbaren Stablecoins aufweist, wird die Integrität des Stablecoins seit geraumer Zeit infrage gestellt. Dabei drehen sich die Diskussionen insb. um die Frage, ob die Emittentin ein rechtswidriges oder zumindest fragwürdiges Teilreservesystem betreibt.¹⁴⁹³ Ein solches Vorgehen wäre mit der für traditionelle Banken typischen Risiken verbunden: Die Konsequenz wäre, dass die Emittentin von USDT bei einem allfälligen «Bank Run» nicht alle Tokeninhaber befriedigen könnte.¹⁴⁹⁴ Ein Hinweis auf die Liquiditätssituation von USDT findet sich sodann in den Transparenzberichten von *Tether Limited*, welche das Unternehmen aufgrund eines Vergleiches mit der New Yorker Staatsanwaltschaft quartalsweise veröffentlichen muss.¹⁴⁹⁵ Aus den Berichten wird erkennbar, dass die von *Tether Limited* gehaltenen Vermögenswerte ihrerseits ein beträchtliches Gegenpartearisiko aufweisen dürften.¹⁴⁹⁶ Aufgrund der Bedeutung des Stablecoins für den Kryptomarkt kann nicht ausgeschlos-

¹⁴⁸⁹ Vgl. WEF, *Decentralized Finance*, 14 m.w.H.

¹⁴⁹⁰ <https://tether.to/>.

¹⁴⁹¹ Siehe *tether*, *Fiat currencies on the Bitcoin blockchain*, 4.

¹⁴⁹² Siehe *tether*, *Legal, Terms of Service*, Ziff. 3.

¹⁴⁹³ Siehe z.B. Griffin/Shams, *Is Bitcoin Really Un-Tethered?*, 7–8; ferner Mueller, *Is Tether a Black Swan?*, *passim*.

¹⁴⁹⁴ Vgl. jedoch zum Unterschied, dass Stablecoin-Emittentinnen i.d.R. «liability-driven» sind, wohingegen Banken Geld durch Ausdehnung der Aktivseite ihrer Bilanz schöpfen («asset-driven»), Aramonte/Huang/Schrimpff, *BIS Quarterly Review* Dezember 2021, 25 m.w.N.

¹⁴⁹⁵ Vgl. OAG, *Settlement Agreement in the Matter of iFinex Inc. et al.*, *passim*.

¹⁴⁹⁶ Siehe De/Hochstein, *Tether's First Reserve Breakdown*, *Coindesk*, *passim*.

sen werden, dass dessen produktspezifisches Gegenparteirisiko sich negativ auf das Gesamtsystem auswirken könnte.¹⁴⁹⁷

c. Transparenzrisiken

i. Öffentlichkeit verteilter Register

Anfänglich schien der Cypherpunk-Traum anonymer Transaktionen im Internet mit Bitcoin in Erfüllung zu gehen.¹⁴⁹⁸ Hinzu kommt die Tatsache, dass in DeFi die Datenhoheit beim Nutzer verbleibt und somit eine deutliche Verbesserung gegenüber Datensilos traditioneller Anwendungen besteht.¹⁴⁹⁹

Allerdings besteht ein inhärenter Widerspruch zwischen der Verwendung von Blockchain-Technologie und der Gewährleistung von Anonymität und Privatsphäre.¹⁵⁰⁰ Da dezentrale Systeme auf zentrale Autoritäten verzichten, müssen alle Netzwerkteilnehmer imstande sein, die Einhaltung der Konsensregeln in Eigenregie zu überprüfen. Daraus folgt, dass die für die korrekte Funktionsweise erforderlichen Informationen *notwendigerweise* in einem verteilten Register öffentlich gemacht werden müssen.¹⁵⁰¹ Dies ist notwendig, damit Nutzer und Teilnehmer das für die Funktionsweise eines offenen Systems notwendige Technologievertrauen entwickeln können. So kann grundsätzlich jeder Nutzer von Bitcoin nachprüfen, dass die Konsensregeln von den übrigen Teilnehmern in der Vergangenheit eingehalten worden sind. Hierzu gehört auch die monetäre Obergrenze von ~ 21 Mio. BTC. Transparenz darüber, dass zu keinem Zeitpunkt in protokollwidriger Weise bitcoins «out of thin air» geschaffen werden, wird von einem Grossteil der Bitcoin Community geradezu als kultureller

¹⁴⁹⁷ Ähnlich sodann Carter/Jeng, in: Coen/Maurice, DeFi Protocol Risks, 7–10, welche auf die potenziell systemische *Verflechtung* von Krypto- mit traditionellen Märkten aufgrund von mit Fiatwährungen hinterlegten Stablecoins hinweisen; ferner Amler et al., DeFi-ning DeFi, 4.

¹⁴⁹⁸ Siehe hinsichtlich des Traums etwa Hughes, in: Ludlow, A Cypherpunk's Manifesto, 82 («Therefore, privacy in an open society requires anonymous transaction systems. Until now, cash has been the primary such system. An anonymous transaction system is not a secret transaction system. An anonymous system empowers individuals to reveal their identity when desired and only when desired; this is the essence of privacy.»).

¹⁴⁹⁹ So auch Ankenbrand/Bieri, Architekturrahmen, *passim*; Aramonte/Huang/Schrimpf, BIS Quarterly Review Dezember 2021, 30–31.

¹⁵⁰⁰ Siehe Zetzsche/Buckley/Arner, University of Illinois Law Review 2018, 1375.

¹⁵⁰¹ Siehe bereits Dai, b-money, *passim*; Szabo, Bit Gold, *passim*; ferner Antonopoulos/Wood, Mastering Ethereum, 59.

Mindeststandard betrachtet.¹⁵⁰² Das verteilte Register kann etwa mithilfe eines Blockchain Explorers¹⁵⁰³ oder durch die eigenständige Ausführung der Protokollsoftware uneingeschränkt eingesehen werden. Mit anderen Worten können dezentrale Systeme niemals auf privaten Datenbanken beruhen, welche Aussenstehende von der Einsicht ausschliessen. Auf das Spannungsverhältnis zur Privatsphäre wies bereits SATOSHI NAKAMOTO hin. Der Erfinder von Bitcoin glaubte aber, dass dank der Verwendung von Pseudonymen in Form von öffentlichen Schlüsseln bzw. Wallet-Adressen und der Vorsichtsmassnahme, für jede Transaktion ein neues Schlüsselpaar zu verwenden, die tatsächlichen Identitäten der beteiligten Parteien geheim gehalten werden können.¹⁵⁰⁴

Trotz der Pseudonymisierung der Identitäten der Nutzer in dezentralen Systemen ist heute empirisch erwiesen, dass dezentrale Netzwerke, wie etwa Bitcoin und Ethereum, ihren Nutzern lediglich einen tiefen Grad an Anonymität und Privatsphäre bieten.¹⁵⁰⁵

Dies ist insb. auf die konkrete Funktionsweise von bitcoin-Transaktionen zurückzuführen: Bitcoin-Einheiten bestehen letztlich aus einer Kette digitaler Signaturen. Mit jeder Übertragung einer Einheit wird eine digitale Signatur, namentlich diejenige des Inhabers des entsprechenden Private Keys, zu dieser Kette hinzugefügt.¹⁵⁰⁶ Eine Transaktion entspricht sodann einem Eintrag im verteilten Register des Netzwerks, der die Übertragung von bitcoin-Einheiten zwischen den beteiligten Parteien aufzeichnet. Der Eintrag enthält indessen nicht nur Informationen über die betreffende Transaktion samt Absender- und Empfängeradresse, sondern erlaubt darüber hinaus aufgrund der erwähnten Verkettung der digitalen Signaturen Einblick in alle vorausgegangen¹⁵⁰⁷

¹⁵⁰² Siehe z.B. Ammous, Bitcoin Standard, 199–200, 225, 249–251; Popper, Digital Gold, 157–158, 165, 182, 219, 286–287.

¹⁵⁰³ Z.B. für Bitcoin <https://blockstream.info/>.

¹⁵⁰⁴ Siehe Nakamoto, Bitcoin, 6 («The public can see that someone is sending an amount to someone else, but without information linking the transaction to anyone.»).

¹⁵⁰⁵ Siehe bereits Bonneau et al., Proceedings 2015 IEEE Symposium on Security and Privacy, 116–117; vgl. ferner hinsichtlich Rückverfolgbarkeit von Transaktionen mit Kryptowährungen die jährlichen Berichte von Chainalysis, z.B. Chainalysis, 2021 Crypto Crime Report, *passim*.

¹⁵⁰⁶ Siehe Nakamoto, Bitcoin, 2.

¹⁵⁰⁷ Die Ähnlichkeiten zum Konzept, wonach Geld bzw. Fiatwährung eine Form von Speicher bzw. Erinnerung vergangener Austauschgeschäfte ist, ist kaum zu übersehen; vgl. hierzu Narayana R. Kocherlakota, Money Is Memory, Journal of Economic Theory 1998, 232–251, 233 («When an individual gives consumption to someone else, his balance rises, and his capacity for receiving future transfers goes up. When he gets consumption from someone else, his balance falls, and his capacity for receiving future transfers declines. In the monetary environment, money is merely a physical way of maintaining this balance sheet.»).

Transaktionen mit den betreffenden bitcoins und alle an den Transaktionen beteiligten Absender- und Empfängeradressen. Daraus entstehen für aussenstehende Beobachter, wenn auch pseudonymisierte, so doch eindeutig nachvollziehbare UTXO-Transaktionsketten.¹⁵⁰⁸

Transparenter stellt sich die Situation in Ethereum und anderen Blockchains dar: Anstelle von UTXO-Transaktionsketten basierenden solche Protokolle auf *Kontenstrukturen* (sog. *Externally Owned Accounts*, EOAs).¹⁵⁰⁹ Hinter einem jeden Konto steht eine bestimmte Wallet-Adresse, die unveränderlich mit dem Konto verknüpft ist.¹⁵¹⁰ Dadurch wird selbst NAKAMOTOS Vorschlag, für jede Transaktion eine neue Adresse zu verwenden, verunmöglicht.¹⁵¹¹

Einige Unternehmen (z.B. die US-Firma Chainalysis¹⁵¹²) haben sich inzwischen auf die Analyse von Blockchain-Informationen spezialisiert. An erster Stelle steht die *Transaction-Graph-Analyse*. Hierzu gelangt in aller Regel ein Clustering von Wallet-Adressen basierend auf probabilistischen Heuristiken (sog. *Idioms of Use*) zur Anwendung.¹⁵¹³ Soweit öffentlich verfügbare Informationen (z.B. auf Twitter), private Informationen, die bspw. im Rahmen von Geschäften auf Kryptobörsen erhoben werden, oder anderweitig beschaffene Informationen, wie etwa durch Tracking von IP-Adressen der Besucher von Blockchain Explorern, mit den in einem verteilten Register enthaltenen Wallet-Adressen in Verbindung gebracht werden können, können Aussenstehende unter Umständen die gesamte Transaktionshistorie sowie den Vermögensstand einer bestimmten oder zumindest bestimmbarer Person in Erfahrung bringen.¹⁵¹⁴

¹⁵⁰⁸ Vgl. zum sog. *Unspent Transaction Output* (UTXO)-Modell Antonopoulos, *Mastering Bitcoin*, 117–121, 145–147.

¹⁵⁰⁹ Vgl. zum EOA-Modell im Allgemeinen Antonopoulos/Wood, *Mastering Ethereum*, 26–27, 99–102.

¹⁵¹⁰ Siehe hierzu Antonopoulos/Wood, *Mastering Ethereum*, 26, 60–61, 127; sodann Béres et al., *Blockchain is Watching You*, 1 («[...] the account-based model essentially relies on address-reuse on the protocol level. This behavior practically renders the account-based cryptocurrencies inferior to UTXO-based currencies from a privacy perspective.»).

¹⁵¹¹ Siehe ferner satoshi, *How anonymous are bitcoins?*, BitcoinTalk, *passim* («For greater privacy, it's best to use bitcoin addresses only once.»).

¹⁵¹² <https://www.chainalysis.com/>.

¹⁵¹³ Siehe hinsichtlich Bitcoin Meiklejohn et al., *IMC '13: Proceedings of the 2013 Internet Measurement Conference*, 128; sodann Bonneau et al., *Proceedings 2015 IEEE Symposium on Security and Privacy*, 116–117; ferner bereits Reid/Harrigan, *2011 IEEE International Conference on Privacy, Security, Risk and Trust and IEEE International Conference on Social Computing 2011*, 1322–1325; Ron/Shamir, in: Sadeghi, *Quantitative Analysis Bitcoin Transaction Graph*, 9–10; hinsichtlich *Ethereum* Victor, in: Bonneau/Heninger, *Address Clustering Heuristics for Ethereum*, 622–628.

¹⁵¹⁴ Vgl. statt vieler Pesch/Böhme, *DuD 2017*, 94–95.

Neben dieser Analyse bezogen auf Wallet-Adressen können sodann allenfalls auch durch Beobachtung der Kommunikationsflüsse innerhalb des P2P-Netzwerks die schwachen Anonymitätsgarantien von Blockchain-Transaktionen durchbrochen werden.¹⁵¹⁵ Die Netzwerkanalyse geht dabei von der Annahme aus, dass die IP des Absenders einer Transaktion in aller Regel zur derjenigen Person gehört, welche die Transaktion veranlassen möchte und somit mutmasslich an den Vermögenswerten wirtschaftlich berechtigt ist.¹⁵¹⁶

Diese Analyseverfahren stellen ein grosses Risiko für die Privatsphäre von Nutzern dezentraler Systeme dar, lassen die öffentlichen Informationen doch Rückschlüsse auf ausserordentlich sensible Daten zu: Dabei kann es sich um die Vermögens- und Einkommensverhältnisse einer Einzelperson oder eines Unternehmens handeln. Eine besondere Problematik ergibt sich insb. auch daraus, dass die digitalen Zahlungsströme einer Person automatisch auch Rückschlüsse auf deren nichtfinanziellen Angelegenheiten erlauben. Im Extremfall kann damit das ganze Leben einer Person transparent gemacht werden.¹⁵¹⁷ Hinzu kommt, dass die Daten in den meisten Blockchains für immer gespeichert bleiben, was Rückschlüsse, die heute noch nicht möglich sind, zu einem späteren Zeitpunkt möglich machen könnte.

Die an Spannungen reiche Beziehung von dezentralen Systemen zum persönlichen Anspruch des Einzelnen auf Schutz seiner Privatsphäre und Persönlichkeit werden in der Datenschutzliteratur ausführlich und teils sehr kontrovers diskutiert.¹⁵¹⁸ Aufgrund des Infrastrukturmutualismus in dezentralen Systemen

¹⁵¹⁵ Siehe etwa Biryukov/Khovratovich/Pustogarov, Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security 2014, 16; ferner Delgado-Segura et al., in: Goldberg/Moore, Discovering Bitcoin's Network Topology, *passim*.

¹⁵¹⁶ Siehe Fanti et al., Proceedings of the ACM on Measurement and Analysis of Computing Systems 2018, 29:2–29:3.

¹⁵¹⁷ Siehe etwa Androulaki et al., in: Sadeghi, Evaluating User Privacy in Bitcoin, 47; vgl. ferner zur Bedeutung von Bitcoin für den Schutz der Menschenrechte Gladstein, Why Bitcoin Matters for Freedom, *passim*; sodann in Bezug auf das Risiko von Social Profiling durch Unternehmen und Regierungen Brito, The Case for Electronic Cash, 14–17 m.w.H.; kritisch auch Edward Snowden; vgl. diesbezüglich Decrypt Media, Edward Snowden Talks Privacy Coins, Youtube, *passim*.

¹⁵¹⁸ Siehe etwa Zetzsche/Buckley/Arner, University of Illinois Law Review 2018, 1376; Böhme/Pesch, DuD 2017, 478–479; Stengel/Aus der Au, sic! 2018, 444–446, 449–450; Wiatrowski, Jusletter IT vom 22. Februar 2018, Rz. 9–12, 31–37, 41, 42–43; ferner Isler, Jusletter vom 4. Dezember 2017, Rz. 3–4, 46–47, wo allerdings fälschlicherweise von Verschlüsselung der Daten gesprochen wird, was in der Bitcoin Blockchain nicht und im Übrigen lediglich ausnahmsweise der Fall ist; Möri, Jusletter IT vom 23. Mai 2019, Rz. 34; Plattner, Datenschutzrechtliche Herausforderungen, Rz. 106–107, spricht von «Paradoxa» zwischen Datenschutzgesetzgebung und Blockchain.

sind sodann auch die Rollenverteilung und in der Folge die rechtlichen Verantwortlichkeiten im Zusammenhang mit der Einhaltung von datenschutzrechtlichen Vorgaben unklar.¹⁵¹⁹

Aufgrund der Ausführungen kann zusammengefasst werden, dass öffentliche Blockchains heute die Privatsphäre des Durchschnittsnutzers nur schlecht gewährleisten können. Ohne eine deutliche Verbesserung der Privatsphäre scheinen die Ideale von Web 3.0 hinsichtlich Self-Sovereign Identity nur ansatzweise realisierbar zu sein.¹⁵²⁰ Was es letztlich braucht, sind Protokolle, die Privacy by Design und by Default durchsetzen.¹⁵²¹

ii. Privacy by Design-Technologien

Aufgrund dieser Umstände wurde das Bedürfnis echter Anonymität in Bitcoin und anderen dezentralen Netzwerken bereits früh erkannt.¹⁵²²

Anfänglich wiesen die ersten Angebote in vielen Fällen noch zentralisierte Strukturen auf, sodass letztlich die Nutzer den Betreibern solcher Angebote vertrauen mussten. Beispiele solcher Entwicklungen waren insb. *Mixing Services*, in deren Rahmen Nutzer ihre Kryptowährungen an den Anbieter der Dienstleistung, den Mixer, senden.¹⁵²³ Nachdem der Mixer in seiner privaten Datenbank die Vermögenswerte unterschiedlicher Nutzer miteinander «vermischt» hat, erhalten die Nutzer andere Vermögenswerte im gleichen Betrag abzüglich einer Dienstleistungsgebühr zurück.¹⁵²⁴ Die Nachteile eines solchen Services für den Nutzer in einem überwiegend pseudonymen Netzwerk sind offensichtlich: Der Betreiber des Mixing Service erlangt sowohl Informationen über den Nutzer als auch die vorübergehende Verfügungsmacht über dessen Kryptovermögenswerte. Ferner kommen solche Dienstleister aufgrund der erlangten Kontrolle über fremde Vermögenswerte rasch in Konflikt mit dem

¹⁵¹⁹ Siehe hierzu die teils ausführlichen Analysen unter der DSGVO in EP, Blockchain and the General Data Protection Regulation, 45–50; EUBOF, Blockchain and the GDPR, 17–18; ferner, allerdings nach vorliegender Auffassung zu *weitgehend* hinsichtlich Einstufung von Minern in dezentralen Netzwerken CNIL, Blockchain et RGPD, 2–5; *ebenfalls* zu *weitgehend* Jaccard/Tharin, Jusletter IT vom 4. Dezember 2018, Rz. 41–55.

¹⁵²⁰ Vgl. Bernabe et al., IEEE Access 2019, 164934.

¹⁵²¹ Vgl. Thür, Jusletter IT vom 21. Mai 2015, Rz. 30.

¹⁵²² So z.B. Barber et al., in: Keromytis, Bitter to Better, 411.

¹⁵²³ Mixing Services werden auch als «Tumblers» oder «Washers» bezeichnet, vgl. Bitcoin Wiki, Privacy, Centralized mixers, *passim*.

¹⁵²⁴ Siehe hierzu Möser/Böhme/Breuker, 2013 APWG eCrime Researchers Summit 2014, 78–79, 86.

heutigen Geldwäschereiregime.¹⁵²⁵ Aus diesem Grund wurden Mixing-Protokolle entwickelt, die mithilfe einfacher Smart Contracts in Bitcoin die Möglichkeit zur Entwendung der involvierten Vermögenswerte ausschliessen.¹⁵²⁶

Ein bekanntes und verbreitetes Mixing-Protokoll ist *CoinJoin*: Dieses Protokoll erlaubt mehreren Nutzern eine gemeinsame Transaktion zu konstruieren, so dass Aussenstehende nicht mehr von den jeweiligen Inputs der Nutzer auf die dazugehörigen Outputs der Transaktion schliessen können.¹⁵²⁷ Softwareentwickler, wie etwa Wasabi¹⁵²⁸ und Samourai¹⁵²⁹, haben *CoinJoin* in ihre Wallets integriert. Nutzer des Wasabi-Wallets konstruieren etwa die gemeinsame Transaktion in einer Computersoftware, indem sie separat Inputs und Outputs zu einer Transaktion beisteuern. Sie sind dabei nicht mehr auf einen Intermediär angewiesen.¹⁵³⁰

Gemeinsames Ziel dieser unterschiedlichen Mixing-Protokolle ist die Aushöhlung der Aussagekraft der von den erwähnten Blockchain-Analysefirmen verwendeten Heuristiken. *CoinJoin* und die Weiterentwicklung *PayJoin* brechen bspw. die Heuristik, dass alle Inputs zu einer Transaktion von derselben Person stammen müssen.¹⁵³¹ *CoinSwap*, ein Projekt, das sich noch im Entwicklungsstadium befindet, bricht sodann mit der Heuristik, dass eine Transaktion des Absenders immer beim nach aussen propagierten Empfänger landen muss.¹⁵³² Folge dieser «Verneblungstaktiken» ist, dass die Wahrscheinlichkeit einer korrekten Aussage aufgrund von Transaction-Graph-Analysen abnimmt. Zudem unterscheiden sich *CoinJoin*-Transaktionen für einen Aussenstehenden grundsätzlich nicht von gewöhnlichen Transaktionen.¹⁵³³ Um aber effektiv eine Verbesserung der Privatsphäre herbeizuführen, hängen diese Massnahmen letztlich davon ab, wie gross das *Anonymity Set* ist. D.h., je grösser der Anteil anonymer Transaktionen an den Gesamttransaktionen innerhalb eines Netzwerks ist, desto wirkungsvoller ist auch die Anonymisierung einzelner Personen.¹⁵³⁴

¹⁵²⁵ Vgl. die Fälle *Helix* und *Coin Ninja* in den USA FinCEN, First Bitcoin «Mixer» Penalized, *passim*; ausführlich zur Funktionsweise dieser Mixer FinCEN, Assessment of Civil Money Penalty, Attachment A, 1–2.

¹⁵²⁶ Siehe für eine Übersicht Bonneau et al., Proceedings 2015 IEEE Symposium on Security and Privacy, 117–118.

¹⁵²⁷ Siehe Maxwell, *CoinJoin*, BitcoinTalk, *passim*.

¹⁵²⁸ <https://wasabiwallet.io/>.

¹⁵²⁹ <https://samouraiwallet.com/>.

¹⁵³⁰ Siehe wasabi docs, *coinjoin*, *passim*.

¹⁵³¹ Siehe etwa Gibson, *Payjoin*, *passim*.

¹⁵³² Siehe Belcher, Design for a *CoinSwap* implementation, *passim*.

¹⁵³³ Siehe Bitcoin Wiki, Privacy, *CoinJoin*, *passim*.

¹⁵³⁴ Vgl. hierzu Murdoch, in: Garcia-Alfaro et al., Quantifying and Measuring Anonymity, 5–7.

Wie oben gesehen, entspricht Mixing grundsätzlich einem legitimen Bedürfnis nach Privatsphäre der Nutzer dezentraler Systeme. Indem Mixing die Verbindung zwischen der vergangenen Transaktionshistorie eines Coins bzw. Tokens und dessen potenziellen zukünftigen Verwendung aufhebt, können sensible Daten des derzeitigen Inhabers geschützt werden. Tatsächlich sollte Mixing in erster Linie mit anderen Praktiken, welche die Privatsphäre der Nutzer verbessert, verglichen werden.¹⁵³⁵ Freilich kann Mixing auch zu anderen Zwecken, insb. der Verschleierung der illegalen Herkunft eines Kryptovermögenswerts durch das geldwäschereirechtlich relevante *Layering*, verwendet werden.¹⁵³⁶ In diesem Fall ist von *Tainted Coins* die Rede. Technisch gesehen sind *Tainted* und *Untainted Coins* identisch; sie unterscheiden sich aber massgeblich durch ihre Transaktionshistorie.¹⁵³⁷ Der Inhaber eines *Tainted Coins* versucht mithilfe des Mixing-Prozesses die ursprünglich uneingeschränkte Fungibilität des Kryptovermögenswerts wiederherzustellen. Dabei ist die Eigenschaft der Fungibilität dem Kryptovermögenswert nicht inhärent, sondern der konkrete Grad an Fungibilität wird dem jeweiligen Vermögenswert aufgrund seiner Historie von Finanzintermediären, insb. zentralen Kryptohandelsplattformen, zugeschrieben.

Allerdings existieren über diese Mixing-Protokolle hinaus, die auch als *Overlays* bezeichnet werden, eigenständige dezentrale Systeme, die im Gegensatz zu Bitcoin und Ethereum, *Privacy by Design*-Technologien bereits auf der Ebene der Konsensregeln implementieren.¹⁵³⁸ Die Eigenschaften, dass Transaktionen nicht rückverfolgt und miteinander verknüpft werden können, wurde bereits früh als grundlegendes Bedürfnis eines verlässlichen elektronischen Zahlungssystems erkannt.¹⁵³⁹ Die Kryptowährungen dieser Systeme werden deshalb regelmässig als *Privacy Coins* bezeichnet. Dazu gehören bspw. die Kryptowährungen Zcash¹⁵⁴⁰, Monero¹⁵⁴¹, Dash¹⁵⁴², Grin¹⁵⁴³ und Beam¹⁵⁴⁴. Er-

¹⁵³⁵ So auch Hodder/Yakobi, Bitcoin Fungibility, Bitcoin Magazine, *passim*; ferner Nadler/Schär, Federal Reserve Bank of St. Louis Review 2023, 123.

¹⁵³⁶ Vgl. in diesem Zusammenhang FATF, Virtual Assets Red Flag Indicators, 9–10; ferner FATF, Professional Money Laundering, 18.

¹⁵³⁷ Siehe Meiklejohn/Orlandi, in: Brenner et al., Privacy-Enhancing Overlays, 131.

¹⁵³⁸ Vgl. zu dieser Unterscheidung Meiklejohn/Orlandi, in: Brenner et al., Privacy-Enhancing Overlays, 128.

¹⁵³⁹ So z.B. van Saberhagen, CryptoNote, 1–2, wobei CryptoNote zu Monero weiterentwickelt wurde; sodann Miers et al., 2013 IEEE Symposium on Security and Privacy 2013, 397, welche Zerocoin als Verbesserung gegenüber Bitcoin vorschlugen.

¹⁵⁴⁰ <https://z.cash/>.

¹⁵⁴¹ <https://www.getmonero.org/>.

¹⁵⁴² <https://www.dash.org/>.

¹⁵⁴³ <https://grin.mw/>.

¹⁵⁴⁴ <https://beam.mw/>.

reicht wird die verbesserte Privatsphäre in aller Regel durch die Nutzung neuartiger kryptografischer Protokolle.¹⁵⁴⁵

Zcash, eine Weiterentwicklung des Bitcoin Protokolls, verwendet etwa eine kryptografische Methode namens Zero-Knowledge Succinct Non-Interactive Argument of Knowledge (zk-SNARKs).¹⁵⁴⁶ Unter ZKP-Kryptografie werden Protokolle verstanden, die den formalen Nachweis einer bestimmten Information («Geheimnis») erlauben, ohne jedoch das eigentliche Geheimnis der Gegenpartei offenlegen zu müssen. Aufgrund der Verwendung von ZKP kann sich die Gegenpartei mit überwiegender Wahrscheinlichkeit darauf verlassen, dass die andere Partei tatsächlich über das Geheimnis verfügt.¹⁵⁴⁷ In Zcash wird das Verfahren auf die Authentifizierung der Parteien sowie Transaktionsdaten angewendet. Die Netzwerkteilnehmer sehen folglich lediglich die ZKP der jeweiligen Transaktionen, ohne jedoch Rückschlüsse auf die öffentlichen Adressen der beteiligten Parteien sowie den Transaktionsbetrag vornehmen zu können. Trotz Verwendung von ZKP bleiben die Netzwerkteilnehmer imstande, die Transaktionen auf ihre Vereinbarkeit mit den Konsensregeln zu überprüfen.¹⁵⁴⁸ Zcash bietet Nutzern sowohl gewöhnliche öffentliche Transaktionen als auch vertrauliche private Transaktionen an,¹⁵⁴⁹ wobei geplant ist, dass künftig alle Transaktionen standardmäßig vertraulich sind und somit das Anonymitätsset ungemein vergrößern.¹⁵⁵⁰ Eine empirische Analyse des Netzwerks hat ergeben, dass das Protokoll erst durch eine massive Vergrößerung des Anonymitätssets eine ausreichende Privatsphäre gewährleisten kann.¹⁵⁵¹

¹⁵⁴⁵ So wird bspw. das *MimbleWimble*-Protokoll in Grin und Beam verwendet; vgl. zu diesem Protokoll Poelstra, *Mimblewimble*, *passim*. Monero setzt demgegenüber u.a. auf *Ring Confidential Transactions* und *Ring (Group) Signatures*, vgl. SerHack/Monero Community, *Mastering Monero*, 2019, 60–70; ausführlich zu Moneros Lösung für erhöhte Privatsphäre Noether/Mackenzie/the Monero Research Lab, *Ledger* 2016, *passim*.

¹⁵⁴⁶ Siehe Zcash, *What are zk-SNARKs?*, *passim*; ferner Wu/Wang, *The Scientific World Journal* 2014, 1.

¹⁵⁴⁷ Siehe Quisquater/Giullou/Berson, in: Brassard, *Explain Zero-Knowledge Protocols*, *passim*; ferner Böhme/Pesch, *DuD* 2017, 480–481.

¹⁵⁴⁸ Siehe Zcash, *What are zk-SNARKs?*, *passim*; in theoretischer Hinsicht Ben-Sasson et al., 2014 IEEE Symposium on Security and Privacy 2014, 459–460.

¹⁵⁴⁹ Siehe für Beispiele Zcash, *How It Works*, *passim*.

¹⁵⁵⁰ Vgl. Powers, *Zcash Announces 'Halo Arc'*, *Coindesk*, *passim*.

¹⁵⁵¹ Siehe Kappos et al., 2018 Proceedings of the 27th USENIX Conference on Security Symposium, Berkeley 2018, 475.

Im Vergleich zur Bitcoin Blockchain, deren Community die absolute Überprüfbarkeit der Einhaltung der Konsensregeln in den Vordergrund stellt,¹⁵⁵² weist der Einsatz von ZKP ein Vertrauenselement auf: Die erstmalige Begründung der kryptografischen Grundlagen der ZKP bedarf derzeit eines sog. *Trusted Setups*.¹⁵⁵³ Nutzer von Zcash müssen darauf vertrauen, dass das dabei verwendete Datenmaterial im Anschluss an das Trusted Setup vollständig und unwiderruflich vernichtet wird. Das Datenmaterial würde dem Inhaber bspw. erlauben, neue Kryptowährungseinheiten zu generieren, ohne dass eine Drittperson dies bemerken könnte.¹⁵⁵⁴ Dieses Vertrauenselement soll in künftigen Iterationen von Zcash vermieden werden können.¹⁵⁵⁵

Demgegenüber nutzt Dash, ebenfalls eine Software Fork des Bitcoin Protokolls, lediglich eine über das Netzwerk ihrer Masternodes integrierte Version von CoinJoin namens *PrivateSend*.¹⁵⁵⁶

Grundlegend neuartig, weil ZKP auf die gesamte Datenstruktur der Blockchain angewendet werden, ist das *Mina*-Protokoll.¹⁵⁵⁷ Da lediglich die ZKP bisheriger Transaktionen und somit nicht die gesamte Transaktionshistorie von den Teilnehmern verifiziert werden müssen, soll die zu verarbeitende Datenmenge sehr gering ausfallen.¹⁵⁵⁸ Zwar ist derzeit die Anonymisierung von Transaktionen im *Mina*-Netzwerk nicht vorgesehen, weshalb nicht von einem eigentlichen Privacy Coin gesprochen werden kann, doch könnte die Anwendung von ZKP künftig ein deutlich höheres Datenschutzniveau für die Nutzer von dezentralen Applikationen bedeuten.¹⁵⁵⁹ Ähnliche Entwicklungen existieren auch für andere Blockchains.¹⁵⁶⁰

¹⁵⁵² Vgl. zum Nakamoto-Konsens oben, [III.3.3b](#).

¹⁵⁵³ Siehe hierzu Bowe/Grigg/Hopwood, Recursive Proof Composition without a Trusted Setup, 1–3.

¹⁵⁵⁴ Siehe Zcash, Parameter Generation, *passim*.

¹⁵⁵⁵ Siehe Electric Coin Company, Halo, *passim*; ferner Casey, Zcash's Halo Breakthrough, Coindesk, *passim*.

¹⁵⁵⁶ Siehe Dash, PrivateSend and InstantSend, *passim*. Interessanterweise ist zu erwähnen, dass die Dash-Community sich gegenüber der Bezeichnung der Kryptowährung als Privacy Coin bzw. «privacy-centric coin» wehrt, siehe insb. Dash, PrivateSend Legal Position, *passim*; sodann Hamwi, Dash Complies with the FATF, *passim*.

¹⁵⁵⁷ Ausführlich Bonneau et al., Mina, 3–4.

¹⁵⁵⁸ Siehe Mina Foundation, 22kB-Sized Blockchain *passim*.

¹⁵⁵⁹ Vgl. hinsichtlich potenzieller Anwendungsfälle von Mina Shapiro, Building a Private Gateway, *passim*.

¹⁵⁶⁰ Vgl. die Hinweise bei Foxley, You Can Now Prove a Whole Blockchain With One Math Problem, Coindesk, *passim*.

Sodann bestehen Protokolle, welche die Privatsphäre mithilfe von ZKP und *Smart Contracts* verbessern. In Tornado Cash¹⁵⁶¹ etwa kann ein Nutzer einen bestimmten Betrag samt eines Hashs des Geheimnisses vorübergehend in einem Ethereum-basierten Smart Contract deponieren. Mit dem Geheimnis kann der Nutzer oder eine andere Person, die über das Geheimnis verfügt, zu einem späteren Zeitpunkt den identischen Betrag auslösen. ZKP stellen sicher, dass tatsächlich nur der deponierte Betrag zur Verfügung steht. Durch die Deponierung von Kryptovermögenswerten in einem Smart Contract, der gleichzeitig von tausenden anderen Nutzern zum gleichen Zweck verwendet wird, kann die Verknüpfung zwischen den Absender- und Empfängeradressen permanent unterbrochen werden.¹⁵⁶² Anders als gewisse Vorgängerversionen kann Tornado Cash nicht frei über die Vermögenswerte der Nutzer verfügen. Die Nutzung des Protokolls weist somit keine traditionellen Kontroll- und Vertrauensrisiken auf. Im August 2022 wurde Tornado Cash sodann von der OFAC sanktioniert, was für US-Personen ohne Ausnahmegewilligung ein Verbot der Nutzung des Protokolls bedeutet, aber auch darüber hinaus Implikationen zeitigt.¹⁵⁶³ Konkret wurden u.a. die Smart Contract-Adressen des Protokolls auf die «Specially Designated Nationals and Blocked Persons List» gesetzt¹⁵⁶⁴ – eine bis dahin unbekannte Praxis der Behörde, die bisher ausschliesslich Personen oder Gruppen von Personen und deren Blockchainadressen sanktioniert hat.¹⁵⁶⁵ Der Anonymisierungsdienst ist heute Gegenstand der bedeutendsten öffentlichen Diskussionen im Kryptobereich¹⁵⁶⁶ und Gegenstand laufender Gerichtsverfahren.¹⁵⁶⁷

Schliesslich hat auch Bitcoin¹⁵⁶⁸ im November 2021 eine Soft Fork mit dem Namen «Taproot» implementiert, welche neben verbesserten Smart Contract-Fähigkeiten und Effizienzgewinnen auch die Privatsphäre von Transaktionen erhöhen soll. Dank des Updates würden für Aussenstehende alle Bitcoin-

¹⁵⁶¹ <https://tornadocash.eth.link>.

¹⁵⁶² Siehe Tornado Cash, *Introducing Private Transactions*, Medium, *passim*; differenzierend Béres et al., *Blockchain is Watching You*, 7–12.

¹⁵⁶³ Siehe Glarner/Mognetti, *Impact for non-US digital asset service providers*, *passim*.

¹⁵⁶⁴ <https://ofac.treasury.gov/recent-actions/20220808>, 8. August 2022.

¹⁵⁶⁵ Siehe etwa für die Sanktionen gegen *Blender.io* U.S. Department of the Treasury, *First-Ever Sanctions on a Virtual Currency Mixer*, *passim*; ferner betreffend *Sinbad.io* .S. Department of the Treasury, *Treasury Sanctions Mixer*, *passim*.

¹⁵⁶⁶ Siehe etwa Farrell/Schneier, *Golem*, *passim*; Van Valkenburgh, *Tool for privacy and free speech*, *passim*.

¹⁵⁶⁷ Siehe hierzu die Ausführungen in FN 2692.

¹⁵⁶⁸ Siehe für die immer noch relativ aktuelle Übersicht unterschiedlicher Verbesserungsvorschläge für die Bitcoin Blockchain van Wirdum, *Bitcoin as a Privacycoin*, *Bitcoin Magazine*, *passim*.

Transaktionen (konkret UTXOs) unabhängig von ihrer inhaltlichen Ausgestaltung künftig identisch aussehen.¹⁵⁶⁹ Ausserdem weisen auch Transaktionen in Bitcoins Lightning Netzwerk¹⁵⁷⁰ oder über Bitcoins Liquid Sidechain¹⁵⁷¹ einen höheren Grad an Privatsphäre als On-Chain-Transaktionen auf.

ZKP und andere Privacy-Enhancing-Technologien stellen Beispiele von *Privacy by Design* dar, welche den Schutz der Rechtsordnung ergänzen.¹⁵⁷² Allerdings können Privacy Coins und CoinJoins in finanzmarktrechtlicher und besonders geldwäschereirechtlicher Hinsicht problematisch sein.¹⁵⁷³ Zcash etwa sieht vor diesem Hintergrund sog. View Keys vor, welche Nutzer (z.B. eine Bank) selektiv mit Dritten (z.B. eine Strafverfolgungsbehörde) teilen können und diesen erlauben, die Transaktionsdetails einer Wallet-Adresse einzusehen.¹⁵⁷⁴

iii. Frontrunning und MEV über dezentrale Handelsplattformen

Die obigen Ausführungen zu Transparenzrisiken in dezentralen Systemen lassen vermuten, dass sie auch für die Nutzer dezentraler Handelsplattformen besondere Konsequenzen mit sich bringen:

Dezentrale Handelsplattformen sind namentlich für «Frontrunning» durch computergestützte Handelssysteme (sog. Arbitrage Trading Bots) sowie allenfalls durch Miner anfällig.¹⁵⁷⁵ In ersterem Punkt unterscheiden sie sich nur be-

¹⁵⁶⁹ Siehe Maxwell, Taproot, *passim*; ausführlich zum Update BitMEX Research, Schnorr Signature & Taproot Softfork Proposal, *passim*.

¹⁵⁷⁰ Siehe Antonopoulos, Mastering Bitcoin, 320; Decker, Privacy in Lightning, *passim* («It's not perfect, but a step forward.»); kritisch demgegenüber die Untersuchungen in Kappos et al., in: Borisov/Diaz, Privacy in the Lightning Network, *passim*; Romiti et al., in: Borisov/Diaz, Deanonymization Methods in the Lightning Protocol, *passim*; Béres/Seres/Benczúr, Cryptoeconomic Systems 2020, 4; differenzierend Ronning, Lightning Network Privacy, *passim*.

¹⁵⁷¹ Siehe Nick/Poelstra/Sanders, Liquid, 2, 10–11.

¹⁵⁷² So wohl auch Weber, Jusletter IT vom 30. September 2020, Rz. 46–47; ähnlich auch EUBOF, Blockchain and the GDPR, 23.

¹⁵⁷³ Siehe EP, Blockchain and the General Data Protection Regulation, 35–36.

¹⁵⁷⁴ Siehe hierzu Wilcox, What is Zcash?, *passim*. Vgl. ferner bereits Hughes, in: Ludlow, A Cypherpunk's Manifesto, 81 («Privacy is the power to selectively reveal oneself to the world.»).

¹⁵⁷⁵ Das Frontrunning-Problem wurde, soweit ersichtlich, erstmals in einer Reddit-Diskussion erkannt; vgl. Pmcgoohan, Miners Frontrunning, Reddit, *passim*.

dingt von den Hochfrequenzhandelsstrategien in traditionellen Märkten.¹⁵⁷⁶ Es ist allerdings darauf hinzuweisen, dass Finanzintermediäre für bestimmte Formen von Frontrunning in Bezug auf Effekten, die an einem Handelsplatz in der Schweiz zum Handel zugelassen sind, unter Umständen aufsichts- und strafrechtlich sanktioniert werden können. Dabei kommt in erster Linie ein Verstoß gegen das Verbot des Insiderhandels infrage.¹⁵⁷⁷ Frontrunning im vorliegenden Sinne erfolgt demgegenüber auf Basis *öffentlicher* Informationen, die grundsätzlich allen beteiligten Personen bekannt sind bzw. sein können.¹⁵⁷⁸

Frontrunning auf dezentralen Handelsplattformen läuft i.d.R. wie folgt ab: Arbitrage Trading Bots können durch Beobachtung des Mempools, in welchem die noch unbestätigten Transaktionen von Nutzern gespeichert werden, höhere Transaktionsgebühren an ihre eigene Transaktionen anhängen, sodass diese noch vor den unbestätigten Transaktionen des Mempools in das verteilte Register aufgenommen werden. Weil sie dadurch steigende oder fallende Preisen antizipieren, partizipieren sie praktisch risikolos an allfälligen Kursentwicklungen.¹⁵⁷⁹ Ferner können solche Bots Aufträge, die aufgrund von Kursentwicklungen aus Sicht des Makers überholt sind, noch vor deren Stornierung akzeptieren und somit dennoch zur Ausführung bringen (*Stale Quote Sniping*).¹⁵⁸⁰ Der Mempool wird in der Literatur auch als «Dark Forest» bezeichnet, wonach bereits die Entdeckung einer Arbitragemöglichkeit durch den Frontrunner einem sicheren Gewinn gleichkommen soll.¹⁵⁸¹ Im Prinzip nutzen Arbitrage Trading Bots – unter Zuhilfenahme entsprechender algorithmischer Handelsstrategien – lediglich öffentliche Informationen aus, die grundsätzlich

¹⁵⁷⁶ Vgl. etwa Fox/Glosten/Rauterberg, *Duke Law Journal* 2015, 226–228; Manahov, *The Financial Review* 2016, 366–367; hinsichtlich «stale quote sniping» und «latency arbitrage» Kirilenko et al., *The Journal of Finance* 2017, 971.

¹⁵⁷⁷ Vgl. Art. 142 und 154 FinfraG; siehe hierzu etwa FINMA-RS 13/8 «Marktverhaltensregeln», Rz. 8; SK FinfraG-Sethe/Fahrländer, Art. 142 N 38; sodann SK FinfraG-Sethe/Fahrländer, Art. 154 N 126–127; ferner Sethe/Fahrländer, in: Jositsch/Schwarzenegger/Wohlers, *Frontrunning als Insiderdelikt*, insb. 511.

¹⁵⁷⁸ Siehe Harvey/Ramachandran/Santoro, *DeFi*, 31, 99.

¹⁵⁷⁹ Siehe hinsichtlich dieser als *Priority Gas Auctions* (PGAs) bezeichneten Verhaltensweise Daian et al., 2020 IEEE Symposium on Security and Privacy 2020, 910, 912; vgl. ferner die *Taxonomie* möglicher Attacken bei Eskandari/Moosavi/Clark, in: Bracciali et al., *Front-Running Attacks on Blockchain*, 173–174, 175–177; sodann Ferreira Torres/Camino/State, *Empirical Study of Frontrunning*, 4; schliesslich Werner et al., *Decentralized Finance*, 7–8, die aus der Risikolosigkeit des Vorgehens schliessen, dass ein Protokoll technisch nicht einwandfrei ist.

¹⁵⁸⁰ Diese Möglichkeit besteht insb. auf dezentralen Handelsplattformen mit On-chain-Orderbuch; vgl. hierzu Schär, *Federal Reserve Bank of St. Louis Review* 2021, 161.

¹⁵⁸¹ Siehe zum Begriff Robinson/Konstantopoulos, *Ethereum is a Dark Forest*, *Medium*, *passim*; ferner Samczsun, *Escaping the Dark Forest*, *passim*.

allen Netzwerkteilnehmern zur Verfügung stehen.¹⁵⁸² Ferner können auch Miner Frontrunning betreiben. Wenn auch Miner lediglich gelegentlich einen Block produzieren, können sie einerseits wie Trading Bots selbst Arbitrage betreiben und andererseits – zusätzlich – die eingehenden Transaktionen zum eigenen Vorteil oder demjenigen eines Dritten innerhalb eines Blocks nach Belieben neu ordnen sowie bei Bedarf eigene Transaktionen einschieben.¹⁵⁸³

Frontrunning ist nach dem Gesagten das Ergebnis sowohl von systeminhärenten Transparenzrisiken als auch von Informationsasymmetrien¹⁵⁸⁴ zwischen den Netzwerkteilnehmern und Nutzern eines dezentralen Systems.¹⁵⁸⁵

Frontrunning wirft nicht nur Fragen der Fairness auf, sondern kann v.a. negative Externalitäten in Form höherer Transaktionsgebühren und vollerer Blöcke erzeugen. Ausserdem ist damit zu rechnen, dass Marktteilnehmer, die regelmässig Opfer von Frontrunning sind, den Markt verlassen könnten, was die Marktliquidität negativ beeinflussen kann (Adverse Selection).¹⁵⁸⁶ Die Gewinne von Arbitragehändlern und Minern, die einerseits aufgrund höherer Transaktionsgebühren und andererseits durch eigenes Frontrunning entstehen, werden als *Miner Extractable Value* bzw. *Maximal Extractable Value* (MEV) bezeichnet.¹⁵⁸⁷

Dezentrale Handelsplätze mit *On-chain*-Liquiditätspools (z.B. Bancor und Uniswap) sind besonders anfällig für Frontrunning durch Trading Bots, werden doch alle Aufträge von Nutzern bereits vor der Abwicklung im dezentralen

¹⁵⁸² Siehe Eskandari/Moosavi/Clark, in: Bracciali et al., *Front-Running Attacks on Blockchain*, 172–173; Zhou et al., 2021 IEEE Symposium on Security and Privacy (SP) 2021, 430–431.

¹⁵⁸³ Siehe Daian et al., 2020 IEEE Symposium on Security and Privacy 2020, 914, 920–921, 922; Eskandari/Moosavi/Clark, in: Bracciali et al., *Front-Running Attacks on Blockchain*, 172; Warren, *Front-running*, Medium, *passim*.

¹⁵⁸⁴ Siehe hierzu unten, [IV.5.2d](#).

¹⁵⁸⁵ Ebenfalls als *Transparenzrisiken* einstufend ESMA, DLT Report, 11–12; Zetzsche/Buckley/Arner, *University of Illinois Law Review* 2018, 1367–1377.

¹⁵⁸⁶ Vgl. hinsichtlich des Verhaltens von Liquiditätsgebern bei Informationsasymmetrien in traditionellen Märkten Fox/Glosten/Rauterberg, *Duke Law Journal* 2015, 217–218, 247–248.

¹⁵⁸⁷ Siehe zu den Begriffen Daian et al., 2020 IEEE Symposium on Security and Privacy 2020, 911, 920–921; Obadia, *Flashbots*, Medium, *passim*; MEV-Explore v0, *What is MEV?*, *passim* («MEV [...] is the total value that can be extracted permissionlessly [i.e. without any special rights] from the re-ordering, insertion or censorship of transactions within a block being produced.»); ausführlich zu dieser Thematik Bankless, *Crypto's Existential Threat*, Bankless Podcast, *passim*.

Netzwerk im Mempool abgebildet.¹⁵⁸⁸ Um die negativen Auswirkungen von Frontrunning zu verringern, hat Uniswap etwa mit einer parametrisierbaren Slippage-Toleranz-Funktion reagiert, die es Nutzern erlaubt, vorab zu bestimmen, wie weit der effektive Ausführungspreis vom erwarteten Preis liegen darf.¹⁵⁸⁹ Dezentrale Handelsplattformen mit *Off-chain*-Orderbüchern (z.B. EtherDelta und OxProtocol) sind besonders anfällig für Frontrunning durch den Betreiber des jeweiligen Orderbuchs.¹⁵⁹⁰ Demgegenüber lassen sich im Fall von Ox und AirSwap die Frontrunning-Möglichkeiten zumindest für Arbitrage Trading Bots deutlich reduzieren.¹⁵⁹¹ Für Frontrunning durch Miner sind grundsätzlich sowohl AMMs als auch Orderbücher anfällig.

iv. Anti-Frontrunning-Technologien

Mit Blick auf dezentrale Handelsplattformen existieren Protokolle, welche das Datenschutzniveau erhöhen sollen. Das Protokoll *Secret Network* etwa ermöglicht Smart Contracts, die keine Transaktionsdaten sowie Vermögensstände nach aussen preisgeben (sog. Secret Contracts). Demnach werden ausschließlich verschlüsselte Daten im verteilten Register abgespeichert.¹⁵⁹² Basierend auf diesem Protokoll wurde sodann die dezentrale Applikation *SecretSwap*¹⁵⁹³ entwickelt. *SecretSwap* erlaubt ähnlich wie etwa Uniswap den Austausch von Kryptovermögenswerten, jedoch in anonymer Weise. Dadurch soll auch Frontrunning verhindert werden können.¹⁵⁹⁴

In einem gewissen Sinne kann dieses Protokoll mit traditionellen Dark Pools verglichen werden, welche typischerweise ein für Aussenstehende intranspa-

¹⁵⁸⁸ Siehe bereits Gün Sirer/Daian, *Bancor Is Flawed*, *passim*; Bogatyy, *Bancor exchange*, *Hackernoon*, *passim*; sodann Buterin, *Improving front running resistance*, *passim*; ferner Lin, *Stanford Journal of Blockchain Law & Policy* 2019, 71 FN 37.

¹⁵⁸⁹ Siehe Uniswap, *Twitter*, *passim*.

¹⁵⁹⁰ Siehe Eskandari/Moosavi/Clark, in: Bracciali et al., *Front-Running Attacks on Blockchain*, 174; Bentov et al., *Cost of Decentralization in Ox and EtherDelta*, *passim*.

¹⁵⁹¹ Siehe Warren, *Front-running*, *Medium*, *passim*; ferner Warren, *Front-running (Part 2)*, *Medium*, *passim*; sodann auch Schär, *Federal Reserve Bank of St. Louis Review* 2021, 163.

¹⁵⁹² Siehe *Secret Network*, *General Overview*, *passim* («*Secret Contracts are similar to smart contracts, such as those used with Ethereum. The key difference is that Secret Contracts can take encrypted inputs and produce encrypted outputs, without exposing any data while it is in-use.*»).

¹⁵⁹³ <https://secretswap.net/>.

¹⁵⁹⁴ Siehe Kisagun, *Front Running Prevention for Automated Market Makers*, *passim*; kritisch Eskandari/Moosavi/Clark, in: Bracciali et al., *Front-Running Attacks on Blockchain*, 183–184.

rentes Orderbuch aufweisen. Eine Verdunklung der Details eines Austauschgeschäfts kann in der Blockchain-Welt paradoxerweise für fairere Ergebnisse sorgen als durchgehend transparente Liquiditätspools und Orderbücher.¹⁵⁹⁵

Sodann bestehen weitere Ansätze zur Lösung des Frontrunning-Problems: DutchX bspw. ist eine dezentrale Handelsplattform mit On-chain-Orderbuch, die den Matching-Mechanismus von *Rückwärtsauktionen* implementiert.¹⁵⁹⁶

Auf DutchX wird der Preis für Kryptovermögenswerte so lange gesenkt, bis das Marktangebot durch die Nachfrage vollständig geräumt wird. Entscheidend ist, dass für alle Teilnehmer der Auktion letztlich derselbe Markträumungspreis zur Anwendung kommt, vorausgesetzt, dass ihr Kaufangebot darüber liegt.¹⁵⁹⁷ Das *Frequent-Batch-Auction-Modell*,¹⁵⁹⁸ wie es etwa in Mesa und Gnosis Auction zur Anwendung gelangt, hat einen vergleichbaren Einfluss auf Frontrunning. Mechanisch basieren solche dezentralen Handelsplattformen auf dem Batch-Ordermodell, wonach in einer ersten Phase die Angebote *en bloc* gesammelt werden, um sie sodann in einer zweiten Phase automatisiert zusammenzuführen.¹⁵⁹⁹ Aufgrund der Tatsache, dass die zeitliche Reihenfolge der Transaktionen für die Abwicklungsphase nicht relevant ist, gilt Frontrunning in einem solchen Auktionssystem als unmöglich oder zumindest deutlich unwirksamer.¹⁶⁰⁰

Eine weitere Vorkehrung gegen Frontrunning in dezentralen Handelsplattformen ist die Verwendung von dezentralen Netzwerken mit *kurzen Abwicklungszeiten* (z.B. Serum). Es ist namentlich damit zu rechnen, dass kürzere Blockzeiten die Ausnutzung vorübergehender Informationsasymmetrien er-

¹⁵⁹⁵ So auch Ferreira Torres/Camino/State, Empirical Study of Frontrunning, 12–13; Zhou et al., 2021 IEEE Symposium on Security and Privacy (SP) 2021, 440 («While the transparency of [decentralized exchanges] is desirable, it can, however, put users' assets at a security risk and allow both liquidity providers and liquidity takers to exploit unknowing traders through a combination of front and back-running.»).

¹⁵⁹⁶ Siehe hierzu oben, [IV.4.2c](#).

¹⁵⁹⁷ Siehe DutchX, *passim*; ausführlich Gnosis, Whitepaper, 16–18.

¹⁵⁹⁸ Siehe hierzu oben, [IV.4.2c](#).

¹⁵⁹⁹ Siehe Smith, Exchange Protocol for the Decentralized Web, 3; eine hilfreiche Darstellung der Funktionsweise des Frequent-Batch-Auction-Modells findet sich in Gnosis Auction, How do Batch Auctions work?, *passim*; sodann in Bezug auf traditionelle Märkte Budish/Cramton/Shim, The Quarterly Journal of Economics 2015, 1549.

¹⁶⁰⁰ Siehe Köppelmann, DutchX, *passim*; ferner Beneš, Main Benefits of the DutchX Mechanism, *passim*; sodann auch Smith, Exchange Protocol for the Decentralized Web, 2; Gnosis Protocol, Introduction to Gnosis Protocol, Benefits, *passim*; Gnosis Auction, Benefits, *passim*; sodann in Bezug auf *Sniping* in traditionellen Märkten Budish/Cramton/Shim, The Quarterly Journal of Economics 2015, 1553–1557; betreffend *Hochfrequenzhandel* in traditionellen Märkten Fox/Glosten/Rauterberg, Duke Law Journal 2015, 269.

schweren.¹⁶⁰¹ Die MEV-Thematik stellt sich ausserdem auch auf Layer-2-Handelsplattformen, denn die an der Ausführung und Abwicklung von Transaktionen verantwortlichen Beteiligten (d.h. Relayers, Sequencers bzw. Operators) können ihre Informationsvorsprünge zulasten der Nutzer ausnutzen und somit für sich selbst oder Dritte MEV generieren.¹⁶⁰² Demgegenüber können Layer-2-Handelsplattformen (z.B. Loopring¹⁶⁰³) sowie Handelsplattformen über Sidechains, wie etwa Liquid¹⁶⁰⁴, je nach Ausgestaltung der Plattform unterschiedliche Präventionsmassnahmen gegen Frontrunning durch Arbitrage Trading Bots implementieren.

Die MEV-Situation ist nicht unähnlich zum verbreiteten, aber umstrittenen *Payment-for-Order-Flow*-Geschäftsmodell in traditionellen Finanzmärkten.¹⁶⁰⁵ In diesem Zusammenhang ist etwa an das Beispiel des GameStop-Skandals der beliebten US-Mobilapplikation Robinhood im Frühjahr 2021 zu denken. Robinhood wird vorgeworfen, Transaktionsdaten ihrer Nutzer an Hochfrequenzhändler verkauft zu haben.¹⁶⁰⁶ Eine solche Entwicklung ist seit dem Aufkommen von passiven Finanzinstrumenten, wie insb. Exchange Traded Funds (ETFs), zu beobachten, denn das Anlegerverhalten solcher Finanzinstrumente kann aufgrund der Notwendigkeit, das Portfolio dauernd im Gleichgewicht zu halten, relativ einfach von anderen Marktteilnehmern antizipiert werden. Darüber hinaus stellen sich bei diesem Geschäftsmodell Fragen im Zusammenhang mit der Best Execution von Kundenaufträgen.¹⁶⁰⁷

¹⁶⁰¹ Vgl. die Ausführungen zur Bedeutung der Netzwerklatenz in Ethereum Daian et al., 2020 IEEE Symposium on Security and Privacy 2020, 910–911, 918; ferner Eskandari/Moosavi/Clark, in: Bracciali et al., *Front-Running Attacks on Blockchain*, 176.

¹⁶⁰² Siehe MEV-Explore v0, *Why MEV as Maximal Extractable Value instead of Miner Extractable Value?*, *passim*.

¹⁶⁰³ Siehe Wang et al., Loopring, 9–10 (*«Loopring operates an OTC model and only supports limit-price orders, meaning that orders' timestamps are ignored. This implies that front-running a trade has no impact on the actual price of that trade, but does impact whether it gets executed or not.»*).

¹⁶⁰⁴ Siehe Nick/Poelstra/Sanders, Liquid, *passim*.

¹⁶⁰⁵ Vgl. für eine Kritik Juels/Eyal/Kelkar, *Front-Running-as-a-Service*, Coindesk, *passim*; demgegenüber weniger skeptisch Daian, MEV, *passim*.

¹⁶⁰⁶ Vgl. etwa MacMillan/Torbati, *Robinhood and Citadel's relationship*, Washington Post, *passim*; Van Doeren, *GameStop*, Cato, *passim*; eine ausführliche Analyse findet sich in SEC, *Equity and Options Market Structure in Early 2021*, 2, 12–13; in *allgemeiner* Hinsicht Lewis, *Flash Boys*, *passim*.

¹⁶⁰⁷ Siehe die Übersicht in FINRA, *Letter of Acceptance, Waiver, and Consent*, 1–2 m.w.H.

Inzwischen ist empirisch nachgewiesen, dass MEV bedeutende Ausmasse im Ethereum-Ökosystem erreichen kann.¹⁶⁰⁸ Die konkreten Konturen und Auswirkungen von MEV sind allerdings umstritten: So wird etwa zwischen «gutem MEV», wie etwa Preisarbitrage und Liquidation in DeFi-Lending-Protokollen, und «schlechtem MEV», namentlich Frontrunning, unterschieden.¹⁶⁰⁹ MEV ist unabhängig von der konkreten Motivation im Einzelfall gewinnmaximierendes Verhalten der Netzwerkteilnehmer. Solches Verhalten ist gerade die zentrale Antriebskraft heutiger dezentraler Systeme und darum in der einen oder anderen Form unverzichtbar. MEV vollständig zu eliminieren, soweit dies wünschbar sein sollte, ist wohl unmöglich. Als Rent-Seeking-Verhalten im klassischen Sinn kann es darum nicht verstanden werden.¹⁶¹⁰ Entsprechend werden MEV-Auktionen als Lösung vorgeschlagen, um zugleich die Dezentralität von Mining bzw. Relaying zu gewährleisten.¹⁶¹¹ Um die negativen Externalitäten für dezentrale Netzwerke zu verringern, machen MEV-Auktionen von separaten privaten Netzwerken Gebrauch, welche Arbitrageuren und Minern erlaubt, direkt einander die Abwicklungsreihenfolge zu kommunizieren.¹⁶¹² Dies schliesst allerdings gerade nicht aus, dass gewisse Fairnesserwägungen Einzug in die Protokolle finden sollten.¹⁶¹³ Dazu dienen etwa Regeln betreffend

¹⁶⁰⁸ Siehe z.B. Qin/Zhou/Gervais, Quantifying Blockchain Extractable Value, *passim*; Wang et al. Impact and User Perception of Sandwich Attacks, *passim*.

¹⁶⁰⁹ Siehe etwa Daian, MEV, *passim* m.w.H. («The existence of a 'bribe to anyone' [permissionless bribe] runs these systems, and indeed runs the blockchains they operate on themselves. MEV is therefore fundamental, and not always harmful. It is often an essential part of how decentralized/'permissionless' protocols operate and how they are secured, and why they do not require permission to achieve certain equilibria.»); ferner sxysun, Short Note on Extractable Value, *passim*, der zwischen MEV aufgrund der Möglichkeit, Blöcke zu produzieren («Monarch MEV»), aufgrund ineffizienter Koordinationsmechanismen («Moloch MEV») und aufgrund von Informationsasymmetrien («Mafia MEV») unterscheidet.

¹⁶¹⁰ Siehe hierzu oben, [IV.5.1f](#).

¹⁶¹¹ So etwa Floersch, MEV Auction, *passim* («[...] we simply auction off the right to reorder transactions within an N-block window to the highest bidder. That is, we create a MEV Auction (MEVA), in which the winner of the auction has the right to reorder submitted transactions and insert their own, as long as they do not delay any specific transaction by more than N blocks.»); sehr kritisch demgegenüber Pmcgoohan, Way Worse Than You Think, CoinDesk, *passim*; ähnlich auch Felten, MEV auctions, Medium, *passim*; darauf replizierend Buterin, Medium, *passim*.

¹⁶¹² Siehe etwa das Projekt «Flashbots»; vgl. hierzu Flashbots Docs, *passim*.

¹⁶¹³ In diesem Sinne Buterin, Credible Neutrality, *passim* («[...] a mechanism is credibly neutral if just by looking at the mechanism's design, it is easy to see that the mechanism does not discriminate for or against any specific people. The mechanism treats everyone fairly, to the extent that it's possible to treat people fairly in a world where everyone's capabilities and needs are so different.»).

Abwicklungsreihenfolge von Transaktionen.¹⁶¹⁴ In dieser Hinsicht wurde auch bereits die Einführung einer mit der Netzneutralität des Internets¹⁶¹⁵ vergleichbaren Blockchain-Neutralität diskutiert.¹⁶¹⁶ Ein anderer Ansatz ist es, die Transaktionsdetails bis zur erfolgreichen Aufnahme der Transaktion in einen Block vor den Minern bzw. Stakern zu verbergen.¹⁶¹⁷

Darüber hinaus bestehen überarbeitete AMM-Designs, wie sie etwa von SwapSwap¹⁶¹⁸ umgesetzt werden. Das Design von SwapSwap wird als Automated Arbitrage Market Maker (A2MM) bezeichnet. Ziel von A2MMs ist es, dass die Arbitrage von Preisunterschieden zwischen unterschiedlichen AMMs, die üblicherweise in Form von MEV von Arbitrage Bots vereinnahmt wird, den Nutzern der Plattform zugutekommt.¹⁶¹⁹

MEV ist letztlich auf die *besondere Stellung* von Minern bzw. Validatoren (Layer 1) und Relayern (Layer 2) als Blockproduzenten in dezentralen Systemen zurückzuführen. Die Effektivität der Prävention von Frontrunning ist darum auch davon abhängig, wie kompetitiv Mining bzw. Relaying ist. Ein hoher Grad an Dezentralität in diesen Bereichen senkt erwartungsgemäss die Häufigkeit von Frontrunning durch solche Akteure. MEV macht somit das soziotechnische Machtgefüge innerhalb von dezentralen Systemen sichtbar.

Die teils postulierte «Base Layer Neutrality»¹⁶²⁰ wird denn auch vor dem Hintergrund der Entwicklungen der OFAC-Sanktionen gegen Tornado Cash in Frage gestellt.¹⁶²¹ Im Wesentlichen geht es um die Fragen, ob und inwieweit die unterschiedlichen am Blockproduktionsprozess beteiligten Personen (in Ethereum: *Searcher*, *Builder*, *Relay* und *Validator/Proposer*) im Rahmen ihrer Tätigkeiten die Transaktionen und Blöcke auf Konformität mit Sanktionslisten abgleichen und sanktionierte Adressen effektiv zensurieren müssen.¹⁶²² Ferner

¹⁶¹⁴ Siehe etwa das Projekt «Fair Sequencing Service (FSS)», das auf ein verteiltes Netzwerk von Orakel setzt, vgl. hierzu Juels/Breidenbach/Tramèr, Fair Sequencing Services, *passim*; ferner Kelkar et al., in: Micciancio/Ristenpart, Order-Fairness for Byzantine Consensus, 452; *allgemein* Mavroudis/Melton, in: AFT '19 – Conference on Advances in Financial Technologies, Fair Order-Matching, *passim*.

¹⁶¹⁵ Vgl. Art. 12e FMG und Art. 10f FDV; ferner hierzu BAKOM, Netzneutralität, *passim*.

¹⁶¹⁶ Vgl. Messias et al., IMC 2021 – ACM Internet Measurement Conference 2021, 12.

¹⁶¹⁷ Siehe etwa das Projekt «LibSubmarine»; vgl. hierzu LibSubmarine, Defeat Front-Running, *passim*; sodann auch Warren, Front-running (Part 2), Medium, *passim*; Bogatyy, Bancor exchange, Hackernoon, *passim*; Antonopoulos/Wood, Mastering Ethereum, 206.

¹⁶¹⁸ <https://swapswap.org/>.

¹⁶¹⁹ Ausführlich hierzu Zhou/Qin/Gervais, Mitigating Frontrunning, 18. Juni 2021, 1–2.

¹⁶²⁰ So etwa Seira/amyaxizhang/Robinson, Base Layer Neutrality, *passim*.

¹⁶²¹ Vgl. hierzu oben, IV.5.2c.ii.

¹⁶²² Ausführlich hierzu Zinaman, Rubber Meets the Road, *passim*.

wird das Phänomen von MEV auch verstärkt mit Blick auf weitere finanzmarktrechtliche Konzepte, wie etwa die bestmögliche Erfüllung von Kundenaufträgen sowie die Verhinderung von Insiderhandel und Marktmanipulation, diskutiert.¹⁶²³ Generell ist es angezeigt, die genauen Konturen und Auswirkungen von MEV auf die Nutzer und Teilnehmer von offenen dezentralen Systemen zu eruieren, bevor überhaupt in Betracht gezogen wird, zu staatlichen Interventionen zu greifen.¹⁶²⁴ Idealerweise werden technische Lösungen entwickelt, welche MEV verhindern oder, soweit sinnvoll, an die betroffenen Parteien zurückgeben. MEV ist und bleibt ein komplexes Phänomen, das nicht nur auf individueller Ebene negative Effekte zeitigen kann, sondern im Extremfall ein Blockchain-System grundsätzlich aus den Fugen heben könnte.¹⁶²⁵

d. Informationsrisiken

i. Informationsasymmetrien als Ausgangspunkt

Informationsasymmetrien sind ein ubiquitäres Phänomen menschlicher Interaktion. Die arbeitsteilige Wirtschaftsordnung, und zwar nicht nur im Bereich der Finanzintermediation,¹⁶²⁶ erhöht zudem die Komplexität von Austauschgeschäften, sodass letztlich die Häufigkeit und Intensität von Informationsvorsprüngen weiter zunimmt. Daraus können sich Interessenkonflikte ergeben, die u.U. rechtlich relevant sind.

Der Umgang mit Interessenkonflikten ist regelmässig Gegenstand der Rechtsordnung.¹⁶²⁷ Dies gilt auch für den Finanzmarktinfrastrukturbereich.¹⁶²⁸ Betreiber von traditionellen Finanzmarktinfrastrukturen sind etwa verpflichtet, eine Finanzmarktinfrastruktur über je einen autonomen Rechtsträger zu betreiben.¹⁶²⁹ Die rechtliche Separierung einer Tätigkeit soll konfliktreiche Überschneidungen

¹⁶²³ Vgl. für einen ersten Überblick Auer/Frost/Vidal Pastor, BIS Bulletin Nr. 58, 16. Juni 2022, 4–5.

¹⁶²⁴ GLM. bereits EC, Roukny Report, 32; Barcentewicz, MEV on Ethereum, 27, der auf die Herausforderung von regulatorischer Arbitrage hinweist; ferner Ramos/Ellul, MEV Saga, 10–11.

¹⁶²⁵ Siehe Barcentewicz, MEV on Ethereum, 15 m.w.N.

¹⁶²⁶ Siehe hierzu oben, [II.1.2](#).

¹⁶²⁷ Siehe für das banktypische Auftragsrecht statt vieler Sethe, Anlegerschutz, 141–142; Abegglen, in: Kunz et al., Bankkonzern, 680.

¹⁶²⁸ Siehe hinsichtlich internationaler Governance-Standards für Finanzmarktinfrastrukturen BIS-CPSS/IOSCO, Principles for financial market infrastructures, 26–31; ferner IOSCO, Methodology Objectives and Principles, insb. Prinzipien 31, 34 und 38.

¹⁶²⁹ Art. 10 Abs. 1 FinfraG.

in den Aktivitäten der einzelnen Betreiber verringern.¹⁶³⁰ Ausserdem sind Betreiber einer Finanzmarktinфраstruktur angehalten, organisatorische Massnahmen zur Feststellung, Verhinderung, Beilegung, Überwachung und allenfalls Offenlegung von Interessenkonflikten zu treffen.¹⁶³¹ Der Zweck von Regeln zum Umgang mit Interessenkonflikten im Allgemeinen und mit den konfliktreichen Aspekten des Betriebs einer Finanzmarktinфраstruktur im Besonderen wird je nach Auffassung im Funktions- und Anlegerschutz, namentlich der Gleichbehandlung der Anleger, gesehen.¹⁶³²

Das Internet stellt ein anschauliches Beispiel dafür dar, dass Informationsungleichgewichte in der Welt durch technologische Innovation, wenn nicht behoben, so doch verringert werden können. Doch das Internet selbst ist für viele Menschen eine unverständliche Technologie. Kaum ein Internetnutzer sieht bei den Protokollen, die tagein tagaus dem einfachen elektronischen Austausch von Informationen dienen, wirklich durch. Ähnlich scheint es sich mit dezentralen Systemen im Allgemeinen und DeFi-Anwendungen im Besonderen zu verhalten. Während die zugrundeliegenden Protokolle zwar den Zugang zu traditionell intermediatisierten Finanzdienstleistungen vereinfachen, stellen sie sehr hohe Ansprüche an das Verständnis technischer und ökonomischer Zusammenhänge durch die Nutzer. Mangels Intermediation sind tatsächlich vorhandene Informationsgefälle im ersten Moment indessen nicht als Problem zu begreifen. Denn im Idealfall, d.h. wenn kein Kontroll- und Machtungleichgewicht zwischen den an einem Austauschgeschäft beteiligten Parteien besteht, kann ein etwaiges Ungleichgewicht in der Informationslage auch nicht einseitig ausgenutzt werden.

Trotz der Verringerung traditioneller Agency Risks bzw. Intermediärrisiken¹⁶³³ können DeFi-Anwendungen und insb. dezentrale Handelsplattformen in der Praxis oftmals von zentralisierter Entscheidungsmacht betroffen sein. Aufgrund von Informationsungleichgewichten zwischen den unterschiedlichen an einem dezentralen System beteiligten Parteien können sich Interessenkon-

¹⁶³⁰ Siehe SK FinfraG-Jungo/Zibung/Roth, Art. 10 N 5 *in fine*, 15; skeptisch hingegen BSK FINMAG/FinfraG-Kuhn, Art. 10 FinfraG N 14.

¹⁶³¹ Art. 20 FinfraG und Art. 18 FinfraV; in Bezug auf OHS gelten Art. 44 FinfraG und Art. 39 FinfraV.

¹⁶³² Siehe Botschaft FinfraG 2014, 7520, 7523; SK FinfraG-Jungo/Zibung/Roth, Art. 20 N 1, 3, 4–5; OFK FinfraG/BEG-Vogel/Heiz/Luthiger, Art. 20 FinfraG N 1; skeptisch hingegen BSK FINMAG/FinfraG-Kuhn, Art. 20 FinfraG N 4–8, 19–20, für welchen die Interessenkonflikte innerhalb eines Konzerns, deren Gesellschaften eine Finanzmarktinфраstruktur betreiben, sowie zwischen Betreiber und Eigentümerschaft einer Finanzmarktinфраstruktur im Vordergrund der Regel in Art. 20 FinfraG stehen.

¹⁶³³ Siehe hierzu oben, [II.5.2c](#).

flikte ergeben, die aufgrund der Kontroll- und Machtstrukturen zu fragwürdigen Ergebnissen und Situationen für die beteiligten Parteien führen können.¹⁶³⁴ Vergleichbare Beobachtungen wurden häufig auch im Rahmen der Bewerbung und des Vertriebs von Token von ICO-Projekten gemacht.¹⁶³⁵

Es folgen Ausführungen zum praktisch relevanten Informationsrisiko von Admin Keys in dezentralen Applikationen sowie zu Wash Trading auf dezentralen Handelsplattformen.

ii. Admin Keys

Dezentralen Applikationen fehlt es theoretisch an einer zentralen Stelle, die zugunsten oder zulasten von Nutzern und anderen Marktakteuren in die laufenden Operationen der Applikation eingreifen kann. Die Smart Contracts dezentraler Applikationen weisen wie gewöhnliche Wallets eine eigene Adresse auf, besitzen allerdings keine Private Keys, weshalb sie im Prinzip niemandem gehören und von niemandem kontrolliert werden können, nachdem sie auf dem dezentralen Netzwerk abgelegt worden sind. Smart Contracts «gehören» sich mit anderen Worten selbst.¹⁶³⁶

Es gibt in der Smart Contract-Praxis allerdings eine bedeutende Ausnahme: Admin Keys. Solche «Schlüssel» räumen einer bestimmten Gruppe von Akteuren – i.d.R. den Entwicklern einer Applikation – spezielle Berechtigungen im Hinblick auf einen eingesetzten Smart Contract ein. Admin Keys sind vergleichbar mit den Berechtigungen, über welche Betreiber zentralisierter Plattformen typischerweise verfügen. Im Nachgang zum aufsehenerregenden Twitter-Hack von Mitte Juli 2020, während dem mehrere Konten berühmter Persönlichkeiten in betrügerischer Absicht missbraucht worden waren, wurde etwa bekannt, welche weitgehenden Berechtigungen Angestellte des Softwareunternehmens in Bezug auf die Moderation der Plattform innehaben.¹⁶³⁷ Die breite DeFi-Öffentlichkeit wurde, soweit ersichtlich, erstmals im Herbst 2019 auf die Admin Key-Thematik aufmerksam.¹⁶³⁸

¹⁶³⁴ Siehe etwa EC, Roukny Report, 28–31, der einen informationsökonomischen Ansatz (vgl. 17–27) anwendet und insb. aus der Tatsache der Pseudonymität Ineffizienzen herleitet.

¹⁶³⁵ Siehe Buckley/Arner/Zetzsche, FinTech, 122.

¹⁶³⁶ Siehe Antonopoulos/Wood, Mastering Ethereum, 26, 127–128.

¹⁶³⁷ Siehe etwa Cox, Hijack Accounts, Vice, *passim*; ferner Thompson/Barrett, How Twitter Survived Its Biggest Hack, Wired, *passim* («[...] one of the first things Twitter realized in the immediate aftermath was that too many people had too much access to too many things.»).

¹⁶³⁸ Siehe Soleimani, What You Should Know, Medium, *passim*.

Die mit Admin Keys verbundenen Berechtigungen können ganz unterschiedlicher Natur sein: Im Rahmen eines ICOs bzw. STOs ist es etwa regelmässig notwendig, Funktionen in den Code des Smart Contract aufzunehmen, um Token herauszugeben (mint), herausgegebene Token zu zerstören (burn), Teilnehmern eines Crowdsales zu erlauben, die an einen Smart Contract transferierten Token zurückzuziehen (withdraw) sowie bspw. aus regulatorischen Gründen den Kreis der Erwerber einzuschränken (whitelist bzw. blacklist). Ferner können Token Stimmrechte vermitteln, die über eine entsprechend programmierte Funktion ausgeübt werden.¹⁶³⁹ Schliesslich können Smart Contracts auch nachträglich gelöscht werden (selfdestruct), wenn dies ein Programmierer im Code vorsieht, was dazu führt, dass alle hinterlegten Kryptovermögenswerte an eine ebenfalls bestimmbare Adresse übertragen werden.¹⁶⁴⁰

Die oben angeführten Privilegien werden den Access Control-Funktionalitäten eines Smart Contracts zugeordnet.¹⁶⁴¹ Die Steuerungslogik hinter Access Control hängt grundsätzlich an der Ownership eines Smart Contracts. Grundsätzlich gilt als Owner diejenige Wallet-Adresse, die den Smart Contract auf der Blockchain abgelegt hat. Access Control kann permanent oder vorübergehend sein. So ist es etwa möglich, die Ownership an einem Smart Contract nachträglich zu übertragen (transferOwnership) oder sie aber gänzlich aufzugeben (renounceOwnership).¹⁶⁴² Gerade letztere Funktion kommt in der Praxis typischerweise dann zur Anwendung, wenn ein Team eines Projekts die Kontrolle über einen Smart Contract aufgeben möchte. In diesem Fall verzichten sie auf die Möglichkeit, von den Admin Keys Gebrauch zu machen. Ebenfalls ist es möglich, unterschiedliche Rollen vorzusehen, sodass bspw. ein Kernteam von Personen neue Token schaffen kann, während gewöhnliche Nutzer lediglich mit den öffentlichen Funktionen des Smart Contracts interagieren können.¹⁶⁴³ Schliesslich kann auch ein anderer Smart Contract Owner eines Smart Contracts sein. Ein beliebter Mechanismus in DeFi ist etwa das Aufsetzen von Smart Contracts, welche von mehreren Personen (Multisig) oder einer DAO

¹⁶³⁹ Siehe etwa OpenZeppelin, Access Control, *passim*; Antonopoulos/Wood, Mastering Ethereum, 208–209.

¹⁶⁴⁰ Siehe Antonopoulos/Wood, Mastering Ethereum, 129, 140, 144–145.

¹⁶⁴¹ Vgl. hierzu Liu/Sun/Szalachowski, 2020 50th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN) 2020, 222–223.

¹⁶⁴² Siehe OpenZeppelin, Access Control, Ownership and Ownable, *passim*.

¹⁶⁴³ Siehe OpenZeppelin, Access Control, Role-Based Access Control, *passim*.

kontrolliert werden.¹⁶⁴⁴ Anbieter solcher Lösungen sind etwa Gnosis Safe¹⁶⁴⁵ und Aragon Govern¹⁶⁴⁶. MakerDAO etwa greift – neben Off-chain-Infrastrukturen – auf ein komplexes System von Smart Contracts für eine möglichst dezentrale Governance der Plattform zurück.¹⁶⁴⁷

Idealerweise sehen Projekte Admin Keys vor, um allfällige notwendige Aktualisierungen in Smart Contracts durchführen, bei Bedarf fehlerhaften Code ersetzen oder gänzlich neue Smart Contracts, welche die alten ersetzen, entwickeln zu können. Wie Erfahrungen mit unvorhergesehenen Programmierfehlern zeigen,¹⁶⁴⁸ entspricht die Möglichkeit, jederzeit in den Lauf von Smart Contracts eingreifen und diese auch *nach* dessen Aktivierung auf der Blockchain bis zu einem gewissen Grad weiterhin kontrollieren zu können, einem praktischen Bedürfnis.¹⁶⁴⁹ Die Existenz von Admin Keys wird darum von einigen Beobachtern zumindest für so lange sinnvoll gehalten, als dass sich DeFi-Applikationen in einem sehr frühen Entwicklungsstadium befinden und deswegen regelmässige Updates benötigen.¹⁶⁵⁰ Argumentativ greift diese Begründung auf das tendenziell idealisierende Konzept des wohlmeinenden Diktators zurück, wie es etwa für die Entwicklung von Open-Source-Software entwickelt wurde. Die Existenz von Ad-

¹⁶⁴⁴ Siehe Antonopoulos/Wood, *Mastering Ethereum*, 124–125, 209; OpenZeppelin, *Access Control, Ownership and Ownable*, *passim*.

¹⁶⁴⁵ <https://gnosis-safe.io/>; siehe hierzu Gnosis Safe, *What is Gnosis Safe?*, *passim* («Gnosis Safe is a smart contract wallet running on Ethereum that requires a minimum number of people to approve a transaction before it can occur (M-of-N). If for example you have 3 main stakeholders in your business, you are able to set up the wallet to require approval from all 3 people before the transaction is sent. This assures that no single person could compromise the funds.»).

¹⁶⁴⁶ <https://aragon.org/govern>.

¹⁶⁴⁷ Siehe MakerDAO, *Governance*, *passim*.

¹⁶⁴⁸ Siehe etwa für den Fall der Parity Multi-Signature Wallet-Programmierfehler, die zum Verlust bzw. zur Blockierung von mehreren hunderttausend ETH geführt haben, Pearson, *Hacker Allegedly Stole Million*, *Vice*, *passim*; ferner Condon, *Parity Wallet Hack 2*, *Hacker-noon*, *passim*.

¹⁶⁴⁹ Siehe Qureshi, *Hacker stole M*, *passim* («In the case of a successful attack, defense is extremely difficult. The white-hats in the Parity hack demonstrated how limited their defense options were – there was no way to secure or dismantle the contracts, or even to hack back the stolen money; all they could do was hack the remaining vulnerable contracts before the attacker did.»).

¹⁶⁵⁰ Siehe Antonopoulos/Wood, *Mastering Ethereum*, 11; wohl auch Harvey/Ramachandran/Santoro, *DeFi*, 65; demgegenüber *strenger* Liu/Sun/Szalachowski, 2020 50th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN) 2020, 2, die von einer «[...] duty of the contract developer to implement proper access control or defensive mechanisms prior to deployment [of the smart contract to the blockchain]» sprechen.

min Keys stellt nach vorliegender Auffassung indessen eine Verletzung der Dezentralität solcher Applikationen dar.¹⁶⁵¹

Die dezentrale Handelsplattform Ox ist im Anschluss an die Entdeckung einer Schwachstelle in ihrem Code, welche sie mit dem Aufsetzen neuer Smart Contracts behoben hat, ausdrücklich auf dieses Spannungsverhältnis eingegangen:

*«The decision to put guard rails in the Ox smart contracts does not reflect our philosophy on decentralization. Today, we are faced with the realities of developing safety-critical financial infrastructure on top of a rapidly evolving tech stack and we must balance our passion for decentralization with what we believe to be common sense security backstops.»*¹⁶⁵²

Admin Keys können als die weitgehendste Access Control-Funktion bezeichnet werden. Sie verleihen ihren Inhabern namentlich die Fähigkeit, *autoritativ* in die laufenden Operationen von Smart Contracts einzugreifen. Im Extremfall könnten Admin Keys dazu verwendet werden, alle Vermögenswerte in einem Smart Contract an eine neue Adresse zu übertragen. In solchen Extremfällen, in denen den Inhabern der Admin Keys praktisch alle möglichen Befugnisse zukommen, ist die Rede von (allgemeiner) *Upgradeability* des Smart Contracts.

Admin Keys sind somit Risiken, die im Ergebnis mit traditionellen Gegenpartei-risiken durchaus vergleichbar sind. Die Existenz und der Umfang von Admin Keys sind Bestandteil des Codes der betreffenden Smart Contracts und können entsprechend von Projekt zu Projekt sehr stark variieren.¹⁶⁵³ Im Falle etwa des Ethereum-kompatiblen Matic/Polygon-Netzwerks werden Kryptovermögenswerte im Umfang mehrerer Milliarden US-Dollar mithilfe einer Multisig-Lösung gesichert, deren einzelnen Private Keys von den Entwicklern des Protokolls kontrolliert werden.¹⁶⁵⁴ Darunter befinden sich etwa auch Vermögenswerte in den Pools der AMM-Plattform Quickswap¹⁶⁵⁵. Auf der Webseite wird inzwischen angekündigt, dass ein Wechsel zu einem Governance-Modell geprüft wird, das sich bei anderen, etablierten DeFi-Protokollen bewährt

¹⁶⁵¹ Vgl. auch Antonopoulos/Wood, *Mastering Ethereum*, 275 («[...] in the long run, true DApps cannot have specialized access for privileged accounts – that's not decentralized.»); sodann Carter/Jeng, in: Coen/Maurice, *DeFi Protocol Risks*, 26 («Ultimately, assets held in contracts mediated by admin keys should be understood as custodial rather than wholly sovereign interactions between users and a protocol.»).

¹⁶⁵² Siehe Ox Core Team, *Post-mortem: Ox v2.0 Exchange Vulnerability*, *passim*.

¹⁶⁵³ Siehe Antonopoulos/Wood, *Mastering Ethereum*, 128.

¹⁶⁵⁴ Siehe Matic, *FAQ*, Polygon Multisigs, *passim*.

¹⁶⁵⁵ <https://quickswap.exchange/>.

hat.¹⁶⁵⁶ Nutzer sollten sich vor diesem Hintergrund bewusst sein, dass dezentrale Applikationen, die Admin Keys vorsehen, je nach Ausgestaltung einen *hohen Grad an Zentralisierung* aufweisen können. Damit zusammenhängend setzen sie interpersonales Vertrauen in die Inhaber der Admin Keys voraus, dass diese einerseits die Private Keys sicher verwahren und andererseits ihre Privilegien ausschliesslich im Interesse der Nutzer und des Netzwerks einsetzen.¹⁶⁵⁷ Dies führt mit anderen Worten zu Informationsasymmetrien zwischen den Inhabern der Admin Keys (Agenten) und den Nutzern der Smart Contracts (Prinzipale).

Daraus leiten sich eine Vielzahl von Informationsrisiken ab:

Zunächst müssen Nutzer für jedes einzelne Projekt abklären, *ob* das jeweilige Entwicklerteam über Admin Keys verfügt und *welche* Privilegien es daraus ableiten kann. Soweit solche existieren, ist es für die Nutzer in den wenigsten Fällen ersichtlich, auf welche Weise das Entwicklerteam die Admin Keys gegen externe und interne Angreifer schützt. Nota: Aus Sicherheitsgründen werden die Schutzmassnahmen in aller Regel aber nicht offengelegt. Diese Frage ist jedoch zentral, denn die unsorgfältige Verwaltung von Admin Keys kann letztlich ein Angriffsvektor von Smart Contracts darstellen, welche die von den Nutzern aufgebrauchten Vermögenswerte verwahren. Dieses Spannungsverhältnis lässt sich bisher nur schwerlich auflösen. Die in der Praxis vorkommenden Key Management-Lösungen variieren von Projekt zu Projekt sehr stark:¹⁶⁵⁸ In einigen Fällen kontrolliert ein einziger Entwickler und damit potenziell auch ein erfolgreicher Angreifer die eingesetzten Smart Contracts einer dezentralen Applikation. Demgegenüber sehen viele Projekte *Multisig*-Mechanismen vor, die vor der Aktivierung einer Modifikation an einem Smart Contract das Signieren der Transaktion durch mehrere Personen (z.B. 3 von 5 Entwicklern) verlangt. Einige Projekte sehen zudem *Timelocks* vor, die es Nutzern bei bevorstehenden Änderungen, mit denen sie nicht einverstanden sind, erlaubt, ihre Vermögenswerte zurückzuziehen.¹⁶⁵⁹

Die Existenz von Admin Keys stellt ferner die *Zensurrestistenz* dezentraler Applikationen nachhaltig in Frage. Mehr noch: Sie liefert die Nutzer auf Gedeih und Verderb der Verwahrungspraxis der Entwickler aus, über welche in der

¹⁶⁵⁶ Siehe Matic, FAQ, Polygon Multisigs, *passim*.

¹⁶⁵⁷ So auch Antonopoulos/Wood, *Mastering Ethereum*, 209.

¹⁶⁵⁸ Für eine allerdings nicht mehr aktuelle Übersicht von DeFi-Projekten in Bezug auf *Admin Key Risks* siehe Blec, *Trustlessness of DeFi*, *passim*; ferner Blec, *Defi Watch*, *passim*.

¹⁶⁵⁹ Siehe hierzu etwa OpenZeppelin, *Governance*, *Timelock*, *passim*.

Praxis bewusst wenig Transparenz herrscht (Security through Obscurity)¹⁶⁶⁰, und selbst für den Fall, dass offen darüber berichtet wird, sind zentrale Elemente der Verwahrung nur schwer nachzuprüfen. Aus Sicht der Nutzer ist darum die Existenz von Admin Keys bedeutungsmässig mit potenziell weitgehenden negativen Folgen für die von ihnen in der betreffenden DeFi-Applikation deponierten Vermögenswerte gleichzusetzen.

Zwar haben viele Projekte trotz erheblicher Informationsrisiken aufgrund von Admin Keys lange Zeit erheblichen Zulauf erhalten, doch haben grössere Projekte in der jüngeren Vergangenheit damit begonnen, die Governance ihrer Smart Contracts zu dezentralisieren. Dies findet typischerweise mittels Übertragung der Admin Keys auf eine DAO statt, welche nunmehr einer Mehrzahl von Personen ermöglicht, mittels spezifischer Governance Token an Verwaltungsentscheidungen teilzuhaben.¹⁶⁶¹ Hinter der Kreditplattform *Compound* bspw. steht eine DAO bestehend aus allen Inhabern von COMP-Token. Die Modifikationen der Smart Contracts können etwa eine Anpassung der Darlehensbedingungen (Zinssatz etc.) sowie die Aufnahme neuer Vermögenswerte als Sicherheiten für Darlehen betreffen. Zudem kommen nach einer erfolgreichen Abstimmung über Modifikationen Timelocks von mindestens zwei Tagen zur Anwendung.¹⁶⁶² Der Minderheit der nicht zustimmenden Nutzer verbleibt damit Zeit, ihre Vermögenswerte bei Bedarf aus dem Protokoll zurückzuziehen, bevor die angenommenen Aktualisierungen in Kraft treten.

Demgegenüber gibt es auch dezentrale Applikationen, insb. dezentrale Handelsplattformen, wie etwa *Uniswap*,¹⁶⁶³ die von Beginn weg keine Admin Keys vorsehen.¹⁶⁶⁴ Alle Aktualisierungen der Smart Contracts müssen darum über das Aufsetzen neuer Smart Contracts erfolgen; dabei bleiben die bisherigen Smart Contracts bestehen, womit sie weiterhin nutzbar sind. Uniswap hat dennoch eine DAO, welche den UNI-Tokeninhabern erlaubt, über künftige Modifikationen am Protokoll abzustimmen. Allerdings verfügt die DAO, wie bereits erwähnt, über keine relevanten Admin Keys. Im Wesentlichen beschränkt sich die Rolle von UNI-Inhabern auf die Festlegung des Verteilungs-

¹⁶⁶⁰ Kritisch zu diesem Sicherheitsprinzip NIST, General Server Security, 2–4 m.w.N.

¹⁶⁶¹ Siehe z.B. betreffend die Lending-Plattform AAVE Kivlighan, Aave Admin Key Handover, Medium, *passim*.

¹⁶⁶² Zum Ganzen <https://compound.finance/docs/governance>. Siehe für ein konkretes Beispiel Behrens, Compound, Decrypt, *passim*.

¹⁶⁶³ Siehe Adams et al., Uniswap v3, 2, 3 («The factory has an owner, which is initially controlled by UNI tokenholders. The owner does not have the ability to halt the operation of any of the core contracts.»).

¹⁶⁶⁴ Vgl. Mapperson, God Mode, Cointelegraph, *passim*.

schlüssels der Handelsgebühren auf Uniswap.¹⁶⁶⁵ Zudem implementiert auch Uniswap V2 vor jeder Änderung einen Timelock über einen entsprechenden Smart Contract.¹⁶⁶⁶ Andere dezentrale Handelsplattformen, wie bspw. Loopring, setzen hinsichtlich der eingesetzten Smart Contracts ebenfalls auf dezentrale Governance durch Tokeninhaber.¹⁶⁶⁷

Es ist zu erwähnen, dass 40% der UNI-Token vom Entwicklerteam sowie von Investoren und Beratern des Projekts gehalten werden.¹⁶⁶⁸ Inhaber einer bedeutenden Anzahl von Token, sog. *Whales*, wie sie in der Krypto-Community bezeichnet werden, haben u.U. einen beachtlichen Einfluss auf die Governance einer Plattform.¹⁶⁶⁹ Hinzu kommt das aus dem traditionellen Lebensbereichen längst bekannte Problem der rationalen Apathie von Stimmberechtigten und Wählern in demokratischen Systemen¹⁶⁷⁰ sowie von Kleinanlegern beim Bezug von Finanzdienstleistungen¹⁶⁷¹ und im Rahmen der Governance eines Unternehmens.¹⁶⁷² Für kleinere Tokeninhaber macht es angesichts ihren geringen Stimmgewichts ökonomisch nur bedingt Sinn, an einer Abstimmung über Protokolländerungen teilzunehmen. WERNER et al. beschreiben den Fall, dass eine einflussreiche Gruppe die Paramater in ihrem Interesse festlegen können, als *Governance Extractable Value (GEV)*.¹⁶⁷³

Aus diesem Grund erlauben Projekte, wie etwa *Sybil*¹⁶⁷⁴, dass Tokeninhaber mit bloss einigen wenigen Stimmen durch *Delegation* ihrer Token ihr volles Stimmgewicht auf effiziente Art und Weise realisieren können. Neu am Pro-

¹⁶⁶⁵ Siehe Adams et al., Uniswap v3, 3. Ende Februar 2024 stand ein Vorschlag der Uniswap Foundation im Raum, die Handelsgebühren für die UNI-Tokeninhaber zu aktivieren, um die Quote der Beteiligung an der Protokoll-Governance zu erhöhen; vgl. eek637, [Temperature Check] – Activate Uniswap Protocol Governance, *passim*.

¹⁶⁶⁶ Vgl. <https://etherscan.io/address/0x1a9c8182c09f50c8318d769245bea52c32be35bc>.

¹⁶⁶⁷ Siehe Wang et al., Loopring, 8–9.

¹⁶⁶⁸ Siehe Behrens, Uniswap Token Launch, Decrypt, *passim*; kritisch Eichholz, The UNI Token, *passim*.

¹⁶⁶⁹ Ebenfalls kritisch Schär, Federal Reserve Bank of St. Louis Review 2021, 170; Buterin, Beyond coin voting governance, *passim*; ausführlich in empirischer Hinsicht hierzu Nadler/Schär, Decentralized Finance, *passim*.

¹⁶⁷⁰ Siehe zur rationalen Ignoranz der Bürger in demokratischen Systemen Downs, Economic Theory of Democracy, 245–247.

¹⁶⁷¹ Siehe Sethe, in: Heiss/Loacker, Konsumentenschutz, N 8.6.

¹⁶⁷² Siehe Watter/Spillmann, GesKR 2006, 100; Fischer, GesKR 2021, 7–8; sodann Gericke/Baum, SZW 2014, 348–349, wo eine solche Apathie selbst für institutionelle Anleger bejaht wird; ferner Yaron Nili/Kobi Kastiel, In Search of «Absent» Shareholders: A New Solution to Retail Investors' Apathy, Delaware Journal of Corporate Law 2016, 55–104, 57, 60–61.

¹⁶⁷³ Siehe Werner et al., Decentralized Finance, 10.

¹⁶⁷⁴ <https://sybil.org/>.

zess ist die Verknüpfung des Ethereum-Kontos des Delegationsempfängers mit dessen digitaler Identität (insb. Twitter- oder GitHub-Konten). Somit können Tokeninhaber ihre Stimmrechte u.U. an reale Identitäten delegieren. Bisher wurde Sybil etwa von Uniswap, Compound und Aave implementiert. Reputationsmechanismen können somit neuerdings verwendet werden, um das kollektive Handlungsproblem der Stimmabgabe marginalisierter Tokenbesitzer zu überwinden und dadurch für ein repräsentativeres Abstimmungsbild innerhalb der Governance von DAOs zu sorgen.¹⁶⁷⁵

Anders als auf der Netzwerkebene kann Zentralisierung auf der Applikationsebene zu einem gewissen Grad erwünscht sein. Dies liegt insb. an der Tatsache, dass dezentrale Applikationen einem kürzeren Produktentwicklungszyklus als dezentrale Netzwerke unterliegen, weswegen sie regelmässig aktualisiert werden müssen. Hinzukommen Programmierfehler, welche die Entwickler zu beheben haben, damit eine Applikation nicht Opfer von Hackerangriffen wird. Angesichts bestehender Rechtsunsicherheiten im Zusammenhang mit DeFi wäre allerdings zu erwarten, dass Entwickler dennoch dazu tendieren, möglichst auf Admin Keys zu verzichten.¹⁶⁷⁶ Gleichermassen müssen Nutzer sich bewusst sein, dass die Existenz von Admin Keys eine dezentrale Handelsplattform unter das Damoklesschwert behördlicher Eingriffe stellen kann.¹⁶⁷⁷

iii. Wash Trading über dezentrale Handelsplattformen

Die mit Frontrunning auf dezentralen Handelsplattformen verbundenen Risiken wurden bereits erwähnt.¹⁶⁷⁸ Frontrunning stellt nach vorliegender Auffassung allerdings in erster Linie ein Transparenzrisiko und erst in zweiter Linie ein Informationsrisiko für die Marktteilnehmer dar.

¹⁶⁷⁵ Vgl. Uniswap, Introducing Sybil, *passim* («Community ownership reduces single points of failure and as protocols begin to develop into products that resemble legacy services – albeit in a structurally decentralized fashion – they naturally require good management. The ability for token holders to delegate their votes, or to stand as a delegate themselves, is key to the success of on-chain governance systems, allowing for high quality community members to build meaningful influence and otherwise-marginalized token holders to engage in a representative fashion. We believe that the most successful protocols will be the ones that are able to attract the best talent and the most engaged communities.»).

¹⁶⁷⁶ Vgl. den Kommentar zum Bank Secrecy Act (BSA) in den USA bei Cochran, Twitter, *passim* («[...] DAO or no DAO you can find that developers with admin keys, users who create front-ends, companies hiring individuals to work on the protocol and others who enable or profit from the contract, to be in violation on the BSA.»).

¹⁶⁷⁷ Siehe hierzu unten, [VII.4.2a.iv.](#)

¹⁶⁷⁸ Siehe oben, [IV.5.2c.iii.](#)

Neben dem Ausnützen von Insiderinformationen sind traditionelle Finanzmärkte¹⁶⁷⁹ und zentrale Kryptohandelsplattformen¹⁶⁸⁰ insb. auch anfällig für Marktmanipulation. Eine besonders verbreitete Methode der Marktmanipulation ist die Durchführung von *Wash Trades* durch den Plattformbetreiber bzw. deren Mitarbeiter oder eine Drittperson, welche solche Transaktionen in aller Regel im Auftrag des Betreibers durchführt.¹⁶⁸¹ Wash Trading kann andererseits auch durch gewöhnliche Marktakteure erfolgen, die bspw. aufgrund der von einer Handelsplattform gesetzten finanziellen Anreizen grössere Volumen mit sich selbst handeln.¹⁶⁸²

Wash Trades fingieren Angebot und Nachfrage und somit eine erhöhte Liquidität in Handelspaaren, die in Tat und Wahrheit nicht existiert. Dies wird auch als *Painting the Tape* bezeichnet.¹⁶⁸³ Eine Präsentation von Bitwise Asset Management gegenüber der SEC vom März 2019 erwähnt, dass rund 95% der ausgewiesenen Handelsvolumen zentraler Kryptohandelsplattformen nicht echt seien.¹⁶⁸⁴ Schätzungen mithilfe statistischer Methoden gehen von fingierten Handelsvolumen von durchschnittlich über 70% für die zweite Jahreshälfte von 2019 aus, wobei das Ausmass von Wash Trades je nach Plattform sehr unterschiedlich hoch ausfällt.¹⁶⁸⁵ Messari unterscheidet laufend ebenfalls zwischen echten und fingierten Volumen, kommt allerdings zu deutlich geringeren Abweichungen als die vorgenannten Studien.¹⁶⁸⁶

Die Tatsache, dass Verkauf und Kauf von Kryptovermögenswerten über eine dezentrale Handelsplattform mit Transaktionsgebühren, welche an die Netzwerkteilnehmer einer Blockchain fließen, verbunden sind, macht Wash Trading-Strategien über dezentrale Handelsplattformen grundsätzlich kostspieli-

¹⁶⁷⁹ Siehe zu den Verhaltensweisen «painting the tape», «wash sales» und «improper matched orders» IOSCO, Investigating and Prosecuting Market Manipulation, 5; sodann FINMA-RS 13/8 «Marktverhaltensregeln», Rz. 22–24.

¹⁶⁸⁰ Siehe etwa hinsichtlich der Verwendung von Bots auf Mt. Gox Gandal et al., *Journal of Monetary Economics* 2018, 89.

¹⁶⁸¹ Siehe für Beispiele aus der Praxis CFTC, Order Coinbase Inc., 2 («[...] between August and September 2016, a former Coinbase employee [‘Employee A’] intentionally placed buy and sell orders in the Litecoin/Bitcoin trading pair on GDAX, which he intended to match with one another and result in no loss or gain while creating the appearance of liquidity and trading interest in Litecoin. Ultimately, the transactions resulted in wash transactions that depicted a misleading picture of the Litecoin/Bitcoin market.»), 3–4; ferner Ontario Securities Commission, Statement of Allegations in the Matter of Coinsquare Ltd. et al., 3–5.

¹⁶⁸² Siehe Singer, *Crypto Exchange Wash Trading*, Cointelegraph, *passim*.

¹⁶⁸³ Siehe IOSCO, Investigating and Prosecuting Market Manipulation, 5 FN 5.

¹⁶⁸⁴ Siehe Bitwise Asset Management, Presentation, 23.

¹⁶⁸⁵ Siehe Cong et al., *Crypto Wash Trading*, 2.

¹⁶⁸⁶ Siehe die Daten in Messari, *Crypto Exchange Real Spot Volume*, *passim*.

ger als Wash Trades auf zentralen Handelsplattformen. Dies trifft noch mehr zu, wenn das Orderbuch on-chain vom dezentralen Netzwerk geführt wird. Wash Trading ist unter Inkaufnahme der Transaktionsgebühren allerdings auch auf dezentralen Handelsplattformen möglich,¹⁶⁸⁷ jedoch gehen erste Untersuchungen von deutlich tieferen fingierten Handelsvolumen aus.¹⁶⁸⁸ Ob demgegenüber Wash Trading über dezentrale Handelsplattformen nach dem AMM-Modell überhaupt möglich ist, ist eine bisher ungeklärte Frage.

iv. Vertrauen in Benutzeroberflächen

Nutzer können mit den Smart Contracts einer dezentralen Handelsplattform grundsätzlich direkt interagieren, ohne dass sie eine von Dritten zur Verfügung gestellte Schnittstelle zu verwenden haben.¹⁶⁸⁹ Mit einer solchen Nutzung sind allerdings hohe technische Anforderungen verbunden. Aus diesem Grund bieten fast alle Projekte bedienungsfreundliche Benutzeroberflächen (GUIs) an.

Nutzer haben allerdings den Betreibern einer GUI – i.d.R. einer Webseite – zu vertrauen, dass sie tut, was sie vorgibt, zu tun. Denn webbasierte Frontends von Plattformen, wie mehrere Vorfälle im Zusammenhang mit EtherDelta in der Vergangenheit gezeigt haben,¹⁶⁹⁰ können durchaus potenzielles Opfer von Hacks sein.

e. Smart Contract- und Plattformrisiken

i. Programmierfehler

Da Menschen unvollkommen sind und Software aufgrund der Komplexität inhärent fehleranfällig ist, sind Programmierfehler eine ständige Begleiterscheinung.

¹⁶⁸⁷ Siehe etwa in Bezug auf *Binance DEX* und *Loopring* Shevchenko, Wash Trading on Decentralized Exchanges, Cointelegraph, *passim*.

¹⁶⁸⁸ Siehe hinsichtlich einer Untersuchung betreffend *EtherDelta* und *IDEX Victor*/Weintraud, in: Leskovec/Grobnik/Najork, Wash Trading on Decentralized Exchanges, 31.

¹⁶⁸⁹ Vgl. auch oben, [IV.2.3](#).

¹⁶⁹⁰ Siehe hinsichtlich der beiden Hackerangriffe im Herbst und Winter 2017, welche einerseits Schadcode im Frontend von *EtherDelta* platzierten und andererseits Nutzer auf eine nachgeahmte Webseite umleiten konnten, wodurch in beiden Fällen die Private Keys der Nutzer den Hackern offenbart wurden, Montoya, Classic code injection, Hackernoon, *passim*; sodann Roberts, Security in Decentralized Exchanges, *passim*.

nung der Softwareentwicklung.¹⁶⁹¹ Programmierfehler können unterschiedliche Ursachen aufweisen und in unterschiedlichen Formen auftreten. In aller Regel wird von einem *Programmierfehler* gesprochen, wenn eine Softwareoperation vom intendierten Resultat abweicht.¹⁶⁹² So gelten auch konzeptionelle oder Designschwächen als Programmierfehler, obschon der Code genau das tut, was er nach Plan des Entwicklers tun soll, dennoch aber unbeabsichtigte und in aller Regel unerwünschte Ergebnisse produziert. In DeFi stellen etwa fehlerhafte ökonomische Modelle einen solchen konzeptionellen Fehler dar.¹⁶⁹³

Programmierfehler können sowohl den Softwarecode eines dezentralen Netzwerks als auch denjenigen dezentraler Applikationen betreffen. Programmierfehler auf der Netzwerkebene stellen aufgrund des Umstandes, dass sie in aller Regel viele Netzwerkteilnehmer gleichzeitig betreffen, ein *Plattformrisiko* dar.¹⁶⁹⁴ Aus diesem Grund unterliegt der Computercode von Netzwerkprotokollen im Gegensatz zu dezentralen Applikationen in aller Regel einer deutlich umfassenderen und langwierigeren Überprüfung durch eine Vielzahl von Entwicklern. Protokollupdates in Bitcoin und Ethereum nehmen in aller Regel zwischen mehreren Monaten und mehreren Jahren in Anspruch.

Die in vielen DeFi-Anwendungen eingesetzten Smart Contracts sind ebenfalls Computerprogramme und deshalb inhärent anfällig für Programmierfehler. «Algorithm incompleteness» beschreibt die praktischen Schwierigkeiten, bereits im Zeitpunkt der Erstausführung alle Eventualsituationen codemässig abdecken zu können.¹⁶⁹⁵ Softwaresicherheit gehört damit zu den wichtigsten Elementen, die es bei der Programmierung von Smart Contract-Code zu beachten gilt.¹⁶⁹⁶ Das Besondere an Smart Contracts ist die öffentliche Natur ihres Computercodes. Jeder Fehler kann zwar von einem interessierten Entwickler entdeckt, aber eben auch von einem Hacker mit Gewinnabsicht ausgenutzt werden.¹⁶⁹⁷ Zudem können Smart Contracts in DeFi regelmässig

¹⁶⁹¹ Siehe Le Goues/Forrest/Weimer, Proceedings of the FSE/SDP workshop on Future of software engineering research 2010, 205–206, die Software als ein «evolving complex system» betrachten.

¹⁶⁹² Siehe etwa Dowd/McDonald/Schuh, Software Security Assessment, 4.

¹⁶⁹³ Vgl. Harvey/Ramachandran/Santoro, DeFi, 132.

¹⁶⁹⁴ Vgl. hinsichtlich Bitcoin Walch, New York University Journal of Legislation & Public Policy 2015, 858, 860; allgemein Buckley/Arner/Zetzsche, FinTech, 122–123.

¹⁶⁹⁵ Siehe BIS, Crypto Ecosystem, 9.

¹⁶⁹⁶ So Antonopoulos/Wood, Mastering Ethereum, 171, ferner 161.

¹⁶⁹⁷ Siehe Harvey/Ramachandran/Santoro, DeFi, 131.

Kryptovermögenswerte für die Nutzer halten, sodass jede Schwachstelle potenziell mit hohen finanziellen Kosten verbunden ist.¹⁶⁹⁸ Dies gilt auch für gewisse Kategorien dezentraler Handelsplattformen.¹⁶⁹⁹

Programmierfehler können unterschiedliche Folgen zeitigen: Einerseits ist denkbar, dass ein Programmierfehler dazu führt, dass ein Smart Contract fehlerhaften Code beinhaltet, ohne aber für Dritte verwertbar zu sein. Der Parity Multisig-Hack Nr. 2, der technisch gesehen gar kein Hackerangriff ist, gehört zu dieser Kategorie. Bis heute befinden sich in den entsprechenden Multisig-Smart Contracts über 500'000 ETH, über welche aufgrund eines Programmierfehlers niemand mehr verfügen kann.¹⁷⁰⁰ Andererseits kann ein Fehler im Code Opfer eines Hacks werden.

ii. Hacking von Smart Contracts

Eine Vielzahl der auf Ethereum abgelegten Smart Contracts weisen gemäss wissenschaftlichen Untersuchungen eine Reihe von Schwachstellen auf.¹⁷⁰¹ Hacking von Smart Contracts ist in der Folge zu einem lukrativen Geschäft geworden.¹⁷⁰²

Der Smart Contract-Fehler im Parity Multisig-Hack Nr. 1 erlaubte es dem Hacker etwa, die in den unterschiedlichen Multisig-Wallets angeblich sicher verwahrten Kryptovermögenswerte für sich in Anspruch zu nehmen. Dies führte zur Entwendung von über 150'000 ETH. Betroffen waren u.a. mehrere ICO-Unternehmen, welche zum damaligen Zeitpunkt Parity als Multisig-Wallet für

¹⁶⁹⁸ Siehe Antonopoulos/Wood, *Mastering Ethereum*, 161, 171–172; ferner WEF, *Decentralized Finance*, 15; Amler et al., *DeFi-ning DeFi*, 5, die darum von einer «public bug bounty» sprechen.

¹⁶⁹⁹ Siehe Harvey/Ramachandran/Santoro, *DeFi*, 143.

¹⁷⁰⁰ Siehe Parity, *Parity Multi-Sig Library Self-Destruct*, *passim*; ausführlich Akentiev, *Parity Multisig Hacked*, Medium, *passim*. Eine Liste der betroffenen Smart Contract-Adressen kann hier gefunden werden: <https://etherscan.io/accounts/label/parity-bug>.

¹⁷⁰¹ Siehe etwa Nikolić et al., 2018 Annual Computer Security Applications Conference (ACSAC '18) 2018, insb. 654–655, die drei unterschiedliche Schwachstellen unterscheiden («[...] we flag contracts which (a) release Ether to arbitrary addresses carelessly, (b) can be killed by arbitrary addresses, and (c) have no way to release Ether after a certain execution state.»); ferner die Beispiele bei Atzei/Bartoletti/Cimoli, in: Maffei/Ryan, *Survey of Attacks*, 169–175; Werner et al., *Decentralized Finance*, 6–7; ausführlich sodann Antonopoulos/Wood, *Mastering Ethereum*, 172–220.

¹⁷⁰² Vgl. die laufend aktualisierte Übersicht von Smart Contract-Hacks auf der Ethereum Blockchain in Arias, *List of Ethereum Smart Contracts Post-Mortems*, *passim*; ferner Avanzo, *DeFi hacks and exploits*, Cointelegraph, *passim*.

die ICO-Erlöse verwendet haben.¹⁷⁰³ Um die Kryptovermögenswerte vor dem Zugriff der «Black Hat Hacker» zu bewahren, wurden nach Entdeckung des Hacks «White Hat Hacker» aktiv. Sie nutzten denselben Softwarefehler aus, um die Kryptovermögenswerte auf ein sicheres Wallet zu übertragen, von wo aus es an die berechtigten Personen zurücküberwiesen wurde. So konnten rund 377'000 ETH und unzählige andere Token gerettet werden.¹⁷⁰⁴

Der wohl berühmteste Smart Contract-Hackerangriff in der noch jungen Geschichte von Blockchains ist die «The DAO»-Attacke vom 17. Juni 2016. Aufgrund eines Programmierfehlers konnte ein Angreifer rund 3.6 Millionen ETH aus den verwendeten Smart Contracts abziehen.¹⁷⁰⁵ Gleichzeitig nutzten White Hat Hacker denselben Softwarebug aus, um die noch nicht abgeschöpften Vermögenswerte sicherzustellen. Es bestanden keine ausreichenden Admin Keys, welche es dem Projektteam erlaubt hätten, eigenständig auf den Angriff zu reagieren. Die The DAO-Attacke führte in der Folge zur bisher grössten Governance-Krise in Ethereum. Dank einer Wartefunktion von 28 Tagen in der Mechanik der Smart Contracts war es der Ethereum Community möglich, unterschiedliche Abwehrmassnahmen zu erarbeiten, bevor der Angreifer die Vermögenswerte auf sein privates Wallet abziehen konnte. Die Gemeinschaft «einigte» sich schliesslich auf eine kontroverse Hard Fork des Netzwerks: In Ethereum wurde die Attacke vollständig rückgängig gemacht, währenddessen das Prinzip der Unveränderlichkeit von Blockchains in der bisherigen Version *Ethereum Classic* hochgehalten wurde.¹⁷⁰⁶

Wie die Diskussionen anlässlich der The DAO-Attacke gezeigt haben, kann sich eine Schere hinsichtlich der Meinungen auftun, was unter einem Softwarefehler zu verstehen ist.¹⁷⁰⁷ Im Falle der eingesetzten Smart Contracts waren scheinbar bereits die mit ihnen verbundenen Intentionen der Entwickler nicht restlos klar.¹⁷⁰⁸ In diesem Sinne war die Aussage des The DAO-Hackers, dass er lediglich den Code, so wie er im Smart Contract programmiert wurde, ausgeführt hatte, nicht völlig unbegründet.¹⁷⁰⁹ Letztlich sah eine überwiegende

¹⁷⁰³ Ausführlich Breidenbach et al., Parity Multisig Bug, *passim*.

¹⁷⁰⁴ Siehe White Hat Group, Vulnerability, Reddit, *passim*.

¹⁷⁰⁵ Vgl. für eine gute Übersicht über die Attacke Leising, Out of the Ether, Kapitel 11; für eine technische Analyse des Hacks vgl. Daian, Analysis of the DAO exploit, *passim*.

¹⁷⁰⁶ Ausführlich Antonopoulos/Wood, Mastering Ethereum, 325–329.

¹⁷⁰⁷ Vgl. in diesem Zusammenhang auch Dowd/McDonald/Schuh, Software Security Assessment, 5.

¹⁷⁰⁸ Ähnlich Gün Sirer, Thoughts on the DAO Attack, *passim*.

¹⁷⁰⁹ Siehe The Attacker, An Open Letter, *passim* («I am disappointed by those who are characterizing the use of this intentional feature as 'theft'. I am making use of this explicitly coded

Mehrheit der Ethereum Community dies aber anders: Sie erachtete die DAO-Attacke wohl als einen Verstoß gegen implizite soziale Normen der Community, weshalb sie in der Folge konsequenterweise eine Hard Fork der Blockchain in zwei inkompatible Versionen in Kauf nahm.¹⁷¹⁰

Ein besonderer Fall von Smart Contract-Risiken sind manipulierte Orakel-Protokolle.¹⁷¹¹ Eine Vielzahl von DeFi-Protokollen ist auf die von Orakel zur Verfügung gestellten Daten angewiesen. Die von manipulierten Orakel falsch eingespeisten Daten können bspw. zu ungerechtfertigten Liquidationsketten von Sicherheiten in dezentralen Kreditprotokollen führen oder einem Angreifer die Möglichkeit zur Preisausnutzung eröffnen (z.B. durch Manipulation des Preises des Basiswerts eines Derivats).¹⁷¹² Die Infragestellung der Datenintegrität durch die Marktteilnehmer könnte in Extremfällen zu einem systemweiten Vertrauensverlust führen.

DeFi-Applikationen befinden sich noch in einem frühen Stadium, sodass Hacks mit gewisser Wahrscheinlichkeit weiterhin eine regelmässige Begleiterscheinung der Branche bleiben werden. Smart Contract-Risiken stehen darum in einem Spannungsverhältnis zu Informationsrisiken, namentlich im Zusammenhang mit Admin Keys. Allerdings ist es wahrscheinlich, dass mit zunehmender Standardisierung der Programmierung und des Audits von Smart Contracts deren Sicherheit zunimmt und im Resultat weniger Angriffsvektoren übrigbleiben.¹⁷¹³

iii. Re-Zentralisierung von Mining und Staking

Die wohl in der Literatur meistdiskutiertesten Plattformrisiken in dezentralen Netzwerken sind Re-Zentralisierungsrisiken, namentlich durch kartellierende Verhaltensweisen von Minern bzw. Mining Pools.¹⁷¹⁴ Diese Risiken sind vorliegend von Relevanz, da der Vertrauensverlust in ein dezentrales Netzwerk sich auch unmittelbar negativ auf die darauf basierenden dezentralen Applikationen inkl. dezentralen Handelsplattformen auswirken würde.

feature as per the smart contract terms [...] A soft or hard fork would amount to seizure of my legitimate and rightful ether, claimed legally through the terms of a smart contract.»).

¹⁷¹⁰ Siehe Antonopoulos/Wood, Mastering Ethereum, 325.

¹⁷¹¹ Vgl. Werner et al., Decentralized Finance, 11, die zwischen manipulierten Daten, die von einem korrekt funktionierenden Orakel verarbeitet werden, und einem manipulierten Orakel unterscheiden.

¹⁷¹² Siehe Carter/Jeng, in: Coen/Maurice, DeFi Protocol Risks, 23–24.

¹⁷¹³ So etwa Werner et al., Decentralized Finance, 12–13; ähnlich wohl auch Harvey/Ramachandran/Santoro, DeFi, 135.

¹⁷¹⁴ Siehe statt vieler Gervais et al., IEEE Security & Privacy 2014, passim.

Das Bitcoin Whitepaper geht davon aus, dass die Dezentralität des Netzwerks gewährleistet ist, wenn eine Mehrheit der Netzwerkteilnehmer «ehrlich» ist.¹⁷¹⁵ Allerdings steht nicht Ehrlichkeit im sozioökonomischen Sinne im Vordergrund, sondern eigennutzenorientiertes Verhalten.¹⁷¹⁶ Kryptoökonomisch ist von der *Anreizkompatibilität* des Protokolls die Rede. Die Annahme geht dahin, dass Sicherheit und Stabilität des Netzwerks so lange gewährleistet sind, als dass Netzwerkteilnehmer die im Protokoll festgelegten Regeln einhalten.¹⁷¹⁷ Die Einhaltung dieser Regeln wird durch die vom Protokoll gesetzten ökonomischen Anreize sichergestellt.¹⁷¹⁸ Es ist darum zu erwarten, dass ein *rationaler* Miner mindestens so lange im Interesse des Netzwerks handelt, als dass die dabei zu verdienenden Vergütungen höher als die aus einer einmaligen Attacke zu realisierenden Gewinne (insb. durch Double Spending) abzüglich der expliziten¹⁷¹⁹ und impliziten Kosten einer solchen Attacke ausfallen.¹⁷²⁰

Theoretische Untersuchungen hinsichtlich der Anreizkompatibilität des Bitcoin Protokolls modellieren, wie das Netzwerk von kolludierenden Netzwerkteilnehmern (i.d.R. Minern) übernommen und für ihre Zwecke missbraucht werden könnte. Umgangssprachlich ist von der 51%-Attacke die Rede, wobei argumentiert wird, dass die Bezeichnung darüber hinwegtäuscht, dass es in manchen Fällen für einen erfolgreichen Angriff geringerer Rechenkapazitäten bedarf.¹⁷²¹ In kleineren Blockchains mit konzentriertem Mining kommt es tendenziell eher zu solchen Attacken.¹⁷²² Ethereum Classic (ETC) war Opfer einer

¹⁷¹⁵ Siehe Nakamoto, Bitcoin, 1 («The system is secure as long as honest nodes collectively control more CPU power than any cooperating group of attacker nodes.»), 3, 4.

¹⁷¹⁶ Vgl. Narayanan et al., Bitcoin, 43.

¹⁷¹⁷ Siehe Eyal/Gün Sirer, in: Christin/Safavi-Naini, Bitcoin Mining, 436–437; Bonneau et al., Proceedings 2015 IEEE Symposium on Security and Privacy, 104, 110.

¹⁷¹⁸ Siehe Werner et al., Decentralized Finance, 9; Antonopoulos, Mastering Bitcoin, 229.

¹⁷¹⁹ Siehe zu den theoretischen expliziten Kosten einer solchen Attacke, Crypto51, PoW 51% Attack Cost, *passim*.

¹⁷²⁰ So auch Rosenfeld, Analysis of hashrate-based double-spending, 11 («[...] this attack is best seen as an attempt to destroy Bitcoin, motivated not by the desire to obtain Bitcoin value, but rather wishing to maintain entrenched economical systems or obtain speculative profits from holding a short position.»).

¹⁷²¹ Siehe Antonopoulos, Mastering Bitcoin, 272–273; Eyal/Gün Sirer, in: Christin/Safavi-Naini, Bitcoin Mining, 438, die von einem Drittel (33.3%) als kritische Grösse für Mining Pools ausgehen, wenn diese vorübergehend die Publikation von gültigen Blöcken zurückhalten, bis sie eine längere alternative Blockchain berechnet haben (*Selfish-Mining*-Attacke); ferner Jang/Lee, Applied Sciences 2020, Nr. 10, 2–3; *demgegenüber* von einer grundsätzlich stabilitätsfördernden ökonomischen Anreizstruktur für Bitcoin ausgehend Badertscher et al., in: Nielsen/Rijmen, Rational Protocol Design Treatment of Bitcoin, *passim*.

¹⁷²² Siehe etwa die Übersicht bei Attah, Five most prolific 51% attacks in crypto, Cryptoslate, *passim*.

solchen Attacke Anfang 2019, die es dem Angreifer erlaubte, die Blockchain über mehrere Blöcke hinweg zu reorganisieren. In diesem Rahmen konnte der Angreifer, indem er mehrfach dieselben ETC-Einheiten ausgab, sich auf Kosten seiner Gegenparteien bereichern.¹⁷²³ Die Konzentration des Minings (oder Stakings) in den Händen einiger weniger Marktteilnehmer ist auch darum ein Problem, da eine kleinere Gruppe eher imstande ist, Angriffe gegen ein Netzwerk zu koordinieren. Der Umstand, dass die Identitäten dieser grossen Player in den meisten Fällen öffentlich bekannt sind, ist darum bei Lichte betrachtet eher ein Nachteil.

Überschreitungen der Mehrheitsgrenze gab es in der Vergangenheit auch in Bitcoin: Nachdem der Mining Pool GHash.IO im Sommer 2014 über 50% der Rechenkapazitäten des Bitcoin Netzwerks erreichte, reduzierten die ihm angeschlossenen Miner aus freien Stücken die bereitgestellte Rechenkapazitäten. Eine 51%-Attacke auf Bitcoin erfolgte nicht.¹⁷²⁴ Daraufhin veröffentlichte der Mining Pool eine Stellungnahme, wonach eine öffentliche Debatte über einschränkende Massnahmen gegen künftige Machtkonzentrationen in der Bitcoin Community zu führen sei.¹⁷²⁵ Anschliessend auferlegte sich GHash.IO eine maximale Quote der netzwerkweiten Rechenkapazitäten von unter 40%.¹⁷²⁶ Eine vergleichbare Situation existierte in Bitcoin Cash Anfang 2019.¹⁷²⁷ In beiden dezentralen Systemen scheinen sich die Mining Pools trotz weiterhin ausgeprägter Konzentration an diese selbst auferlegten Regeln zu halten.

Theoretische Untersuchungen ignorieren in aller Regel die spieltheoretische Dimension einer 51%-Attacke. Diese ist nach vorliegender Auffassung als nicht wiederholbares Endspiel für kolludierende Angreifer zu betrachten: Bereits eine zeitlich befristete Zentralisierung von Kontrolle und Macht über ein dezentrales Netzwerk setzt nicht nur die Werthaltigkeit der betreffenden Kryptowährung aufs Spiel, sondern insb. auch die mit dem Mining verbundenen Investitionen in spezialisierte Hardware.¹⁷²⁸ Es droht zudem, dass Nutzer sich bereits im Verlauf des kontinuierlichen Aufbaus einer solchen Machtkonzentration von ihren Ver-

¹⁷²³ Siehe etwa Nesbitt, Deep Chain Reorganization, *passim*; sodann Carter/Jeng, in: Coen/Maurice, DeFi Protocol Risks, 16.

¹⁷²⁴ Siehe Rizzo, Ghash.io, *passim*.

¹⁷²⁵ Siehe Kerya, GHash.IO open for discussion, *passim* («We also recognise however that a long term preventative solution to the threat of a 51% attack does have to be found, the current situation we find ourselves in [essentially being punished for our success] is damaging not only to us, but to the growth and acceptance of Bitcoin long term, which is something we are all striving for.»).

¹⁷²⁶ Siehe Wilhelm, Popular Bitcoin Mining Pool, TechCrunch, *passim*.

¹⁷²⁷ Siehe Gola, Single Mining Pool Controls 50%, CCN, *passim*.

¹⁷²⁸ Siehe Carter/Jeng, in: Coen/Maurice, DeFi Protocol Risks, 16–17.

mögenswerten trennen könnten, was den Preis der Kryptowährung unter Druck setzt und eine Attacke ökonomisch nochmals unsinniger macht.¹⁷²⁹ Grosse Mining Pools und Miner werden aus diesen Gründen, wie im Falle von GHash.IO geschehen, bereits zu vermeiden versuchen, dass der Anschein entsteht, dass sie tatsächlich eine 51%-Attacke erfolgreich ausüben könnten. In diesem Sinne kann nicht davon gesprochen werden, dass die Netzwerkteilnehmer den Minern zu vertrauen haben, dass sie von Angriffen absehen.¹⁷³⁰

Selbst wenn eine Attacke auf Bitcoin oder Ethereum erfolgreich ausgeführt wird, was mit sehr grosser Wahrscheinlichkeit zu einem starken Preiserückgang der jeweiligen Kryptowährung führen würde, ist an dieser Stelle zu ergänzen, dass ein Angreifer ein dezentrales Netzwerk nicht nach Belieben kontrollieren kann: Ein Angreifer kann einerseits lediglich seine eigenen Kryptovermögenswerte mehrfach ausgeben, indem er die Blöcke samt seiner Transaktionen im verteilten Register reorganisiert (Double Spending). Der Angreifer kann demgegenüber nicht auf die Private Keys und somit die Kryptovermögenswerte anderer Nutzer zugreifen. Er kann auch nicht neue Einheiten der betreffenden Kryptowährung *ex nihilo* erschaffen.¹⁷³¹ Andererseits kann ein Angreifer mit über 50% aller Rechenkapazitäten die Blöcke anderer Miner und Transaktionen von Nutzern zurückweisen.¹⁷³² Aufgrund der mangelhaften Zensurresistenz wäre die Dezentralität des angegriffenen Netzwerks nachhaltig infrage gestellt. Ein allgemeiner Vertrauensverlust des Marktes wäre mit hoher Wahrscheinlichkeit die Folge.

Allerdings muss ein Angreifer mit einer Reaktion der Community rechnen, welche bspw. in einem Protokollupdate bestehen kann, das den Mining-Algorithmus ändert und somit den Angreifer *de facto* ausschliesst.¹⁷³³ Diese Au-

¹⁷²⁹ Siehe Felten, Bitcoin Mining Now Dominated by One Pool, *passim*; Narayanan et al., Bitcoin, 49; Kroll/Davey/Felten, Economics of Bitcoin Mining, 11–13; ferner bereits Nakamoto, Bitcoin, 4; kritisch Walch, New York University Journal of Legislation & Public Policy 2015, 862–863, welche auf die sog. *Goldfinger Attack* durch Staaten oder andere finanziell einflussreiche Marktakteure hinweist.

¹⁷³⁰ So aber Courtois/Bahack, Subversive Miner Strategies, 12.

¹⁷³¹ Siehe Antonopoulos, Mastering Bitcoin, 271; Narayanan et al., Bitcoin, 48–49; Berentsen/Schär, Bitcoin, 233–235.

¹⁷³² Siehe Bonneau et al., Proceedings 2015 IEEE Symposium on Security and Privacy, 110; Eyal/Gün Sirer, How A Mining Monopoly Can Attack Bitcoin, *passim*; Rosenfeld, Analysis of hashrate-based double-spending, 10–11; Kroll/Davey/Felten, Economics of Bitcoin Mining, 11–12.

¹⁷³³ So Antonopoulos, Mastering Bitcoin, 273; Narayanan et al., Bitcoin, 49; ferner Eyal/Gün Sirer, It's Time For a Hard Bitcoin Fork, *passim*, welche eine Bitcoin-Hard Fork vorschlagen, um Mining Pools zu verunmöglichen.

tonomie des Netzwerks gegenüber Minern ist darauf zurückzuführen, dass dezentrale Governance etwa in Bitcoin letztlich von einer Mehrzahl von Personen unterhalten wird. Jeder Netzwerkteilnehmer, unabhängig davon, ob er selbst ein Miner ist oder nicht, entscheidet autonom darüber, welchen Konsensregeln er folgen will.¹⁷³⁴ Ist eine genügend grosse Zahl von Netzwerkteilnehmern der Meinung, eine Hard Fork ist die einzige Option, um einen 51%-Angreifer abzuwehren, so können sie dies durch ein entsprechendes Update der Konsensregeln tun.

iv. Kollusion von Softwareentwicklern

Bei der oben angesprochenen Kollusionsgefahr von Minern (und freilich auch Stakern) handelt es sich um eine generelle Herausforderung sozialer Institutionen im Allgemeinen und dezentraler Systeme im Besonderen.¹⁷³⁵ Die Literatur untersucht darum ferner die Bedeutung der Rolle von *Softwareentwicklern*.¹⁷³⁶

Zwar zeigt das Beispiel der Bitcoin Blockchain, dass Nakamoto in den ersten Jahren mit grossem Gestaltungsspielraum agieren konnte und die Community ihm im Wesentlichen vertraute. Allerdings wurde bereits in Diskussionen vom November 2011 gefordert, dass auch die Entwicklung des Bitcoin Protokolls auf mehrere Köpfe zu verteilen sei.¹⁷³⁷ Neben der von Nakamoto begonnen Referenzimplementierung des Protokolls, Bitcoin Core, existierten über die Jahre mehrere Alternativen.¹⁷³⁸ Es arbeiteten mit anderen Worten unterschiedliche

¹⁷³⁴ Siehe oben, [III.2.2.](#)

¹⁷³⁵ Vgl. Buterin, On Collusion, *passim*.

¹⁷³⁶ So etwa bereits Laurie, Decentralised Currencies Probably Impossible, 3; Grinberg, Hastings Science & Technology Law Journal 2012, 175–176, der von «exercise discretionary authority» spricht; Martin Christopher, Nevada Law Journal 2015, 139–180, 150, welche fälschlicherweise davon spricht, dass Entwickler kleine Änderungen selbständig durchführen können; De Filippi/Loveluck, Internet Policy Review 2016, 16, die von einem «technocratic approach» sprechen; Bonneau et al., Proceedings 2015 IEEE Symposium on Security and Privacy, 109, welche die Situation als «de facto governance» bezeichnen; ferner Abramowicz, Arizona Law Review 2016, 369–370; Zetzsche/Buckley/Arner, University of Illinois Law Review 2018, 1384, und Kroll/Davey/Felten, Economics of Bitcoin Mining, 18; sehr kritisch Walch, New York University Journal of Legislation & Public Policy 2015, 870, welche in der Art und Weise, wie Software in Bitcoin entwickelt wird, eine «systemic operational risk» zu erkennen meint; offenbar *vermittelnd* Bayern, Northwestern University Law Review Online 2014, 262–263.

¹⁷³⁷ Ausführlich aufgearbeitet wurde diese Periode in Rizzo, The Last Days of Satoshi, Bitcoin Magazine, *passim*.

¹⁷³⁸ Vgl. für eine Übersicht Antonopoulos, Mastering Bitcoin, 31, 52–53.

Teams an der Weiterentwicklung von Bitcoin. Seit der Hard Fork in Bitcoin und Bitcoin Cash ist allerdings Bitcoin Core die mit Abstand verbreitetste Implementierung in Bitcoin.

Wie Erfahrungen aus der Praxis zeigen, ist die Funktion von Softwareentwicklern zentral für die langfristige Funktionsfähigkeit des Netzwerks. Entwickler verfügen in technischer Hinsicht typischerweise über einen immensen Informationsvorsprung gegenüber den übrigen Angehörigen des Ökosystems.¹⁷³⁹ Die Legitimität eines Entwicklers innerhalb der Community mag ausserdem einen gewissen Einfluss auf die Mitglieder mit der Wirkung eines Nudge¹⁷⁴⁰ haben.¹⁷⁴¹ Ein gutes Beispiel dafür ist die Rolle von Buterin und anderer wichtiger Entwickler der Ethereum Foundation im Nachgang zur The DAO-Attacke, deren Empfehlung einer Hard Fork schlussendlich die überwiegende Zustimmung in der Community fand.¹⁷⁴²

Die Befürchtung, dass die gesellschaftliche Bedeutung von Software zu einer Machtballung in den Händen von Entwicklern (und Hackern) führen könne, ist deutlich älter als die Erfindung der Blockchain.¹⁷⁴³ Trotz ihrer zentralen Rolle ist der effektive Grad an Autorität und Kontrolle durch die Entwicklergemeinschaft, geschweige denn ein einzelnes Mitglied, letztlich sehr gering.¹⁷⁴⁴

Es sei daran erinnert, dass die Netzwerkteilnehmer ein von der Entwicklergemeinschaft vorgeschlagenes Protokollupdate nicht akzeptieren müssen.¹⁷⁴⁵ Dezentrale Governance in Bitcoin (und auch in Ethereum) bedeutet, dass jeder einzelne Netzwerkteilnehmer autonom darüber entscheidet, ob ein vorge-

¹⁷³⁹ Siehe Szabo, Social scalability, *passim* («[...] those who are not expert developers or computer scientists who have invested a great deal of time in learning the design principles and codebase of a blockchain must place a great deal of faith in the expert developer community [...]»).

¹⁷⁴⁰ Siehe zum Konzept Thaler/Sunstein, Nudge, 6.

¹⁷⁴¹ Zum Begriff der Legitimität und einigen praktischen Beispielen Buterin, Legitimacy, *passim*.

¹⁷⁴² Siehe auch oben, [II.4.1b.ii](#).

¹⁷⁴³ Vgl. etwa Galloway, Protocol, 121–122, 241–246.

¹⁷⁴⁴ Siehe van Wirdum, A Primer on Bitcoin Governance, Bitcoin Magazine, *passim* («Developers are, therefore, perhaps best understood as tool providers with what could be considered a sort of advisory role. Their influence is limited to offering people software they can use to connect to the Bitcoin network if they want to.»); ferner Haque et al., Stanford Journal of Blockchain Law & Policy 2019, 177–179; a.M. demgegenüber Walch, in: Hacker et al., Software Developers as Fiduciaries, insb. 63–64; ebenso kritisch Finck, Blockchain Regulation, 199–200.

¹⁷⁴⁵ Siehe oben, [II.5.3b.ii](#).

schlagenes Protokollupdate durchzuführen ist.¹⁷⁴⁶ Die subjektive Wahrnehmung von Autorität mag zudem von Community zu Community sehr unterschiedlich ausfallen.

Während nur wenige Personen, die Bitcoin Core entwickeln, Schreibzugriff auf das GitHub-Repository des Softwarecodes besitzen (sog. *Maintainer*),¹⁷⁴⁷ arbeiten heute schätzungsweise über hundert Personen regelmässig an der Weiterentwicklung mit.¹⁷⁴⁸ Einige der Entwickler sind zu diesem Zweck Voll- oder Teilzeit bei Unternehmen oder Universitäten angestellt oder erhalten Fördergelder von gemeinnützigen Organisationen und Projekten, wie etwa die *Human Rights Foundation*¹⁷⁴⁹ sowie *brink* und *OpenSats*.¹⁷⁵⁰ Im gesamten Ökosystem von Bitcoin sind es wohl mehrere zehntausend Personen, die in irgendeiner Form an der Entwicklung des Netzwerks und von dezentralen Applikationen arbeiten. So entwickeln mehrere unterschiedliche Teams etwa das Lightning Netzwerk. Von einem Key-Person-Risiko in Bitcoin kann darum heute keine Rede mehr sein.¹⁷⁵¹ Ähnlich verhält es sich in *Ethereum*, dessen Protokoll mehrere Clients aufweist (insb. Geth und Parity bzw. OpenEthereum),¹⁷⁵² die derzeit wohl von einigen hundert Entwicklern unterhalten werden. Entwicklerfinanzierung erfolgt dabei über unterschiedliche Kanäle, so etwa die Ethereum Foundation, private Unternehmen, wie namentlich ConsenSys, die Community-Plattform Gitcoin oder DAOs, die sich dem Zweck angenommen haben.¹⁷⁵³ Das Ethereum Ökosystem selbst

¹⁷⁴⁶ Ausführlich zu dieser Balance in der dezentralen Governance von Bitcoin Ammous, Bitcoin Standard, 224–225; Narayanan et al., Bitcoin, 171, 173–175.

¹⁷⁴⁷ Vgl. etwa für eine Übersicht des Auswahlprozesses von Maintainers <https://github.com/bitcoin/bitcoin/issues/26751>.

¹⁷⁴⁸ Siehe für eine Übersicht der Entwicklergemeinde Bitcoin Core, Bitcoin Core contributors, *passim*.

¹⁷⁴⁹ Siehe Human Rights Foundation, Bitcoin Development Fund, *passim*.

¹⁷⁵⁰ Vgl. etwa Acheson, How Bitcoin Development Is Evolving, Coindesk, *passim* («In the early days of the Bitcoin network, almost all developer funding came from one source, the Bitcoin Foundation. Since then, other funders have entered the scene, including several companies dedicated to Bitcoin work, such as Blockstream, Chaincode Labs and Lightning Labs. Also involved are well-known crypto businesses such as Square Crypto, Coinbase, OKCoin, BitMEX and others, as well as not-for-profit organizations such as MIT's Digital Currency Initiative and the Human Rights Foundation. In addition, many developers work on Bitcoin for free, out of passion.»)

¹⁷⁵¹ So aber noch Zetzsche/Buckley/Arner, University of Illinois Law Review 2018, 1381–1382; ähnlich Martin Christopher, Nevada Law Journal 2015, 150, wonach gewisse Entwickler «password access to the code» haben.

¹⁷⁵² Vgl. für eine Übersicht verfügbarer Ethereum-Implementierungen Ethereum, Nodes and Clients, *passim*; ferner Antonopoulos/Wood, Mastering Ethereum, 42.

¹⁷⁵³ Siehe für eine unvollständige Übersicht Ethereum, Ethereum Grants, *passim*.

hat nach groben Schätzungen mehrere hunderttausend aktive Entwickler weltweit.¹⁷⁵⁴ Eine Kollusionsgefahr ausgehend von Entwicklern scheint zumindest für grosse dezentrale Systeme nicht relevant zu sein.¹⁷⁵⁵

Nichtsdestotrotz wurde in der Vergangenheit auf dem Rechtsweg gegen Protokollentwickler vorgegangen. Im bisher bedeutendsten Fall behauptet der Kläger vor einem englischen Gericht, dass 110'000 BTC und weitere Coins, deren Private Keys er aufgrund eines angeblichen Hacks verloren habe, von den beklagten Entwicklern aufgrund vermeintlicher Treue- und Sorgfaltspflichten wiederherzustellen seien.¹⁷⁵⁶ Faktisch verlangt der Kläger von den Entwickler, eine Backdoor in die Bitcoin-Software einzubauen, welche es ihnen erlauben würde, arbiträre Transaktionen zugunsten des Klägers auszulösen.

Zum Vergleich: Die Situation stellt sich bei jüngeren Projekten der Applikationsebene und damit auch bei dezentralen Handelsplattformen regelmässig anders dar. Hier ist die Entwicklung und Weiterentwicklung einer *dezentralen Applikation* trotz grundsätzlicher Offenheit des verwendeten Computercodes bis zu einem gewissen Grad von den Beiträgen lokaler und überschaubarer Entwicklergruppen abhängig. Diese Teams arbeiten zudem in den meisten Fällen in traditionellen hierarchischen Strukturen, d.h. typischerweise innerhalb eines Unternehmens. Die damit verbundene höhere Kollusionswahrscheinlichkeit ist insofern weniger dramatisch, als dass von dezentralen Applikationen in aller Regel keine Plattformrisiken ausgehen. Im Rahmen der Diskussion von Dezentralität als Rechtsprinzip wird auf diesen Punkt zurückzukommen sein.¹⁷⁵⁷

f. Neuartige Systemrisiken

i. Composability Risiko

Dezentrale Netzwerke und Applikationen können aufgrund ihrer Offenheit und Interoperabilität in vielfältiger Weise miteinander verknüpft werden (*Composability*). Diese Fähigkeit ist insb. im DeFi-Bereich auf grosses Interesse

¹⁷⁵⁴ Siehe etwa Shen, Electric Capital Developer Report, Medium, *passim*.

¹⁷⁵⁵ Unklar diesbezüglich Schreppel, Harvard Journal of Law & Technology 2019, 139.

¹⁷⁵⁶ Sog. *Tulip Trading Case*, vgl. hierzu <https://bitcoindefense.org/our-work/> m.w.H. und Zugang zu den Prozessakten; zu Recht kritisch Nabilou, Stanford Journal of Blockchain Law & Policy 2021, 32–33, der von einem Corporate Governance-Standpunkt her argumentiert.

¹⁷⁵⁷ Siehe unten, [VII](#).

gestossen. Von der «Legoartigkeit» von Anwendungen und Protokollen in DeFi verspricht man sich bspw. die Erfindung neuartiger Finanzprodukte und Anlagestrategien.¹⁷⁵⁸

Zur Veranschaulichung mag folgendes Beispiel dienen: (1) Ein Nutzer, der über BTC verfügt, kann diese mithilfe des RenVM-Protokolls zu renBTC «umwandeln».¹⁷⁵⁹ (2) renBTC stellt einen ERC 20-Token auf Ethereum dar. Diese synthetische Repräsentation von BTC weist darum alle Funktionalitäten eines gewöhnlichen ERC 20-Token auf. Der Token kann bspw. über den entsprechenden Pool von Uniswap in wBTC getauscht werden kann. (3) Die so erhaltenen wBTC können sodann mithilfe des MakerDAO-Protokolls zur Besicherung eines DAI-Darlehens verwendet werden. (4) Anschliessend können die neu erhaltenen DAI als Sicherheit für ein Darlehen des Compound-Protokolls dienen. Nun verfügt der Nutzer über zinstragende cDAI-Token. (5) Diese cDAI können in der Folge zusammen mit ETH dem bestehenden Liquidity Pool ETH/cDAI beigelegt werden, wofür der Nutzer temporär bis zum Rückzug der eingebrachten Kryptovermögenswerte aus dem Liquidity Pool UNI-cDAI-Token erhält. (6) Usw. usf. An Punkt (5) angelangt, kontrolliert der Nutzer neben dem temporären Liquiditätstoken UNI-cDAI die in den entsprechenden Smart Contracts als Sicherheiten hinterlegten wBTC und DAI.

Die Fähigkeit von DeFi-Applikationen, praktisch unbeschränkt miteinander verknüpft werden zu können, ist nicht folgenlos für dezentrale Systeme: Ein Programmier- oder Designfehler in einem Smart Contract des einen Protokolls etwa kann sich kaskadenartig auf andere Smart Contracts und somit auf die Funktionslogik von Protokollen und dezentralen Applikationen auswirken.¹⁷⁶⁰ Vorliegend soll dieses Risiko als *Composability Risiko* bezeichnet werden. Das Composability Risiko entspringt aus dem Umstand, dass trotz der weitgehenden transaktionalen Transparenz auf Ebene der einzelnen Applikationen schwerwiegende Abhängigkeiten und Interdependenzen innerhalb eines dezentralen Systems existieren können, die nicht im Voraus entdeckt oder vollständig kontrolliert werden können.¹⁷⁶¹ Mit Blick auf dezentrale Systeme

¹⁷⁵⁸ Siehe Schär, Federal Reserve Bank of St. Louis Review 2021, 169, der von «open financial engineering» spricht.

¹⁷⁵⁹ Dies erfolgt über folgende Plattform: <https://bridge.renproject.io/>. Ausführlich hierzu Wang, How RenVM Actually Works, Medium, *passim*.

¹⁷⁶⁰ Siehe Gudgeon et al., Proceedings Crypto Valley Conference on Blockchain Technology 2020, 1–2, 2–3 Schär, Federal Reserve Bank of St. Louis Review 2021, 171.

¹⁷⁶¹ Vgl. Schär, Federal Reserve Bank of St. Louis Review 2021, 171; ausführlich Schär, DeFi Is Transparent, Unless You Look Closely, Coindesk, *passim* («Theoretical transparency does not necessarily correspond to actual transparency.»); sodann Werner et al., Decentralized Finance, 11–12.

sind Composability Risiken als Systemrisiken aufzufassen. MATTHIAS NADLER und FABIAN SCHÄR sprechen in diesem Zusammenhang auch von Wrapping Complexity, welche dadurch entsteht, dass ein Token basierend auf einem anderen Token, der für die Emission des ersteren als Sicherheit dient, herausgegeben wird.¹⁷⁶² Die Folge von Composability ist, dass sich das Risiko- und Vertrauensmodell für den Nutzer mit jeder weiteren Ebene (Applikation, Smart Contract, Schnittstellen, Benutzeroberflächen, ...), die hinzukommt, ändert und allenfalls zu seinen Lasten verändern könnte. So können sich namentlich Admin Key-Risiken eines Protokolls in eine Transaktion einschleichen, die für den Nutzer eines anderen Protokolls nicht direkt ersichtlich sind. Bei diesen Phänomenen handelt sich um neuartige Risiken, die in dieser Form im traditionellen Finanzsystem nicht existieren.

Eine besondere Form des Composability Risikos geht von *Flash Loans* aus: Flash Loans sind die Aufnahme eines *unbesicherten* Darlehens und dessen Rückzahlung innerhalb *derselben* Transaktion.¹⁷⁶³ Für Ethereum bedeutet dies, dass grundsätzlich alle Operationen einer Flash Loan innerhalb einer Blockzeit des Netzwerks ausgeführt werden müssen. Gelangen nicht alle Operationen einer Transaktion zur Ausführung, findet gar keine Operation der Transaktion statt.¹⁷⁶⁴ Es gilt also das Prinzip «Alles oder nichts», was in den Computerwissenschaften mit *Atomarität* beschrieben wird.¹⁷⁶⁵

Flash Loans werden typischerweise zur Arbitrage von unterschiedlichen Preisen auf verschiedenen dezentralen Handelsplattformen eingesetzt und sind somit ein wesentlicher Bestandteil für die Funktionsweise etwa von Smart Contract-basierten Liquiditätspools.¹⁷⁶⁶ Darüber hinaus können Flash Loans bspw. für den atomistischen Swap der für ein Darlehen gewährten Sicherheiten oder die atomistische Liquidation von Schuldenpositionen mit bevorstehendem Margin Call verwendet werden.¹⁷⁶⁷ Um Flash Loans zu nutzen, wird typischerweise ein Smart Contract programmiert, (i) der ein Darlehen auf der einen Plattform aufnimmt (z.B. AAVE oder dYdX), (ii) anschliessend gewisse

¹⁷⁶² Siehe Nadler/Schär, Decentralized Finance, 7.

¹⁷⁶³ Siehe Gudgeon et al., Proceedings Crypto Valley Conference on Blockchain Technology 2020, 4; ferner Wang et al., 2021 Proceedings of the Ninth International Workshop on Security in Blockchain and Cloud Computing 2021, 25.

¹⁷⁶⁴ Siehe Daian et al., 2020 IEEE Symposium on Security and Privacy 2020, 913; Werner et al., Decentralized Finance, 4.

¹⁷⁶⁵ Siehe zu den Grundlagen von Atomarität Rahm/Saake/Sattler, Verteiltes und Paralleles Datenmanagement, 30; ferner Antonopoulos/Wood, Mastering Ethereum, 129.

¹⁷⁶⁶ Siehe Schär, Federal Reserve Bank of St. Louis Review 2021, 164 m.w.N.

¹⁷⁶⁷ Ausführlich mit Beispielen Wang et al., 2021 Proceedings of the Ninth International Workshop on Security in Blockchain and Cloud Computing 2021, 27–28.

Operationen (z.B. mehrere Swaps zu unterschiedlichen Preisen) vornimmt und (iii) schliesslich – immer noch als Teil derselben Transaktion – das Darlehen samt Zins zurückzahlt.¹⁷⁶⁸ Die Rückzahlung kann auch in einem anderen als dem ausgeliehenen Vermögenswert erfolgen (sog. Flash Swaps).¹⁷⁶⁹ Es sei angemerkt, dass Flash Loans nur innerhalb von DeFi existieren können, setzen sie doch die Existenz von Smart Contracts und den zugrundeliegenden Protokollen voraus.¹⁷⁷⁰

Flash Loans weichen vom Risikoprofil traditioneller Darlehen und Kredite fundamental ab: Sie enthalten aus Sicht des Smart Contracts, der die Vermögenswerte für das Darlehen bereitstellt, keine Ausfalls- bzw. Rückzahlungsrisiken, denn der Smart Contract wickelt die einzelnen Operationen einer Flash Loan nacheinander ab. Entweder die Bedingungen jeder Operation der Transaktion sind erfüllt und werden darum vom Smart Contract und dem Netzwerk abgewickelt oder die Transaktion scheitert in ihrer Gesamtheit. Weil Flash Loans unbesichert sind, weisen sie abgesehen von den anfallenden Netzwerkgebühren für eine Transaktion praktisch keine (Opportunitäts-)Kosten für den Darlehensnehmer auf. Dieser Mangel an *Skin in the Game* wird von einigen Beobachtern als geradezu systemwidrig betrachtet.¹⁷⁷¹

Entsprechend ist es wenig überraschend, dass Flash Loans in der Vergangenheit in komplexen Smart Contract-Angriffen eingesetzt worden sind: Dezentralen Handelsplattformen kommt dabei eine zentrale Rolle zu, denn sie stellen für viele andere dezentrale Applikationen (insb. Lending-Protokolle) aktuelle Marktpreise zur Verfügung.¹⁷⁷² Allgemein formuliert versuchen die Angreifer die Preise auf dezentralen Handelsplattformen so zu manipulieren, dass es zu einer Störung der Funktionslogik anderer dezentraler Applikationen kommt, welche sie sodann zu ihren Gunsten ausnützen können. Im Februar 2020 etwa konnten Angreifer mittels Aufnahme grösserer Flash Loans in ETH auf dezen-

¹⁷⁶⁸ Das Konzept hinter *Flash Loans* geht zurück auf Wolff, Smart Contract Bank, Medium, *passim*; siehe ferner Gudgeon et al., Proceedings Crypto Valley Conference on Blockchain Technology 2020, 4; Daian et al., 2020 IEEE Symposium on Security and Privacy 2020, 913. Eine gute Darstellung zu Flash Loans findet sich in AAVE, Protocol Whitepaper, 15.

¹⁷⁶⁹ Siehe hierzu Harvey/Ramachandran/Santoro, DeFi, 100–102.

¹⁷⁷⁰ Siehe Qureshi, Flash Loans, Medium, *passim*; ferner Daian et al., 2020 IEEE Symposium on Security and Privacy 2020, 913; Harvey/Ramachandran/Santoro, DeFi, 57.

¹⁷⁷¹ So etwa Qureshi, Flash Loans, Medium, *passim*; Werner et al., Decentralized Finance, 6–7, die daraus schliessen, dass ein Protokoll, das risikolose Gewinne zulässt, technisch nicht einwandfrei ist; ähnlich Gudgeon et al., Proceedings Crypto Valley Conference on Blockchain Technology 2020, 4.

¹⁷⁷² Siehe zu den unterschiedlichen Preisfindungsmechanismen ausführlich Samczsun, Price manipulation, *passim*.

tralen Lending-Plattformen (dYdX, bZx) die Preise von Kryptovermögenswerten in relativ illiquiden Liquiditätspools dezentraler Handelsplattformen (Kyber Network, Uniswap) künstlich hochtreiben, was dazu führte, dass die Smart Contracts von bZx aufgrund verzerrter Preisinformationen fälschlicherweise zu hohe Darlehenssummen an die Angreifer ausbezahlten, die sich bei normalisierten Marktpreisen als *unterbesichert* herausstellten. Während die Flash Loans noch in derselben Transaktion zuzüglich Zins an die Smart Contracts von dYdX bzw. bZx zurückbezahlt wurden,¹⁷⁷³ konnten die Angreifer die Rückzahlung der unterbesicherten bZx-Darlehen ganz einfach verweigern und die Zwangsliquidation der Positionen in Kauf nehmen, denn die Gewinne hatten sie in diesem Moment bereits eingesackt.¹⁷⁷⁴ Ein weiterer möglicher Angriffsvektor stellen die Governance Token einer dezentralen Applikation dar: Durch den Flash Loan-finanzierten Erwerb einer genügend grossen Menge an Governance Tokens könnte eine Person das Projekt bzw. dessen Governance vorübergehend kontrollieren, was dem Angreifer je nach Protokoll unterschiedliche Vermögensvorteile verschaffen kann.¹⁷⁷⁵

Flash Loan-Angriffe sind vergleichbar mit *Hacks* im herkömmlichen Sinne, denn die erfolgreiche Ausführung solcher Angriffe setzt entweder Programmierfehler in Smart Contracts, unzuverlässige Preisfindungsmechanismen oder zumindest Logikfehler im Design dezentraler Applikationen voraus.

In der Praxis fällt die Bestimmung von Composability-Fehlerquellen im Nachhinein (d.h. *post mortem*) relativ banal aus, doch sind deren Implikationen für die Funktionsweise der einzelnen dezentralen Applikationen in vielen Fällen nicht oder nur schwer vorhersehbar. Da sich DeFi noch in einem frühen Stadium der Entwicklung befindet, ist allerdings damit zu rechnen, dass gewisse Standardisierungen infolge Versuchs und Irrtums zu Verbesserungen führen werden. In diesem Sinne kann jeder erfolgreiche Hackerangriff oder sonstiger Vorfall aufgrund eines Programmierfehlers als kostspieliger, aber notwendiger Entwicklungsschritt für das DeFi-Ökosystem betrachtet werden.

¹⁷⁷³ Vgl. die Anatomie der beiden fraglichen Flash Loan-Transaktionen unter <https://etherscan.io/txs/label/bzx-exploit>.

¹⁷⁷⁴ Siehe Foxley, DeFi 'Flash Loan' Attack, Coindesk, *passim*; für eine ausführliche Darstellung der Vorgänge der ersten Angriffs siehe PeckShield, bZx Hack Full Disclosure, Medium, *passim*.

¹⁷⁷⁵ Die Beschreibung eines theoretischen Hackerangriffs des Governance-Modells des MakerDAO-Protokolls findet sich bei Gudgeon et al., Proceedings Crypto Valley Conference on Blockchain Technology 2020, 3–6; ferner Zoltu, How to turn M into 0M in 15 seconds, Medium, *passim*.

ii. Black Thursday-Risiken

Nicht als Composability Risiko einzustufen, ist das Risiko, dass ein in DeFi-Lending-Protokollen als Sicherheit dienender Vermögenswert überraschend stark an Wert einbüsst, weshalb das Protokoll die Position zwangsliquidieren muss, bevor es zu einer Unterbesicherung des Darlehens kommt.¹⁷⁷⁶ Eine solche Zwangsliquidation hat typischerweise ihrerseits einen negativen Effekt auf den Preis des zu liquidierenden Kryptovermögenswerts. Vergleichbare Ansteckungseffekte, die ihren Ursprung in den Bilanzen einzelner bedeutender Finanzinstitute haben und sich sodann negativ auf andere Finanzinstitute und letztlich auf die Realwirtschaft auswirken können, sind im traditionellen Finanzsystem bekannte Krisenursachen.¹⁷⁷⁷

Aufgrund der Interoperabilität von DeFi-Protokollen (s. oben) können diese «Verpfändungsketten» ungemein lange ausfallen und die Tokenpreise bei Notliquidationen trotz anfänglicher Überbesicherung durch die Lending-Protokolle entsprechend stark unter Druck geraten. Die Kryptowelt scheint hier ein Problem zu reproduzieren, das in traditionellen Märkten bereits stark kritisiert wurde, jedoch überwiegend ungelöst ist.¹⁷⁷⁸ Immerhin scheinen die Verpfändungsketten in DeFi-Lending-Protokollen nicht mehr gleich stark von der Intermediation einzelner Finanzintermediäre abzuhängen.¹⁷⁷⁹

Der heute als «Black Thursday» der Kryptoindustrie bekannte Vorfall stellt die Materialisierung eines solchen Risikos dar: Im März 2020 kam es aufgrund der COVID-19-Pandemie zu starken Kurseinbrüchen sowohl in den traditionellen als auch in den Kryptomärkten. Infolge verbreiteter Panik, die ihren Anfang an den Derivatemärkten nahm, kam es zur vollständigen Auslastung der Netzwerkkapazitäten von Ethereum, sodass ein Grossteil der Transaktionen vorübergehend keinen Platz in einem Block fand. Die Überlastung verhinderte dabei nicht nur, dass aktuelle Orakelpreise den Marktteilnehmern mitgeteilt werden konnten, sondern auch, dass Lending-Protokolle die drohenden Unterbesicherungen ausgleichen konnten. Die Lending-Protokolle etwa von Ma-

¹⁷⁷⁶ Vgl. etwa die Ausführungen in MakerDAO, *Maker Protocol*, 8–10.

¹⁷⁷⁷ Siehe z.B. Allen/Gale, *Journal of Political Economy* 2000, 4–5; Brunnermeier, *Journal of Economic Perspectives* 2009, 91–98; Roukny et al., *Default Cascades in Complex Networks: Topology and Systemic Risk*, *Scientific Reports* 2013, 6; Hautsch/Schaumburg/Schienle, *Review of Finance* 2015, 689; Avgouleas, *Global Financial Markets*, 118.

¹⁷⁷⁸ Siehe etwa zum Problem, das scheinbar aus makroökonomischen Liquiditätsgründen ungelöst ist, Singh/Aitken, *IMF Working Paper* Juli 2010, 3, 9; Singh, *Banque Stratégie* 2012, 17; ferner Long, *Repo Market Meltdown*, *Forbes*, *passim*.

¹⁷⁷⁹ Vgl. Singh, *IMF Working Paper* November 2011, 4–5.

ker, AAVE und Compound gehen bei allzu starken negativen Preisentwicklungen der als Sicherheiten hinterlegten Kryptovermögenswerte dazu über, diesen an den meist bietenden Liquidator zu veräußern.¹⁷⁸⁰ Die temporäre Überlastung des Ethereum Netzwerks verhinderte allerdings gerade diesen Korrekturmechanismus.¹⁷⁸¹ Die Inhaber von MKR-Token, welche letztlich die Solvenz des Maker-Protokolls gewährleisten,¹⁷⁸² realisierten an diesem Tag (auch aufgrund eines Designfehlers im Auktionsmodell) einen Verlust von mehreren Millionen US-Dollar.¹⁷⁸³

Im Verlauf der oben erwähnten Ereignisse mangelte es ferner auch an der für die korrekte Funktionsweise der involvierten DeFi-Protokolle notwendigen Liquidität. Zurückzuführen war dies auf das Fehlen der entsprechenden Marktteilnehmer.¹⁷⁸⁴ Liquiditätsengpässe bzw. das Ausbleiben von Market-Making-Aktivitäten sind allerdings allgemeine Krisenphänomene in Finanzmärkten.¹⁷⁸⁵

iii. Interdependenzen zwischen dezentralen Systemen

Atomic-Swap-basierte P2P-Handelsplattformen erlauben den Austausch von Kryptovermögenswerten unterschiedlicher dezentraler Netzwerke. Trotz des Umstandes, dass die beiden involvierten Netzwerke im Rahmen eines solchen Cross-chain Atomic Swaps nicht direkt interagieren, ist der Nutzer eines solchen Austauschgeschäfts darauf angewiesen, dass die Transaktion auf beiden Netzwerken korrekt ausgeführt wird. Programmierfehler in einem Smart Con-

¹⁷⁸⁰ Eine gute Darstellung solcher Protokolle findet sich bei Schär, Federal Reserve Bank of St. Louis Review 2021, 164–165.

¹⁷⁸¹ Siehe Frangella, Crypto Black Thursday, Medium, *passim*.

¹⁷⁸² Vgl. MakerDAO, Recent Market Activity, *passim*.

¹⁷⁸³ Siehe whiterabbit, Black Thursday for MakerDAO, Medium, *passim*; ausführlich silto, Black Thursday Response Thread, *passim* («What happened today is that during the big drop in ETH price, a lot of vaults became available for liquidation, at the same time as the Ethereum network became clogged with lots of transactions, leading to a sharp rise in gas price. This confluence of circumstances led to keepers either stoping their activity for fear of slippage (price dropping fast + transactions taking a long time to validate) and for lack of liquidity to absorb all those liquidations. This lead to a situation where only one keeper continued triggering liquidations, and bidding 0\$ for the ETH, with no competition. This situation lasted around 2/3hours, before other keepers came in and resumed normal operation.»).

¹⁷⁸⁴ Siehe Frangella, Crypto Black Thursday, Medium, *passim*; ferner Werner et al., Decentralized Finance, 9–10.

¹⁷⁸⁵ Siehe etwa OECD, Tokenisation and Implications for Financial Markets, 25, und Bech et al., BIS Quarterly Review März 2020, 74, welche die Bedeutung von Intermediären in Krisensituationen hervorheben.

tract der einen Blockchain, die bspw. durch einen Hack ausgenutzt werden können, können die Funktionsweise der anderen Blockchain ebenfalls beeinträchtigen.¹⁷⁸⁶

Als derzeit grösstes systemisches Risiko gelten regelmässig die bereits erwähnten Orakel-Risiken.¹⁷⁸⁷ Während dezentrale Handelsplattformen als Preisorakel für anderen Applikationen fungieren können, spielen Orakelrisiken für Nutzer dezentraler Handelsplattformen typischerweise nur eine sekundäre Rolle. Im Wesentlichen handelt es sich um das Risiko, dass Orakel dem System falsche oder manipulierte Off-chain-Informationen einspeisen, weshalb dezentrale Applikationen unzuverlässige Funktionen ausführen. So können etwa Lending-Protokolle Kredite zu liquidieren beginnen, welche ohne die Einspeisung falscher oder manipulierter externer Daten weiterhin genügend überbesichert wären.

iv. Probabilistische Finalität

Wie oben ausgeführt,¹⁷⁸⁸ kann die konkrete Ausgestaltung der rechtlichen Finalität von Effektingeschäften eine potenzielle Quelle von Gegenpartei- und somit Systemrisiken darstellen. Abwicklungsfinalität bedeutet in traditionellen Finanzmarktinfrastrukturen, dass eine Verpflichtung zur Lieferung oder Bezahlung unwiderruflich und bedingungslos erfüllt wird. Wann dies der Fall ist, bestimmt sich im traditionellen Finanzbereich nach den einschlägigen Rechtsnormen und/oder Regeln der jeweiligen Finanzmarktinfrastuktur.¹⁷⁸⁹

Finalität in diesem Sinne bezieht sich auf den Umstand, dass die Parteien an den involvierten Vermögenswerten in rechtlicher Hinsicht definitiv Eigentum erworben haben. Dies ist insb. im Konkurs einer der an einem Austauschgeschäft beteiligten Parteien von praktischer Bedeutung. Art. 3 Abs. 1 und Abs. 2 der *Directive 98/26/EC on settlement finality in payment and securities settlement systems* sieht etwa vor:

¹⁷⁸⁶ Siehe Narayanan et al., Bitcoin, 259; ECB/BOJ, STELLA, 25; Komodo, Order Matching with Full-Relay and Non-Relay Nodes, *passim*.

¹⁷⁸⁷ So etwa Harvey/Ramachandran/Santoro, DeFi, 137–138; ferner Amler et al., DeFi-ning DeFi, 6, 7 («major concern»); BIS, Crypto Ecosystem, 10–11.

¹⁷⁸⁸ Siehe oben, [IV.5.1c.iii](#).

¹⁷⁸⁹ Siehe BIS-CPSS/IOSCO, Principles for financial market infrastructures, 64–66; IOSCO, Fintech Report, 52. Für schweizerische Finanzmarktinfrastrukturen gelten hinsichtlich Finalität Art. 89 Abs. 2 FinfraG; vgl. ferner für Zahlungssysteme Art. 82 FinfraG i.V.m. Art. 66 FinfraV.

«Transfer orders and netting shall be legally enforceable and, even in the event of insolvency proceedings against a participant, shall be binding on third parties, provided that transfer orders were entered into a system before the moment of opening of such insolvency proceedings [...]. [...]»

No law, regulation, rule or practice on the setting aside of contracts and transactions concluded before the moment of opening of insolvency proceedings [...] shall lead to the unwinding of a netting.»

Ein spezifisches Risiko, das mangels Gegenpartei grundsätzlich nichts mit einem Gegenparteirisiko nach traditioneller Lesart zu tun hat, aber dennoch ein Erfüllungsrisiko darstellt, ergibt sich aus der Tatsache, dass die Abwicklung von Transaktionen in dezentralen Netzwerken grundsätzlich *keine rechtliche Finalität* garantiert.¹⁷⁹⁰ Demgegenüber handelt es sich vorbehaltlich abweichender rechtlicher Vorgaben oder vertraglicher Abmachungen um eine rein technische Finalität. Die Finalitätsmechanik dezentraler Netzwerke ist insb. im Zusammenhang mit einer 51%-Attacke praktisch bedeutsam.¹⁷⁹¹ Sollte ein solcher Angriff erfolgreich ausgeführt werden, wird der Angreifer in aller Regel bereits abgewickelte Transaktionen rückgängig machen wollen – um bspw. eine Double Spending-Attacke zu lancieren. In solchen Angriffen könnte sich ein systemisches Erfüllungsrisiko (Settlement Risk) für die Nutzer eines dezentralen Netzwerks materialisieren.¹⁷⁹²

In PoW-Netzwerken, die einen rein *probabilistischen* Finalitätsmechanismus aufweisen, ist die Empfängerpartei einer Transaktion potenziell mit dem Risiko konfrontiert, dass die Gegenpartei faktisch doch nicht erfüllt hat. Probabilistische bzw. mathematische Finalität beschreibt die mit jeder Bestätigung (d.h. Block) abnehmende Wahrscheinlichkeit, dass eine von den Netzwerkteilnehmern in das verteilte Register aufgenommene Transaktion rückgängig gemacht werden kann.¹⁷⁹³ In Bitcoin etwa wird für grössere Transaktionen das Abwarten von sechs Bestätigungen – d.h. sechs Blöcke à ungefähr zehn Minuten – empfohlen.¹⁷⁹⁴ Die Reversibilität von Transaktionen, die unter einer Viel-

¹⁷⁹⁰ Vgl. etwa Botschaft DLT 2019, 286 («im Allgemeinen offengelassen»).

¹⁷⁹¹ Siehe oben, [IV.5.2e.iii](#).

¹⁷⁹² So auch PWG/FDIC/OCC, Stablecoin Report, 13; Swanson, Settlement Risks Involving Public Blockchains, *passim*; ähnlich Sams, The Capco Institute Journal of Financial Transformation 2015, 44.

¹⁷⁹³ Siehe Antonopoulos, Mastering Bitcoin, 212; Narayanan et al., Bitcoin, 37; Bonneau et al., Proceedings 2015 IEEE Symposium on Security and Privacy, 107, 109 («eventual consensus»).

¹⁷⁹⁴ Siehe Antonopoulos, Mastering Bitcoin, 212; Narayanan et al., Bitcoin, 37; Bonneau et al., Proceedings 2015 IEEE Symposium on Security and Privacy, 107.

zahl von Blöcken «begraben» sind, gilt angesichts der prohibitiv hohen ökonomischen Kosten, eine alternative Blockchain zu berechnen, als praktisch ausgeschlossen, so dass für Bitcoin-Transaktionen von einer *de facto*-Finalität gesprochen werden kann. Die Wahrscheinlichkeit einer erfolgreichen 51%-Attacke nimmt über den Zeitverlauf exponentiell ab.¹⁷⁹⁵ Theoretisch ist die Wahrscheinlichkeit der Reversibilität damit zu keinem Zeitpunkt jemals null,¹⁷⁹⁶ was allerdings auch für traditionelle Finanzmarktinfrastrukturen gilt. Man denke nur an ein Gerichtsverfahren, in dem ein Richter die Klage auf Rückabwicklung eines Effktengeschäfts gutheisst, worauf entsprechende Umbuchungen vorgenommen werden.

Ethereum führt mit dem Wechsel zu PoS einen Mechanismus ein, der die Irreversibilität von Transaktionen durch technische Vorkehrungen sicherstellen soll, die namentlich in der Sanktionierung des Fehlverhaltens von Netzwerkteilnehmern bestehen.¹⁷⁹⁷ Selbstredend führt auch dieser Mechanismus noch nicht zu einer rechtlichen Finalität der auf diese Weise abgewickelten Transaktionen.¹⁷⁹⁸

Der Gesetzgeber kann die Finalität von Blockchain-basierten Transaktionen in einer spezifischen Regelung anordnen. Art. 89 Abs. 2 FinfraG ordnet heute ausschliesslich die *aufsichtsrechtliche* Finalität bei Teilnahme an einer traditionellen Finanzmarktinfrastuktur an. Bei Nutzung einer dezentralen Handelsplattform wird es mangels Intermediärs bereits an einer «Weisung eines Teilnehmers» fehlen.¹⁷⁹⁹

¹⁷⁹⁵ Vgl. Auer, BIS Working Papers Nr. 765, Januar 2019, 10–12, der von «economic payment finality» spricht («[...] a cryptocurrency payment can be considered as final once it is certain that from a certain moment of time onwards, it will never be profitable to undo the payment via a double-spending attack.»).

¹⁷⁹⁶ Siehe Buterin, On Settlement Finality, *passim*.

¹⁷⁹⁷ Siehe Buterin, On Settlement Finality, *passim* («This is what we mean by 'economic finality': we can't guarantee that 'X will never be reverted', but we can guarantee the slightly weaker claim that 'either X will never be reverted or a large group of validators will voluntarily destroy millions of dollars of their own capital'.»).

¹⁷⁹⁸ Vgl. etwa Konstantopoulos/Buterin, Ethereum Reorgs, *passim* («Finally, long reorgs are not possible because all blocks that are deeper than 2 epochs in the past are considered 'finalized', i.e. it is impossible to revert past them. If an attacker caused two conflicting blocks to be finalized [e.g by controlling 67% of the stake], the system would need to fall back to social intervention to recover.»).

¹⁷⁹⁹ Ähnlich für den Fall der Herausgabe von CBCDs in Form von Registerwertrechten Eggen/Stengel, GesKR 2020, 213.

Im Rahmen der DLT-Revision hat der Gesetzgeber jedoch die zivilrechtliche Finalität von Übertragungen von Registerwertrechten in Art. 973f Abs. 2 OR geregelt.¹⁸⁰⁰ Im Übrigen hat der Bundesrat in der Botschaft festgehalten, dass privatautonomen Regelungen der Vorzug zu geben ist: «Die Frage der Finalität – wann eine Verfügung über ein Registerwertrecht wirksam wird – wird im Allgemeinen offengelassen und ist den Regeln des Wertrechtregisters oder eines anderen benutzten Handelssystems bzw. der Vereinbarung der Parteien überlassen.»¹⁸⁰¹ In Bezug auf dezentrale Handelsplattformen wird sich regelmässig keine generelle Regelung betreffend Finalität finden lassen. Ohnehin spielt das Gegenparteirisiko der an einem Austauschgeschäft beteiligten Parteien aufgrund des Atomic Settlement-Mechanismus eine geringfügigere Rolle als in zentralen Systemen.¹⁸⁰²

Demgegenüber können die an einem Austauschgeschäft beteiligten Parteien vereinbaren, wann sie eine Transaktion für die Vertragserfüllung als final betrachten, was bei einer P2P-Betrachtungsweise der Vorgänge auch durchaus einleuchtet. Damit bleibt es im Wesentlichen den Marktteilnehmern überlassen, nach welchen Regeln sie die Finalität in dezentralen Systemen regeln.

g. Kollektive Handlungsprobleme

i. Ostroms «drei Rätsel»

Die Wirtschaftsnobelpreisträgerin OSTROM spricht von «drei Rätseln», welche die an einem Gemeingut beteiligten Personen zu lösen haben: (i) *the problem of supply*, (ii) *the problem of credible commitment* und (iii) *the problem of mutual monitoring*.¹⁸⁰³ Im Rahmen ihrer empirischen Analyse von Gemeingütern hat OSTROM eine Reihe von Bedingungen herausgearbeitet, die sich in der Praxis als wesentlich für die nachhaltige Lösung dieser drei Rätsel herausgestellt haben.¹⁸⁰⁴ Danach ist kollektives Handeln in Bezug auf Gemeingüter möglich, wenn gewisse Gestaltungsprinzipien gegeben sind. Zu diesen Gestaltungsprinzipien gehören u.a., dass (i) der Kreis der teilnehmenden Parteien sowie

¹⁸⁰⁰ Art. 973f Abs. 2 OR regelt die zivilrechtliche Verbindlichkeit von Verfügungen des Gläubigers eines Registerwertrechts und deren Wirksamkeit gegenüber Dritten im Falle der Konkurseröffnung, des Pfändungsvollzugs oder der Nachlassstundungsbewilligung über den Gläubiger.

¹⁸⁰¹ Siehe Botschaft DLT 2019, 286.

¹⁸⁰² So auch Weber, SZW 2021, 460.

¹⁸⁰³ Siehe Ostrom, *Governing the Commons*, 42–45.

¹⁸⁰⁴ Vgl. für eine Übersicht Ostrom, *Governing the Commons*, 90.

das Gemeingut selbst klar bestimmt sind, (ii) die betroffenen Parteien die Systemregeln mitbestimmen können, (iii) Überwachungs- und Sanktionsmechanismen bestehen und (iv) die Rechtsordnung der betreffenden Gruppe einen institutionellen Freiraum belässt.¹⁸⁰⁵ Durch Orientierung an diesen Prinzipien und deren Einhaltung kann einer Gemeinschaft die angeblich zwangsläufige Tragik der Allmende¹⁸⁰⁶ ersparen.

Mit Blick auf dezentrale Systeme wird vorliegend zwischen vier kollektiven Handlungsproblemen unterschieden, welche namentlich in der Bereitstellung des Netzwerks bzw. der Applikation, der Softwareentwicklung und der Governance i.w.S. bestehen. Die oben erwähnten drei Rätsel treten je nach Handlungsproblem und untersuchter Blockchain in unterschiedlichem Ausmass auf. Ein kollektives Handlungsproblem, mit welchem derzeit *Ethereum* konfrontiert ist, ist die Skalierung der Verarbeitungskapazitäten des Netzwerks. Sollten die Netzwerkteilnehmer, die Softwareentwickler und das Ökosystem als Ganzes nicht fähig sein, eine nachhaltige Skalierungslösung entwickeln zu können, so ist nicht ausgeschlossen, dass DeFi-Anwendungen vermehrt andere dezentrale Netzwerke als Grundlage verwenden werden.¹⁸⁰⁷

ii. Bereitstellung des Netzwerks

Dezentrale Systeme lösen, wie oben ausgeführt, kollektive Handlungsprobleme grundsätzlich über kryptoökonomische Mechanismen.¹⁸⁰⁸ Diese Anreizstrukturen spielen im Rahmen der Bereitstellung des Netzwerks als kollektives Gut eine zentrale Rolle.¹⁸⁰⁹ Namentlich aufgrund entsprechender finanzieller Entschädigungen (Mining- bzw. Staking-Belohnung sowie Transaktionsgebühren), allfälliger Investitionen (z.B. in Hardware) und des allfälligen Slashing-Risikos (in PoS-Netzwerken) stellen Miner und Staker die Sicherheit und Stabilität einer Blockchain sicher. Damit ist ein wesentliches Gestaltungsprinzip nach OSTROM erfüllt: Sanktionsmechanismen lassen sich durch entsprechende positive und negative Anreizsysteme einfach um- und durchsetzen. Die Opportunitätskosten der Nichteinhaltung der Protokollregeln sind für rationale Netzwerkteilnehmer in aller Regel zu hoch.

¹⁸⁰⁵ Ausführlich Ostrom, *Governing the Commons*, 88–102.

¹⁸⁰⁶ Vgl. hierzu Hardin, *Science* 1968, *passim*.

¹⁸⁰⁷ Siehe zu diesem *Scaling Risk* Harvey/Ramachandran/Santoro, DeFi, 138–141; ferner Amler et al., *DeFi-ning DeFi*, 6; bereits IOSCO, *Fintech Report*, 60, 61–62.

¹⁸⁰⁸ Siehe hierzu oben, [II.5.2b](#).

¹⁸⁰⁹ So auch Berentsen/Schär, *Bitcoin*, 214

Neben der incentivierten Bereitstellung des Gutes (supply), welche für die Netzwerkteilnehmer mit entsprechenden Kosten verbunden ist (credible commitment), sind Abweichungen von den allseits abgemachten Protokollregeln durch die übrigen Netzwerkteilnehmer relativ rasch feststellbar (mutual monitoring). Gerade letzter Punkt hinsichtlich Überwachung scheint für ein loses Kollektiv wie dezentrale Systeme zentral zu sein: Können die Parteien ihr Verhalten nicht genügend überwachen, so können sie nicht wissen, ob die anderen ebenfalls zum Gemeingut beitragen; können sie den übrigen Teilnehmern aber nicht vertrauen, dass sie ebenfalls beitragen, werden sie aufhören, zum gemeinsamen Projekt beizutragen (unabhängig davon, ob die anderen Parteien tatsächlich beigetragen haben oder nicht).¹⁸¹⁰ Dieser Tatsache kommt die Transparenz von dezentralen Systemen zugute. Sie erlaubt einem Teilnehmer die mehr oder weniger effektive Überwachung anderer Teilnehmer, was ihm sodann die informierte Entscheidung überlässt, ob er unter den gegebenen Umständen weiterhin zur Bereitstellung des Netzwerks beitragen möchte.

Darüber hinaus weisen dezentrale Netzwerke gewisse Ähnlichkeiten mit *Clubgütern* auf. Auf der einen Seite existiert die Mining- bzw. Staking-Entschädigung, die aufgrund dauernder Inflationierung der Kryptowährung als sozialisierte Subvention betrachtet werden kann.¹⁸¹¹ Die Nutzer einer Blockchain leisten sodann eine Nutzungsgebühr an die Miner bzw. Staker in Form der Transaktionsgebühr. Die Kosten der Nutzung des Netzwerks ist davon abhängig, wie stark das Netzwerk ausgelastet ist. Die Aufnahmekapazität der Blockchain wird mit zunehmender Auslastung rivalisierend.¹⁸¹² Die Kosten des gemeinsamen Netzwerksunterhalts werden im Ergebnis auf die Netzwerkteilnehmer und Nutzer verteilt.¹⁸¹³ «Nichtberechtigte», d.h. Personen, welche diese Entschädigungsmechanismen nicht mittragen wollen, sind von der Nutzung des Netzwerks technisch ausgeschlossen. Der Beteiligtenkreis am Gemeingut ist damit ökonomisch betrachtet klar abgrenzbar.

¹⁸¹⁰ Siehe Ostrom, *Governing the Commons*, 45 («Without monitoring, there can be no credible commitment; without credible commitment, there is no reason to propose new rules.»).

¹⁸¹¹ Siehe zu diesem Subventionsprozess Berentsen/Schär, *Bitcoin*, 245–248.

¹⁸¹² Vgl. Buchanan, *Economica* 1965, 3, 7–8.

¹⁸¹³ Vgl. Buchanan, *Economica* 1965, 1–3; ferner Sandler, *Constitutional Political Economy* 2013, 266.

iii. Governance-Risiko von dezentralen Applikationen

Soweit eine dezentrale Applikation in den Händen einer DAO ist, manifestiert sich das kollektive Handlungsproblem in einem eigenständigen Governance-Risiko.¹⁸¹⁴ Typischerweise nehmen an der Governance einer Applikation alle Tokeninhaber einer DAO teil. Inhaber mit einer grossen Anzahl an Governance Token können auf die Entwicklung eines Protokolls oder einer Applikation wesentlich Einfluss nehmen. Dies kann ohne entsprechende Schutzvorkehrungen selbstredend auch zulasten der Minderheits-Tokeninhaber erfolgen.¹⁸¹⁵

iv. Softwareentwicklung

Ferner bestehen auch Handlungsbereiche, die in vielen Fällen keinen codierten kryptoökonomischen Anreizen unterliegen. Typischerweise gehören die Aufbringung von finanziellen Mitteln für die Softwareentwicklung sowie die Governance des Netzwerks oder einer Applikation dazu.

Bei beiden Bereichen handelt es sich aus Sicht der Netzwerkteilnehmer und Nutzer um öffentliche Güter. Nach der ökonomischen Theorie ist zu erwarten, dass Private mangels genügender Anreize keine öffentlichen Güter produzieren oder dass die Menge produzierter Güter ungenügend ist.¹⁸¹⁶ Eine Alternative zu einem reinen Marktmechanismus ist der Rückgriff auf zentralisierte Prozesse und Strukturen. Ein Beispiel dafür ist die *Ethereum Foundation*¹⁸¹⁷, welche den Grossteil der Einnahmen aus dem ICO vom Sommer 2014 verwaltet.¹⁸¹⁸ Die Stiftung hält derzeit gut 350'000 ETH.¹⁸¹⁹ Entwickler können sowohl finanzielle als auch nichtfinanzielle Unterstützung bei der Ethereum Foundation beantragen.¹⁸²⁰ Andere Blockchains haben sich ebenfalls für das Modell einer gemeinnützigen Organisation und damit gegen profitorientierte Modelle entschieden.¹⁸²¹ Nicht vergleichbar ist demgegenüber die *Bitcoin Foundation*¹⁸²²,

¹⁸¹⁴ Siehe Harvey/Ramachandran/Santoro, DeFi, 135–136.

¹⁸¹⁵ Siehe etwa das Bsp. in CertiK, Analysis of True Seigniorage Dollar Attack Event, *passim*.

¹⁸¹⁶ So etwa Samuelson/Nordhaus, Microeconomics, 36; Mankiw, Microeconomics, 214.

¹⁸¹⁷ <https://ethereum.foundation/>.

¹⁸¹⁸ Siehe Buterin, Ether Sale, *passim*; ausführlich Russo, Infinite Machine, Kapitel 14.

¹⁸¹⁹ Siehe <https://etherscan.io/address/0xde0b295669a9fd93d5f28d9ec85e40f4cb697bae>.

¹⁸²⁰ Siehe Ecosystem Support, Guide to ESP, *passim*.

¹⁸²¹ So z.B. die Tezos Foundation (<https://tezos.foundation/>). Allerdings war dieser Entscheid alles andere als unumstritten bei den Gründern von Ethereum; vgl. hierzu Paumgarten, Boom and Bust, New Yorker, *passim*.

¹⁸²² <https://bitcoinfoundation.org/>. Vgl. zu den Koordinationsherausforderungen im Bitcoin-Ökosystem Nabilou, Stanford Journal of Blockchain Law & Policy 2021, 41–43.

die nur zu Beginn des Netzwerks, als sie noch den damaligen Hauptentwickler von Bitcoin, Gavin Andresen, angestellt hatte, eine prominente Stellung im Bitcoin Ökosystem eingenommen hat.¹⁸²³

In dezentralen Systemen sind allerdings zentralisierte Prozesse und Strukturen soziokulturell eher verpönt, weshalb für das Unterproduktionsrisiko im Softwarebereich Alternativen zu finden sind. Gewisse Protokolle sehen darum vor, dass ein Teil der im Rahmen des Minings neu geschaffenen Kryptowährungseinheiten in einen Escrow-Mechanismus fließen, über deren Verteilung in aller Regel die Netzwerkteilnehmer gemeinsam bestimmen. Ein Vorreiter in dieser Hinsicht ist die *Dash* Blockchain: Deren Protokoll sieht ein «Governance Budget» von 10% der monatlichen Geldmengeninflation vor. Über die Verteilung des Budgets stimmen die «Masternodes» des Netzwerks ab. Das Budget steht im Anschluss an die Annahme von Anträgen aus der *Dash*-Community für die Finanzierung von Projekten und Protokollverbesserungen zur Verfügung.¹⁸²⁴ Das *Zcash* Protokoll sieht ferner vor, dass während vier Jahre 20% der in einem Block neu geschaffenen ZEC an die Gründer (und Investoren) der Kryptowährung fließen, damit diese weiterhin zum Unterhalt der Software beitragen.¹⁸²⁵ Einige Gründer und Investoren haben sodann einen Teil dieses «Founders' Reward» an die *Zcash* Foundation gespendet.¹⁸²⁶

Neuere Finanzierungsansätze gehen demgegenüber (wieder) einen weniger institutionalisierten Weg. BUTERIN schlägt etwa vor, dass die Projektfinanzierung im Wesentlichen über Spenden aus der Community erfolgen soll. Allerdings unterliegen Spenden typischerweise dem Free-Riding-Problem. Zusammen mit seinen Koautoren präsentiert er darum einen Allokationsmechanismus mit der Bezeichnung *Quadratic Funding*.¹⁸²⁷ Aufgrund der anwendbaren mathematischen Formel erhält aus einem vorfinanzierten Fonds (Matching Fund) dasjenige Projekt die grösste Zuwendung, das von der grössten Zahl an Teilnehmern unterstützt wird, und zwar unabhängig von deren tatsächlichen Beitragshöhen. Kleinere Beiträge von einer grösseren Anzahl Personen werden mit anderen Worten subventioniert, um den Trittbrettfahreneffekt zu verringern.¹⁸²⁸ *Quadratic Funding* soll deshalb einen demokratischen Ansatz für die Finanzierung von öffentli-

¹⁸²³ Siehe Bustillos, Bitcoin Boom, New Yorker, *passim*; vgl. ferner EUBOF, Governance of and with Blockchains, 9; die Rolle der Bitcoin Foundation überschätzend darum Hofert, Regulierung der Blockchains, 72–73.

¹⁸²⁴ Siehe Dash, Governance, *passim*.

¹⁸²⁵ Siehe Wilcox, Funding, Incentives, and Governance, *passim*.

¹⁸²⁶ Siehe Cincinatti, Zcash Governance, *passim*.

¹⁸²⁷ Siehe Buterin/Hitzig/Weyl, Management Science 2019, *passim*.

¹⁸²⁸ Buterin/Hitzig/Weyl, Management Science 2019, 1–2.

chen Gütern darstellen.¹⁸²⁹ Plattformen, wie etwa *Gitcoin*¹⁸³⁰, haben den Allokationsmechanismus bereits implementiert, um Open-Source-Projekte zu fördern. Ein Nachteil von Quadratic Funding über Plattformen, welche die bürgerlichen oder digitalen Identitäten der Teilnehmer nicht zuverlässig überprüfen können, besteht darin, dass ein Teilnehmer versucht sein könnte, mithilfe mehrerer Pseudonyme an einer Abstimmung teilzunehmen, oder dass mehrere Teilnehmer konspirieren, um die Ergebnisse zu ihren Gunsten zu beeinflussen.¹⁸³¹ Ferner hat Quadratic Funding keinen Einfluss auf die Informationsrisiken der Teilnehmer. Der Allokationsmechanismus nimmt Spendern nicht die Aufgabe ab, einen Finanzierungsantrag und die Antragsteller dahinter genau unter die Lupe zu nehmen, bevor sie ein Projekt unterstützen. Um Informationsasymmetrien zwischen den Teilnehmern zu verringern, sind andere Mechanismen notwendig, wie etwa Prediction Markets.¹⁸³²

Eine ausreichende Produktion von sicherer Software scheint nach dem Gesagten zumindest für die Netzwerkebene plausibel (supply).¹⁸³³ Die Community kann die Qualität der Leistung der geförderten Entwickler allerdings erst *ex post* überprüfen (mutual monitoring), was freilich einem verbreiteten Problem jeder arbeitsteiligen Wirtschaft entspricht.¹⁸³⁴ Darum tendiert die Community in vielen Fällen dazu, die Finanzierung von Projekten von der Qualität der Eingabe sowie der Reputation des Teams abhängig zu machen (credible commitment). Entwicklervertrauen spielt in diesem Zusammenhang eine grosse Rolle. Dieser Umstand belegt aber auch gerade, dass öffentliche Güter in einer Variantenvielfalt auftreten und dass die Softwareentwicklung in vielen Fällen bereits dank der Beiträge einiger weniger exzellenter Entwickler gewährleistet sein kann.¹⁸³⁵

Dezentrale Applikationen haben ihrerseits neue Modelle entwickelt, um das kollektive Handlungsproblem der Softwareentwicklung zu lösen. Viele DeFi-Projekte setzen einerseits auf gewinnorientierte Softwareunternehmen, die regelmässig Finanzmittel bei Venture-Capital-Firmen einsammeln, und ande-

¹⁸²⁹ Siehe Buterin/Hitzig/Weyl, Management Science 2019, 6–7 m.w.H.

¹⁸³⁰ <https://gitcoin.co/>.

¹⁸³¹ Siehe Vivek, How to Attack and Defend Quadratic Funding, *passim*; ferner Buterin/Hitzig/Weyl, Management Science 2019, 10–11.

¹⁸³² Vgl. etwa Buterin, Quadratic Payments, *passim*.

¹⁸³³ Kritisch demgegenüber Walch, New York University Journal of Legislation & Public Policy 2015, 870.

¹⁸³⁴ Vgl. statt vieler Jensen/Meckling, Journal of Financial Economics 1976, 308–309; Alchian/Demsetz, The American Economic Review 1972, 780.

¹⁸³⁵ Vgl. etwa zur Best-Shot-Regel Hirshleifer, Public Choice 1983, 372–373.

rerseits auf die Emission eines applikationseigenen Token. Die Herausforderung mit solchen Tokenemissionen liegt neben regulatorischen Risiken insb. darin, eine Verteilung zu erreichen, die aus Sicht der Community als ausgeglichen wahrgenommen wird. Nach dem ICO-Boom von 2017/18 ist darum insb. zu Airdrops und Liquidity Mining übergegangen worden, so etwa im Falle von Uniswap.¹⁸³⁶ Viele Projekte weisen jedoch konzentrierte Tokeninhaberstrukturen auf, da sie einen beachtlichen Teil der neu geschaffenen Token als Anreiz und Entschädigung an das Entwicklerteam sowie Investoren und Berater ihres Softwareunternehmens zuweisen.¹⁸³⁷ Aufgrund zunehmender Kritik an dieser Entwicklung ist ein grosser Tokenbesitzer des Uniswap Protokolls dazu übergegangen, seine Governance Token mittels rechtlicher Strukturen an von ihm unabhängige Dritte zu delegieren. Als ein Kriterium für die Auswahl der Delegationsempfänger werden die positiven Auswirkungen auf die Dezentralität des Protokolls genannt.¹⁸³⁸

Abschliessend ist zu erwähnen, dass Softwareentwicklung aus anderen als rein pekuniären Gründen erfolgen kann (credible commitment). Tatsächlich fällt es der ökonomischen Literatur nicht immer leicht, alle Phänomene und die unterschiedlichen Kollaborationsformen in der Open-Source-Softwareentwicklung zufriedenstellend zu erklären.¹⁸³⁹ Neuere Theorien kommen zum Schluss, dass Open-Source-Software weder das Produkt von Markttransaktionen noch der Organisation innerhalb von Firmenhierarchien ist.¹⁸⁴⁰ YOCHLAI BENKLER spricht in diesem Zusammenhang von *Peer Production* als die in vielen Fällen wohlfahrtsökonomisch effizienteste Produktionsweise von Informationsgütern in einer netzwerkartig strukturierten Gemeinschaft.¹⁸⁴¹ Viele Projekte (allen voran Linux) haben sich trotz – oder gerade wegen – ihrer vermeintlichen Ignoranz gegenüber dichotomischen Modellvorhersagen der Ökonomie durchsetzen können. Abschliessend kann festgehalten werden, dass digitale Innovation die Kosten und den Nutzen von Koordination und Zusammenarbeit nachhaltig verändert hat.

¹⁸³⁶ Siehe Uniswap, Introducing UNI, *passim*.

¹⁸³⁷ Siehe hierzu etwa die Übersicht in Nadler/Schär, *Decentralized Finance*, 5.

¹⁸³⁸ Siehe Amico, *Token Delegate Program*, *passim*.

¹⁸³⁹ Siehe etwa Lerner/Tirole, *The Journal of Industrial Economics* 2002, 198–199; ebenfalls Dalle/Jullien, *Research Policy* 2003, 2.

¹⁸⁴⁰ Siehe Benkler, *The Yale Law Journal* 2002, 372–373, 375–377, 401–403; weitergehend Benkler/Nissenbaum, *The Journal of Political Philosophy* 2006, insb. 403.

¹⁸⁴¹ Ausführlich hierzu Benkler, *The Yale Law Journal* 2002, 404–422; ferner bereits Arrow, in: *National Bureau of Economic Research, Economic Welfare*, 617 («underutilization of information»), 619.

v. Governance i.w.S.

Governance i.e.S., d.h. die Durchsetzung der Konsensregeln, ist Teil der Bereitstellung des Netzwerks. Dafür sorgen Miner und Staker. Governance i.w.S. ist demgegenüber eine weniger eindeutige Angelegenheit. Wird Softwareentwicklung nicht als ein rein technischer Umsetzungsprozess verstanden, wovon ausgegangen werden muss,¹⁸⁴² so hängt Governance i.w.S. im Wesentlichen von der Softwareentwicklung ab.

Eine Mehrzahl der Vorstöße hinsichtlich Protokolländerungen stammt letztlich aus der Entwicklergemeinschaft. Für diesen Prozess greift sie auf gewisse Standardisierungen zurückgreift: In Bitcoin handelt es sich um einen als *Bitcoin Improvement Proposal* (BIP) bezeichneten Governance-Prozess;¹⁸⁴³ in Ethereum verfolgt das *Ethereum Improvement Proposal* (EIP) dasselbe Ziel.¹⁸⁴⁴ Ohne auf Details einzugehen, durchläuft ein Vorschlag eines Entwicklers ein vordefiniertes Prozedere. Im Idealfall schafft es ein Vorschlag nach einem ausgiebigen Revisionsprozess innerhalb der Entwicklergemeinschaft in eine Implementierung des fraglichen Protokolls. Die Verwaltung des derzeit autoritativen Codes sowie von Aktualisierungsvorschlägen werden der Einfachheit halber über GitHub und andere Plattformen koordiniert.

Wie bereits ausgeführt, bedeutet die Aufnahme von Code in eine Implementierung noch nicht, dass das Netzwerk die neuen Regeln anwendet. Kollektive Handlungsprobleme entstehen im Wesentlichen an diesem Punkt: Die an der Übernahme eines Vorschlags interessierten Personen haben auf einen sozialen Konsens innerhalb der Community hinzuarbeiten. Wie zahlreiche Beispiele in Bitcoin zeigen, kann dieser Konsensbildungsprozess sehr aufwendig, ja oft sogar unmöglich sein. Bitcoin hat etwa einen ausgeprägten *Status Quo Bias*, welcher die Propagierung neuer Ideen erschwert. Dieser Bias gibt dem Netzwerk allerdings die notwendige Stabilität. Die Entwicklung von Ethereum folgt demgegenüber dem Pfad iterativer Innovationen innert kurzer Zeiträume.¹⁸⁴⁵ Die Gemeinschaften hinter den beiden Blockchains haben gänzlich unterschiedliche kulturelle Vorstellungen von Governance.¹⁸⁴⁶

¹⁸⁴² Siehe etwa oben, [II.5.3](#) und [IV.5.2g.iv](#).

¹⁸⁴³ In BIP 2 wird dieser Prozess ausführlich dargelegt; vgl. Bitcoin, BIPs, BIP 2, GitHub, *passim*.

¹⁸⁴⁴ Siehe Ethereum, Introduction to EIPs, *passim*.

¹⁸⁴⁵ Siehe Antonopoulos/Wood, Mastering Ethereum, 11–12; Antonopoulos, Mastering Bitcoin, 283–284.

¹⁸⁴⁶ Eine anekdotische, aber doch gute Darstellung der unterschiedlichen kulturellen Mentalitäten findet sich bei Paumgarten, Boom and Bust, New Yorker, *passim*.

Im Anschluss an eine erfolgreiche Konsensfindungsphase stimmen die Netzwerkteilnehmer über das vorgeschlagene Update ab: Dies kann auf dem Weg eines On-chain-Voting-Systems geschehen, wie etwa in Tezos und Decred¹⁸⁴⁷, oder mithilfe eines Aktivierungsprozesses. Ein solcher Aktivierungsprozess ist, grob dargestellt, in aller Regel zweistufig: In einer ersten Phase signalisieren Netzwerkteilnehmer lediglich ihre Zustimmung; in einer zweiten Phase, nachdem in der ersten Phase genügend Netzwerkteilnehmer (i.d.R. die Miner) die Aktivierung signalisiert haben, werden die neuen Regeln von den zustimmenden Netzwerkteilnehmern aktiv durchgesetzt.¹⁸⁴⁸ Letztlich ist es damit jedem Netzwerkteilnehmer überlassen, ob er den neuen Regeln zustimmen möchte oder nicht, womit Ostrows Gestaltungsprinzip des Mitbestimmung rudimentär nachgelebt wird.

h. Rechtsunsicherheit

Nach einem von Ostrows Gestaltungsprinzipien sollte das Recht sich selbst-verwaltenden Gemeingütern genügend Handlungs- und Entfaltungsspielraum einräumen, damit diese sich nachhaltig entwickeln können.¹⁸⁴⁹ Verbote würden dezentrale Lösungen wohl an den Rand der Gesellschaft drängen. Nicht optimal ist allerdings auch ein Rechtsumfeld, welches keine klaren Aussagen zur Legalität einer Aktivität zulässt.

Das eine oder andere Silicon Valley-Unternehmen lebt bekanntlich nach dem Motto «*It's easier to ask forgiveness than to get permission.*», was heute nach der zugeschriebenen Urheberin des Ausspruchs als Hopper's Law bezeichnet wird.¹⁸⁵⁰ Mancher Blockchain-Befürworter hat wohl eine ähnliche Kultur verinnerlicht. Hinzukommt eine gewisse Ignoranz gegenüber bestehenden Regeln.¹⁸⁵¹ Dies ist allerdings wenig überraschend, weisen dezentrale Systeme doch gerade eine eigene dezentrale Governance auf, sodass die korrigierende Rolle des Staates tatsächlich sekundär erscheinen mag. Der Umstand, dass mit DeFi im Allgemeinen und dezentralen Handelsplattformen im Besondern

¹⁸⁴⁷ Vgl. Decred, Decred Governance, *passim*.

¹⁸⁴⁸ Siehe Antonopoulos, Mastering Bitcoin, 280–283.

¹⁸⁴⁹ Siehe hierzu oben, [IV.5.2g.i](#).

¹⁸⁵⁰ Siehe hierzu Thierer, Permissionless Innovation, 140.

¹⁸⁵¹ Vgl. Zetzsche/Buckley/Arner, University of Illinois Law Review 2018, 1407 («Part of the thrill of blockchain to date has been its disregard of the law.»).

durchaus gewisse rechtliche Risiken verbunden sind, führt aber dazu, dass insb. Projekte, die neue Wege gehen wollen, mit erheblicher Rechtsunsicherheit konfrontiert sind.¹⁸⁵²

Die meisten Stellungnahmen nationaler und internationaler Organisationen, Gesetzgeber und Aufsichtsbehörden im Zusammenhang mit Blockchains, DeFi und/oder dezentralen Handelsplattformen sind in erster Linie deskriptiver und einordnender Natur. US-amerikanische Behörden haben demgegenüber auf verschiedenen Wegen Stellung zu den Entwicklungen genommen.¹⁸⁵³ Zu erwähnen sind insb. die Akte der SEC, namentlich die einflussreichen öffentlichen Stellungnahmen ihrer Vertreter¹⁸⁵⁴, die zahlreichen Entscheidungen im Rahmen des ICOs-Booms¹⁸⁵⁵ sowie der vielbeachtete The DAO-Bericht der SEC¹⁸⁵⁶. Auch die FINMA hat sich einige Male insb. zu ICOs und Stablecoins öffentlich geäußert.¹⁸⁵⁷ Informativ, aber leider wenig produktiv für die Industrie war hingegen der zweimalige Praxiswechsel der FINMA im Bereich der aufsichtsrechtlichen Einordnung von Custodial Staking innert sechs Monate.¹⁸⁵⁸

¹⁸⁵² Ausführlich zu regulatorischen Risiken in US-amerikanischer Hinsicht Carter/Jeng, in: Coen/Maurice, DeFi Protocol Risks, 28–31; Humbel, GesKR 2022, 13–14; vgl. ferner Zetzsche/Buckley/Arner, University of Illinois Law Review 2018, 1405 («The claim that risk vanishes simply due to the use of a blockchain is, from a legal perspective, ridiculous.»).

¹⁸⁵³ Kritisch allerdings, was die unterschiedlichen Signale der SEC anbelangt, Guseva, The Journal of Corporation Law 2021, 633–634.

¹⁸⁵⁴ Vgl. etwa Clayton, Cryptocurrencies and Initial Coin Offerings, *passim*; Clayton, Chairman's Testimony on Virtual Currencies, *passim* («But by and large, the structures of ICOs that I have seen involve the offer and sale of securities and directly implicate the securities registration requirements and other investor protection provisions of our federal securities laws.»); Peirce, Renegade Pandas, *passim*; Peirce, Atomic Trading, *passim*.

¹⁸⁵⁵ Vgl. etwa i.S. Munchie SEC, Order Instituting Cease-and-Desist Proceedings in the Matter of Munchie Inc., 11. Dezember 2017; i.S. Kik SEC, Complaint against Kik Interactive Inc., 4. Juni 2019; i.S. EOS SEC, Order Instituting Cease-and-Desist Proceedings in the Matter of Block.one, 30. September 2019; i.S. Telegram SEC, Complaint against Telegram Group Inc. and Ton Issuer Inc., 11. Oktober 2019; i.S. Ripple SEC, Complaint against Ripple Labs, Inc., Bradley Garlinghouse, and Christian A. Larsen, 22. Dezember 2020; vgl. für eine Übersicht der Verfahren gegen ICOs SEC, Cyber Enforcement Actions, *passim*.

¹⁸⁵⁶ Siehe SEC, The DAO Report, *passim*.

¹⁸⁵⁷ Siehe etwa FINMA, Aufsichtsmitteilung 04/2017, *passim*; sodann die ICO-Wegleitungen der FINMA in FINMA, Wegleitung ICOs, *passim*, und FINMA, Ergänzung Wegleitung ICOs, *passim*; ferner FINMA, Aufsichtsmitteilung 02/2019, *passim*; sodann im Enforcement-Bereich etwa FINMA, Scheinkryptowährungen, *passim*; ferner FINMA, envion AG, *passim*.

¹⁸⁵⁸ Vgl. hierzu Andreotti/Zimmermann/Prantl, GesKR 2023, *passim*; nunmehr aber doch (fast) gleicher Ansicht, obschon auch die weiterhin bestehende Rechtsunsicherheit betont wird, FINMA-Aufsichtsmitteilung 08/2023.

Schliesslich haben auch der Bundesrat und das EFD einerseits zu «virtuellen Währungen» und andererseits im Rahmen der Vorarbeiten zur DLT-Revision mehrmals ausführlich Stellung bezogen.¹⁸⁵⁹

Trotzdem bleiben zentrale Fragen – zumindest für die vorliegende Arbeit – weiterhin offen.¹⁸⁶⁰ So gibt etwa die SEC-Verfügung i.S. Coburn bzw. Ether-Delta erste Anhaltspunkte, wann der Entwickler und Betreiber einer dezentralen Handelsplattform einer Registrierungspflicht nach US-amerikanischem Wertpapierrecht unterliegt.¹⁸⁶¹ Dazu kommen öffentliche Stellungnahmen der SEC zu Handelsplattformen vom März und November 2018.¹⁸⁶² Nicht vollständig klar ist demgegenüber, welche Massnahmen Coburn hätte ergreifen können, damit die SEC die Kontrolle von EtherDelta durch Coburn verneint hätte. Sodann hat sich auch die US-amerikanische Commodity Futures Trading Commission (CFTC) zum Derivatehandel an dezentralen Handelsplattformen geäussert.¹⁸⁶³

Viele Beobachter kommen darum zum Schluss, dass die Aufsichtspraxis einen «Dezentralitätstest» entwickeln sollte.¹⁸⁶⁴ Die vorliegende Arbeit wird darum im siebten Kapitel die Eckpunkte eines solchen Tests präsentieren. Im Zentrum des Tests steht die Frage, ob ein Netzwerk und die darauf basierenden Applikationen genügend dezentralisiert sind, um sie in rechtlicher und regulatorischer Hinsicht freizustellen.

¹⁸⁵⁹ Siehe Bundesrat, Bericht zu virtuellen Währungen, *passim*; Bundesrat, DLT-Bericht 2018, *passim*; EFD, Erläuternder Bericht DLT-Vernehmlassungsvorlage 2019, *passim*; Botschaft DLT 2019, *passim*.

¹⁸⁶⁰ Freilich muss sich die Rechtswissenschaft auch ausserhalb des Finanzmarktrechts mit vielen neuen spannenden Fragen beschäftigen; so etwa bereits Lehmann, Minnesota Journal of Law, Science & Technology 2019, 106.

¹⁸⁶¹ Siehe hierzu oben, [IV.3.6a](#).

¹⁸⁶² Siehe SEC, Statement on Potentially Unlawful Online Platforms, *passim*; SEC, Statement on Digital Asset Securities Issuance and Trading, *passim*.

¹⁸⁶³ Siehe etwa Berkovitz, Decentralized Finance, *passim*.

¹⁸⁶⁴ So etwa Schuler/Cloots/Schär, DeFi and On-Chain CeFi, 8–9.

6. Definition einer dezentralen Handelsplattform

6.1 Vorbemerkungen

Im Anschluss an die bisherigen Ausführungen in diesem Kapitel verbleibt noch der Versuch, dezentrale Handelsplattformen in *technischer* Hinsicht zu definieren. Eine Definition, wenngleich eine solche aufgrund der Dynamik des Themas nicht abschliessend ausfallen dürfte, ist notwendig, um dezentrale Handelsplattformen in den verbleibenden Teilen dieser Arbeit einer vertieften Analyse zu unterziehen.

Von der vorliegenden Definition ist die Formulierung eines *Rechtsprinzips der Dezentralität* zu unterscheiden.¹⁸⁶⁵ Während die bisher unternommene vorwiegend technische und ökonomische Analyse einen ersten Anhaltspunkt für die konzeptionelle Einordnung dezentraler Handelsplattformen geben soll, wird der Dezentralitätsbegriff v.a. in finanzmarktrechtlicher Hinsicht relevant sein.

6.2 Definitionsversuch

Nach der vorausgegangenen technischen Untersuchung unterschiedlicher Plattfortmtypen und deren Chancen und Risiken sollen dezentrale Handelsplattformen im Sinne eines *Mindeststandards* wie folgt definiert werden:

- Eine dezentrale Handelsplattform ist eine dezentrale Applikation, die auf einem eigenständigen Protokoll beruhen kann, aber nicht muss, und die auf einem dezentralen Netzwerk zur Ausführung gelangt.
- Die Applikation bezweckt den bilateralen oder multilateralen Austausch von Kryptovermögenswerten.
- Dabei kommt den an einem Austausch beteiligten Nutzern der Plattform jederzeit die ausschliessliche Kontrolle über ihre Kryptovermögenswerte zu. Davon ausgenommen ist lediglich die Phase der Ausführung, während

¹⁸⁶⁵ Siehe hierzu unten, [VII](#).

derer sich die Vermögenswerte zwecks Abwicklung des Austauschgeschäfts in einem Smart Contract oder dergleichen befinden können, soweit solche Mechanismen vorgesehen sind.

- Das ausgeführte Austauschgeschäft, aber wenigstens der Nachweis des Austausches von Kryptovermögenswerten, wird im verteilten Register des dezentralen Netzwerks abgebildet.
- Ausserdem findet der Austausch atomistisch, d.h. ohne traditionelle Gegenparteirisiken statt.
- Schliesslich liegen auch die übrigen Eigenschaften dezentraler Systeme vor.¹⁸⁶⁶ Namentlich beruhen dezentrale Handelsplattformen auf offenen, interoperablen Protokollen. Hierzu gehört etwa die Eigenschaft, dass die Nutzung einer dezentralen Handelsplattform jeder Person unabhängig von einer Registrierung, Kontoeröffnung oder der Offenlegung der bürgerlichen Identität offensteht. Zudem können Dritte den Computercode dezentraler Handelsplattformen aufgrund der Quelloffenheit der Protokolle frei überprüfen.

Der soeben unternommene Definitionsversuch stellt in erster Linie auf technische und somit insb. formelle Aspekte ab. Der Begriff der Dezentralität ist sodann aber auch in materieller Hinsicht konkretisierungsbedürftig. Im zweiten Kapitel dieser Arbeit wurde Intermediation als die Zentralisierung von Kontrolle und Entscheidungsgewalt definiert.¹⁸⁶⁷ Dezentralität ist darum als eine Frage der verteilten Kontrolle bzw. dezentralen Entscheidungsautonomie zu verstehen. Im weiteren Verlauf dieser Arbeit soll der Dezentralität als Rechtsprinzip auf den Grund gegangen werden. Zuvor ist allerdings eine rechtliche Einordnung dezentraler Handelsplattformen in das Schweizer Finanzmarktrecht vorzunehmen.

¹⁸⁶⁶ Siehe diesbezüglich oben, [III.2.](#)

¹⁸⁶⁷ Siehe hierzu oben, [II.1.5.](#)

7. Zusammenfassung Kapitel IV

Das Kapitel zeigt im *ersten Abschnitt* auf, dass die vorliegende Arbeit von der Begriffsverwendung in den Materialien des Bundes leicht abweicht. Im Zentrum steht der Begriff der dezentralen Handelsplattform. Er bildet einen Sammelbegriff, der unterschiedliche Plattformkategorien vereint. Anders als der DLT-Bericht von 2018 des Bundesrates unterscheidet die vorliegende Arbeit namentlich nicht zwischen dezentralen Handelsplattformen und «verteilten Peer-to-Peer Plattformen». Dessen ungeachtet zeigt sich in den nachfolgenden Ausführungen, dass dezentrale Handelsplattformen in einer Vielzahl unterschiedlicher Erscheinungsformen auftreten (siehe unten).

Im *zweiten Teil* des Kapitels werden übersichtshalber die in der Literatur festgestellten Gemeinsamkeiten dezentraler Handelsplattformen erwähnt: Die Plattformen sind typischerweise non-custodial, die Abwicklung von Handelsgeschäften erfolgt on-chain und sie sind für jedermann über das Internet zugänglich. Es wird erwähnt, dass dezentrale Handelsplattformen in der Praxis sowohl als Protokoll als auch als Anwendung auftreten. Dezentrale Handelsplattformen erweisen sich sodann als historische Antwort auf die Mängel zentraler Handelsplattformen. Dabei haben dezentrale Handelsplattformen bereits einige Entwicklungsschritte durchlaufen.

Der *dritte Teil* setzt sich ausführlich mit den in der Realität feststellbaren Plattformkategorien auseinander. Dabei wird sichtbar, dass in der Praxis eine Vielzahl von Handelsplattformen unterschieden werden kann. Um die Unterschiede besser herauszuarbeiten, wird kurz auch auf die heute vorherrschenden zentralen Modelle eingegangen, welche klarerweise über eine Betreiberstruktur verfügen. Anschliessend werden die Funktionsweisen und der Kreis der beteiligten Parteien der unterschiedlichen Plattformkategorien an praktischen Beispielen erläutert. Geschlossen wird dieser Abschnitt mit einer tabellarischen Übersicht der Plattformkategorien anhand der Merkmale «Verwahrung», «Handel», «Abrechnung und Abwicklung» und «Zugang».

Darauf aufbauend werden im *vierten Abschnitt* die Gemeinsamkeiten und Unterschiede dezentraler Handelsplattformen herausgearbeitet. Es zeigt sich, dass insb. in Bezug auf die Handelsmechanik grosse Unterschiede bestehen können. Einige Plattformkategorien greifen bspw. auf ein Orderbuch zurück,

das typischerweise mit einem LOB-Matching-Modell gepaart wird. Andere Plattformkategorien basieren auf Liquiditätspools, wobei das Matching auf Grundlage einer Bonding Curve erfolgt.

Der *fünfte* Teil dieses Kapitels geht sodann ausführlich auf die Chancen und Risiken dezentraler Handelsplattformen ein. Im Wesentlichen führen dezentrale Handelsplattformen zu einer Verringerung traditioneller Gegenparti- und Systemrisiken. Sie ermöglichen aufgrund der Offenheit und Zugänglichkeit der Protokolle, dass die Inhaber von Kryptovermögenswerten ihre Handlungs- und Verfügungsrechte selbständig ausüben können. In der Folge lassen sich etwa traditionelle Verwahrungsriskien eliminieren. Dezentrale Systeme können sodann aufgrund ihrer Globalität die heute oftmals bestehende Fragmentierung des Handels und insb. der Liquidität verbessern. Schliesslich können dezentrale Systeme die Bedeutung politischer Entscheidungsprozesse relativieren, indem die Erfolgsaussichten von Rent-Seeking-Verhalten und Regulatory Capture verringert werden.

Demgegenüber weisen dezentrale Handelsplattformen auch eine Handvoll Risiken auf, welche teilweise im traditionellen Finanzsystem unbekannt sind oder aber in anderer Form auftreten. Einige dieser Risiken ergeben sich aus der Nutzung dezentraler Netzwerke als Grundlage für die Handelsplattform. Die Analyse bezieht die nachfolgenden spezifischen Risiken mit ein:

Die Öffentlichkeit verteilter Register bringt nicht nur eine Verbesserung der Handelstransparenz mit sich, sondern beinhaltet auch ein Transparenzrisiko: So können Arbitrageure und Miner bzw. Staker im Hinblick auf Transaktionen Frontrunning betreiben, das allerdings anders als in traditionellen Märkten auf öffentlichen Informationen beruht. Nicht jede Plattformkategorie ist gleich stark von solchen Praktiken betroffen. Sodann können auch Informationsrisiken aufgrund von Informationsasymmetrien bestehen. Ausgeprägt ist dieses Risiko beim Vorliegen von Admin Keys, welche einer bestimmten Gruppe von Personen privilegierte Eingriffsrechte im Zusammenhang mit Smart Contracts einräumen. Ferner scheinen Programmierfehler die Achillesferse von DeFi-Anwendungen zu sein. Verwundbarkeiten im Softwarecode führen in der Praxis regelmässig zu erfolgreichen Hackerangriffen mit grossen Vermögensschäden. Neben Smart Contract-Risiken bestehen sodann auch Plattformrisiken, welche ihren Ursprung im dezentralen Netzwerk haben. An dieser Stelle sei an potenzielle Re-Zentralisierungseffekte von Mining- und Staking-Aktivitäten erinnert. Sodann weisen dezentrale Systeme Systemrisiken auf, welche im traditionellen Finanzsystem nur bedingt existieren. Ein wichtiges Beispiel sind Composability Risiken, die sich aus der Zusammensetzung unterschied-

licher Applikationen, Protokolle und Smart Contracts ergeben können. Ein fehlerhafter Smart Contract kann theoretisch die Funktionsweise der weiteren mit ihm verbundenen Komponenten beeinträchtigen. Schliesslich spielen in dezentralen Systemen aufgrund der Gemeinschaftlichkeit der Verwaltung kollektive Handlungsprobleme eine grosse Rolle. Die Bereitstellung der Infrastruktur (d.h. Netzwerk oder Applikation) erfolgt typischerweise über kryptoökonomische Anreize. Im Bereich der Softwareentwicklung sind indessen die Motive für die Partizipation weniger eindeutig. Allerdings muss darauf geachtet werden, die Softwareentwicklung nicht ausschliesslich aus einem ökonomischen Blickwinkel zu betrachten.

Das vorliegende Kapitel *schliesst* mit dem Versuch, dezentrale Handelsplattformen in technischer Hinsicht zu definieren.

V. Rechtliche Einordnung dezentraler Handelsplattformen in das Schweizer Finanzmarktrecht

I think that the Internet is going to be one of the major forces for reducing the role of government. The one thing that's missing, but that will soon be developed, is a reliable e-cash, a method whereby on the Internet you can transfer funds from A to B without A knowing B or B knowing A. [...] That kind of thing will develop on the Internet and that will make it even easier for people using the Internet.

– Milton Friedman¹⁸⁶⁸

1. Vorbemerkungen

1.1 Einleitung

Die Frage nach dem anwendbaren Finanzmarktrecht ist in Zeiten, in denen regelmässig Finanzinstrumente übers Internet angeboten und Finanzdienstleistungen grenzüberschreitend erbracht werden, vorrangig. Im Bankenbereich sind «virtuelle Institute», die über eine Schweizer (Webseite-)Adresse und Telefonnummer verfügen, seit längerer Zeit ein Begriff, wobei den hiesigen Behörden in vielen Fällen die Hände gebunden sind.¹⁸⁶⁹ Auch verlassen Anleger auf der Suche nach Waren und Dienstleistungen zunehmend freiwillig ihre Heimatrechtsordnung.¹⁸⁷⁰ Die räumliche Segmentierung der Finanzmärkte entlang nationalstaatlicher Grenzen wird nach und nach von der «Transnatio-

¹⁸⁶⁸ National Taxpayers Union, Interview with Milton Friedman.

¹⁸⁶⁹ Vgl. etwa EBK, Jahresbericht 2003, 63.

¹⁸⁷⁰ Dabei fällt typischerweise die Konstellation, in der sich ein Kunde auf eigene Initiative an einen ausländischen Finanzdienstleister wendet, ausschliesslich unter das am Ort des Finanzdienstleisters geltende Finanzmarktrecht (reverse solicitation bzw. passive Dienstleistungsfreiheit); siehe hierzu Sethe, SZW 2014, 622–623; vgl. nunmehr auch Art. 2 Abs. 2 FID-LEV.

nalisierung des Vermögens» verdrängt.¹⁸⁷¹ Eine einzelstaatliche Betrachtungsweise verliert aufgrund dieser Entwicklungen zunehmend an Bedeutung.¹⁸⁷²

Diese Entwicklung kann etwa am Beispiel des US-amerikanischen Verfahrens gegen BitMEX, einer zentralisierten Handelsplattform für Derivate, die auf Kryptovermögenswerten geschrieben werden, veranschaulicht werden. Die Gesellschaften hinter BitMEX haben mit einer Ausnahme ihren Sitz ausserhalb den USA. Konkret wirft die CFTC der Derivateplattform vor, dass auch US-amerikanische Kunden die Derivate über das Internet erwerben konnten, ohne über die entsprechenden lokalen finanzmarktrechtlichen Bewilligungen zu verfügen.¹⁸⁷³ Die zentralisierte Kryptohandelsplattform Binance hat 2021 mit ihrem bisherigen Ansatz, überall auf der Welt über Domizile zu verfügen, ohne jedoch klar darzulegen, aus welcher Entität welche Dienstleistungen erbracht werden, ebenfalls die Aufsichtsbehörden auf den Plan gerufen.¹⁸⁷⁴

Dezentrale Systeme sind ein *inhärent* globales und grenzüberschreitendes Phänomen, das nur bedingt nach den im heutigen Recht geltenden Anknüpfungskriterien beurteilt werden kann.¹⁸⁷⁵ Dezentrale Netzwerke werden von einer Vielzahl von Computern an unterschiedlichen Standorten unterhalten;¹⁸⁷⁶ Kryptowährungen passieren in der Folge friktionslos das Territorium von Nationalstaaten und somit unterschiedliche Rechtsordnungen; ein Smart Contract ist schliesslich völlig gleichgültig gegenüber der Nationalität oder dem Domizil einer Person, die seine Funktionen abrufen. Gleichermassen sind dezentrale Handelsplattformen aufgrund ihrer offenen Natur grundsätzlich von überall aus zugänglich. Der Handel von Kryptovermögenswerten über solche Plattformen steht jeder Person offen, unabhängig von ihrem Wohnsitz, Sitz oder Aufenthaltsort. Ihre Identität spielt auch darüber hinaus keine Rolle.

¹⁸⁷¹ So Sethe/Lehmann, in: Tietje/Nowrot, § 15 Rz. 1, ferner Rz. 4.

¹⁸⁷² Vgl. bereits BIS/BCBS, Cross-Border Electronic Banking, 2–4; ferner BCBS/OGBS, Supervision of Cross-Border Banking, *passim*.

¹⁸⁷³ Siehe CFTC v. HDR Global Trading Limited et al., Civil Action Nr. 20-cv-8132, 1. Oktober 2020, 3 («BitMEX operated its trading platform in large part from the United States, and engaged in transactions with thousands of U.S. persons. BitMEX accepted bitcoin deposits worth more than billion from at least 85,000 user accounts with a U.S. nexus.»), 23–25.

¹⁸⁷⁴ Siehe Chipolina, We Need a Centralized Entity, Decrypt, *passim*.

¹⁸⁷⁵ Siehe etwa Kerkemeyer, ZHR 2020, 811–812 («Hier prallen die Netzwerklogik der Blockchain und die souveränitätsfixierte Logik des Völkerrechts aufeinander, weshalb ein Spannungsbogen entsteht, der sich nie vollständig auflösen lassen wird.»), 828; ferner Cambridge Centre for Alternative Finance, Legal and Regulatory Considerations, 34–35.

¹⁸⁷⁶ Gerade aber die *geografische* Verteilung der Nodes, aber auch anderer Computerinfrastrukturelemente scheint für US-Gerichte von gewisser Bedeutung zu sein; vgl. die Übersicht bei Levi/Drylewski/Michael, Borderless Worlds, *passim*.

Der Zugriff auf das dezentrale Netzwerk oder eine dezentrale Applikation ist grundsätzlich nicht einschränkbar. Davon ausgenommen ist der Zugriff auf eine Webseite, die als GUI fungiert und dem Nutzer den Zugang zu den Smart Contracts einer dezentralen Handelsplattform ermöglicht. Die Betreiber solcher Schnittstellen können die IP-Adressen von Personen aus bestimmten Ländern oder Regionen blockieren.¹⁸⁷⁷

Dezentralisierung stellt eine erhebliche Herausforderung für das öffentliche Recht dar.¹⁸⁷⁸ In der Folge stellen sich Fragen des nationalen und internationalen Wirtschaftskollisionsrechts. Darüber hinaus scheinen aber auch althergebrachte *finanzmarktrechtliche* Konzepte, wie etwa diejenigen des Finanzintermediärs oder der Gruppenbetrachtung als Ausfluss des Rechtsmissbrauchsverbots, an ihre Grenzen zu stossen.

1.2 Wirtschaftskollisionsrechtliche Aspekte

Im Völkerrecht gilt der Grundsatz, dass die Staatsgewalt die Gebiets- und Personalhoheit umfasst.¹⁸⁷⁹ Anders als im Zivilrecht¹⁸⁸⁰ fallen im Verwaltungsrecht die örtliche Zuständigkeit und das anwendbare Recht zusammen. Denn zur Anwendung kommt das Recht des Gemeinwesens, in dessen örtliche Zuständigkeit der fragliche Sachverhalt fällt.¹⁸⁸¹ Dabei richten sich die örtliche Zuständigkeit und das anwendbare Verwaltungsrecht in erster Linie nach dem *Territorialitätsprinzip* und sodann nach dem *Personalitätsprinzip*. Vorbehaltlich abweichender staatsvertraglicher Bestimmungen und hinreichend klarer Anordnung durch den Gesetzgeber gilt das Territorialitätsprinzip grundsätzlich für das Hoheitsgebiet des kommunalen, kantonalen oder eidgenössischen Gemeinwesens.¹⁸⁸² Die Zuordnung unter den Gemeinwesen bestimmt sich in erster Linie nach den Regeln der verfassungsrechtlichen Kompetenzordnung.

¹⁸⁷⁷ Siehe hierzu unten, VII.4.2b.iii.

¹⁸⁷⁸ So auch Jacquemart, Offene Blockchainsysteme, Rz. 533; ferner Bärtschi/Jacquemart/Meyer, in: Emmenegger, Zahlung und Verzug, 179, die von einer Durchbrechung institutioneller Schranken durch virtuelle Währungen sprechen. Vgl. hinsichtlich der vielen ungeklärten Fragen im *internationalen Privatrecht* Guillaume, in: Richa/Canapa, Smart contracts, 55; ferner Dickinson, in: Fox/Green, Conflict of Laws, N 5.07–5.12.

¹⁸⁷⁹ Siehe Kau, in: Graf Vitzthum/Proelf, Völkerrechtssubjekte, Rz. 154.

¹⁸⁸⁰ Vgl. etwa LugÜ und IPRG.

¹⁸⁸¹ Siehe Tschannen/Zimmerli/Müller, Allgemeines Verwaltungsrecht, § 24 N 5.

¹⁸⁸² Siehe Tschannen/Zimmerli/Müller, Allgemeines Verwaltungsrecht, § 24 N 3; Merkli, Territorialitätsprinzip, 4; BGE 133 II 331, E. 6.1; siehe auch BGE 95 II 109, E. 3c; 82 I 196, E. 1; 93 II 189, 191.

gen des Bundes und der Kantone.¹⁸⁸³ Dabei ist die Zuordnung zu einem Gemeinwesen selbst bei reinen Binnensachverhalten nicht immer einfach.¹⁸⁸⁴

Nach dem Territorialitätsprinzip knüpft das Verwaltungsrecht typischerweise an den Wohnsitz, die Niederlassung oder den Aufenthalt einer Person, den Ort der Ausübung einer bestimmten Aktivität bzw. Tätigkeit oder den Ort der gelegenen Sache an.¹⁸⁸⁵ Man spricht in diesem Zusammenhang von Anknüpfungspunkten, die einen hinreichenden Bezug oder Nähe (sog. *Genuine Link*) zu einem Territorium schaffen und damit die Anwendbarkeit des Verwaltungsrechts rechtfertigen.¹⁸⁸⁶

Eine spezielle Ausprägung des Territorialitätsprinzips stellt das *Auswirkungsprinzip* dar, das vom Bundesgericht ursprünglich im Wettbewerbs- und Kartellrecht entwickelt wurde,¹⁸⁸⁷ aber inzwischen auch für andere Rechtsgebiete des öffentlichen Rechts Geltung beansprucht.¹⁸⁸⁸ Bestimmungen, die auf dem Auswirkungsprinzip beruhen, sollen in der Regel die Erbringung grenzüberschreitender Dienstleistungen durch ausländische Unternehmen abdecken, die aktiv einen lokalen Markt erschliessen, und die potenziellen negativen Externalitäten eindämmen, die ihren Ursprung in der Tätigkeit dieser Unternehmen mit Sitz im Ausland haben.¹⁸⁸⁹

¹⁸⁸³ Siehe Reich, in: Biaggini/Gächter/Kiener, Staatsrecht, § 12 N 1–2; für den Kanton Zürich Jaag/Rüssli, Staats- und Verwaltungsrecht Kanton Zürich, Rz. 2303, wo auch auf die Bedeutung des kantonalen Gesetzesrechts hingewiesen wird.

¹⁸⁸⁴ Siehe Tschannen/Zimmerli/Müller, Allgemeines Verwaltungsrecht, § 24 N 4.

¹⁸⁸⁵ Siehe Häfelin/Müller/Uhlmann, Allgemeines Verwaltungsrecht, Rz. 310; Tschannen/Zimmerli/Müller, Allgemeines Verwaltungsrecht, § 24 N 5 m.w.H.

¹⁸⁸⁶ Siehe Merkli, Territorialitätsprinzip, 3; von Arnald, Völkerrecht, Rz. 346; Jarass, RIW 2017, 643.

¹⁸⁸⁷ Siehe BGE 93 II 192, E. 3 («*Cette disposition doit dès lors réprimer les entraves à la concurrence d'où qu'elles viennent, dès qu'elles ont un effet direct sur le jeu de la concurrence à l'intérieur du territoire suisse.*»); vgl. nunmehr in kodifizierter Form Art. 2 Abs. 2 KG: «Das Gesetz ist auf Sachverhalte anwendbar, die sich in der Schweiz auswirken, auch wenn sie im Ausland veranlasst werden.»; ferner BGE 127 III 219, E. 3a, der zudem von einer «*contrôle préventif*» im Hinblick auf Unternehmenszusammenschlüsse spricht; sodann ausführlich unter Berücksichtigung völkerrechtlicher Prinzipien BGer 2C_180/2014 vom 28. Juni 2016, E. 3.2–3.7 m.w.H. In Bezug auf unlautere Handlungen vgl. schliesslich BGE 82 II 159, E. 2c und 3.; 89 II 422, E. 4b.

¹⁸⁸⁸ Siehe Häfelin/Müller/Uhlmann, Allgemeines Verwaltungsrecht, Rz. 311–313; siehe etwa BGE 133 II 331, E. 6.1; 138 II 346, E. 3.3; für das interkantonale Verhältnis vgl. etwa BGE 118 Ia 137, E. 2b und 2c; 125 I 474, E. 1d.

¹⁸⁸⁹ Vgl. in *allgemeiner* Hinsicht Martiny, in: Basedow/Hopt/Kötz, Anknüpfung 389; Schnyder, Wirtschaftskollisionsrecht, Rz. 163–164; in Bezug auf *finanzmarktrechtliche* Sachverhalte Sethe, in: Gericke, Drittstaatenzugang, 139; ferner Eggen/Schaefer, GesKR 2013, 373;

Gemäss Rechtsprechung genügt jedoch nicht jede Auswirkung für die Anwendbarkeit des öffentlichen Rechts, sondern im Ausland eintretende Ereignisse müssen sich «in einem ausreichenden Mass» auf dem Territorium der Schweiz bzw. des betreffenden Gemeinwesens auswirken.¹⁸⁹⁰ Ist dieses Mass nicht erreicht, kann schweizerisches öffentliches Recht nur dann auf Sachverhalte, die sich im Ausland zutragen, zur Anwendung gelangen, wenn sich dies aus einer Rechtsnorm hinreichend klar ergibt.¹⁸⁹¹ In politisch heiklen Bereichen, wie etwa dem schweizerischen Bankkundengeheimnis vor dem Hintergrund der Besteuerung ausländischer Bürger, kann es schliesslich zu ausgeprägten Anwendungskonflikten kommen, wenn sowohl die ausländische als auch die schweizerische Rechtsordnung die Anwendbarkeit für sich beanspruchen.¹⁸⁹²

Die Geltung des orts- oder auswirkungsorientierten Territorialitätsprinzips alleine sagt allerdings noch nichts über die (allenfalls extraterritoriale) Durchsetzbarkeit der anwendbaren Regeln aus. Damit wird die im Völkerrecht anerkannte Unterscheidung zwischen «*jurisdiction to prescribe*» und «*jurisdiction to enforce*» angesprochen.¹⁸⁹³

1.3 Anknüpfung an den Finanzintermediär

Die schweizerischen Finanzmarktgesetze verwenden den Begriff der Finanzintermediation nicht unmittelbar.¹⁸⁹⁴

Jutzi/Schären, GesKR 2019, 415; ausführlich zum Ganzen in Bezug auf die *internationale Bankenregulierung* Herdegen, International Economic Law, 556–562.

¹⁸⁹⁰ Siehe BGE 133 II 331, E. 6.1; 93 II 192, E. 3 («[...] *un effet direct sur le jeu de la concurrence à l'intérieur du territoire suisse*»); siehe ferner im interkantonalen Verhältnis BGE 118 Ia 137, E. 2c («*ausreichend erhebliche Berührung*») und BGE 125 I 474, E. 1d bb («*en rapport avec le territoire cantonal de manière importante*»); vgl. demgegenüber, allerdings unter Berücksichtigung des präventiven Charakters der Unternehmenszusammenschlusskontrolle BGE 127 III 219, E. 5a («*effets potentiels déterminants sur le marché suisse*»).

¹⁸⁹¹ Siehe BGE 133 II 331, E. 6.1; fürs deutsche Recht Jarass, RIW 2017, 643–644.

¹⁸⁹² Vgl. etwa zur Kundendatenherausgabe durch die UBS an die USA Ender/von der Crone, SZW 2010, 513–517.

¹⁸⁹³ Siehe für dieses Konzept in der Marktmissbrauchsverordnung der EU Sethe/Lehmann, in: Tietje/Nowrot, § 15 Rz. 158.

¹⁸⁹⁴ Eine Ausnahme bildete die Verordnung über die berufsmässige Finanzintermediation (VBF) vom 18. November 2009, die allerdings per 1. Januar 2016 aufgehoben wurde. Die VBF wurde materiell per 1. Januar 2016 in die Geldwäschereiverordnung (GwV) überführt. Der Begriff der Finanzintermediation verschwand in der Folge allerdings.

Das Geldwäschereigesetz, dessen persönlicher Geltungsbereich Finanzintermediäre und Händler umfasst, enthält allerdings eine zweifache kategoriale Umschreibung der *Personen*, welche die Finanzintermediation betreiben und somit formell als Finanzintermediäre gelten. Art. 2 Abs. 2 GwG enthält eine abschliessende Aufzählung von Bewilligungsträgern, wie etwa Banken, Vermögensverwaltern, Versicherungen¹⁸⁹⁵, Wertpapierhäusern und Zahlungssystemen¹⁸⁹⁶, die als Finanzintermediäre i.e.S. gelten.¹⁸⁹⁷ Art. 2 Abs. 3 GwG bietet sodann durch die Formulierung einer Generalklausel der Finanzintermediation eine uneigentliche Legaldefinition des Finanzintermediärs an.¹⁸⁹⁸ Es handelt sich dabei um *Personen, die berufsmässig fremde Vermögenswerte annehmen oder aufbewahren oder helfen, sie anzulegen oder zu übertragen*. Bei Personen nach Art. 2 Abs. 3 GwG (Finanzintermediäre i.w.S.) handelt es sich um Personen, die keiner Bewilligungspflicht nach einem Finanzmarktgesetz unterstehen.¹⁸⁹⁹ Darüber hinaus enthält das Gesetz eine Ausnahme für gewisse Personen, die zwar faktisch die Finanzintermediation ausüben, aber aus anderen Gründen nicht unter das Gesetz fallen sollen (Art. 3 Abs. 4 GwG).

Es stellt sich die Frage, ob Bewilligungsträger nach Art. 2 Abs. 2 GwG *unabhängig* von ihrer konkreten Tätigkeit der Geldwäschereiregulierung unterstellt sind. Dies ist klarerweise zu verneinen, bezweckt das GwG doch die Verhinderung der Geldwäscherei und der Terrorismusfinanzierung sowie die Sicherstellung der Sorgfalt bei Finanzgeschäften (siehe Art. 1). Im Endeffekt will das GwG ausschliesslich Tätigkeiten des Finanzsektors erfassen, die ein typisches Geldwäschereirisiko aufweisen.¹⁹⁰⁰ Das Konzept der Finanzintermediation in Art. 2 Abs. 3 GwG muss nach vorliegender Auffassung aus Rechtssicherheitsgründen auch einschränkende Bedeutung für die Unterstellung von Finanzintermediären i.e.S. haben. Der Finanzintermediationsbegriff grenzt mit anderen

¹⁸⁹⁵ Versicherungen, welche die direkte Lebensversicherung betreiben oder Anteile einer kollektiven Kapitalanlage anbieten oder vertreiben, sind vom GwG erfasst (Art. 2 Abs. 2 lit. c GwG).

¹⁸⁹⁶ Zahlungssysteme, die nach Art. 4 Abs. 2 FinfraG eine Bewilligung der FINMA benötigen, sind vom GwG erfasst (Art. 2 Abs. 2 lit. d^{ter} GwG). Ein Zahlungssystem benötigt jedoch nur dann eine Bewilligung der FINMA, wenn die Funktionsfähigkeit des Finanzmarkts oder der Schutz der Finanzmarktteilnehmer es erfordern und das Zahlungssystem nicht durch eine Bank betrieben wird.

¹⁸⁹⁷ Siehe SHK GwG-Schären, Art. 2 N 2, 6–8.

¹⁸⁹⁸ Siehe hinsichtlich der Frage der *Legaldefinition* Nagel, Geltungsbereich GwG, Rz. 183 m.w.N.; ferner SHK GwG-Schären, Art. 2 N 2.

¹⁸⁹⁹ Siehe SHK GwG-Schären, Art. 2 N 2–3, 53; Graber/Oberholzer, Kommentar GwG, Art. 2 N 10.

¹⁹⁰⁰ GLM. SHK GwG-Schären, Art. 2 N 9, 62 inkl. FN 57; OFK GwG-Wyss, Art. 2 N 15.

Worten vorbehaltlich einer ausdrücklichen abweichenden Regelung im Gesetz den sachlichen Geltungsbereich des GwG für *sämtliche* unterstellten Finanzintermediäre ein.¹⁹⁰¹

Ferner bezeichnet der Gesetzgeber im Finanzdienstleistungsgesetz Bewilligungsträger nach dem BankG, FINIG und KAG als *Finanzintermediäre*.¹⁹⁰² Danach gelten etwa Banken, Vermögensverwalter, Wertpapierhäuser, SICAVs und Depotbanken von vertraglichen Anlagefonds als Finanzintermediäre. Der Begriff wird hier allerdings breiter verwendet, gelten doch nach GwG bspw. auch zentrale Gegenparteien und Zentralverwahrer nach FinfraG oder – je nach Tätigkeit – Versicherungen nach VAG als Finanzintermediäre.

Schliesslich findet sich auch im Finanzmarktinfrastrukturgesetz der Begriff des Finanzintermediärs wieder.¹⁹⁰³ Das FinfraG verwendet ihn offenbar, um Finanzmarktinfrastrukturen von Finanzintermediären abzugrenzen. Nach diesem Begriffsverständnis stellen Börsen, multilaterale Handelssysteme, zentrale Gegenparteien, Zentralverwahrer, DLT-Handelssysteme, Transaktionsregister und Zahlungssysteme Finanzmarktinfrastrukturen und somit keine Finanzintermediäre dar.¹⁹⁰⁴ Diese begriffliche Zweiteilung steht grundsätzlich im Einklang mit dem FIDLEG und FINIG. Demgegenüber vertritt das GwG einen anders gelagerten Finanzintermediationsbegriff, denn Handelsplätze und Transaktionsregister werden mangels einer Tätigkeit mit Geldwäschereirisiko nicht erfasst. Etwas anderes gilt für DLT-Handelssysteme, die neu Funktionen ausüben können, welche bisher Zentralverwahrern und Zahlungssystemen vorbehalten waren. Zudem können Retail-Kunden je nach Ausgestaltung direkt an einem DLT-Handelssystem teilnehmen, was nach Auffassung des Bundesrates eine Unterstellung unter das GwG notwendig macht.¹⁹⁰⁵

Ungeachtet dieser Abgrenzungen in Einzelgesetzen dient der Begriff des Finanzintermediärs als *generischer Anknüpfungspunkt* für die Finanzmarktregulierung. Es ist demnach so, dass überall dort, wo ein Finanzintermediär eine Tätigkeit ausübt, potenziell ein Regulierungsanlass besteht. Freilich hat der Geltungsbereich eines Finanzmarktgesetzes im Einzelfall immer vor des-

¹⁹⁰¹ So wohl auch GwG-Schären, Art. 2 N 9, der zudem davon ausgeht, dass die Generalklausel resp. die Spezialtatbestände in Art. 2 Abs. 3 GwG als «Anhaltspunkt» dienen können; sodann auch Nagel, Geltungsbereich GwG, Rz. 199, 220; vgl. ferner OFK GwG-Wyss, Art. 2 N 15, 31; Graber/Oberholzer, Kommentar GwG, Art. 2 N 3.

¹⁹⁰² Siehe z.B. Art. 4 Abs. 3 lit. a FIDLEG, der *Finanzintermediäre* nach dem BankG, dem FINIG und dem KAG als «professionelle Kunden» definiert.

¹⁹⁰³ Siehe etwa Art. 22 und 120 Abs. 2 FinfraG.

¹⁹⁰⁴ Siehe die Legaldefinition einer Finanzmarktinfrastuktur in Art. 2 lit. a FinfraG.

¹⁹⁰⁵ Siehe Botschaft DLT 2019, 306.

sen spezifischen Schutzziel eingegrenzt zu werden: So muss eine Bank den Vermieter ihrer Büroräumlichkeiten mangels Geldwäschereirisikos nicht nach den Vorgaben in Art. 3 GwG identifizieren. Ferner hat die Eigen- bzw. Selbstemission von Aktien durch einen Finanzintermediär mangels Bezugs zum Finanzdienstleistungsmarkt nicht zur Folge, dass dieser in der Funktion eines Finanzdienstleisters im Sinne von Art. 3 lit. d FIDLEG gegenüber den Investoren auftritt.

1.4 Anknüpfung an den ausländischen Finanzintermediär

Das Bundesgericht hat in Bezug auf den Geltungsbereich finanzmarktrechtlicher Erlasse in mehreren Urteilen festgehalten, dass in der – allenfalls extraterritorialen – Anwendung aufsichtsrechtlicher Bestimmungen «[...] keine Verletzung der ausländischen Souveränität [liegt], ist die Schweiz doch befugt, die Folgen einer Geschäftstätigkeit, die auf ihrem Territorium ausgeübt wird, von diesem ausgeht oder sich auf dieses auswirkt, zu regeln, auch wenn die entsprechende Aktivität einer ausländischen Gesellschaft zuzuschreiben ist [...]».¹⁹⁰⁶

Somit kommen im schweizerischen Finanzmarktrecht grundsätzlich ebenfalls die im Verwaltungsrecht etablierten Territorialitäts- und Auswirkungsprinzipien zur Anwendung.¹⁹⁰⁷ Im Rahmen der Anwendung des Auswirkungsprinzips sind jedoch «schutzwürdige schweizerische Interessen» zu wahren – dies unter Berücksichtigung der in den Finanzmarktgesetzen statuierten Schutzziele.¹⁹⁰⁸

Typischerweise knüpft das schweizerische Aufsichtsrecht an den Finanzintermediär an, von welchem eine unterstellungspflichtige Aktivität nach Schweizer Recht ausgeht. Dies gilt im Prinzip auch für den ausländischen Finanzintermediär. Dabei setzt der räumliche Geltungsbereich der meisten Finanzmarktgesetze eine physische Präsenz in der Schweiz voraus, die in aller Regel von einer

¹⁹⁰⁶ BGE 130 II 351, E. 6.1; ferner 125 II 450, E. 2c und 2d; 108 Ib 513, E. 2b; BGer 2A.320/2001 vom 5. Dezember 2001, E. 5b; siehe in Bezug auf den räumlichen Geltungsbereich des GwG auch den unveröffentlichten Entscheid BGer 2A.91/2005 vom 9. Februar 2006, E. 5.2 (zit. in EBK-Bulletin 49/2006, 62–63).

¹⁹⁰⁷ GL.M. mit Blick auf das GwG Zysset/Nagel, GesKR 2018, 143 m.w.N.; allgemein, aber differenzierend hinsichtlich des völkerrechtlichen Territorialitätsprinzips Kronke/Haubold, in: Kronke/Melis/Kuhn, Teil L Rz. 1, 43–47.

¹⁹⁰⁸ Siehe BGE 130 II 351, E. 6.1, ferner E. 5.3.5, 6.2.4; ferner BVGer B-5081/2012, B-5073/2012 vom 24. September 2014, E. 4.3.5; verneint in Bezug auf das Interesse an der Verkehrssicherheit in der Schweiz in BGE 133 II 331, E. 6.2.

gewissen Dauerhaftigkeit sein muss.¹⁹⁰⁹ Es kann sich dabei – abgesehen von einer Tochtergesellschaft – um eine Zweigniederlassung oder eine Vertretung des ausländischen Finanzintermediärs in der Schweiz handeln.¹⁹¹⁰ Die vom Ausland aus *grenzüberschreitend* erbrachte Finanzdienstleistung war – insb. mit Ausnahme des Vertriebs bzw. Angebots ausländischer kollektiver Kapitalanlagen und strukturierter Produkte in der Schweiz und von der Schweiz aus¹⁹¹¹ sowie gewisser Formen der Versicherungstätigkeit¹⁹¹² – bis zur Einführung des FIDLEG kaum je erfasst.¹⁹¹³

Unter FIDLEG ist jedoch nunmehr die grenzüberschreitende Erbringung von Finanzdienstleistungen mit Ausnahme von Konstellationen der Reverse Solicitation Gegenstand des schweizerischen Aufsichtsrechts.¹⁹¹⁴ Im Bereich grenzüberschreitender Aktivitäten wird damit vom bisherigen Erfordernis einer dauerhaften physischen Präsenz in der Schweiz für die Anwendbarkeit schweizerischen Rechts abgewichen.¹⁹¹⁵

Ähnliches gilt für ausländische Finanzintermediäre, die nach ausländischem Recht konstituiert worden sind, d.h. weder einen Wohnsitz in der Schweiz haben noch im Handelsregister eingetragen sind, und eine unterstellungspflichtige faktische Struktur hierzulande unterhalten, ohne aber für letzteres eine Bewilligung der Finanzmarktaufsichtsbehörde einzuholen. In diesem Fall wird regelmässig – in relativ unspezifischer Weise – von einer *faktischen Zweignie-*

¹⁹⁰⁹ Siehe ausführlich hinsichtlich Banken und Effektenhändler unter altem Recht du Pasquier/Fischer, GesKR 2010, 437–443; SK FIDLEG-Sethe/Aggteleky, Art. 3 lit. d N 9; hinsichtlich Geldwäschereirecht FINMA-RS 2011/1 «Tätigkeit als Finanzintermediär nach GwG», Rz. 28.3–28.4 («dauernd»).

¹⁹¹⁰ Siehe etwa für *ausländische Banken* Art. 2 Abs. 2 BankG i.V.m. Art. 2 Abs. 1 ABV-FINMA; für *ausländische Finanzinstitute* Art. 52 und 58 FINIG; für *ausländische Finanzintermediäre* Art. 2 Abs. 1 lit. a GwV und FINMA-RS 2011/1 «Tätigkeit als Finanzintermediär nach GwG», Rz. 28.3–28.4.

¹⁹¹¹ Art. 120 KAG bzw. Art. 5 aKAG; vgl. hierzu und darüber hinaus zum Auswirkungsprinzip Frick/Aggteleky, CapLaw-2015–59, *passim*.

¹⁹¹² Vgl. Art. 2 Abs. 1 lit. b VAG.

¹⁹¹³ Siehe du du Pasquier/Fischer, GesKR 2010, 449; Bahar/Nedwed, SZW 2019, 622, 624–625; Abegglen/Andreotti, GesKR 2020, 44; BSK BankG-Bahar/Stupp, Art. 1 N 85; in Bezug auf das aBEHG BSK-FINMAG/FinfraG-Watter, Art. 1 N 28–29; UK KSt GwG, Rz. 353.

¹⁹¹⁴ Siehe Art. 3 lit. c und d FIDLEG i.V.m. Art. 2 FIDLEV.

¹⁹¹⁵ Siehe Bahar/Nedwed, SZW 2019, 628 («[...] das schweizerische Finanzmarktrecht erhält eine klare extraterritoriale Wirkung.»), ferner 638, wo die Autoren zu Recht die Schliessung des schweizerischen Finanzmarkts bedauern; sodann Schleiffer/Schärli, GesKR 2020, 24, ferner 35, wobei die Autoren weniger skeptisch hinsichtlich Abschottungstendenzen sind. Ausführlich zu den Änderungen SK FIDLEG-Sethe/Aggteleky, Art. 3 lit. d N 19–21, 34; kritisch demgegenüber auch Abegglen/Andreotti, GesKR 2020, 44.

derlassung gesprochen.¹⁹¹⁶ Die FINMA kann etwa gegen Unternehmen, die in der Schweiz über keinen statutarischen oder gesellschaftsvertraglichen Sitz verfügen, aber dennoch faktisch in oder von der Schweiz aus verwaltet werden, vorgehen, d.h. diese ins Handelsregister eintragen lassen und anschliessend liquidieren.¹⁹¹⁷ Unternehmen, die im Ausland ihren statutarischen oder gesellschaftsvertraglichen Sitz haben, unterstehen etwa dem Bankengesetz, wenn ihre Willensbildung organisiert und regelmässig in der Schweiz erfolgt oder für sie hier eine organisierte regelmässige Tätigkeit ausgeübt wird.¹⁹¹⁸ Hierunter fallen nicht nur faktische Zweigniederlassungen (bzw. faktische Vertretungen), sondern auch sog. *Shell Banks*, deren Führung tatsächlich von der Schweiz aus erfolgt, die hierzulande aber über keine Bankbewilligung verfügen.¹⁹¹⁹ Die Auslandsbankenverordnung-FINMA sieht eine explizite Regelung dieser Konstellation für ausländische Banken vor: «Wird die ausländische Bank tatsächlich in der Schweiz geleitet oder wickelt sie ihre Geschäfte ausschliesslich oder überwiegend in oder von der Schweiz aus ab, so muss sie sich nach schweizerischem Recht organisieren und untersteht den Bestimmungen über die inländischen Banken.»¹⁹²⁰ In diesem Fall kommt die ausländische Bank nicht in den Genuss der liberalen Bestimmungen der ABV-FINMA betreffend grenzüberschreitende Bankdienstleistungen.¹⁹²¹ Die damit verbundene Abweichung von der privatrechtlichen Inkorporationstheorie gemäss Art. 154 Abs. 1 IPRG wird mit Anleger- und Funktionsschutzgründen im Aufsichtsrecht begründet.¹⁹²² Die von der FINMA zu ergreifenden Massnahmen gegen faktische Zweigniederlassungen haben mit Blick auf die Schutzziele der Regulierung angemessen zu sein und dürfen nicht zu einem überbordenden Extraterritorialismus schweizerischer Ausprägung führen.¹⁹²³

¹⁹¹⁶ Vgl. etwa für die Begriffsverwendung im Geldwäschereirecht FINMA-RS 2011/1 «Tätigkeit als Finanzintermediär nach GwG», Rz. 28.3–28.4; siehe hierzu SHK GwG-Schären, Art. 2 N 69–71; ferner Zysset/Nagel, GesKR 2018, 145. Demgegenüber differenzierend Art. 2 Abs. 1 ABV-FINMA klar zwischen (faktischer) Zweigniederlassung und (faktischer) Vertretung.

¹⁹¹⁷ Siehe z.B. BGE 130 II 351, E. 6.1; 126 II 71, E. 5b cc) und dd); vgl. ferner BGer 2A.65/2002 vom 22. Mai 2002, E. 5.2.3 und 5.3.1; BGer 2A.565/2002 vom 2. April 2003, E. 4.3.

¹⁹¹⁸ Siehe BGE 130 II 351, E. 5.1.

¹⁹¹⁹ Siehe z.B. BGer 2A.127/2007 und 2A.717/2006 vom 11. Oktober 2007, E. 6.1–6.3; vgl. zur Abgrenzung von *Shell Branches* zu *Shell Banks* du Pasquier/Fischer, GesKR 2010, 439–440.

¹⁹²⁰ Art. 1 Abs. 2 ABV-FINMA.

¹⁹²¹ Siehe BSK BankG-Chapuis, Art. 2 N 5.

¹⁹²² Siehe BGE 130 II 351, E. 6.1, 6.2.5; hinsichtlich Inkorporations- und Sitztheorie EBK Bulletin 29/1995, 29–30; Merkli, Territorialitätsprinzip, 13; Wyss/Zulauf, in: Spühler, Fiktiver Sitz oder faktische Zweigniederlassung, 134–137.

¹⁹²³ So das Bundesgericht in BGE 130 II 351, E. 6.1 («[...] es liegt in erster Linie an den ausländischen Behörden, für die Einhaltung ihres Rechts und ihrer Verpflichtungen zu sorgen.»).

Mit Blick auf dezentrale Handelsplattformen ist allenfalls insb. der Betrieb einer Finanzmarktinфраstruktur von Bedeutung. Diesbezüglich sieht das anwendbare Finanzmarktrecht ausdrückliche Vorschriften für die Bewilligung ausländischer Teilnehmer an Schweizer Handelsplätzen¹⁹²⁴ sowie die Anerkennung ausländischer Finanzmarktinфраstrukturen (konkret: Handelsplätze, zentrale Gegenparteien und Transaktionsregister)¹⁹²⁵ durch die FINMA vor. Sodann spielt das Auswirkungsprinzip eine bedeutende Rolle in der internationalen Derivatregulierung.¹⁹²⁶ Ferner enthält auch das Nationalbankengesetz eine Vorschrift, dass systemisch bedeutsame Finanzmarktinфраstrukturen mit Sitz im Ausland u.U. Schweizer Recht unterstehen.¹⁹²⁷

1.5 Anknüpfung an die arbeitsteilig vorgehende Gruppe

Das Bundesgericht und Bundesverwaltungsgericht sowie die FINMA haben in ständiger Rechtsprechung bzw. Aufsichtspraxis einen Gruppenbegriff entwickelt, der im gesamten Finanzmarktaufsichtsrecht zur Anwendung gelangt.¹⁹²⁸ Danach sollen staatliche Bewilligungspflicht und Aufsicht nicht dadurch *umgangen* werden können, dass jedes einzelne Unternehmen bzw. die dahinterstehenden Personen für sich allein nicht alle Voraussetzungen für die Bewilligungspflicht erfüllen, im Ergebnis *gemeinsam* aber dennoch eine bewilligungspflichtige Tätigkeit ausüben.¹⁹²⁹

Rechtsdogmatisch scheint dieser Auffassung das Verbot des Rechtsmissbrauchs zugrunde zu liegen. Demnach verdient die missbräuchliche Berufung auf eine zivilrechtliche, jedoch wirtschaftlich nicht gewollte Rechtsgestaltung keinen Schutz.¹⁹³⁰ Dieses im Aktien- und Steuerrecht etablierte Rechtskonzept

¹⁹²⁴ Art. 40 FinfraG.

¹⁹²⁵ Art. 41, 60 und 80 FinfraG.

¹⁹²⁶ Siehe hierzu Kuhn, SZW 2014, 375–377.

¹⁹²⁷ Art. 19 Abs. 2 NBG.

¹⁹²⁸ Vgl. hierzu insb. Jutzi/Schären, GesKR 2012, 413–415.

¹⁹²⁹ Siehe BGE 136 II 43, E. 4.3; ferner BGE 135 II 356, E. 3.2; BGer 2C_1055/2014 vom 2. Oktober 2015, E. 1.3.2.5, 2.2; 2C_729/2020 vom 5. August 2021, E. 4.3.2; 2C_74/2009 vom 22. Juni 2009, E. 2.2.2; 2A.332/2006 vom 6. März 2007, E. 5.2.4.

¹⁹³⁰ Siehe BGE 136 II 43, E. 4.3.3; BGer 2C_1055/2014 vom 2. Oktober 2015, E. 1.3.2.5; 2C_929/2010 vom 13. April 2011, E. 2.2.; 2C_352/2016 vom 9. Dezember 2016, E. 3.2. («konstruierte zivilrechtliche Rechtsgestaltungen»); vgl. aber auch Nobel, SJZ 2017, 467–468 m.w.N., wonach die wirtschaftliche Betrachtungsweise, da sie auf das beabsichtigte Wirkungspotenzial abstellt, «Teil einer teleologischen Interpretation» ist; ferner Kunz, recht 2017, 152 m.w.N., der ebenfalls eine Abgrenzung zur Rechtsumgehung vornimmt.

wird somit in die Finanzmarktaufsicht übernommen.¹⁹³¹ Die Aufsicht und Gerichte wenden in der Folge eine *einheitliche wirtschaftliche Betrachtungsweise* des Sachverhalts an (substance over form).¹⁹³² Darüber hinaus argumentiert das Bundesgericht auch mit dem Gebot der rechtsgleichen Behandlung der Marktteilnehmer.¹⁹³³

Anleger- und Funktionsschutz gemäss Art. 4 FINMAG rechtfertigen trotz formaljuristischer Trennung der Strukturen finanzmarktrechtlich eine einheitliche wirtschaftliche Betrachtungsweise, «[...] falls zwischen den einzelnen Personen und/oder Gesellschaften enge wirtschaftliche (finanzielle/geschäftliche), organisatorische oder personelle Verflechtungen bestehen und vernünftigerweise einzig eine Gesamtbetrachtung den faktischen Gegebenheiten und der Zielsetzung der Finanzmarktaufsicht gerecht wird [...]».¹⁹³⁴ Ein gruppenweises Handeln kann insb. dann vorliegen, «[...] wenn die Beteiligten gegen aussen als Einheit auftreten bzw. aufgrund der Umstände (Verwischen der rechtlichen und buchhalterischen Grenzen zwischen den Beteiligten; faktisch gleicher Geschäftssitz; wirtschaftlich unbegründete, verschachtelte Beteiligungsverhältnisse; zwischengeschaltete Treuhandstrukturen) davon auszugehen ist, dass koordiniert – ausdrücklich oder stillschweigend arbeitsteilig und zielgerichtet – eine gemeinsame Aktivität im aufsichtsrechtlichen Sinn ausgeübt wird [...]».¹⁹³⁵

Dezentrale Systeme weisen *prima facie* Parallelen zu gruppenmässig erbrachten Finanzdienstleistungen auf, weshalb an verschiedenen Stellen auf die Rechtsprechung des Bundesgerichts zurückzukommen sein wird.¹⁹³⁶ Da die einzelnen Beiträge zudem in aller Regel (auch) im Ausland erbracht werden, stellt sich in erster Linie die Frage der Geltung und Anwendbarkeit der schweizerischen Finanzmarktgesetze. In einem kürzlich ergangenen Urteil hat das Bundesgericht die Auffassung der FINMA geschützt, wonach schweizerisches Aufsichtsrecht auf ein unbewilligtes Emissionshaus zur Anwendung gelangte, obwohl die Gruppenmitglieder überwiegend im Ausland domiziliert waren.¹⁹³⁷

¹⁹³¹ Vgl. zum aktienrechtlichen Durchgriff BGE 132 III 489, E. 3.2 m.w.N.; zur Steuerumgehung im Steuerrecht BGE 138 II 239, E. 4.1.

¹⁹³² Siehe Jutzi/Schären, GesKR 2012, 415.

¹⁹³³ Siehe BGE 136 II 43, E. 4.3.3 («besser gestellt»); ferner BGer 2C_30/2011 und 2C_543/2011 vom 12. Januar 2012, E. 3.1.2.

¹⁹³⁴ BGE 136 II 43, E. 4.3.1.

¹⁹³⁵ BGE 136 II 43, E. 4.3.1.

¹⁹³⁶ Siehe etwa unten, [V.2.10b](#).

¹⁹³⁷ Siehe BGer 2C_729/2020 vom 5. August 2021, E. 5.2.

Nachfolgend erfolgt, ungeachtet der konkreten Unterstellung dezentraler Handelsplattformen unter das schweizerische Rechts- und Aufsichtsregime im Einzelfall, eine theoretische Einordnung solcher Plattformen *de lege lata*.

2. Geldwäschereirecht

2.1 Einleitung

Das Geldwäschereigesetz (GwG) regelt gemäss seinem Art. 1 die Bekämpfung der Geldwäscherei im Sinne von Art. 305^{bis} StGB, die Bekämpfung der Terrorismusfinanzierung im Sinne von Art. 260^{quinquies} Abs. 1 StGB und die Sicherstellung der Sorgfalt bei Finanzgeschäften. Der Zweck des Geldwäschereirechts liegt nach Aussage in der originalen Botschaft «ausschliesslich» in der Bekämpfung der Geldwäscherei.¹⁹³⁸ Der Schutzzweck wurde nach den Terroranschlägen um «9/11» sodann um die Bekämpfung der Terrorismusfinanzierung ergänzt.¹⁹³⁹ In den Materialien und der Literatur wird die Zielsetzung des GwG in aller Regel dem Funktionsschutz des Finanzmarktrechts zugeordnet.¹⁹⁴⁰ Daneben, und häufig sogar vorrangig, dienen die aufsichtsrechtlichen Vorschriften des GwG den Interessen der Strafverfolgung.¹⁹⁴¹

2.2 Geldwäscherei- und Terrorismusfinanzierungsrisiko

a. Kryptowährungen

Praktisch seit Anbeginn ihrer Existenz stehen Kryptowährungen, wie etwa bitcoin, ether und Privacy Coins, im Verdacht, als Mittel für Geldwäscherei und Terrorismusfinanzierung zu dienen.¹⁹⁴² Die risikospezifische Besonderheit von Kryptowährungen im Vergleich zu anderen Vermögenswerten, wie insb. Bargeld¹⁹⁴³, die für die erwähnten Zwecke ebenfalls eine Eignung aufweisen, liegt

¹⁹³⁸ Siehe Botschaft GwG 1996, 1106.

¹⁹³⁹ Siehe Botschaft GwG 2007, 6282–6283.

¹⁹⁴⁰ Siehe etwa Botschaft FINMAG 2006, 2859–2860 («Vertrauen in die Finanzintermediation»); Botschaft GwG 2007, 6282 («Funktionsfähigkeit»); BSK FINMAG/FinfraG-Winzeler, Art. 5 FINMAG N 6.

¹⁹⁴¹ Siehe Botschaft FINMAG 2006, 2859.

¹⁹⁴² Siehe insb. FATF, Virtual Currencies Report 2014, 9–10; FATF, VASP Guidance 2015, *passim*; BIS/CPMI, Digital Currencies 2015, 10–11; ferner bereits Schmid/Schmid, Jusletter vom 4. Juni 2012, Rz. 44–45.

¹⁹⁴³ Allerdings wird die Geldwäschereirole von Bargeld relativ zu anderen Methoden gemeinhin überschätzt, vgl. etwa Schneider, in: Deutsche Bundesbank, Restricting or abolishing

in der einzigartigen «Kombination von Anonymität[sic]¹⁹⁴⁴, Schnelligkeit und Mobilität».¹⁹⁴⁵ Dass Kryptovermögenswerte für Geldwäscherei und Terrorismusfinanzierung verwendet werden (können), ist wenig überraschend, handelt es sich doch letztlich in kriminologischer Hinsicht um eine indifferente Technologie, mit welcher sich legale und illegale Ziele gleichermaßen verfolgen lassen.

Über das genaue Ausmass der Geldwäscherei- und Terrorismusfinanzierungsrisiken besteht jedoch bis heute Uneinigkeit, wobei tendenziell eher von einem kleinen bis mittleren Risiko auszugehen ist.¹⁹⁴⁶ Im National Risk Assessment (NRA) vom Oktober 2018 betreffend Geldwäscherei- und Terrorismusfinanzierungsrisiken von Kryptovermögenswerten und Crowdfunding heisst es ein wenig umwunden: *«Die wenigen Fälle könnten ein reales, aber letztlich geringes Risiko widerspiegeln, das sich aus einer zwar expandierenden, aber immer noch neuen Technologie ergibt, die nur sehr selten zu kriminellen Zwecken der Geldwäscherei oder Terrorismusfinanzierung genutzt wird. [...] Die grosse Gefährdung, die von Kryptowährungen ausgeht, hat sich bestätigt und die Verwundbarkeiten der Schweiz in diesem Bereich sind erheblich, auch wenn sie alle Länder betreffen.»*¹⁹⁴⁷ Auch das NRA vom Oktober 2021 hat an dieser grundsätzlichen

cash, 66–71 m.w.N., 79; ferner für die Schweiz KGGT, NRA Bargeld 2018, 28 (*«Trotz erwiesener Gefahr des Bargeldmissbrauchs für Geldwäscherei und Terrorismusfinanzierung kann das Risiko aufgrund der geltenden und in diesem Bericht später erörterten präventiven und repressiven Massnahmen und in Anbetracht der Besonderheit des Schweizer Finanzplatzes mit einem stark international ausgerichteten Bankensektor als moderat eingestuft werden.»*); ferner zur überragenden Bedeutung von Briefkastenfirmen Findley/Nielson/Sharman, Global Shell Games, passim.

¹⁹⁴⁴ Anonymität besteht in aller Regel gerade nicht, sondern gewährleistet ist lediglich die Pseudonymität der Nutzung.

¹⁹⁴⁵ KGGT, NRA Krypto 2018, 22; ähnlich KGGT, NRA 2021, 51; ähnlich, aber v.a. auf die angebliche Anonymität abstellend EP, Cryptocurrencies and blockchain, 53–54.

¹⁹⁴⁶ Siehe z.B. Chainalysis, 2021 Crypto Crime Report, 5 (*«In 2020, the illicit share of all cryptocurrency activity fell to just 0.34%, or .0 billion in transaction volume.»*); CipherTrace, Report 2021, 9 (*«[...] illicit transactions making up less than 0.5% of Bitcoin's yearly volume in 2020.»*); Morell/Kirshner/Schoenberger, Bitcoin's Use in Illicit Finance, 4 (*«[...] the illicit use of cryptocurrencies in general and Bitcoin in particular, as a share of total market activity, is certainly not higher than it is in the traditional banking system and is most likely less.»*); ähnlich Comolli/Korver, Department of Justice Journal of Federal Law and Practice 2021, 196; demgegenüber Foley/Karlsen/ Putniņš, The Review of Financial Studies 2019, 1800 (*«[...] approximately one-quarter of all users [26%] and close to one-half of bitcoin transactions [46%] are associated with illegal activity.»*); vgl. ferner Silfversten et al., Exploring the use of Zcash cryptocurrency, 12–14, welche für den Privacy Coin Zcash keine bedeutende Rolle in illegalen Aktivitäten insb. im Dark Web feststellen konnten.

¹⁹⁴⁷ KGGT, NRA Krypto 2018, 36; ähnlich bereits KGGT, NRA 2015, 98 (*«Gefährdung [...] gering»*).

Einschätzung nicht geändert, wobei in diesem Bericht Stablecoins und dezentrale Applikationen als «neue Risikofaktoren» eingestuft werden.¹⁹⁴⁸ Im neuesten NRA-Bericht zu Krypto-Assets von 2024 droht nach Auffassung des Verfassers hingegen ein Zirkelschluss: Der Risikoanstieg im Zusammenhang mit Kryptovermögenswerten wird primär auf die Zunahme der MROS-Meldungen zurückgeführt. Jedoch hat sich auch die Zahl der Finanzintermediäre, die Kryptodienstleistungen anbieten, seit dem letzten Bericht stark vergrössert. Die Finanzintermediäre werden (und wurden) ihrerseits zudem angewiesen, mehr und früher zu melden.¹⁹⁴⁹

Die FINANCIAL ACTION TASK FORCE (FATF)¹⁹⁵⁰ hat sodann einen qualitativen Bericht im September 2020 veröffentlicht, der basierend auf Fallstudien Indizien für Geldwäscherei und Terrorismusfinanzierung mithilfe von Kryptovermögenswerten erarbeitet.¹⁹⁵¹

Ungeachtet des Vorliegens von qualitativen oder quantitativen Studien hinsichtlich des Geldwäschereirisikos für die Schweiz wurde hierzulande das Geldwäschereirecht bereits per 1. Januar 2016 erweitert, um *virtuelle Währungen* ausdrücklich im Rahmen der Geld- und Wertübertragung («Money Transmission») zu erfassen.¹⁹⁵²

b. Dezentrale Handelsplattformen

Auch dezentralen Handelsplattformen ist in erster Linie im Rahmen der Verhinderung von Geldwäscherei und Terrorismusfinanzierung politische Aufmerksamkeit zuteil geworden. Auf nationaler Ebene wird dies insb. in den Publikationen des Bundesrates und des EFD sowie im Rahmen der National Risk Assessments ersichtlich.¹⁹⁵³ Auf internationaler Ebene wird die politische Agenda sodann durch die FATF bestimmt.¹⁹⁵⁴ Zu erwähnen sind auch die Arbei-

¹⁹⁴⁸ Siehe KGGT, NRA 2021, 51–53.

¹⁹⁴⁹ Siehe EJPd/fedpol, NRA 2024, 7–9.

¹⁹⁵⁰ Die FATF wird auch als *Groupe d'action financière (GAFI)* bezeichnet.

¹⁹⁵¹ Siehe FATF, Virtual Assets Red Flag Indicators, *passim*.

¹⁹⁵² Siehe hierzu FINMA, Erläuterungsbericht GwV-FINMA 2015, 11–12; sodann EFD, Erläuterungsbericht GwV 2015, 5.

¹⁹⁵³ Siehe etwa Bundesrat, DLT-Bericht 2018, 146–147; EFD, Erläuternder Bericht DLT-Vernehmlassungsvorlage 2019, 24–25; Botschaft DLT 2019, 270–271; KGGT, NRA Krypto 2018, 19, 38–39.

¹⁹⁵⁴ Vgl. FATF, VASP Guidance 2019, 15–16; sodann FATF, Draft VASP Guidance 2021, 23; schliesslich FATF, VASP Guidance 2021, 26–27.

ten der US-amerikanischen Behörde FinCEN, welche eine gewisse Ausstrahlung auf andere Rechtsordnungen haben dürften.¹⁹⁵⁵

Evidenz, dass Kryptovermögenswerte mithilfe von dezentralen Handelsplattformen gewaschen werden können, gibt es erstmals seit dem KuCoin-Hack vom 26. September 2020. Im Anschluss an den erfolgreichen Hack der Hot Wallets der zentralen Handelsplattform KuCoin flossen mehrere Tausend ethers durch u.a. das Uniswap-Protokoll. Uniswap und andere Plattformen fungierten in diesem Fall als «Mixer» der gestohlenen Vermögenswerte.¹⁹⁵⁶ Allerdings ist wichtig zu wissen, dass sowohl Absender- als auch Empfängeradressen identisch waren, d.h. lediglich die Kryptovermögenswerte durch die Austauschhandlung wechselten, sodass das Entdeckungsrisiko durch das «Mixing» nur marginal verringert wurde.¹⁹⁵⁷

Bei solchen Austauschgeschäften besteht nach vorliegender Auffassung in aller Regel kein erhöhtes Geldwäschereirisiko: Bei Handelsgeschäften kommt es grundsätzlich lediglich zum Austausch von Vermögenswerten (z.B. ETH gegen einen ERC-20-Token) zwischen zwei Personen oder einem Smart Contract und einer Person, *ohne dass* die persönliche, sachliche und örtliche Distanz zwischen der betreffenden Person, den ausgetauschten Vermögenswerten und/oder dem Lageort der Vermögenswerte erhöht würde und bereits dadurch die Einziehung¹⁹⁵⁸ vereitelt würde. Die auszutauschenden Vermögenswerte werden mit *derselben* Wallet-Adresse empfangen und gehalten. Die Nachverfolgbarkeit von illegal erlangten Kryptovermögenswerten ist mit anderen Worten beim reinen Austauschgeschäft nicht übermässig erschwert.¹⁹⁵⁹

Schliesslich von einem gewissen Interesse vorliegend ist der quantitative Bericht der FATF vom Juli 2021 zu P2P-Transaktionen, worin mit Unterstützung von Unternehmen für Blockchain-Analysen untersucht wurde, in welcher Grössenordnung P2P-Transaktionen tatsächlich auftreten und welchen Anteil davon illegale Zwecke ausmachen.¹⁹⁶⁰ Der Bericht ist allerdings aufgrund der

¹⁹⁵⁵ Siehe insb. FinCEN, Guidance CVC 2019, 18, 23–24.

¹⁹⁵⁶ Siehe Chainalysis, 2021 Crypto Crime Report, 87–89; ferner CipherTrace, Report 2021, 45. Vgl. Chainalysis, KuCoin Hack, *passim*.

¹⁹⁵⁷ Vgl. betreffend die (zu verneinende) Frage, ob Art. 305^{bis} StGB auch die Restitutionsvereitelung mitbezweckt Ackermann/Zehnder, in: Ackermann, Art. 305^{bis} StGB N 397, 402.

¹⁹⁵⁹ Siehe auch die neue Rechtsprechung des Bundesgerichts zu Auslandüberweisungen, welche für sich alleine noch nicht Geldwäscherei darstellen, solange ein *Paper Trail* besteht, BGE 144 IV 172, E. 7.2.2.; ferner zu Tathandlungen, die den Paper Trail bloss *verlängern*, d.h., es treten keine weiteren Kaschierungshandlungen hinzu, Ackermann/Zehnder, in: Ackermann, Art. 305^{bis} StGB N 406–407 m.w.N., 646.

¹⁹⁶⁰ Vgl. FATF, Second Review FATF Standards, 23–30.

Bandbreite der Ergebnisse nicht sehr aussagekräftig, was in der Vielzahl der Vorbehalte gut zum Ausdruck kommt.¹⁹⁶¹ So scheint der Bericht etwa dem typischen Vorgehen von Kriminellen, Kryptovermögenswerte zwischen mehreren Adressen zu bewegen, bevor die Vermögenswerte den Weg an eine zentrale Handelsplattform finden, wo sie gegen Fiatwährungen getauscht werden, nicht Rechnung zu tragen.

2.3 FATF-Empfehlungen

a. Einleitung zu VAs und VASPs

Im Juni 2019 veröffentlichte die FATF eine Guidance zu Virtual Assets (VAs) und Virtual Asset Service Providers (VASPs). Das Dokument stellt ein Update der Guidance zu Virtual Currencies vom Juni 2015 dar. Die damalige Guidance erfasste u.a. noch lediglich zentrale Handelsplattformen an der Schnittstelle des Austausches von Fiatwährungen und VAs.¹⁹⁶² Es sollten mit anderen Worten primär die «on- and off-ramps» des traditionellen Finanzsystems den FATF-Empfehlungen unterstellt werden.¹⁹⁶³ VASPs sollen nach Auffassung der FATF letztlich wie traditionelle Finanzintermediäre oder Händler im Rahmen ihrer Geschäftsaktivitäten Sorgfalts- und Meldepflichten einhalten müssen.¹⁹⁶⁴

Die 2019er-Guidance wurde nach Aussage der FATF vor dem Hintergrund sich verändernder technologischer Entwicklungen notwendig. Erwähnt werden neben dezentralen Handelsplattformen etwa auch Privacy Coins (in der Terminologie der FATF «anonymity-enhanced cryptocurrencies», AECs), Mixing Services und ICOs.¹⁹⁶⁵

Die Guidance definiert fünf Typen von Aktivitäten, welche nach Auffassung der FATF ein erhöhtes Geldwäschereirisiko aufweisen:¹⁹⁶⁶

- *Exchange between virtual assets and fiat currencies;*
- *Exchange between one or more forms of virtual assets;*
- *Transfer of virtual assets;*

¹⁹⁶¹ Siehe zu den Ergebnissen FATF, Second Review FATF Standards, 28–30.

¹⁹⁶² Siehe FATF, VASP Guidance 2015, 4, 6 («points of intersection that provide gateways to the regulated financial system»), 9 («convertible virtual currency exchangers»).

¹⁹⁶³ So FATF, VASP Guidance 2019, 6.

¹⁹⁶⁴ Siehe FATF, VASP Guidance 2019, 4, 7–8.

¹⁹⁶⁵ Vgl. FATF, VASP Guidance 2019, 6.

¹⁹⁶⁶ Siehe FATF, VASP Guidance 2019, 13–14; unverändert FATF, VASP Guidance 2021, 22.

- *Safekeeping and/or administration of virtual assets or instruments enabling control over virtual assets;*
- *Participation in and provision of financial services related to an issuer's offer and/or sale of a virtual asset.*

Das Vorliegen einer dieser Aktivitäten impliziert den Status einer Person als VASP. Neben zentralen Handelsplattformen gelten als VASPs etwa Anbieter von Wechsel- und Übertragungsgeschäften mit VAs, Anbieter von Hosted Wallets sowie Dienstleister im Zusammenhang mit der Herausgabe, des Angebots oder des Verkaufs von VAs (so z.B. im Rahmen eines ICOs).¹⁹⁶⁷ Anbieter von Self-Hosted Wallets, Produzenten von Hardware Wallets sowie Softwareentwickler fallen demgegenüber grundsätzlich nicht unter die VASP-Definition.¹⁹⁶⁸ Zu klären ist vorliegend, inwieweit dezentrale Handelsplattformen von der VASP-Definition erfasst werden.

b. Empfehlung Nr. 15

Die Akronyme VA und VASP haben bereits im Oktober 2018 Eingang in die Empfehlungen der FATF gefunden. Demnach empfiehlt die FATF in Nr. 15 («New Technologies»), dass VASPs den nationalstaatlichen Bestimmungen zur Verhinderung von Geldwäscherei und Terrorismusfinanzierung zu unterstellen sind.¹⁹⁶⁹ VASP sollen wie traditionelle Finanzintermediäre geldwäschereirechtlich erfasst werden: *«To manage and mitigate the risks emerging from virtual assets, countries should ensure that virtual asset service providers are regulated for AML/CFT purposes, and licensed or registered and subject to effective systems for monitoring and ensuring compliance with the relevant measures called for in the FATF Recommendations.»*¹⁹⁷⁰

Sodann konkreter wird die FATF in der Auslegungshilfe zu Empfehlung Nr. 15: *«VASPs should be required to be licensed or registered. At a minimum, VASPs should be required to be licensed or registered in the jurisdiction(s) where they are created. In cases where the VASP is a natural person, they should be required to be licensed or registered in the jurisdiction where their place of business is located. Jurisdictions may also require VASPs that offer products and/or services*

¹⁹⁶⁷ Siehe FATF, VASP Guidance 2019, 14.

¹⁹⁶⁸ Siehe FATF, VASP Guidance 2019, 17.

¹⁹⁶⁹ Siehe hierzu FATF, Recommendations Oktober 2020, 17, 76–77.

¹⁹⁷⁰ FATF, Recommendations Oktober 2020, 17.

to customers in, or conduct operations from, their jurisdiction to be licensed or registered in this jurisdiction.»¹⁹⁷¹

c. Travel Rule (Exkurs)

Im Rahmen von Empfehlung Nr. 15 hat die FATF sodann auch die in Empfehlung Nr. 16 etablierte *Travel Rule* auf die Übertragung von VAs zwischen VASPs ausgeweitet. Dieser traditionellerweise als «Wire Transfer Rule» bezeichnete Regel gelangt bei Zahlungsaufträgen zwischen Kunden unterschiedlicher Banken bereits seit längerem zur Anwendung. Die *Travel Rule* verlangt von VASPs, dass sie Informationen zum Auftraggeber und der begünstigten Person einer Transaktion mit VA erfassen und diese Informationen sodann zusammen mit der Transaktion oder über einen separaten Kommunikationskanal übermitteln.¹⁹⁷² Dies setzt voraus, dass VASPs ihre Kunden als Vertragsparteien identifizieren und die wirtschaftlich berechtigten Personen an den Vermögenswerten feststellen.

Für den Zahlungsverkehr traditioneller Finanzintermediäre, wie insb. Banken, ist die *Travel Rule* in Art. 10 GwV-FINMA verankert.¹⁹⁷³ Die FINMA hat diese Bestimmung in einer Aufsichtsmitteilung vom 26. August 2019 auf VASPs ausgedehnt und – im Sinne eines *Swiss Finish* –¹⁹⁷⁴ auch Transaktionen zwischen VASPs (Hosted Wallets) und Personen mit Self-Hosted Wallets der Bestimmung unterstellt.¹⁹⁷⁵ Darüber hinaus haben schweizerische VASPs auch abzuklären, ob sich der VASP der Empfängerpartei in einer Jurisdiktion mit genügender Geldwäschereiregulierung befindet.¹⁹⁷⁶ Entsprechungen der Swiss

¹⁹⁷¹ FATF, Recommendations Oktober 2020, 76.

¹⁹⁷² Siehe FATE, Recommendations Oktober 2020, 77.

¹⁹⁷³ Siehe zum rechtshistorischen Hintergrund der Bestimmung, die ursprünglich in Art. 15 GwV-EBK bzw. GwV-FINMA 1 war, EBK, EBK-Geldwäschereibericht 2002, in: EBK-Bulletin 44/2003, 102 («[...] der von der [FATF] entwickelten Standards zur Bekämpfung der Terrorismusfinanzierung [...]»), 146–148; EBK, Bericht EBK-Geldwäschereiverordnung 2007, 13–14, 18–19, wonach die Bestimmung auf den ausländischen (SWIFT, SEPA) und inländischen (SIC) Interbankenzahlungsverkehr zur Anwendung gelangt; ferner ausführlich zum Hintergrund der Bestimmung Taube, Sorgfaltspflichten Schweizer Banken, 221–225.

¹⁹⁷⁴ Ferner haben auch Länder, wie etwa *Singapur* und die *Niederlande*, ähnliche Regeln implementiert. Die EU hat die Richtlinie (EU) 2023/1113 des Europäischen Parlaments und des Rates vom 31. Mai 2023 über die Übermittlung von Angaben bei Geldtransfers und Transfers bestimmter Kryptowerte und zur Änderung der Richtlinie (EU) 2015/849 (ABl. L 150) erlassen.

¹⁹⁷⁵ Siehe FINMA, Aufsichtsmitteilung 02/2019, 3; vgl. *demgegenüber* FATF, VASP Guidance 2019, 30; ferner FATE, VASP Guidance 2021, 56, 65.

¹⁹⁷⁶ Siehe CVA, *Travel Rule and its Impact on Cryptocurrency*, 4.

Travel Rule bestehen nunmehr auch in den SRO-Reglementen.¹⁹⁷⁷ Der Erlass von Regeln, die über den internationalen Mindeststandard hinausgehen, scheint im schweizerischen Geldwäschereirecht seit längerer Zeit einen festen Stellenwert einzunehmen.¹⁹⁷⁸

Als Begründung für den umfassenden Regulierungsansatz führt die FINMA an, dass eine Ausnahme von der Travel Rule eine Besserstellung nichtunterstellter Dienstleister darstellen und die Vermeidung problematischer Zahlungen durch unterstellte Anbieter unmöglich machen würde.¹⁹⁷⁹ Ungeachtet der Stichhaltigkeit dieser Argumentation, welche die Ausdehnung der Regel auf Privatpersonen ohne Dienstleistereigenschaft in Kauf nimmt, ist fraglich, ob die Travel Rule mit dem geltenden Recht vereinbar ist.

Mit der Publikation der Aufsichtsmitteilung hat die FINMA die geldwäschereirechtlichen Sorgfaltspflichten potenziell auf Nichtkunden eines VASP ausgedehnt («wie bei einer eigenen Kundenbeziehung»)¹⁹⁸⁰ Freilich unterhält der VASP gerade keine Geschäftsbeziehung mit solchen Personen. Diese Ausweitung auf Personen ausserhalb des Kundenbereichs eines Finanzintermediärs dürfte einem geldwäschereirechtlichen Novum entsprechen. Art. 10 GwV-FINMA spricht ausdrücklich vom Finanzintermediär *des Auftraggebers* bzw. *der* begünstigten Person, wobei der Finanzintermediär *des Auftraggebers* gemäss Abs. 4 den Vertragspartner in angemessener Weise (z.B. in den AGB) über die Weitergabe seiner Angaben im Zahlungsverkehr zu informieren hat. Wenn überhaupt,¹⁹⁸¹ kann nur der Vertragspartner «sicherstellen», dass die Angaben der Gegenpartei «zutreffend und vollständig» sind (Art. 10 Abs. 1 *in fine*). Die Ausdehnung der Bestimmung auf Nichtkunden bringt praktische Umsetzungsschwierigkeiten mit sich, woraus ein *faktisches Verbot oder zumindest eine faktische Einschränkung* von Transaktionen an externe (Self-Hosted) Wallets durch den VASP resultieren kann. Selbstredend ist, dass indirekte, faktische Einschränkungen und Verbote einer Tätigkeit grundsätzlich demselben grundrechtlichen Prüfungsstandard wie direkte, formelle Eingriffe zu genügen

¹⁹⁷⁷ Vgl. etwa Art. 14 VQF-Reglement vom 16. November 2020.

¹⁹⁷⁸ Vgl. bereits EBK, Jahresbericht 2004, 30; kritisch hingegen CVA RWG, CVA's answer to the DLT Ordinance, 8–9.

¹⁹⁷⁹ Siehe FINMA, Aufsichtsmitteilung 02/2019, 3.

¹⁹⁸⁰ Siehe FINMA, Aufsichtsmitteilung 02/2019, 3.

¹⁹⁸¹ Skeptisch diesbezüglich bereits zum regulären Interbankenzahlungsverkehr Zollinger, ContraLegem 2018, 119; ferner zur fragwürdigen Auslegung der Bestimmung vor Einführung der Sicherstellungspflicht des Finanzintermediärs am 1. Januar 2020 Bacharach, Base légale suffisante, *passim*.

haben.¹⁹⁸² Konkret wird in der Literatur darauf abgestellt, ob die tatsächlichen Auswirkungen eines faktischen staatlichen Eingriffes eine wirtschaftliche Tätigkeit der betroffenen Person noch zulassen.¹⁹⁸³

Nicht erfasst von der Travel Rule sind nach Ansicht der FATF hingegen Transaktionsgebühren, welche als Teil der Zahlung an die Netzwerkteilnehmer (z.B. Miner) übermittelt werden.¹⁹⁸⁴ Bei Minern handelt es sich ebenfalls um Nichtkunden des Finanzintermediärs.

Als Antwort auf die FINMA-Aufsichtsmitteilung hat die Industrie *technische Massnahmen* entwickelt:

- Um namentlich die Ausdehnung von Art. 10 GwV-FINMA bzw. der entsprechenden SRO-Bestimmung¹⁹⁸⁵ auf Wechselgeschäfte zwischen dem VASP und einer nichtunterstellten Person zu vermeiden, müssen VASPs überprüfen können, ob ihr Kunde über das angegebene Self-Hosted Wallet tatsächlich die Verfügungsmacht innehat bzw. dieses kontrolliert.¹⁹⁸⁶ Sie haben diesbezüglich einen Kontrollnachweise über das Kunden-Wallet zu erbringen. Solange eine Transaktion den einschlägigen Schwellen-

¹⁹⁸² GLM. wohl Kunz, Jusletter vom 7. Mai 2018, Rz. 36, der festhält, dass die «Macht des Faktischen» eine Grundrechtseinschränkung darstellen kann. Vgl. in allgemeiner Hinsicht Schweizer, in: SGK BV, Art. 36 N 2. Ferner in Bezug auf die *Judikatur*: siehe zu *faktischen Einschränkungen* der Eigentumsgarantie gemäss Art. 26 BV BGE 140 I 176, E. 9.2 m.w.N. («ähnliche Wirkung»); VGer Kt. GR A 11 59, A 12 2, A 12 5 und A 12 6 vom 3. Juli bzw. 28. September 2012, E. 11.b) («nahezu wie ein vollständiges Zweitwohnungsverbot wirken würde»); zu faktischen Einschränkungen der Handels- und Gewerbefreiheit in Art. 31 aBV Bundesgericht, I. Öffentlichrechtliche Abteilung, 12. Dezember 1979, in: ZBl 1980, 229–232, 231–232 *e contrario*; zu faktischen Einschränkungen der Versammlungs- und Vereinigungsfreiheit gemäss Art. 11 EMRK Villiger, Handbuch EMRK, Rz. 821 m.w.N.; in Bezug auf den (indirekten) Impfwang durch die Covid-19-Massnahmen, vgl. Gerber, Jusletter Coronavirus Blog, *passim*; ferner zum sog. *Chilling Effect* bei mittelbaren staatlichen Eingriffen in die Meinungsfreiheit gemäss Art. 16 BV BGE 143 I 147, E. 3.3. Sodann Hauser-Spühler, Innovation vs. Regulation, Rz. 116, die darin eine Frage der Verhältnismässigkeit nach Art. 5 Abs. 2 BV sieht. Schliesslich für ähnliche Argumente unter *US-amerikanischem Recht* Coin Center, Comments on Requirements for Certain Transactions Involving Convertible Virtual Currency, 16–22.

¹⁹⁸³ Siehe Poldena/Schlauri/Schweizer, Open-Source-Software in der öffentlichen Verwaltung, Rz. 221–223, 322, wonach für die Schwere eines Grundrechtseingriffs danach unterschieden wird, ob noch eine «sinnvolle wirtschaftliche Tätigkeit» möglich ist.

¹⁹⁸⁴ Siehe FATF, VASP Guidance 2021, 56 FN 43.

¹⁹⁸⁵ Vgl. Art. 14 Abs. 3 VQF-Reglement vom 16. November 2020.

¹⁹⁸⁶ Eine ähnliche Situation bestand bei den damaligen Bitcoin-Wechselautomaten der Bitcoin Suisse AG, die eine technische Lösung mit Papier Wallets implementierte, welche sicherstellte, dass lediglich ein Zweiparteienverhältnis vorlag.

wert für Wechselgeschäfte¹⁹⁸⁷ nicht erreicht, geht es bei dieser Lösung nicht primär darum, die Gegenpartei zu identifizieren und die wirtschaftlich berechnete Person an den Vermögenswerten festzustellen.

Zum Zweck des Kontrollnachweises sehen VASPs etwa die Signierung einer an den VASP gerichteten Mitteilung mittels Private Keys des Empfängers-Wallets¹⁹⁸⁸ oder die Vorabübertragung eines spezifischen Betrages an den VASP¹⁹⁸⁹ vor.¹⁹⁹⁰ Eine Lösung, die bspw. in den Niederlanden praktiziert wird bzw. wurde,¹⁹⁹¹ ist die Erstellung eines Bildschirmfotos oder die Durchführung von Videotelefonie mit dem Wallet-Inhaber, worin die Wallet-Adresse des Empfängers klar ersichtlich ist. Dass dieses Vorgehen allerdings wenig effektiv ist, da es relativ einfach umgangen werden kann, ist offensichtlich. Ein neuer Ansatz, welche einige Defizite der oben erwähnten Lösungen behebt, für eine Vereinfachung des Nachweisprozesses sorgt und zudem einen höheren Grad an Privatsphäre gewährleisten könnte, ist das *Address Ownership Proof Protocol* (AOPP).¹⁹⁹² Bei entsprechender technischer Integration in ein Wallet kann ein Nutzer eine von der VASP übermittelte Mitteilung mit seinem Private Key signieren, woraus für den VASP erkennbar wird, dass die Wallet vom entsprechenden Nutzer kontrolliert wird.

Diese technischen Massnahmen betreffen, wie bereits erwähnt, in aller Regel den Umgang mit Kunden des VASP, welche Kryptovermögenswerte auf ihr Self-Hosted Wallet übertragen wollen. Dies ist insb. der Fall beim Geldwechsel sowie beim gewöhnlichen Rückzug von Kryptovermögenswerten von einem Hosted Wallet des VASP bzw. beim umgekehrten Vorgang der Übertragung auf das Hosted Wallet des VASP.

¹⁹⁸⁷ Vgl. Art. 51a GwV-FINMA.

¹⁹⁸⁸ Siehe etwa Bity SA, *How do I buy cryptocurrencies without a Bity account?*, *passim*.

¹⁹⁸⁹ Sog. *Satoshi-Test*; siehe Hablützel, *Proof-of-Ownership and Crypto Adoption*, *passim* («By asking clients to send a very specific amount to us within a limited time frame, we can be reasonably sure that the person sending funds is the client which passed our onboarding process – according to standards set out under the Swiss AML framework.»).

¹⁹⁹⁰ Vgl. in diesem Zusammenhang CMTA, *AML Standards for Digital Assets*, 27–28.

¹⁹⁹¹ Vgl. etwa das Verfahren des niederländischen Unternehmens Bitonic B.V. gegen die Niederländische Nationalbank, welches dazu führte, dass die Nationalbank mangels genügender Rechtsgrundlage die Verifizierung von externen Wallets als Registrierungsbedingung zurückzog, Bitonic, *DNB formally acknowledges complaints*, *passim*; weitere juristische Ausführungen hierzu bei Lelieveldt, *Dutch judge slaps Dutch central bank on the wrist*, Medium, *passim*.

¹⁹⁹² <https://aopp.group/>.

- Pikanterweise hat die FINMA der lokalen Kryptoindustrie die Pflichten im Zusammenhang mit der Travel Rule, die nach eigener Aussage als «eine der strengsten weltweit» gelten,¹⁹⁹³ zu einem Zeitpunkt auferlegt, als noch keine technische Lösung zur Einhaltung der Pflichten existierte, geschweige denn eine, welche den Schutz und die Sicherheit der derart übertragenen Personendaten gewährleistete.¹⁹⁹⁴ Zum Vergleich: Gemäss der deutschen Kryptowertetransferverordnung, welche eine vergleichbare Travel Rule erst im September 2021 einführte, konnte u.a. die BaFin VASPs einen Aufschub der Anwendung der Bestimmung von bis zu 24 Monate erteilen.¹⁹⁹⁵

Um einander die in Art. 10 GwV-FINMA geforderten Angaben übermitteln zu können, bedürfen VASPs eines *Kommunikationssystems*, das analoge Funktionalitäten wie SWIFT im Interbankenzahlungsverkehr aufweist.¹⁹⁹⁶ Schweizerische Finanzintermediäre haben sich zu diesem Zweck insb. OpenVASP¹⁹⁹⁷ und dem Travel Rule Protocol¹⁹⁹⁸ angeschlossen.¹⁹⁹⁹ Diese technischen Massnahmen betreffen Transaktionen zwischen VASPs bzw. deren Kunden, mit welchen die VASPs eine dauernde Geschäftsbeziehung unterhalten.

Die Aufsichtsmitteilung der FINMA ist sodann in einem weiteren Punkt problematisch: Die angedrohte Anwendung von Art. 10 GwV-FINMA auf Kassageschäfte mit Kryptowährungen bzw. Zahlungen-Token, wie namentlich den Geldwechsel, ist in dogmatischer Hinsicht fragwürdig.²⁰⁰⁰ Weil die Bestimmung im traditionellen Finanzbereich eine *dauernde* Geschäftsbeziehung zwi-

¹⁹⁹³ Siehe FINMA, Jahresbericht 2019, 18.

¹⁹⁹⁴ Vgl. FINMA, Aufsichtsmitteilung 02/2019, 3; vgl. nunmehr Rieglinig, OpenVASP, 4, wo «Privacy by Design» als Design-Prinzip des OpenVASP-Protokolls bezeichnet wird. Die *inter-VASP Messaging Standards* schliessen Fragen des Datenschutzes demgegenüber explizit aus, vgl. hierzu JWG, interVASP, 12.

¹⁹⁹⁵ Siehe § 5 der Verordnung über verstärkte Sorgfaltspflichten bei dem Transfer von Kryptowerten (Kryptowertetransferverordnung bzw. KryptoWTransferV) vom 24. September 2021.

¹⁹⁹⁶ Vgl. für einen Überblick unterschiedlicher Kommunikationslösungen gwp/InCore, Travel Rule, *passim*.

¹⁹⁹⁷ <https://openvasp.org/>.

¹⁹⁹⁸ <https://www.travelruleprotocol.org/>.

¹⁹⁹⁹ Vgl. in diesem Zusammenhang die gemeinsame Medienmitteilung von 21 Analytics, Crypto Finance AG und Mt Pelerin hinsichtlich der *Demonstration* eines solchen Datenaustausches zwischen VASPs, siehe hierzu 21 Analytics, First Automated Travel Rule Compliant Bitcoin Transaction, *passim*.

²⁰⁰⁰ Vgl. Kunz, Jusletter vom 18. November 2019, Rz. 7.

schen einem Finanzintermediär und dem Kunden voraussetzt, gelangt sie bei Wechselgeschäften über Fiatwährungen gerade nicht zur Anwendung. Bei Kryptowährungen bzw. Zahlungs-Token soll dies nun aber nach Meinung der FINMA anders sein.

Fraglich ist ferner, ob solche Wechselgeschäfte in funktionaler Hinsicht²⁰⁰¹ überhaupt mit einer Banküberweisung, die typischerweise den Transfer von Buchgeld beinhaltet, im Sinne der Bestimmung gleichgesetzt werden können. Ausserhalb des «Zahlungsverkehr[s] auf der Blockchain»²⁰⁰², namentlich bei Austauschgeschäften über eine dezentrale Handelsplattform, soll darum nach vorliegender Ansicht Art. 10 GwV-FINMA keine Bedeutung zukommen. Ohnehin mangelt es in diesen Fällen in der Regel an der Involvierung eines VASPs.

Sodann stellt sich die Frage, ob VAs aufgrund ihrer inhaberpapierähnlichen Eigenschaften geldwäschereirechtlich nicht viel eher wie Bargeld und somit wie Kassageschäfte zu behandeln wären. Eine *technologieneutrale* Herangehensweise, die dem Gleichbehandlungsgrundsatz in Art. 8 BV Rechnung trägt, bestünde demnach in der regulatorischen Gleichstellung von VA-Transaktionen zwischen VASPs und Self-Hosted Wallets mit der Einzahlung und Auszahlung von Bargeld bei einem regulierten Finanzintermediär.²⁰⁰³ Die Regeln zu gewöhnlichen Kassageschäften könnten in diesem Fall zur Anwendung gelangen. Aufgrund der deutlich besseren Nach- und Rückverfolgbarkeit von kryptobasierten Transaktionen wären allenfalls sogar Erleichterungen im Vergleich zu Bargeldrückzügen angezeigt.²⁰⁰⁴

Sodann trägt die Travel Rule generell nicht Rechnung der Möglichkeit, dass Kunden von VASPs *direkt* mit einer DeFi-Applikation interagieren könnten. In einem solchen Fall mangelt es an den geforderten Empfängerinformationen, ist doch die Adresse eines Smart Contracts involviert, weshalb die Travel Rule wohl auch diesbezüglich zu einem faktischen Verbot solcher Transaktionen in der Praxis führen dürfte. Dies würde zu einer rechtspolitisch unerwünschten Gabelung des traditionellen und Krypto-Finanzsystems beitragen.²⁰⁰⁵

²⁰⁰¹ Vgl. FATE, VASP Guidance 2019, 29 («functionally analogous to wire transfers»).

²⁰⁰² FINMA, Aufsichtsmitteilung 02/2019, *passim*.

²⁰⁰³ So wohl auch Kunz, Jusletter vom 18. November 2019, Rz. 10–12, der von Bitcoin als digitalem Bargeld spricht.

²⁰⁰⁴ Wohl ebenso Hess, AJP 2023, 947. Vgl. demgegenüber die generelle Verschärfung betreffend Transaktionen mit virtuellen Währungen in Art. 51a GwV-FINMA; siehe hierzu auch oben, [V.2.7b](#) und [V.2.7e](#).

²⁰⁰⁵ Siehe hierzu auch unten, [V.2.12i](#).

Schliesslich wurde nicht bedacht, dass die Einführung der Travel Rule für Kryptotransaktionen datenschutzrechtlich bedenklich sein könnte: Der Umstand, dass VASPs sowie deren Kunden und Nichtkunden Daten miteinander auszutauschen haben, ist mit dem Risiko behaftet, dass Dritte aufgrund eines entsprechenden Datenlecks Einblick in die gesamte Wallet-Historie eines Kunden erlangen. Diese Problematik besteht im traditionellen Zahlungsverkehr hingegen viel weniger, da mit Ausnahme der an die involvierten Finanzintermediäre übertragenen Daten diese grundsätzlich privat bleiben.

d. VASP-Guidance

i. Guidance vom Juni 2019

Die FATF hat in der Guidance vom Juni 2019, soweit ersichtlich, erstmals *dezentrale Handelsplattformen* zum Gegenstand ihrer Empfehlungen gemacht.

Darin wird unterschieden zwischen «order-book exchange services», wobei EtherDelta in der Fussnote namentlich als Beispiel erwähnt wird, «peer-to-peer trading platforms» und «decentralized exchanges or platforms».²⁰⁰⁶ Die FATF erwähnt, dass Handelsplattformen, welche den Austausch oder die Übertragung von VAs ermöglichen (*facilitate*), bei Erfüllung der übrigen Voraussetzungen unter die Empfehlungen fallen könnten. Dass die fraglichen Handelsplattformen in irgendeiner Form eine zentrale Komponente aufweisen, scheint die FATF implizit vorauszusetzen. So werden etwa die Fälle erfasst, in denen eine Person in der Funktion einer Gegenpartei selbst Kauf- und Verkaufsangebote einstellt, Aufträge zentral ausführt und abwickelt oder den Nutzern die Führung von Hosted Wallets anbietet und somit Verfügungsmacht über fremde Vermögenswerte innehat.²⁰⁰⁷

Der Guidance fehlt es nach vorliegender Auffassung an logischer Kohärenz. Einerseits wird im Hinblick auf DApps richtigerweise festgehalten, dass solche Anwendungen grundsätzlich von keiner bestimmbar Person (*administrator*) verwaltet werden; doch können nach Auffassung der FATF Eigentümer (*owner*) und Betreiber (*operator*) einer DApp allenfalls doch als VASP qualifizieren. Ferner wird ausgeführt, dass selbst eine DApp als VASP gelten könne, wenn eine

²⁰⁰⁶ Siehe FATF, VASP Guidance 2019, 15–16.

²⁰⁰⁷ Siehe FATF, VASP Guidance 2019, 15.

solche den Austausch oder die Übertragung von VAs ermöglicht.²⁰⁰⁸ Die direkte Unterstellung von Software unter die Regeln des Geldwäschereirechts macht offensichtlich wenig Sinn. Die eingesetzte Software ist letztlich lediglich das technologische Mittel, mit welcher eine regulierte finanzintermediäre Tätigkeit ausgeübt werden kann.²⁰⁰⁹

Man kommt nicht um das Gefühl herum, dass die FATF «auf Teufel komm raus» dezentrale Handelsplattformen und andere dezentrale Applikationen in das traditionelle Finanzintermediationskorsett zwingen möchte. Eine eigentliche Differenzierung zwischen Handelsplattformen mit unterschiedlicher Dezentralität findet, soweit ersichtlich, gar nicht erst statt. Zu diesem Bild passt auch, dass etwa bereits Disintermediationseffekte als potenzielles Geldwäschereirisiko eingestuft werden.²⁰¹⁰ Denn die FATF befürchtet, dass die Rolle von Finanzintermediären als Gatekeepers an Bedeutung verlieren und somit der regulatorische Anknüpfungspunkt wegfallen könnte.²⁰¹¹

Demgegenüber wird in der Guidance festgehalten, dass die FATF dezentrale Handelsplattformen, welche interessierten Marktteilnehmern lediglich ein Forum für Kauf- und Verkaufsaufträge bietet, die jeweilige Aufbewahrung der VAs über Self-Hosted Wallets erfolgt und die Abwicklung des Austauschgeschäfts ausserhalb der Plattform stattfindet, nicht als VASP betrachtet («peer-to-peer trading platforms»)²⁰¹²

Dasselbe muss *a maiore ad minus* auch für reine P2P-Transaktionen direkt zwischen den Self-Hosted Wallets der Endbegünstigten eines Geschäfts gelten. Damit sind P2P-Transaktionen definitionsgemäss keine VASPs oder sonst wie unterstellten Intermediäre involviert. P2P-Transaktionen sind konzeptionell relativ nahe bei dezentralen Handelsplattformen, wie etwa Atomic Swap- oder Smart Contract-basierten P2P-Handelsplattformen. Die FATF spricht davon, dass P2P-Transaktionen derzeit nicht explizit von den Empfehlungen erfasst seien, wobei nicht ausgeschlossen werden könne, dass solche Transaktionen künftig allenfalls erfasst würden.²⁰¹³ Geldwäschereirisiken von P2P-

²⁰⁰⁸ Siehe FATF, VASP Guidance 2019, 15–16 («When DApps facilitate or conduct the exchange or transfer of value [whether in VA or traditional fiat currency], the DApp, its owner/operator(s), or both may fall under the definition of a VASP.»).

²⁰⁰⁹ Diesbezüglich unzweideutig FinCEN, Guidance CVC 2019, 18.

²⁰¹⁰ Vgl. FATF, VASP Guidance 2019, 18; ferner FATF, Second Review FATF Standards, 35.

²⁰¹¹ Siehe FATF, Second Review FATF Standards, 34.

²⁰¹² Siehe FATF, VASP Guidance 2019, 15.

²⁰¹³ Vgl. etwa FATF, Review FATF Standards, 14–15; FATF, Second Review FATF Standards, 23 («The revised FATF Standards do not explicitly apply to P2P transactions, which are transactions that do not involve a VASP or other AML/CFT-obliged entity, except for obligations

Transaktionen werden insb. im Zusammenhang mit Stablecoins thematisiert.²⁰¹⁴

ii. Draft Guidance vom März 2021

Die FATF verfolgt mit der Draft Guidance vom März 2021 augenscheinlich den in der 2019-Guidancen eingeschlagenen Weg weiter. Die FATF macht klar, dass die beiden Begriffe VA und VASP *expansiv* zu verstehen sind, sodass grundsätzlich keine Lücken mehr zwischen traditionellen Finanzintermediären und VASPs sowie zwischen traditionellen und virtuellen Vermögenswerten des Finanzsektors bestehen.²⁰¹⁵ Insb. kommen damit auch NFTs je nach Ausgestaltung in den Fokus der Geldwäschereiregulierung.²⁰¹⁶

Die FATF stellt nunmehr entgegen der 2019er-Guidance ausdrücklich klar, dass eine Softwareapplikation oder Technologie selbst nicht Gegenstand der Regulierung ist.²⁰¹⁷ Damit gelten neben dezentralen Applikationen inkl. deren Smart Contracts und dergleichen richtigerweise auch die Protokolle dezentraler Netzwerke nicht als VASPs. Allerdings widerspricht sich die internationale Behörde selbst, wenn sie an anderer Stelle und damit gleich wie in der bisherigen Guidance ausführt, dass Plattformen, die eine unterstellte Tätigkeit ermöglichen (*facilitate*), notwendigerweise den VASP-Begriff erfüllen.²⁰¹⁸ Im Resultat ist es darum weiterhin unklar, ob Software, welche Prozesse und Strukturen automatisiert, erfasst ist oder nicht.²⁰¹⁹

on all persons [such as those for targeted financial sanctions].»), sodann 34 («[...] the FATF's focus on placing AML/CFT controls on intermediaries [such as VASPs] should be maintained for the time being»); siehe ferner die Grafik hinsichtlich Unhosted Wallets bei Comolli/Korver, Department of Justice Journal of Federal Law and Practice 2021, 196.

²⁰¹⁴ Siehe FATF, Stablecoins Report 2020, 18–19.

²⁰¹⁵ Siehe FATF, Draft VASP Guidance 2021, 7 («[...] this Guidance was updated in [June 2021] to [...] clarify the definitions of VA and VASP to make clear that these definitions are expansive and there should not be a case where a relevant financial asset is not covered by the FATF Standards [either as a VA or as a traditional financial asset] [...]»), ausführlich zu den Begriffen sodann 19–21, 26–27.

²⁰¹⁶ Siehe FATF, Draft VASP Guidance 2021, 26–27, 30 («Some items – or tokens – that on their face do not appear to constitute VAs may in fact be VAs that enable the transfer or exchange of value or facilitate ML/TF.»).

²⁰¹⁷ Siehe FATF, Draft VASP Guidance 2021, 23.

²⁰¹⁸ Siehe FATF, Draft VASP Guidance 2021, 29 («Where the platform facilitates the exchange, transfer, safekeeping or other financial activity involving VAs [...], then the platform is necessarily a VASP conducting exchange and/or transfer activity as a business on behalf of its customers.»).

²⁰¹⁹ GLM. BA, Comments on FATF Guidance, 9–10.

Die Draft Guidance dehnt sodann namentlich den VASP-Begriff auf weitere Personen aus und dies insb. mit Blick auf dezentrale Applikationen und Stablecoins:

«These applications or platforms are often run on a distributed ledger but still usually have a central party with some measure of involvement, such as creating and launching an asset, setting parameters, holding an administrative ‘key’ or collecting fees. Often, a DApp user must pay a fee to the DApp, which is commonly paid in VAs, for the ultimate benefit of the owner/operator/developer/community in order to develop/run/maintain the software. DApps can facilitate or conduct the exchange or transfer of VAs.

[...] entities involved with the DApp may be VASPs under the FATF definition. For example, the owner/operator(s) of the DApp likely fall under the definition of a VASP, as they are conducting the exchange or transfer of VAs as a business on behalf of a customer. The owner/operator is likely to be a VASP, even if other parties play a role in the service or portions of the process are automated. Likewise, a person that conducts business development for a DApp may be a VASP when they engage as a business in facilitating or conducting the activities previously described on behalf of another natural or legal person.»²⁰²⁰

Der Entwurf erfasst potenziell alle Personen, die irgendeine Funktion im Zusammenhang mit einer dezentralen Applikation innehaben. Demnach können nach Ansicht der FATF Personen als VASPs qualifizieren, wenn sie eine der folgenden Aktivitäten ausüben:

- Personen, welche eine DApp bzw. Rechte an ihr besitzen (*owner*);
- Personen, welche eine DApp zur Ausführung bringen oder betreiben (*operator*);
- Personen, welche *Business Development* für eine DApp betreiben;
- Personen, welche Gebühren aufgrund der Nutzung einer DApp durch Dritte vereinnahmen (*collect fees*).

An der Breite und Vagheit der VASP-Definition wurde zu Recht breite Kritik geübt.²⁰²¹ Wesentliche Elemente der vorgeschlagenen Umschreibungen sind ausserdem, wenn nicht widersprüchlich, so zumindest sehr schwammig for-

²⁰²⁰ FATF, Draft VASP Guidance 2021, 23.

²⁰²¹ Siehe statt vieler Coin Center, Comments on FATF Guidance, *passim*; BA, Comments on FATF Guidance, *passim*; BAS, Comments on FATF Guidance, *passim*; SBF, Comments on FATF Guidance, *passim*.

muliert.²⁰²² Festzuhalten ist zudem, dass grundsätzlich keine der erwähnten Aktivitäten den involvierten Personen die Verfügungsmacht über fremde Vermögenswerte verschafft. Und selbst wenn das Anknüpfungskriterium der Verfügungsmacht über fremde Vermögenswerte generell aufgegeben werden soll, geht die FATF weit über das hinaus, was heute gemeinhin als finanzintermediäre Tätigkeit bzw. Finanzintermediation bezeichnet wird.

Noch nachvollziehbar ist die Einstufung als VASP von Personen, welche eine VASP betreiben (*operator*) und diesem Rahmen indirekt Kontrolle über fremde Vermögenswerte haben, indem sie etwa Smart Contracts mithilfe von Admin Keys zu ihren Gunsten beeinflussen können. Wie erwähnt im Zusammenhang mit Art. 4 Abs. 1 lit. b GwV ist dieser Ansatz unter Berücksichtigung der Zwecksetzung zumindest vertretbar.²⁰²³ Fraglich ist hingegen die Unterstellung als VASP, wenn eine Person lediglich eine DApp zur Ausführung auf einem dezentralen Netzwerk bringt (*launch*). Dies soll nach Ansicht der FATF selbst dann gelten, wenn der Betreiber unmittelbar nach dem Start einer Plattform die Kontrolle über diese aufgibt oder an Dritte (z.B. eine DAO) abtritt, wobei nicht zwingend notwendig ist, dass er in finanzieller Hinsicht fortlaufend vom Betrieb der Plattform profitiert.²⁰²⁴ Das ist eine klar abzulehnende²⁰²⁵ Ausdehnung des heutigen Gatekeeper-Konzepts auf Personen, insb. Entwickler, welche eine DApp weder «as a business» noch «on behalf of a customer» zur Ausführung bringen.²⁰²⁶ Eigengeschäfte, sofern man diesen Begriff in diesem Kontext überhaupt verwenden kann, sind demgegenüber unbestrittenermaßen nicht Gegenstand der FATF-Empfehlungen.

Weiter gibt es keine sinnvolle Verwendung des Konzepts der Eigentümer- oder Inhaberschaft (*owner*) bei dezentralen Applikationen, denn die zugrundeliegende Software kann aufgrund der Verwendung von Open-Source-Lizenzen fast ausschliesslich²⁰²⁷ immer frei weiterverwendet werden.²⁰²⁸ Allenfalls könnte noch beim Markeninhaber einer Applikation angeknüpft werden, denn Marken werden bei DApps häufig «monopolisiert». Eine solche enge Lesart von Ownership geht aber aus den Ausführungen der FATF nicht hervor. Wie-

²⁰²² Vgl. zur Problematik vager Rechtsnormen, die zudem einen breiten Anwendungsbereich aufweisen, Brennan-Marquez, Arizona Law Review 2019, insb. 652–653.

²⁰²³ GLM. wohl Coin Center, Comments on FATF Guidance, 6, 19, 38.

²⁰²⁴ Siehe FATF, Draft VASP Guidance 2021, 29, 30.

²⁰²⁵ GLM. Van Valkenburgh, FinCEN's new cryptocurrency guidance, allerdings in Bezug auf die FinCEN Guidance von 2019; BA, Comments on FATF Guidance, 7.

²⁰²⁶ Siehe zu diesen Begriffen FATF, Draft VASP Guidance 2021, 22.

²⁰²⁷ Vgl. jedoch zur einschränkenden Lizenzierung von Uniswap oben, [IV.5.1f.ii](#).

²⁰²⁸ Ähnlich Coin Center, Comments on FATF Guidance, 6.

derum käme die Unterstellung von Personen aufgrund der Registrierung von Markenrechten einer enormen Ausweitung der Sorgfaltspflichten auf bisher nicht unterstellte Personen gleich.

Auch mit spezifischem Blick auf dezentrale Handelsplattformen überzeugt der FATF-Ansatz nicht: Hier liegt regelmässig keine Dienstleistung für einen Dritten bzw. in dessen Auftrag vor. Nutzer, welche eine dezentrale Handelsplattform verwenden möchten, müssen selbständig die eingesetzten Smart Contracts oder sonstigen Mechanismen instruieren, dass diese die von ihnen erwünschten, aber im Voraus programmierten Prozesse ausgeführt werden. Dabei ist keine Drittpartei involviert, welche eine Handlung für die an einem Austauschgeschäft beteiligten Nutzer vorzunehmen hätte. Gleichermassen erfolgen Handelsaktivitäten, so etwa im Falle von Liquiditätsgebern im AMM-Modell, ebenfalls in Form von Geschäften auf eigene Rechnung. Liquiditätsgeber sind sodann regelmässig über eine DAO an der Governance eines Protokolls beteiligt (so z.B. in Uniswap). Die FATF impliziert, dass bereits das Festlegen von Parametern eines Protokolls durch Inhaber von Governance Token den Begriff eines VASPs erfüllen könnte.²⁰²⁹ Allerdings könnte dies überhaupt nur dann gelten, wenn die festzulegenden Parameter einen vergleichbaren Einfluss wie Admin Keys erlauben, die den Inhabern die Kontrolle über die Smart Contracts und somit fremde Vermögenswerte verschaffen. Die FATF macht allerdings keine Aussagen zur Frage der Wesentlichkeit solcher Parameter. Ohnehin ist offen, wie eine verteilte Governance-Community bestehend aus hunderten, ja tausenden Mitgliedern einerseits als «a legal person [or] a natural (individual) person»²⁰³⁰ im Sinne der Guidance qualifizieren und andererseits gemeinsam die Sorgfaltspflichten eines VASPs erfüllen kann.²⁰³¹

Unklar erscheint auch die Einstufung als VASPs von Personen, welche aufgrund ihrer Stellung oder ihres Beitrages zu einer DApp die von den Nutzern bezahlten Gebühren vereinnahmen (*collect fees*).²⁰³² Die Belastung von Gebühren gegenüber Kunden wird teilweise als ein Hauptargument für das Vorliegen von Tätigkeiten «as a business», die typischerweise von VASP ausgeübt werden, betrachtet.²⁰³³ Gerade im Rahmen der Aufbringung von Liquidität für dezentrale Handelsplattformen ist die Incentivierung über Handelsgebühren

²⁰²⁹ Vgl. FATF, Draft VASP Guidance 2021, 27 in Bezug auf «managing the stabilisation function» eines Stablecoins, jedoch relativierend «depending on the extent of the influence each party has».

²⁰³⁰ Vgl. FATF, Draft VASP Guidance 2021, 22.

²⁰³¹ Ebenfalls skeptisch BA, Comments on FATF Guidance, 6.

²⁰³² Vgl. FATF, Draft VASP Guidance 2021, 27 («the party that profits from the use of a VA»)

²⁰³³ So etwa BA, Comments on FATF Guidance, 8.

zentral für die Funktionsweise einer Plattform. Dies spricht zwar grundsätzlich für das Vorliegen der Bedingung «as a business», aber wiederum erfolgt die Tätigkeit nicht «on behalf of a customer». Die Gebühren sind entgegen der Ansicht der FATF lediglich die einer Vielzahl von «Leistungserbringern» zuge dachte Gegenleistung der Nutzer, welche aufgrund der bereitgestellten Liquidität effizientere Austauschgeschäfte eingehen können.

Nicht als VASP gelten richtigerweise Personen, welche die Software einer DApp lediglich entwickeln und unterhalten (*develop and maintain*) und den Softwarecode oder Teile einer Applikation allenfalls an Dritte verkaufen (*sell*), sie jedoch nicht selbst zur Ausführung bringen (*run*).²⁰³⁴ Letztere Einschränkung ist allerdings aus den bereits oben erwähnten Gründen problematisch. Fast vollständig im Dunkeln befindet sich der Leser bei der Frage, welche Formen von *Business Development* nach Auffassung der FATF als VASP-Aktivität gelten.²⁰³⁵ Als *Business Development* im Softwarebereich können denn auch sehr unterschiedliche Tätigkeiten (z.B. technische Dienstleistungen, Ausbildung und Softwareentwicklung) verstanden werden, die allerdings allesamt wenig mit einer finanzintermediären Tätigkeit zu tun haben.²⁰³⁶ Eine Erweiterung des Geltungsbereichs des schweizerischen Geldwäschereiregimes auf Tätigkeiten *ausserhalb* des Finanzsektors, was vorliegend konsequent abgelehnt wird, würde auf jeden Fall einer Revision des GwG bedürfen.²⁰³⁷

In Bezug auf DApps im Allgemeinen und dezentrale Handelsplattformen im Besonderen soll, so scheint es dem Leser, künftig jede Person geldwäschereirechtlich erfasst sein, die in irgendeiner Form zum Erfolg eines Protokolls oder einer Plattform beiträgt oder in irgendeiner Form von der Ausführung eines Protokolls oder einer Plattform finanziell profitiert.²⁰³⁸ In der Praxis entwi-

²⁰³⁴ Vgl. FATF, Draft VASP Guidance 2021, 26; so bereits FATF, VASP Guidance 2019, 17. Ausführlich zu den US-verfassungsrechtlichen Vorbehalten gegenüber der *Regulierung* von Softwareentwicklern resp. der Softwareentwicklung Van Valkenburgh, *Electronic Cash*, 30–32, 45–53.

²⁰³⁵ Mit Fragen der Verfassungsmässigkeit von vage formulierten Exportbeschränkungen mussten sich US-amerikanische Gerichte bereits im Zusammenhang mit den *Crypto Wars* der 1990er Jahre beschäftigen, vgl. hierzu Stay, *Georgia State University Law Review* 1997, 596–600.

²⁰³⁶ Siehe Coin Center, *Comments on FATF Guidance*, 6.

²⁰³⁷ Vgl. zur ursprünglichen Beschränkung des persönlichen und sachlichen Geltungsbereichs auf den Finanzsektor Botschaft GwG 1996, 1115–1116.

²⁰³⁸ Vgl. FATF, Draft VASP Guidance 2021, 30 («When there is a need to assess a particular entity to determine whether it is a VASP or evaluate a business model where VASP status is unclear, a few general questions can help guide the answer. Among these would be who profits from the use of the service or asset, who established and can change the rules, who can make deci-

ckeln Personen regelmässig Smart Contracts und Protokolle, die sie anschliessend zur Ausführung bringen, ohne davon unmittelbar finanziell zu profitieren. Berühmt für dieses auch als «Fair Launch» bezeichnete Vorgehen ist etwa der Softwareentwickler Andre Cronje, der hinter Yearn Finance steht.²⁰³⁹ Cronje und andere Entwickler könnten künftig dem GwG unterstellt sein, wenn die Mitgliedsstaaten der Auffassung der FATF folgen würden.

Wiederum wird ersichtlich, wie weit die FATF bereit ist, das traditionelle Finanzintermediationskorsett auf dezentrale Geschäftsmodelle anzuwenden. Die FATF geht explizit davon aus, dass künftig nur noch wenige Geschäftsmodelle zu jeder Phase der Entwicklung und des Absatzes eines Produktes bzw. einer Dienstleistung über keine VASP verfügt.²⁰⁴⁰ *«Only entities that provide very limited functionality falling short of exchange, transfer, safekeeping, administration, control, and issuance will generally not be a VASP.»*²⁰⁴¹ Die FATF geht so weit in ihren Ausführungen, dass je nach Interpretation selbst vollständig dezentralisierte Handelsplattformen erfasst wären: *«The decentralization of any individual element of operations does not eliminate VASP coverage if the elements of any part of the VASP definition remain in place.»*²⁰⁴² Aufgrund der schwammigen Ausführungen der FATF bleibt indessen Vieles im Dunkeln.

Zwar hat die FATF die längeren Ausführungen zu «peer-to-peer trading platforms», deren allfällige Betreiber nach der 2019er-Guidance keine VASP darstellen, im Entwurf gestrichen,²⁰⁴³ doch sollen nach Ansicht der FATF zumindest Plattformen, die ausschliesslich einen «pure-matching service for buyers and sellers of VAs» anbieten, weiterhin nicht vom VASP-Begriff erfasst sein.²⁰⁴⁴ Dies ist offensichtlich richtig, bieten solche Plattformen doch lediglich ein «elektronisches Anschlagbrett» oder Bulletin Board (i.d.R. als Teil einer eigenständigen oder webbasierten Software), das sich auf die Publikation von Anzeigen für Angebote zum Kauf oder Verkauf von Kryptovermögenswerten beschränkt.

sions affecting operations, who generated and drove the creation and launch of a product or service, who possesses and controls the data on its operations, and who could shut down the product or service.»).

²⁰³⁹ Siehe Dale, Andre Cronje, Coindesk, *passim*.

²⁰⁴⁰ Siehe FATF, Draft VASP Guidance 2021, 26, 29.

²⁰⁴¹ FATF, Draft VASP Guidance 2021, 29.

²⁰⁴² FATF, Draft VASP Guidance 2021, 23.

²⁰⁴³ Siehe FATF, Draft VASP Guidance 2021, 31.

²⁰⁴⁴ Siehe FATF, Draft VASP Guidance 2021, 23, 29 («websites which offer only a forum for buyers and sellers to identify and communicate with each other»).

Die Draft Guidance vom März 2021 hat im Rahmen der öffentlichen Konsultation des Privatsektors eine Reihe von Rückmeldungen erhalten. Im Zentrum der Kritik stand v.a. der VASP-Begriff, der, wie oben dargestellt, bei Annahme der Vorschläge durch die FATF-Mitglieder eine problematische Ausdehnung erfahren würde.²⁰⁴⁵

Die laufenden Arbeiten der FATF wurden nach Aussage des EFD bereits die Grundlage in der oben erwähnte Revision von Art. 4 GwV berücksichtigt.²⁰⁴⁶ Allerdings ist es aufgrund des oben Gesagten fraglich, inwieweit dies mit Blick auf die Draft Guidance vom März 2021 tatsächlich der Fall ist. Der Bereich nichtunterstellter dezentraler Handelsplattformen würde bei unreflektierter Übernahme der Draft Guidance ins nationale Recht wohl nochmals deutlich enger werden.

iii. Updated Guidance vom Oktober 2021

Die finale Version der Updated Guidance vom Oktober 2021 hat im Wesentlichen die vorgeschlagenen Änderungen der Draft Guidance vom März 2021 übernommen. Sie verfolgt weiterhin denselben expansiven konzeptionellen Ansatz, um bestehende Unterstellungslücken zwischen dem traditionellen Finanzinstituten bzw. Vermögenswerten und VASPs bzw. VAs zu schliessen.²⁰⁴⁷ Namentlich sei auch für NFTs ein funktionaler Ansatz zu verwenden.²⁰⁴⁸ Von der technologieneutralen Anwendung der Empfehlungen müssen VASPs hingegen in Bezug auf den Schwellenwert betreffend Identifikationspflicht und der Travel Rule abweichen. Dabei handelt es sich um die Empfehlungen 10 und 16.²⁰⁴⁹

Die FATF versucht in der Updated Guidance die einzelnen Begriffselemente der VASP-Definition genauer zu umschreiben als bisher, was grundsätzlich zu begrüßen ist. Allerdings bleiben die Umschreibungen immer noch ziemlich vage. Unter dem zentralen Tatbestandsmerkmal «conduct activities or operations» versteht die FATF sowohl die Bereitstellung (*provision*) einer Dienstleis-

²⁰⁴⁵ Vgl. hierzu FATE, Second Review FATF Standards, 33–34 («[...] the FATF should further review its draft Guidance to ensure it is providing a clear message on how to apply the standards to decentralized structures, including the definition of a VASP, taking into account the risks, limitations and size of this sector.»).

²⁰⁴⁶ So aber scheinbar EFD, Erläuterungen Verordnung DLT 2021, 7; ferner auch FATE, VASP Guidance 2021, 96.

²⁰⁴⁷ So FATE, VASP Guidance 2021, 5, 9, 22–23, 24.

²⁰⁴⁸ Siehe FATE, VASP Guidance 2021, 24.

²⁰⁴⁹ Siehe FATE, VASP Guidance 2021, 25.

tung als auch die aktive Förderung oder Begünstigung (*active facilitation*) einer Dienstleistung, welche sich auf eine der unterstellten Aktivitäten bezieht. Der Zusatz «active» bzw. «actively» wurde im Gegensatz zum März-Entwurf wieder aufgenommen.²⁰⁵⁰ Er scheint nunmehr eine bewusst qualifizierende Rolle in der Guidance einzunehmen.

In der aktualisierten Guidance wurde zudem bestätigt, dass Technologie und Software weiterhin keine VASP-Position einnehmen können, sondern nur die allenfalls dahinterstehenden Personen.²⁰⁵¹ Dabei handele es sich um Personen, welche die DeFi-Anwendung kontrollieren oder genügend Einfluss auf sie haben:

«[...] creators, owners and operators or some other persons who maintain control or sufficient influence in the DeFi arrangements, even if those arrangements seem decentralized, may fall under the FATF definition of a VASP where they are providing or actively facilitating VASP services. This is the case, even if other parties play a role in the service or portions of the process are automated. Owners/operators can often be distinguished by their relationship to the activities being undertaken. For example, there may be control or sufficient influence over assets or over aspects of the service's protocol, and the existence of an ongoing business relationship between themselves and users, even if this is exercised through a smart contract or in some cases voting protocols. Countries may wish to consider other factors as well, such as whether any party profits from the service or has the ability to set or change parameters[,] to identify the owner/operator of a DeFi arrangement. [...] An individual token holder in such a scenario does not have such responsibility if the holder does not exercise control or sufficient influence over the VASP activities undertaken as a business on behalf of others.»²⁰⁵²

Dieser Abschnitt stellt eine wichtige Klarstellung gegenüber der Draft Guidance dar. Die FATF stellt namentlich klar, dass ein gewisses Kontrollelement existieren muss, damit überhaupt von einer VASP gesprochen werden kann.²⁰⁵³ Absurde Tatbestände, wie namentlich Business Development, tauchen darum zu Recht nicht mehr in der Guidance auf. Der Fokus auf ein Kontrollkonzept gegenüber vagen Begrifflichkeiten in der Draft Guidance ist eine spürbare Verbesserung nicht nur wegen der tendenziell grösseren Rechtssicherheit für die Marktteil-

²⁰⁵⁰ Vgl. etwa FATF, VASP Guidance 2021, 4, 25, 26, 27, 29.

²⁰⁵¹ Siehe FATF, VASP Guidance 2021, 27, 31–32.

²⁰⁵² FATF, VASP Guidance 2021, 27–28.

²⁰⁵³ Dies wird bestätigt in FATF, VASP Guidance 2021, 32, 35–36.

nehmer.²⁰⁵⁴ Die Schwierigkeit besteht natürlich immer noch darin, zu bestimmen, wann «Kontrolle» oder «genügender Einfluss» vorliegt. Gerade mit Blick auf die Verteilung von Governance Tokens in DAOs ist dies eine ungeklärte Frage, welche letztlich wohl von Fall zu Fall zu beantworten wäre. Ein damit zusammenhängendes Problem besteht sodann darin, dass Technologie und Gemeinschaft in soziotechnischen Systemen zusammenwachsen, was die theoretisch klare Unterscheidung zwischen nichtunterstellter Software und allenfalls unterstellten DAO-Teilnehmern in der Praxis verschwimmen lässt. Schliesslich sind glücklicherweise bisherige *Catch-all*-Klauseln, die kaum praktikabel gewesen wären, aus dem Text verschwunden.²⁰⁵⁵

Die FATF baute in der Guidance auf den bereits früher angedeuteten «Test»²⁰⁵⁶, welcher als Hilfsmittel dazu dienen soll, ein Geschäftsmodell unter Berücksichtigung der VASP-Kriterien einzuordnen: «[...] *a few general questions can help guide the answer. Among these would be who profits from the use of the service or asset, who established and can change the rules, who can make decisions affecting operations, who generated and drove the creation and launch of a product or service, who maintains an ongoing business relationship with a contracting party or another person who possesses and controls the data on its operations, and who could shut down the product or service.*»²⁰⁵⁷ Diese Liste von Faktoren ist nach vorliegender Ansicht immer im Lichte des von der FATF eingeführten Kontrollkonzepts zu lesen. Andernfalls führt dieser Test zu kaum vertretbaren Unterstellungen von Personen, die weit entfernt von der traditionellen Finanzintermediation sind.²⁰⁵⁸

Nicht unterstellt sind nach dem Gesagten etwa Nutzer und Händler, welche im Austausch für VAs Güter und Dienstleistungen erbringen. Diese Personen über gar nicht erst eine VASP-typische Aktivität aus.²⁰⁵⁹ Ebenfalls nicht erfasst sind Softwareentwickler und dies selbst dann, wenn sie für ihre Produkte Lizenzen vergeben. Als Software zählen etwa Protokolle für dezentrale Netz-

²⁰⁵⁴ GLM. Van Valkenburgh, Long-awaited FATF crypto guidance, *passim*; zurückhaltender BA, Response to FATF's Updated Guidance, Medium, *passim*.

²⁰⁵⁵ So wurde etwa die frühere, schwierig zu entschlüsselnde Aussage «*The decentralization of any individual element of operations does not eliminate VASP coverage if the elements of any part of the VASP definition remain in place.*» (FATF, Draft VASP Guidance 2021, 23) gestrichen.

²⁰⁵⁶ So etwa TRM, FATF Provides Final Guidance, *passim*, wo von einem «owner/operator test» die Rede ist.

²⁰⁵⁷ FATF, VASP Guidance 2021, 36.

²⁰⁵⁸ GLM. wohl auch Van Valkenburgh, Long-awaited FATF crypto guidance, *passim*.

²⁰⁵⁹ Siehe FATF, VASP Guidance 2021, 32.

werke und Applikationen oder Computercode für Self-Hosted Wallets. In diesen Fällen fehlt es regelmässig nicht nur an der Bereitstellung, sondern auch an der *aktiven* Förderung und Begünstigung einer Dienstleistung mit Bezug zu einer VASP-relevanten Aktivität.²⁰⁶⁰ Bei den Aktivitäten von Anbietern von Internet- und Cloudhosting-Dienstleistungen, Teilnehmern eines dezentralen Netzwerks (insb. Miner und Staker), Produzenten von Hardware Wallets und Anbietern von Self-Hosted Wallets handelt es sich nach Ansicht der FATF um zusätzliche Dienstleistungen oder Produkte (ancillary services or products), welche ebenfalls nicht den VASP-Begriff erfüllen.²⁰⁶¹

Für *dezentrale Handelsplattformen* hat sich im Wesentlichen das bisherige Bild bestätigt: Webseiten, welche Erwerber und Veräusserer lediglich zusammenführen, ohne selbst den Austausch oder die Übertragung von VAs abzuwickeln, gelten nach Auffassung der FATF nicht als VASP. Sog. Matching- oder «Finding»-Plattformen können demgegenüber nach Aussage der FATF ein VASP darstellen, selbst wenn diese Plattformen nicht in den Austauschvorgang involviert seien.²⁰⁶²

Die Guidance hebt wie bisher die besonderen Risiken von P2P-Transaktionen zwischen zwei Self-Hosted Wallets hervor, ist jedoch in der Tonlage deutlich zurückhaltender. Gleichzeitig anerkennt die FATF, dass P2P-Transaktionen aufgrund der Öffentlichkeit des verteilten Registers verfolgt und allenfalls mit anderen öffentlichen Informationen über die Transaktionsparteien verknüpft werden können, was der Strafverfolgung entgegen kommen könne.²⁰⁶³ Mit anderen Worten öffnet sich die FATF hier für einen technologischen Lösungsansatz zum «AML problem».²⁰⁶⁴ Dennoch scheint die FATF eine Welt ohne traditionelle Finanzintermediäre zu fürchten, welche die Wirksamkeit der heutigen Standards infrage stellen würde.²⁰⁶⁵ Weiterhin in der Kritik der FATF stehen etwa die Nutzung von AECs, Mixing- bzw. Tumbling-Dienstleistungen, Privacy Wallets sowie von Protokollen zur Anonymisierung der IP-Adresse (z.B. Tor).²⁰⁶⁶ Ferner stellt die Übertragung von Kryptovermögenswerten an Self-Hosted Wallets nach Auffassung der FATF einen besonderen

²⁰⁶⁰ Siehe FATF, VASP Guidance 2021, 29, 32, 33.

²⁰⁶¹ Siehe FATF, VASP Guidance 2021, 25, 32.

²⁰⁶² Siehe FATF, VASP Guidance 2021, 28, 35.

²⁰⁶³ Siehe FATF, VASP Guidance 2021, 18, 20, 21.

²⁰⁶⁴ Siehe zur Wirksamkeitsfrage des heutigen Geldwäschereiregimes unten, [V.2.12f.](#)

²⁰⁶⁵ Siehe FATF, VASP Guidance 2021, 19.

²⁰⁶⁶ Siehe FATF, VASP Guidance 2021, 20.

Risikofaktor dar.²⁰⁶⁷ Dasselbe gelte schliesslich bereits für die Verwendung oder den Einsatz eines Smart Contracts durch einen VASP.²⁰⁶⁸

Als Fazit kann festgehalten werden, dass die Updated Guidance vom Oktober 2021 im Vergleich zur Draft Guidance vom März 2021 ein wenig zurückhalten-der ist. Dies kommt in der differenzierteren Umschreibung des VASP-Begriffs als auch in der teils relativierenden Wortwahl zum Ausdruck. Aus den Ausführungen der FATF wird sogar erkennbar, dass selbst nach den Vorstellungen der Behörde nichtunterstellte DeFi-Anwendungen existieren können, wobei es allerdings nur «very few VA arrangements without VASPs» sein dürften.²⁰⁶⁹ Im praktisch gleichen Atemzug lässt die FATF die Tür zur Reintermediation durch die Mitgliedsstaaten weit offen: «Countries should consider, where appropriate, any mitigating actions, where DeFi services operating in this manner are known to them. [...] where no VASP is identified, countries may consider the option of requiring that a regulated VASP be involved in activities related to the DeFi arrangement [...]»²⁰⁷⁰

Die FATF verfolgt mit ihrer neuen Guidance offenbar das Ziel, den Start neuer dezentraler Systeme möglichst zu verhindern²⁰⁷¹ und existierende Systeme in die Konturen des bestehenden Finanzintermediationssystems zurückzudrängen.²⁰⁷²

2.4 Aufgreifkriterien der Finanzintermediation

Die Geldwäschereigesetzgebung enthält praktischerweise in Form einer Generalklausel in Art. 2 Abs. 3 GwG eine uneigentliche Legaldefinition des Finanzintermediärs. Diese beschränkt nach vorliegender Auffassung ohne eine klare gegenteilige gesetzliche Regelung auch den sachlichen Geltungsbereich der Finanzintermediäre nach Art. 2 Abs. 2 GwG.²⁰⁷³

Aus dieser Generalklausel lassen sich namentlich die Annahme *fremder* Vermögenswerte, die Aufbewahrung *fremder* Vermögenswerte, die Hilfe, *fremde* Vermögenswerte anzulegen, und die Hilfe, *fremde* Vermögenswerte zu übertragen, als finanzintermediäre Tätigkeiten herleiten. Damit lehnt sich das GwG

²⁰⁶⁷ Siehe FATF, VASP Guidance 2021, 21.

²⁰⁶⁸ Siehe FATF, VASP Guidance 2021, 21.

²⁰⁶⁹ Siehe FATF, VASP Guidance 2021, 28, 31, ferner 35.

²⁰⁷⁰ FATF, VASP Guidance 2021, 28.

²⁰⁷¹ Vgl. etwa die Ausführungen in FATF, VASP Guidance 2021, 27, 28, 32, 33, 36.

²⁰⁷² Ähnlich wie hier Whitehouse-Levine, Twitter, *passim*; Boiron, Twitter, *passim*.

²⁰⁷³ Siehe auch oben, [V.1.3](#).

an den Geltungsbereich von Art. 305^{ter} Abs. 1 StGB an.²⁰⁷⁴ «Fremd» sind die Vermögenswerte²⁰⁷⁵, wenn sie, soweit dinglich, nicht im Eigentum des Finanzintermediärs stehen und, soweit obligatorisch, der Finanzintermediär nicht Gläubiger des Rechts (z.B. einer Forderung) ist.²⁰⁷⁶ Mit dem Fremdheit der Vermögenswerte ist konkret ein Geldwäschereirisiko verbunden.²⁰⁷⁷ Geschäfte mit *eigenem* Vermögen fallen *e contrario* grundsätzlich nicht in den Geltungsbereich des GwG.²⁰⁷⁸ Ausnahmen von dieser klaren Zweiteilung können, wie erwähnt, dort bestehen, wo der Gesetzgeber dies explizit anordnet. Die Unterscheidung zwischen fremdem und eigenem Vermögen ist etwa bei Multisig-Verwahrungslösungen von Bedeutung.²⁰⁷⁹

*Die Intermediation fremder Vermögenswerte im Finanzsektor bildet damit das massgebliche Aufgreifkriterium für die Geldwäschereiregulierung.*²⁰⁸⁰ Nach dem Gesagten ist etwa klar, weshalb die reine Anlageberatung, d.h. die Tätigkeit eines Anlageberaters, der auch nicht ausnahmsweise auf Grundlage einer Einzelvollmacht Finanzanlagen auf Rechnung des Kunden tätig, nicht unter das GwG fällt.²⁰⁸¹

Die Generalklausel in Art. 2 Abs. 3 GwG ist nach verbreiteter Auffassung bewusst unscharf und darum weit auszulegen.²⁰⁸² Überraschend ist dennoch, dass in *systemwidriger* Abweichung zum klaren Wortlaut der Bestimmung nicht alle der aufgezählten Spezialtatbestände in Art. 2 Abs. 3 GwG die Intermediation *fremder* Vermögenswerte betreffen. Entsprechend kann unterschieden werden zwischen Fällen, in denen der Finanzintermediär tatsächlich

²⁰⁷⁴ Siehe Botschaft GwG 1996, 1117; ferner Botschaft StGB 1989, 1089 («Die Umschreibung der Tätigkeiten [...] sollte dabei das Gesamtfeld der typischen Transaktionen des Finanzsektors abdecken.»).

²⁰⁷⁵ Siehe SHK GwG-Schären, Art. 2 N 73 («subjektive Rechte [...], die mit dem Finanzsektor zusammenhängen»).

²⁰⁷⁶ Siehe OFK GwG-Wyss, Art. 2 N 26; ferner SHK GwG-Schären, Art. 2 N 75.

²⁰⁷⁷ Vgl. etwa BGer 2A.62/2007 vom 30. November 2007, E. 4 («Es liegt auf der Hand, dass die genannten Tätigkeiten, bei denen der Finanzintermediär meist direkt in den Besitz fremder Vermögenswerte gelangt, eine erhöhte Gefahr der Geldwäscherei mit sich bringen.»).

²⁰⁷⁸ Siehe Rohr, Finanzintermediär, 8–9; ferner Nagel, Geltungsbereich GwG, Rz. 203.

²⁰⁷⁹ Siehe etwa zu Self-Hosted Multisig-Wallets unten, [V.2.8c](#).

²⁰⁸⁰ Siehe auch OFK GwG-Wyss, Art. 2 N 28; ferner Kuster, SZW 1999, 243; ferner SHK GwG-Schären, Art. 2 N 72, 75.

²⁰⁸¹ Vgl. Art. 2 Abs. 3 lit. f GwG; FINMA-RS 11/1 «Tätigkeit als Finanzintermediär nach GwG», Rz. 96.

²⁰⁸² Siehe Botschaft GwG 1996, 1117–1118; BGer 2A.62/2007 vom 30. November 2007, E. 3.2 («Die gewählte Regelungstechnik erschwert es, den Begriff des Finanzintermediärs in einer eindeutigen und kohärenten Weise abzugrenzen.»); ausführlich zu den Gründen solcher Gesetzgebung SHK GwG-Schären, Art. 2 N 57.

die rechtliche (oder auch nur faktische) *Verfügbarmacht über fremde Vermögenswerte* erhält, und Fälle, die einer ähnlichen Risikotypologie entsprechen. Ein Beispiel der ersten Fallgruppe ist die berufsmässige Vermögensverwaltung, in deren Rahmen der Vermögensverwalter hilft, fremde Vermögenswerte anzulegen.²⁰⁸³ Ein Beispiel der zweiten Fallgruppe ist die Tätigkeit einer Investmentgesellschaft nach Art. 2 Abs. 3 KAG,²⁰⁸⁴ die zwar zivilrechtlich *eigene Vermögenswerte* verwaltet, deren Tätigkeit bei wirtschaftlicher Betrachtungsweise aber vergleichbare Geldwäschereirisiken mit sich bringen kann.²⁰⁸⁵ Klar systemwidrig ist die geldwäschereirechtliche Erfassung des Handels des Finanzintermediärs, der in eigenem Namen auf eigene Rechnung, d.h. auf *eigenes Risiko*, mit Banknoten und Münzen, Geldmarktinstrumenten, Devisen, Edelmetallen, Rohwaren und Effekten (Wertpapiere und Wertrechte) sowie deren Derivaten handelt (Art. 2 Abs. 3 lit. c GwG).²⁰⁸⁶ Eine weitere Systemwidrigkeit mag auch in Art. 2 Abs. 3 lit. a GwG erblickt werden, wonach das Betreiben des Kreditgeschäfts unterstellungspflichtig ist.²⁰⁸⁷ Dies gilt selbst dann, wenn der Finanzintermediär Kredite mit eigenen Mitteln finanziert. Ein erhöhtes Risiko der Geldwäscherei ergibt sich beim Kreditgeschäft bei den Zins- und Amortisationszahlungen des Kreditnehmers. Allerdings ist nicht der Kreditnehmer, der für solche Zahlungen verbrecherisch erlangte Mittel einsetzen könnte, sondern der Kreditgeber dem GwG unterstellt.²⁰⁸⁸ Sowohl die Unterstellung der Handelstätigkeit des Finanzintermediärs als auch von dessen Kreditgeschäft sind gesetzlich normiert, sodass der Gesetzgeber offenbar die rechtsdogmatischen Systemwidrigkeiten bewusst in Kauf nimmt.

Das Bundesgericht fordert wegen der unscharfen Regulierungstechnik im GwG, dass dem *konkreten Geldwäschereirisiko* des Einzelfalles Rechnung zu tragen ist.²⁰⁸⁹ Der Geltungsbereich des GwG darf mit anderen Worten nicht auf alle Geschäfte ausgedehnt werden, die allein nach dem Wortlaut von Art. 2

²⁰⁸³ Die Vermögensverwaltung erfolgt in aller Regel im Rahmen eines Mandatsverhältnisses auf Basis einer Vollmacht des Kunden des Vermögensverwalters; siehe FINMA-RS 11/1 «Tätigkeit als Finanzintermediär nach GwG», Rz. 90.

²⁰⁸⁴ Siehe FINMA-RS 11/1 «Tätigkeit als Finanzintermediär nach GwG», Rz. 94.

²⁰⁸⁵ Siehe SHK GwG-Schären, Art. 2 N 132; *anders noch* Graber, Kommentar GwG, Art. 2 N 21; zu den *Geldwäschereirisiken* Luthiger, Investmentgesellschaften, Rz. 300–303; *generell* kritisch zur Unterstellung Kunz, ZBJV 2006, *passim*.

²⁰⁸⁶ So auch SHK GwG-Schären, Art. 2 N 115 m.w.N.; ferner OFK GwG-Wyss, Art. 2 N 26.

²⁰⁸⁷ Vgl. BGer 2A.62/2007 vom 30. November 2007, E. 4.

²⁰⁸⁸ Siehe Art. 3 lit. a GwV; hierzu ausführlich SHK GwG-Schären, Art. 2 N 84–85.

²⁰⁸⁹ BGer 2A.62/2007 vom 30. November 2007, E. 8 («Der vorinstanzlichen Gesetzesauslegung, welche die Frage, ob ein Risiko der Geldwäscherei bei den Kundenbeziehungen der Beschwerdeführerin bestehen kann, gänzlich ausblenden will, ist daher nicht zu folgen.»), siehe so dann auch E. 9.

Abs. 3 erfasst werden. Wenn es faktisch nicht möglich ist, mit einer bestimmten Tätigkeit Geld zu waschen, so soll auch keine Unterstellung unter das Geldwäschereigesetz erfolgen.²⁰⁹⁰ SIMON SCHÄREN geht richtigerweise noch einen Schritt weiter, indem er aus Gründen der Verhältnismässigkeit und des (fehlenden) öffentlichen Interesses fordert, dass bei überschaubaren und transparenten Verhältnissen von einer Unterstellung *abzusehen* ist, wenn die Anwendung der GwG-Bestimmungen keinen entscheidenden Beitrag zur Verringerung des Geldwäschereirisikos beiträgt.²⁰⁹¹

Es kann zusammengefasst werden, dass die Bestimmungen zur Verhinderung von Geldwäscherei und Terrorismusfinanzierung, soweit auf gesetzlicher Ebene nichts Anderes angeordnet wird, aus Gründen der Rechtssicherheit an den Begriff der Finanzintermediation anknüpfen sollte. Dieser Begriff ist so auszulegen, dass er grundsätzlich ausschliesslich die Intermediation fremder Vermögenswerte im Finanzsektor betrifft. Das konkrete Geldwäschereirisiko einer unter diesen Tatbestand fallenden finanzintermediären Tätigkeit ist gegebenenfalls als Korrektiv einzusetzen, um risikoarme Aktivitäten von der Unterstellung auszunehmen.

2.5 Dezentrale Handelsplattformen

a. Definition virtueller Währungen

Eine Begriffsdefinition virtueller Währungen findet sich erstmals im Bericht des Bundesrats vom Juni 2014. Danach gilt als virtuelle Währung eine *«[d]igitale Darstellung eines Wertes, welche im Internet handelbar ist und zwar Funktionen von Geld übernimmt, jedoch als Zahlungsmittel nur von Mitgliedern einer spezifischen virtuellen Gemeinschaft akzeptiert wird. Sie ist jedoch nirgends gesetzliches Zahlungsmittel. Diese Währungen haben eine eigene Denomination. Sie werden von einer nichtregulierten Institution oder einem Netzwerk von Rechnern emittiert und kontrolliert. Sie unterscheiden sich von E-Geld folglich insofern, dass diese Währungen nicht durch ein gesetzliches Zahlungsmittel unterlegt sind [...]»*²⁰⁹²

²⁰⁹⁰ Siehe SHK GwG-Schären, Art. 2 N 58.

²⁰⁹¹ Siehe SHK GwG-Schären, Art. 2 N 59.

²⁰⁹² Bundesrat, Bericht zu virtuellen Währungen, 30.

Die FINMA hält darüber hinaus fest: «[Virtuelle Währungen] existieren lediglich als digitaler Code und haben deswegen auch kein materialisiertes Gegenstück bspw. in Form von Münzen oder Noten. Jedoch können virtuelle Währungen als Zahlungsmittel für reale Güter und Dienstleistungen verwendet werden. Aufgrund des Gesagten sind die virtuellen Währungen als Vermögenswerte einzuordnen.»²⁰⁹³

Virtuelle Währungen sind Kryptovermögenswerte, die eine Zahlungsmittelfunktion erfüllen. Darunter fallen nach der Terminologie der FINMA in erster Linie Kryptowährungen bzw. Zahlungs-Token. Nutzungs- und Anlage-Token dienen demgegenüber typischerweise nicht als Zahlungsmittel für reale Güter und Dienstleistungen.²⁰⁹⁴ Dies ist in Einklang mit der neuen Bestimmung in Art. 4 Abs. 1^{bis} lit. c GwV, worin bestimmt wird, dass virtuelle Währungen als «nicht in Bargeld bestehende Zahlungsmittel» gelten, die tatsächlich oder nach der Absicht des Organisators oder Herausgebers als Zahlungsmittel für den Erwerb von Waren oder Dienstleistungen eingesetzt werden oder der Geld- und Wertübertragung dienen.²⁰⁹⁵

Die von den Behörden verwendete Terminologie ist insoweit ungenau, als dass virtuelle Währungen angesichts der Realität des Phänomens nicht als rein *virtuell* zu betrachten sind, wie etwa ein Zahlungsmittel, das ausschliesslich in einem Computerspiel verwendet wird.²⁰⁹⁶ Die von einem dezentralen Netzwerk emittierten virtuellen Währungseinheiten bilden zudem grundsätzlich keinen Wert ab, der innerhalb oder ausserhalb der Blockchain existiert. Virtuelle Währungen in diesem Sinne sind demgegenüber der Funktionsweise eines dezentralen Systems inhärent. Will man sie als digitale Darstellung eines Werts bezeichnen, so bestünde der Wert in der Verfügungsmacht über Datenstrukturen, die in einem verteilten Register abgespeichert sind und somit gegebenenfalls dem ökonomischen Gesetz der Knappheit gehorchen. Der Begriff der Kryptowährung ist mit Blick auf dezentrale Systeme entsprechend vorzuziehen.²⁰⁹⁷

²⁰⁹³ FINMA, Erläuterungsbericht GwV-FINMA 2015, 11; ferner FINMA, Faktenblatt Virtuelle Währungen, 1. Januar 2020, *passim*.

²⁰⁹⁴ Vgl. FINMA, Wegleitung ICOs, 3.

²⁰⁹⁵ Vgl. auch die Begriffsumschreibung in EFD, Erläuterungen Verordnung DLT, 23 FN 13 («Virtuelle Währungen sind eine Art von kryptobasierten Vermögenswerten und zeichnen sich besonders dadurch aus, dass sie als Zahlungsmittel eingesetzt werden können.»).

²⁰⁹⁶ Vgl. statt vieler Busch, El Salvador, NZZ, *passim*; skeptisch demgegenüber selbst für Bitcoin Omlor, ZHR 2019, 313–314, 319.

²⁰⁹⁷ Siehe zum Begriff der Kryptowährungen in technischer Hinsicht oben, [III.2.4b](#).

b. Definition dezentraler Handelsplattformen

Der Begriff der dezentralen Handelsplattform verwendete der Bundesrat, soweit ersichtlich, erstmals im DLT-Bericht von 2018: Dabei wird darauf hingewiesen, dass die «Token-Guthaben» grundsätzlich bei den Nutzern zunächst auf ihren eigenen Blockchain-Adressen verbleiben. Zwecks Ausführung eines Handelsgeschäfts würden die Kryptovermögenswerte typischerweise vorgängig an einen Smart Contract überwiesen, wobei für die Abwicklung, welche direkt zwischen den beteiligten Parteien erfolgt, in der Regel wie bei einer herkömmlichen Blockchain-Transaktion wieder die kryptographische Signierung der Transaktion durch den Anwender selbst notwendig sei.²⁰⁹⁸

Mit Blick auf das Geldwäschereirecht scheint das EFD in seinen Erläuterungen vom 18. Juni 2021 zum neuen Art. 4 Abs. 1 lit. b GwV einen engeren Begriff zu verwenden, wobei es nicht um eine abschliessende Definition handeln soll: «Darunter fallen beispielsweise Handelsplattformen, die nicht im Besitz des privaten Schlüssels der Kunden sind, die Übertragung der virtuellen Währungen jedoch mittels Smart Contract ermöglichen und dabei die Aufträge bestätigen, freigeben oder sperren können oder anderweitig Kontrolle über den Smart Contract haben (sogenannte dezentrale Handelsplattformen)».²⁰⁹⁹

Namentlich im Rahmen der vertieften Analyse von Art. 4 Abs. 1 lit. b GwV soll dieses engere Begriffsverständnis zugrunde gelegt werden. Es sei einmal mehr darauf hingewiesen, dass das Konzept der dezentralen Handelsplattform in dieser Arbeit von der Begriffsverwendung des Bundesrates oder des EFD abweichen kann.²¹⁰⁰

c. Vorliegen einer finanzintermediären Tätigkeit?

Aufgrund der Tatsache, dass unter Zuhilfenahme einer dezentralen Handelsplattform ein Transfer von Kryptovermögenswerten bewirkt werden kann, stellt sich die Frage, ob eine solche Plattform bzw. allenfalls dahinterstehende Personen eine finanzintermediäre Tätigkeit im Sinne von Art. 2 Abs. 3 GwG erbringen.

²⁰⁹⁸ Siehe Bundesrat, DLT-Bericht 2018, 29, 144, 146–147; leicht *früher* war allerdings das NRA betreffend Kryptovermögenswerte KGGT, NRA Krypto 2018, 19, 38–39.

²⁰⁹⁹ EFD, Erläuterungen Verordnung DLT 2021, 22.

²¹⁰⁰ Siehe hierzu oben, [IV.1.2](#).

Das heutige Regime zur Verhinderung von Geldwäscherei und Terrorismusfinanzierung beruht auf dem Konzept des Gatekeeping. *Gatekeeping* geht über die bloße Intermediation hinaus, indem Gatekeepers etwa für die Sicherstellung der Einhaltung von Regeln durch einen Marktteilnehmer (typischerweise Emittenten von Kapitalmarktpapieren) verantwortlich sind und somit für andere Marktteilnehmer (typischerweise Investoren) verlässliche Qualitätssignale über ersteren produzieren können.²¹⁰¹ Gatekeeping im Bereich der Geldwäschereiregulierung ist nicht unähnlich zu dieser kapitalmarktökonomischen Sichtweise, doch werden in diesem Bereich Qualitätssignale in Bezug auf die regulatorische Qualität von Finanzströmen gegenüber den staatlichen Strafverfolgungsbehörden produziert. Die KGGT spricht davon, dass Finanzintermediäre für die «Tauschbedingungen bürg[en]».²¹⁰² Dabei tritt im GwG das Interesse an der Strafverfolgung neben den aufsichtsrechtlich motivierten Funktionsschutz.²¹⁰³ Finanzintermediäre und staatliche Behörden kollaborieren hier in enger rechtlicher Verzahnung –²¹⁰⁴ darunter in manchem Fall aus primär politischen Motiven.²¹⁰⁵ Der Finanzbereich ist wohl einer der wenigen Bereiche, in denen das Meldesystem zur Sammlung von heiklen Personendaten führt (Art. 9 GwG), ohne diesbezüglich die Bedingungen der Anordnung von Zwangsmassnahmen nach der Strafprozessordnung (Art. 196 ff. StPO) einhalten zu müssen. Zumindest in technischer Hinsicht ähnlich ist die Rolle

²¹⁰¹ Siehe grundlegend Kraakman, *Journal of Law, Economics, & Organization* 1986, 62, 93–100, der zwischen «market gatekeepers» und «public gatekeepers» unterscheidet; Coffee, *Gatekeepers*, 1–3, der von einem «reputational intermediary» spricht; ferner Payne, in: Moloney/Ferran/Payne, *Role of Gatekeepers*, 256–257; ausführlich zu Investmentanalysten und Kreditratingfirmen Moloney, *Securities and Markets Regulation*, 202–204, 637–639 («investment intermediation process»); ausführlich sodann zur Rolle von Gatekeepern Bühler, *Corporate Governance*, Rz. 528–538, der einen Schwerpunkt auf die Reduktion von Informationsasymmetrien legt.

²¹⁰² Siehe KGGT, NRA 2015, 98.

²¹⁰³ Siehe Botschaft FINMAG 2006, 2859–2860.

²¹⁰⁴ Vgl. zur Garantenstellung von Finanzintermediären, die insb. für die Frage der Strafbarkeit der Geldwäscherei durch Unterlassung im Sinne von Art. 305^{bis} i.V.m. 11 StGB relevant ist, BGE 136 IV 188, E. 6.2.2 («Il résulte désormais des normes concernant la lutte contre le blanchiment d'argent que les intermédiaires financiers doivent, dans les limites fixées par la loi [...], collaborer avec les autorités compétentes. Ces obligations légales créent une position de garant.»); 119 IV 242, E. 1e («Verbindungsstück zwischen legal und illegaler Ökonomie»); Botschaft StGB 1989, 1064 («Achillesferse»); sodann die Übersicht bei Ackermann/Zehnder, in: Ackermann, Art. 305^{bis} StGB N 121; kritisch zu dieser Kollaborationsfunktion von Finanzintermediären insb. Arzt, in: Diederichsen/Dreier, *Missglücktes Strafgesetz*, *passim*; ferner Strasser, SJZ 2011, *passim*.

²¹⁰⁵ Siehe die rechtspolitischen Überlegungen zur Unterstellung der *Steuergeldwäscherei* in SHK GwG-Basse, Art. 1 N 17–44 m.w.H.; sodann prägnant Arzt, ST 2011, 268–270.

der finanzmarktrechtlichen Prüfgesellschaften zwischen beaufsichtigten Unternehmen und der FINMA, als deren «verlängerter Arm» sie fungieren.²¹⁰⁶

Im Kryptobereich üben heute insb. zentrale Handelsplattformen, die den Austausch von Fiat- gegen Kryptowährungen ermöglichen, eine Gatekeeping-Funktion aus. Die Unterscheidung von Gatekeepern, die das traditionelle Finanzsystem und DeFi miteinander verbinden, und solchen, die *innerhalb* von DeFi operieren, ist den schweizerischen Finanzmarktgesetzen aber grundsätzlich fremd und findet, soweit ersichtlich, auch keine Abbildung in der Praxis der FINMA.

Dem Konzept des Gatekeeping folgend, kann festgehalten werden, dass Transaktionen, die *unmittelbar* zwischen den endbegünstigten Parteien eines Geschäfts, d.h. ohne Zuhilfenahme eines Intermediärs erfolgen, sich grundsätzlich ausserhalb des Geltungsbereichs des Geldwäschereirechts befinden. In diesem Fall ist kein Gatekeeper in den Abwicklungsprozess involviert.²¹⁰⁷

Eine Ausnahme von dieser Regel findet sich in Art. 8a GwG und Art. 13 ff. GwV hinsichtlich der Verwendung von Bargeld im Rahmen von Handelsgeschäften.²¹⁰⁸ Bei *Handelsgeschäften* handelt es sich um Rechtsgeschäfte, welche zum Austausch von Gütern gegen Bargeld führen (vgl. Art. 2 Abs. 1 lit. b GwG). Hier kommen die GwG-Vorschriften direkt auf die an einem Kaufvertrag beteiligten Parteien zur Anwendung.²¹⁰⁹ Nach Art. 8a GwG hat der Händler für die Einhaltung von Sorgfaltspflichten zu sorgen. Nach vorliegender Auffassung ist wenig umstritten, dass die im Rahmen von solchen Handelsgeschäften geltenden Sorgfaltspflichten keine Bedeutung für die Übertragung von Kryptovermögenswerten haben. Ihre Anwendung auf Kryptovermögenswerte bzw. dezentrale Handelsplattformen ist aufgrund des klaren Wortlauts

²¹⁰⁶ Vgl. FINMA-RS 13/3 «Prüfwesen», Rz. 1; vgl. auch BGE 99 Ib 104, E. 5 m.w.H. («Die Revisionsstelle wird zwar von der beaufsichtigten Bank ausgewählt, beauftragt und honoriert, doch besorgt sie eine im öffentlichen Interesse liegende Aufgabe. Aus der richtigen Ausübung dieser Funktion können sich indessen Reibungen zwischen Bank und Revisionsstelle ergeben. Diese ist unter Umständen verpflichtet, den Gläubigerinteressen gegen den Widerstand der Bank Nachachtung zu verschaffen [...] Ihre Stellung ist also nicht einmal mit derjenigen des Anwaltes voll vergleichbar, da dieser grundsätzlich die Interessen seines Klienten zu vertreten hat.»).

²¹⁰⁷ Vgl. Bundesrat, Bericht zu virtuellen Währungen, 16; KGGT, NRA Krypto 2018, 34.

²¹⁰⁸ Siehe SHK GwG-Schott/Kessler, Art. 8a N 9, die von einem Paradigmenwechsel sprechen; vgl. sodann in Bezug auf *Designated Non-Financial Businesses and Professions* (DNFBPs) FATF, Recommendations Oktober 2020, 19–21.

²¹⁰⁹ Vgl. Botschaft GAFI 2013, 629, 676.

(«Bargeld», «in bar») ausgeschlossen.²¹¹⁰ Beim fraglichen Handelsgeschäft handelt es sich zudem entweder um einen Kaufvertrag nach Art. 184 ff. OR oder ein Kommissionsgeschäft nach Art. 425 ff. OR.²¹¹¹ Bei der Nutzung dezentraler Handelsplattformen steht demgegenüber nicht der Kauf von Gütern, sondern in aller Regel der Tausch unterschiedlicher Kryptovermögenswerte im Vordergrund.²¹¹² Vergleichbar mit einem Devisenhandelsgeschäft (z.B. CHF gegen USD), dessen rechtliche Einordnung notabene umstritten ist,²¹¹³ qualifizieren Tauschgeschäfte über Kryptovermögenswerte abhängig von den konkreten auszutauschenden Kryptovermögenswerten als Kaufvertrag, Tauschvertrag oder Innominatvertrag.²¹¹⁴ Wenn demgegenüber eine tokenisierte Aktie gegen eine virtuelle Währung getauscht werden soll, handelt es sich zivilrechtlich in aller Regel um ein Kaufgeschäft. In diesen Fall besteht eine Effekten- und Geldseite, wie es für den traditionellen Börsenhandel üblich ist,²¹¹⁵ wobei die Nutzung einer dezentralen Handelsplattformen die beteiligten Wertpapierhäuser freilich obsolet macht.²¹¹⁶ Selbstredend liegt auch in diesem Fall kein Handelsgeschäft im Sinne des GwG vor. Der Vollständigkeit halber sei erwähnt, dass Bargeldtransaktionen, die sich im *privaten* Bereich zutragen, ohnehin nicht von der GwG-Regelung erfasst sind.²¹¹⁷

Aufgrund der in dieser Arbeit gewonnenen Erkenntnis, dass es sich bei dezentralen Netzwerken um eine neuartige Form der netzwerkbasierten Interme-

²¹¹⁰ Ähnlich SHK GwG-Schott/Kessler, Art. 8a N 13, die allerdings hinsichtlich virtueller Währungen lediglich davon ausgehen, dass es keine Anhaltspunkte für eine extensive Auslegung des Bargeldbegriffs gibt; *ungenau* allerdings FINMA, Erläuterungsbericht GwV-FINMA 2015, 12, wo die Begriffe Händler und Finanzintermediär offenbar austauschbar verwendet werden.

²¹¹¹ So ausdrücklich EFD, Erläuterungsbericht GwV 2015, 8; vgl. ferner Art. 15 GwV, wo bestimmt wird, dass als Güter Gegenstände eines Fahrniskaufs oder Grundstücke, die Gegenstand eines Grundstückkaufs sein können, gelten.

²¹¹² Vgl. hinsichtlich der Einstufung von Kryptowährungen als *Tauschmittel* BGer 6B_99/2019, 6B_148/2019 vom 18. April 2019, E. 2.3.2.

²¹¹³ Siehe hierzu etwa BGE 51 II 199, E. 1 (*Kauf*); 103 II 190, E. 1 (*Kauf*); CR CO I-Vulliét, Art. 237 N 2 (*Tausch*); HGer ZH vom 24. Januar 2006, E. 2.3.1, ZR 105/2006, 122 (*Innominat*); Kleiner, Internationales Devisen-Schuldrecht, Rz. 31.36–31.42 (*Innominat*); Koenig, Interbankendevisenhandel, 35–36 (*Innominat* bzw. Vertrag sui generis); BSK OR I-Koller, Art. 184 N 10 m.w.H., 19 (*offenlassend*).

²¹¹⁴ Für das Vorliegen eines *Innominatvertrages* beim Erwerb digitaler Währungen, die als verbreitetes Tauschmittel dienen und somit Geldcharakter aufweisen, im Austausch gegen Fiatwährungen aussprechend Eggen, Jusletter vom 4. Dezember 2017, Rz. 36, 39, 42.

²¹¹⁵ Vgl. diesbezüglich Zobl/Kramer, Kapitalmarktrecht, Rz. 1243.

²¹¹⁶ Siehe hierzu Weber, SZW 2021, 454–456.

²¹¹⁷ Siehe EFD, Erläuterungsbericht GwV 2015, 8.

diation handelt,²¹¹⁸ ist zu prüfen, ob dezentrale Handelsplattformen in geldwäschereirechtlicher Hinsicht tatsächlich lediglich unmittelbare Transaktionen zwischen den Endbegünstigten ermöglichen. Falls dem so ist, würden Austauschgeschäfte über dezentrale Handelsplattformen am ehesten mit der Verwendung von Bargeld vergleichbar sein.

d. Keine alleinige Verfügungsmacht über fremde Vermögenswerte

Das Kriterium der alleinigen Verfügungsmacht über fremde Vermögenswerte nimmt eine prominente Stellung im schweizerischen Geldwäschereirecht ein. Namentlich ist es eines der Definitionselemente des Finanzintermediärs nach Art. 2 Abs. 3 GwG.²¹¹⁹

Nach der bisherigen Auffassung der FATF kommt dem Umstand, dass eine Person die Kontrolle über die *Virtual Assets* einer anderen Person innehat, eine vorrangige Stellung zu.²¹²⁰ Die FATF hat dies in der Vergangenheit selbst für Kryptovermögenswerte festgehalten, die in Smart Contracts aufbewahrt werden, über deren ausschliessliche und unabhängige Kontrolle eine Drittperson verfügt.²¹²¹ Der Bundesrat hat ausserdem das Vorliegen von Verfügungsmacht in den vergangenen Jahren als zentral bezeichnet für die Frage der Abgrenzung unterstellter Anbieter von Custodial Wallets und nichtunterstellter Anbieter von Non-Custodial Wallets.²¹²² Das Kriterium der rechtlichen oder faktischen Verfügungsmacht über fremde Vermögenswerte ist denn auch wesentlicher Bestandteil der heutigen FINMA-Aufsichtspraxis.²¹²³ Vergleichbar

²¹¹⁸ Siehe oben, [II.5](#).

²¹¹⁹ Siehe UK KSt GwG, Rz. 324; Rimle, Recht des schweizerischen Finanzmarktes, N 16; Rohr, Finanzintermediär, 9; ferner Nagel, Geltungsbereich GwG, Rz. 204, der Verfügungsmacht oder zumindest «ein gewisses Mass an Kontrolle» durch den Finanzintermediär voraussetzt.

²¹²⁰ Siehe insb. FATF, VASP Guidance 2019, 14 («Further, countries should consider whether the activities involve a natural or legal person that conducts as a business the five functional activities described for or on behalf of another natural or legal person, both of which are essential elements to the definition and the latter of which implies a certain level of 'custody' or 'control' of the virtual asset [...]»); ferner FATF, Recommendations Oktober 2020, 130.

²¹²¹ Siehe FATF, VASP Guidance 2019, 16. Jedoch wird *nunmehr* ein deutlich relativierender Kontrollbegriff vertreten, der insb. auch Multisig-Mechanismen erfassen könnte; vgl. hierzu FATF, VASP Guidance 2021, 29.

²¹²² Siehe etwa Bundesrat, DLT-Bericht 2018, 145–146.

²¹²³ Siehe zur Aufsichtspraxis FINMA, Jahresbericht 2018, 31–32; ferner der Bundesrat, DLT-Bericht 2018, 146 m.w.N., 147, 150; ebenfalls KGGT, NRA Krypto 2018, 38–39; sodann mit Blick auf ICOs FINMA, Wegleitung ICOs, 7.

stellt sich die Situation für Wallet-Anbieter in den USA dar, wo die «total independent control over the value» vorausgesetzt wird.²¹²⁴

Das Nichtvorliegen von Verfügungsmacht hat auch praktische Konsequenzen: Ohne Verfügungsmacht über die Vermögenswerte seiner Kunden kann ein Finanzintermediär bspw. der Pflicht zur Vermögenssperre der ihm anvertrauten Vermögenswerte gemäss Art. 10 GwG nicht nachkommen.²¹²⁵ Das Vorliegen von Verfügungsmacht kann namentlich bei *Dienstleistungen im Zahlungsverkehr* wesentlich sein. Im Rahmen solcher Dienstleistungen werden die Vermögenswerte regelmässig zwecks Abwicklung von Zahlungsaufträgen oder sonstigen Übertragungsgeschäften dem Finanzintermediär übertragen bzw. anvertraut.²¹²⁶ Anders ist dies etwa bei Kassageschäften, wie etwa beim Geldwechsel, welche Zug um Zug erfüllt werden.

Eine Grundbedingung einer dezentralen Handelsplattformen ist, wie gesehen,²¹²⁷ der Umstand, dass den an einem Austausch beteiligten Nutzern einer Plattform jederzeit die *ausschliessliche Kontrolle über ihre Kryptovermögenswerte* zukommt. Sie alleine verfügen über die dazugehörigen Private Keys.

Selbst in denjenigen Fällen, in denen Kryptovermögenswerte sich zwecks Ausführung eines Austauschgeschäfts vorübergehend in einem Smart Contract befinden (z.B. bei EtherDelta), haben ausschliesslich die beteiligten Nutzer die Verfügungsmacht über die Vermögenswerte. Sie alleine sind imstande, die von ihnen eingebrachten Vermögenswerte mithilfe ihres Private Keys auf eine andere Person zu übertragen oder auf ihr eigenes Wallet zurückzuziehen. Verfügungsmacht über fremde Vermögenswerte liegt ausserdem noch weniger vor im Falle von Smart Contract-basierten Liquiditätspools, wie etwa Uniswap. Nutzer einer solchen Plattform tauschen Kryptovermögenswerte unmittelbar gegen einen von Dritten aufgebrauchten Liquiditätspool aus. Es ist mit anderen Worten nicht einmal notwendig, dass ein Nutzer den zu veräussernden Kryptovermögenswerte für die Ausführung des Handelsgeschäfts vorübergehend in einem Smart Contract hinterlegt. Die geldwäschereirechtliche relevante Verfügungsmacht liegt ausschliesslich beim Nutzer.

²¹²⁴ Siehe FinCEN, Guidance CVC 2019, 15–17.

²¹²⁵ Siehe etwa OFK GwG-Thelesklaf, Art. 10 N 3; ferner SHK GwG-Luchsinger, Art. 10 N 15 m.w.H., 22; Hutzler, in: Ackermann, Art. 10 GwG N 14.

²¹²⁶ Vgl. die Ausführungen in FINMA-RS 11/1 «Tätigkeit als Finanzintermediär nach GwG», Rz. 58–69; ferner hinsichtlich der Ausführung von Zahlungsaufträgen sowie der Definition des Geld- und Wertübertragungsgeschäfts in Art. 4 Abs. 1 lit. a GwV bzw. Art. 4 Abs. 2 GwV.

²¹²⁷ Siehe oben, [IV.6.2](#).

Das Konzept der Verfügungsmacht über fremde Vermögenswerte scheint darum *prima facie* als Abgrenzungs- und Ausschlusskriterium im Kontext dezentraler Handelsplattformen weiterhin relevant zu sein. Das Nichtvorliegen der Verfügungsmacht Dritter legt namentlich den Schluss nahe, von einer Unterstellung unter das GwG abzusehen. In rechtstatsächlicher Hinsicht gleichen dezentrale Handelsplattformen ohne Verfügungsmacht Dritter dem Betrieb eines Handelsplatzes, wie einer Börse oder eines MHS, welche ebenfalls nicht dem GwG unterstellt sind.

Im DLT-Bericht gelangte der Bundesrat zum expliziten Schluss, dass am Kriterium der Verfügungsmacht über fremde Vermögenswerte für die Unterstellung von Handelsplattformen festzuhalten sei.²¹²⁸ Die Nützlichkeit des Konzepts wurde vom Bundesrat sodann noch im Erläuterungsbericht zur DLT-Revision ausdrücklich anerkannt – allerdings unter dem Hinweis, dass es hinsichtlich dezentraler Handelsplattformen einer weiten Auslegung des Begriffs der Verfügungsmacht bedürfen würde.²¹²⁹ Von dieser Ansicht weicht der Verordnungsgeber nunmehr mit dem am 1. August 2021 in Kraft getretenen Art. 4 Abs. 1 lit. b GwV ab.

2.6 Analyse des revidierten Art. 4 Abs. 1 lit. b GwV

a. Einleitung und Wortlaut

Dass eine dezentrale Handelsplattform, wie sie vom Bundesrat definiert werden, überhaupt dem GwG unterstellt sein kann, wurde, soweit ersichtlich, erstmals im DLT-Bericht des Bundesrates erwähnt.²¹³⁰ Art. 4 GwV behandelt gestützt auf Art. 2 Abs. 3 lit. b GwG unterstellungspflichtige «Dienstleistungen für den Zahlungsverkehr». Ein Anpassungsvorhaben betreffend diese Bestimmung geht sodann zurück auf Ausführungen im Erläuterungsbericht zur DLT-Revision.²¹³¹ Diese Absicht wurde sodann in der Botschaft zur DLT-Revision bestätigt. Eine Präzisierung der Bestimmung wurde in Aussicht gestellt.²¹³² In der Folge wurde das EFD beauftragt, Art. 4 GwV anzupassen.

²¹²⁸ Siehe Bundesrat, DLT-Bericht 2018, 151.

²¹²⁹ Siehe EFD, Erläuternder Bericht DLT-Vernehmlassungsvorlage 2019, 24–25; ferner Bundesrat, DLT-Bericht 2018, 147; sodann KGGT, NRA Krypto 2018, 38–39; Bundesrat, Bericht zu virtuellen Währungen, 16.

²¹³⁰ Siehe Bundesrat, DLT-Bericht 2018, 147.

²¹³¹ Siehe EFD, Erläuternder Bericht DLT-Vernehmlassungsvorlage 2019, 25.

²¹³² Siehe Botschaft DLT 2019, 271.

Der Wortlaut der neuen Bestimmung ist wie folgt:

¹ Eine Dienstleistung für den Zahlungsverkehr nach Artikel 2 Absatz 3 Buchstabe b GwG liegt insbesondere vor, wenn der Finanzintermediär: [...]

b. hilft, virtuelle Währungen an eine Drittperson zu übertragen, sofern er mit der Vertragspartei eine dauernde Geschäftsbeziehung unterhält oder sofern er für die Vertragspartei Verfügungsmacht über virtuelle Währungen ausübt, und er die Dienstleistung nicht ausschliesslich gegenüber angemessen beaufsichtigten Finanzintermediären erbringt; [...]

Die Formulierung ist in rechtsetzungstechnischer Hinsicht leider nicht gelungen: Namentlich impliziert sie durch die Verwendung des Worts «sofern» eine Rangordnung zwischen «hilft, virtuelle Währungen an eine Drittperson zu übertragen» und «dauernde Geschäftsbeziehung» (Variante 1) bzw. «Verfügungsmacht über virtuelle Währungen» (Variante 2). Wenn eine der beiden Varianten vorliegt, ist der Tatbestand erfüllt, soweit der Finanzintermediär im Rahmen der Übertragung geholfen hat. Im Ergebnis ist dies richtig. Wie die nachfolgenden Ausführungen zeigen, ist jedoch von einer *inhaltlichen Gleichordnung* zwischen «hilft, virtuelle Währungen an eine Drittperson zu übertragen» und «Verfügungsmacht über virtuelle Währungen» (Variante 2) auszugehen.

b. Verzicht auf das Kriterium der alleinigen Verfügungsmacht über fremde Vermögenswerte

Im Erläuternden Bericht vom 19. Oktober 2020 hat das EFD trotz anderslautender Aussagen in vorausgegangenen Stellungnahmen angekündigt, dass für die Unterstellung insb. von «dezentralen Handelsplattformen» unter das Geldwäschereirecht nicht mehr auf das Konzept der Verfügungsmacht des Finanzintermediärs abzustellen sei. Bisher wurde demgegenüber vorausgesetzt, dass der Finanzintermediär – wenigstens für einen kurzen Moment – die ausschliessliche und unmittelbare Verfügungsmacht über die fremden Vermögenswerte innehatte.²¹³³ Als Begründung für die Abweichung von der bisher Praxis wird angeführt: «Bei immer dezentraleren Modellen der Vermögensübertragung tragen mehrere Personen zur Verfügung über die Vermögenswerte bei, weshalb die technische Verfügungsmöglichkeit nicht alleiniges Kriterium für geldwäschereirechtliche Pflichten sein kann, bei denen der Dienstleister hilft,

²¹³³ Vgl. in diesem Zusammenhang auch Van Valkenburgh, FATF interpretive note not doomsday for cryptocurrency, *passim*.

die Vermögenswerte zu übertragen.»²¹³⁴ Mit anderen Worten muss ein allfälliger «Betreiber» einer dezentralen Handelsplattform nicht mehr zwingend die ausschliessliche und unmittelbare Verfügungsmacht über fremde Vermögenswerte ausüben können, damit das GwG auf ihn zur Anwendung kommt.

Der Verzicht auf das Kriterium der Verfügungsmacht über fremde Vermögenswerte wird damit begründet, dass Applikationen technisch so ausgestaltet werden könnten, dass eine geldwäschereirechtliche Unterstellung bewusst vermieden würde. Die Überprüfung der geldwäschereirechtlich relevanten Verfügungsmacht im Einzelfall sei zudem sehr aufwendig, unverhältnismässig und impraktikabel.²¹³⁵

Die technologisch motivierte Abweichung vom Konzept der ausschliesslichen und unmittelbaren Verfügungsmacht wurde seitens Kryptoindustrie und Lehre *breit kritisiert*.²¹³⁶

Die vom EFD angeführte Begründung ist insoweit nachvollziehbar, als dass die effektive Kontrolle über die Funktionsweise einer «dezentralen Handelsplattform» im Einzelfall tatsächlich zu einer Situation führen kann, der mit der Verfügungsmacht über fremde Kryptovermögenswerte *vergleichbar* ist, ohne dass jedoch eine solche Verfügungsmacht rechtlich oder faktisch bestünde. Dies bedeutet aber auch, dass im Einzelfall abzuklären ist, ob eine Kontrolle vorliegt, die mit demjenigen des Innehabens von ausschliesslicher und unmittelbarer Verfügungsmacht *vergleichbar* ist. Ganz allgemein scheint sich der Bundesrat – in Anlehnung an die FATF –²¹³⁷ vom Gedanken leiten zu lassen, dass der Finanzintermediationsgedanken im Zeitalter des Internets und von Blockchains immer weiter zu fassen sei.

Angesichts der zentralen Bedeutung des Kriteriums der ausschliesslichen und unmittelbaren Verfügungsmacht über fremde Vermögenswerte für Fälle der Finanzintermediation, die unter Art. 2 Abs. 3 GwG subsumiert werden, wäre es, wenn überhaupt, angezeigt gewesen, die Änderung auf dem Gesetzesweg vorzunehmen.²¹³⁸

²¹³⁴ EFD, Erläuternder Bericht Verordnung DLT 2020, 16, ferner 7.

²¹³⁵ Siehe EFD, Erläuterungen Verordnung DLT 2021, 22.

²¹³⁶ Siehe für einen Überblick der Kritik EFD, Ergebnisbericht Vernehmlassungsverfahren DLT-Verordnung 2021, 9; ferner Stengel/Bianchi, in: Weber/Kuhn, Geldwäscherei und Terrorismusfinanzierung, Rz. 22, welche das Argument des EFD als *ungenügend* betrachten; CVA RWG, CVA's answer to the DLT Ordinance, 7–9.

²¹³⁷ Siehe hierzu oben, [V.2.3](#).

²¹³⁸ GLM. CVA RWG, CVA's answer to the DLT Ordinance, 8. Ein Formulierungsvorschlag auf Gesetzesstufe findet sich etwa bei Nagel, Geltungsbereich GwG, Rz. 890, der allerdings

Als neu unterstellungsrelevantes Kriterium soll demgegenüber neu die «Hilfe zur Übertragung von virtuellen Währungen in Zusammenhang mit einer dauernden Geschäftsbeziehung» eingeführt werden. Unterstellungsrelevant soll darum sein, dass der Plattformbetreiber eine dauernde Geschäftsbeziehung mit dem Plattformnutzer unterhält und dass für den Gebrauch der technischen Lösung die Verfügbarkeit der Dienstleistung des Plattformbetreibers erforderlich ist.²¹³⁹ Gemäss Erläuterungen des EFD vom 18. Juni 2021 zum finalisierten Wortlaut der Bestimmung fallen bspw. «dezentrale Handelsplattformen» darunter, «die nicht im Besitz des privaten Schlüssels der Kunden sind, die Übertragung der virtuellen Währungen jedoch mittels Smart Contract ermöglichen und dabei die Aufträge bestätigen, freigeben oder sperren können oder anderweitig Kontrolle über den Smart Contract haben [...]».²¹⁴⁰ In dieser Aussage kommt allerdings lediglich die Erforderlichkeit der Verfügbarkeit der Dienstleistung des Plattformbetreibers und somit lediglich das Kriterium der Hilfe zur Übertragung zum Ausdruck.

Das EFD macht ferner deutlich, dass es mit der neuen Regelung nur bestimmte Typen von dezentralen Handelsplattformen im Auge hat: «Von der Pflicht zur Unterstellung unter das GwG ausgeschlossen [sind demgegenüber] vollständig autonome Systeme, [die] ohne dauernde Geschäftsbeziehung [auskommen]. Des Weiteren sollen weiterhin ebenfalls keine Handelsplattformen dem Geldwäschereigesetz unterstellt werden, die lediglich Käufer und Verkäufer zusammenführen und die Abwicklung der Transaktion ohne Smart Contract mit Zugriffsmöglichkeit der Handelsplattform erfolgt. Dabei handelt es sich um eine reine Vermittlungstätigkeit ohne Einbezug in die Übertragung der virtuellen Währungen.»²¹⁴¹

c. Hilfe zur Übertragung von virtuellen Währungen

Das Kriterium der Hilfe zur Übertragung von virtuellen Währungen gemäss Art. 4 Abs. 1 lit. b GwV soll vermutlich weit ausgelegt werden, sodass jede für

nach vorliegender Auffassung viel zu weit geht, indem er bspw. auch Anbieter von Non-Custodial Wallets erfassen würde. Vgl. demgegenüber Bundesrat, DLT-Bericht 2018, 146, wo der Bundesrat die Unterstellung von Anbietern von Non-Custodial Wallets als mit dem geltenden Recht unvereinbar bezeichnet.

²¹³⁹ Siehe EFD, Erläuternder Bericht Verordnung DLT 2020, 16; EFD, Erläuterungen Verordnung DLT 2021, 23.

²¹⁴⁰ EFD, Erläuterungen Verordnung DLT 2021, 22.

²¹⁴¹ So auch EFD, Erläuternder Bericht Verordnung DLT 2020, 16; bestätigt in EFD, Erläuterungen Verordnung DLT 2021, 23.

die Übertragung von virtuellen Währungen notwendige Interaktion seitens einer Drittpartei zu einer Unterstellung führen könnte. Die Hilfe zur Übertragung von Kryptovermögenswerten ist umso grösser, desto stärker der Plattformbetreiber in den Austauschprozess involviert ist. Davon scheint auch das EFD auszugehen, wenn es schreibt, dass neben der Bestätigung, Freigabe oder Sperrung von Aufträgen auch *anderweitige* Formen der Kontrolle über den Smart Contract relevant sein können.

Nach vorliegender Auffassung kann allerdings nicht *jede* anderweitige Form von Kontrolle über einen Smart Contract zur Unterstellung unter das GwG führen.²¹⁴² Es hat ein klarer Bezug zu den Aufträgen der Plattformnutzer zu bestehen. Mit anderen Worten muss – in Einklang mit der bisherigen Praxis der FINMA –²¹⁴³ der Plattformbetreiber oder ein Dritter in relevanter Form in den Transaktionsfluss zwischen den beiden Endbegünstigten eingreifen können, sodass er bspw. eine Transaktion an der Ausführung dauerhaft hindern kann oder dass die Ausführung einer Transaktion von dessen Bestätigung abhängig ist.²¹⁴⁴ In Anlehnung an den Bundesrat wird somit eine *Zugriffsmöglichkeit* auf die Aufträge über entsprechende Admin Keys vorausgesetzt.²¹⁴⁵ Lediglich die Parametrisierung der konkreten Ausführungsbedingungen (z.B. Änderung der Handelsgebühren) genügt nach vorliegender Auffassung für die Unterstellung nicht. Mit anderen Worten wäre im Falle von EtherDelta mangels Kontrollmöglichkeit seitens Coburn keine Unterstellung unter das GwG angezeigt gewesen.²¹⁴⁶

Dezentrale Handelsplattformen, wie etwa Uniswap, über welche die Aufträge der Nutzer zusammengeführt werden oder deren Aufträge gegen bestehende Liquiditätspools ausgeführt werden, gelten demgegenüber unter GwG-Ge-

²¹⁴² GL.M. BSK GwG-Bachelard/Hess, Art. 2 Abs. 3 lit. b N 16 («faktische Kontroll- und Eingriffsmöglichkeit»); Nagel, GesKR 2023, 77 («hohes Mass an Kontrolle»); ausführlich hierzu Glarner/Ganzoni/Hepp, AJP 2023, 1096–1102; EJPD/fedpol, NRA 2024, 32 («bestimmte Kontroll- oder Eingriffsmöglichkeiten»).

²¹⁴³ Siehe FINMA, Jahresbericht 2018, 32.

²¹⁴⁴ Vgl. zur vergleichbaren Situation bei Escrow-Verhältnissen, bei denen der Escrow-Agent bloss über eine eingeschränkte Verfügungsmacht verfügt, Glarner/Meyer, Jusletter vom 4. Dezember 2017, Rz. 65 2. Lemma.

²¹⁴⁵ Dies scheint der Bundesrat anzuerkennen, wobei er allerdings noch Bezug nimmt auf das Konzept der Verfügungsmacht, vgl. Bundesrat, DLT-Bericht 2018, 147 («Die Unterstellungspflicht hängt somit davon ab, ob Plattformen die Möglichkeit haben, auf die Transaktionen der Kunden einzuwirken.»); ferner EFD, Erläuternder Bericht DLT-Vernehmlassungsvorlage 2019, 24–25; KGGT, NRA Krypto 2018, 31, 38–39; FINMA, Jahresbericht 2018, 32.

²¹⁴⁶ Siehe hierzu oben, [IV.3.6b](#).

sichtspunkten als «vollständig autonome Systeme».²¹⁴⁷ Eine Zugriffsmöglichkeit auf die Aufträge oder Zahlungsflüsse ist in solchen Systemen technisch ausgeschlossen.²¹⁴⁸ Im Falle von Uniswap etwa kommt der DAO keine relevante Kontrolle über die Smart Contracts zu, welche eine entsprechende Unterstellung nötig machen würde.²¹⁴⁹

Fraglich ist die Kontrolle in Fällen, in denen *relevante* Admin Keys bestehen, diese aber entweder in einer Multisig gehalten werden oder deren Nutzung von einem entsprechenden DAO-Beschluss abhängig ist. Mit anderen Worten ist zwar eine prinzipiell unterstellungsrelevante Kontrolle gegeben, nur ist diese für die Funktionsweise der Plattform nicht weiter relevant. So hat etwa die Existenz dieser Admin Keys noch keinen direkten Einfluss auf die Aufträge von Nutzern oder die Ausführung derer Transaktionen über den betreffenden Smart Contract. Solange die Kontrolle nicht effektiv ausgeübt werden kann, ist nach vorliegender Auffassung von einer Unterstellung abzusehen.²¹⁵⁰ Mit anderen Worten ist die *effektive Zugriffsmöglichkeit* auf die Aufträge von Nutzern vorzusetzen.

Ferner ist offen, ob Layer-2-Handelsplattformen (z.B. Loopring) über eine unterstellungsrelevante Kontrolle über die eingesetzten Smart Contracts verfügen. Gemäss Ausführungen in Kapitel IV. bündeln Layer-2-Protokolle typischerweise eine Vielzahl von Transaktionen, um sie sodann in regelmässigen Zeitabständen im dezentralen Netzwerk mit Finalität abzuwickeln. Diese vorgelagerte Abwicklung erfolgt in vielen Fällen durch die Teilnehmer eines separaten verteilten Netzwerks.²¹⁵¹ Die Teilnehmer dieses Layer-2-Netzwerks haben die Möglichkeit, Transaktionen nicht zur Abwicklung zu bringen, indem sie sie bspw. ignorieren. Insoweit verfügen sie über die Möglichkeit, Aufträge zu blockieren bzw. diese nicht für die Abwicklung freizugeben. Ihnen kommt mit anderen Worten die effektive Zugriffsmöglichkeit auf die Aufträge der Nutzer zu. Allerdings sehen solche Plattformen in aller Regel die Möglichkeit vor, dass Nutzer mithilfe einer Smart Contract-Funktion einseitig ihre Transaktionen auf dem dezentralen Netzwerke zur Ausführung bringen und somit einen Eintrag in der Blockchain veranlassen können (*force withdraw*).²¹⁵² Zu-

²¹⁴⁷ Siehe EFD, Erläuterungen Verordnung DLT 2021, 23.

²¹⁴⁸ Gl.M. wohl Wherlock/Haeberli, IFLR 2021, *passim*; vgl. Bundesrat, DLT-Bericht 2018, 147.

²¹⁴⁹ Siehe betreffend Admin Keys in Uniswap oben, [IV.5.2d.ii](#).

²¹⁵⁰ Gl.M. wohl Poskriakov, in: Richa/Canapa, *Conservation et négoce de cryptoactifs*, 120 FN 127, der voraussetzt, «que le contrôle et l'influence technique soient données de fait, et ne soient pas uniquement potentielles».

²¹⁵¹ Vgl. hierzu oben, [IV.3.9](#).

²¹⁵² Siehe hierzu oben, [IV.3.9b](#).

dem ist zu erwähnen, dass ein einzelner Netzwerkteilnehmer des Layer-2-Protokolls nicht über die ausschliessliche Kontrolle über den Smart Contract verfügt, sondern eine solche Kontrolle die Unterstützung einer Mehrzahl kolludierender Teilnehmer voraussetzen würde. Selbstredend haben auch kolludierende Teilnehmer des Layer-2-Netzwerks zu keinem Zeitpunkt Zugriff auf die Vermögenswerte der Nutzer.

d. Dauernde Geschäftsbeziehung

Sodann ist neben dem Kriterium der Hilfe zur Übertragung von virtuellen Währungen der Begriff der dauernden Geschäftsbeziehung zentral für die neue Bestimmung in Art. 4 Abs. 1 lit. b GwV. Für die Auslegung dieses Begriffes ist mangels abweichender Regelung aus gesetzessystematischen Gründen auf die bisherige Verwendung des Begriffs im Geldwäschereirecht zu verweisen.

Unter einer *Geschäftsbeziehung* wird in der Literatur das Eingehen von tatsächlichen vertraglichen Beziehungen gemäss Art. 1 ff. OR verstanden, soweit sich diese auf Finanzgeschäfte beziehen.²¹⁵³ Geschäftsbeziehungen können sodann weiter in dauernde und einmalige Beziehungen zwischen Finanzintermediär und Vertragspartei unterteilt werden. Nach der FINMA-Praxis gilt als *dauernde* Geschäftsbeziehung eine Kundenbeziehung, die bei einem schweizerischen Finanzintermediär gebucht oder überwiegend von der Schweiz aus betreut wird und die sich nicht in der Vornahme einmaliger unterstellungspflichtiger Tätigkeiten erschöpft.²¹⁵⁴

Keine dauernde Geschäftsbeziehung ist regelmässig mit dem Geldwechsel und den Geld- und Wertübertragungsgeschäften verbunden, wobei solche Geschäfte freilich auch im Rahmen einer dauernden Geschäftsbeziehung erbracht werden können.²¹⁵⁵ Die Dauerhaftigkeit einer Geschäftsbeziehung dient somit der Abgrenzung von *einmaligen* Beziehungen, wie sie etwa regelmässig beim Geldwechsel und der Geld- und Wertübertragung vorkommen. Dauerhafte und einmalige Beziehungen können insoweit als komplementär angesehen werden. Typischerweise liegt bei solchen einmaligen Geschäften zuerst eine Annahme fremder Vermögenswerte gefolgt von einer finanzintermediären Handlung vor, d.h. insb. der Umtausch oder die Übertragung von fremden

²¹⁵³ Siehe SHK GwG-Dobrauz-Saldapenna/Derungs, Art. 3 N 3; OFK GwG-Wyss, Art. 3 N 1.

²¹⁵⁴ Art. 2 lit. d GwV-FINMA; vgl. ferner z.B. Art. 7 lit. b VQF-Reglement vom 16. November 2020.

²¹⁵⁵ Vgl. Art. 2 lit. b und c GwV-FINMA.

Vermögenswerten.²¹⁵⁶ Die Sorgfaltspflichten bei Kassageschäften, wie insb. dem Wechselgeschäft, und bei der Geld- und Wertübertragung von virtuellen Währungen richten sich nach Art. 51a und 52 GwV-FINMA bzw. den entsprechenden Bestimmungen des Reglements²¹⁵⁷ einer Selbstregulierungsorganisation.²¹⁵⁸

Dass diese Formen der Finanzintermediation weiterhin auch für dezentrale Handelsplattformen relevant sein können, wird ausdrücklich in den Erläuterungen des EFD festgehalten.²¹⁵⁹ Auf diesen Punkt wird noch in den Ausführungen zur Bereitstellung von Liquidität über dezentrale Handelsplattformen einzugehen sein.²¹⁶⁰

Mangels identifizierbaren Intermediärs sowie aufgrund der Nutzungs- und Teilnahmeoffenheit der zugrundeliegenden Technologie kommt es nach vorliegender Auffassung bei der Nutzung dezentraler Handelsplattformen weder formell noch faktisch zu einem Abschluss einer dauernden oder einmaligen Geschäftsbeziehung. Der Bundesrat spricht in diesem Fall von «vollständig autonomen Systemen», denen keine dauerhafte Beziehung zugrunde liegen.²¹⁶¹ Eine Unterstellung unter den sachlichen Anwendungsbereich des GwG würde mangels Vertragsbeziehung und Möglichkeit zur Kontaktaufnahme mit einem Nutzer weitgehend leerlaufen. In Ermangelung eines identifizierbaren Betreibers der Handelsplattform wäre sodann eine objektive Zuordnung der Pflichten zur Identifizierung des Nutzers nach den materiellen geldwäschereirechtlichen Vorschriften nicht möglich.²¹⁶² Den faktischen Grenzen der Einhaltung von Sorgfaltspflichten sollte entsprechend Rechnung getragen werden. Eine dauernde Geschäftsbeziehung darüber hinaus mit den Teilnehmern des dezentralen Netzwerks (z.B. Minern) konstruieren zu wollen, findet in aller Regel bereits mangels Rechtsbindungswille der beteiligten Parteien keine Grundlage.²¹⁶³ Zudem würde eine solche Konstruktion das Konzept der Dezentralität

²¹⁵⁶ Siehe zum unselbständigen Tatbestandselement der Annahme UK KSt GwG, Rz. 9; ausführlich SHK GwG-Schären, Art. 2 N 77–78.

²¹⁵⁷ Vgl. etwa Art. 24–25 VQF-Reglement vom 16. November 2020.

²¹⁵⁸ Vgl. zum Hintergrund der neuen Bestimmung in Art. 51a GwV-FINMA FINMA, Erläuterungen Ausführungsbestimmungen FIDLEG/FINIG 2020, 41–42.

²¹⁵⁹ Siehe EFD, Erläuterungen Verordnung DLT 2021, 23.

²¹⁶⁰ Siehe weiter unten, [V.2.7](#).

²¹⁶¹ Siehe EFD, Erläuterungen Verordnung DLT 2021, 23.

²¹⁶² Vgl. zur faktischen Unmöglichkeit eines Finanzintermediärs, die Sorgfaltspflichten des GwG wahrzunehmen, BGer 2A.62/2007 vom 30. November 2007, E. 8; 2C_488/2018 vom 12. März 2020, E. 5.1; ferner zur Rolle des Abschlusses eines Vertrages im Geldwäschereirecht UK KSt GwG, Rz. 282–283.

²¹⁶³ Siehe zu Minern und Stakern unten, [V.2.10](#).

überstrapazieren.²¹⁶⁴ Damit ist es auch den Netzwerkteilnehmern faktisch unmöglich, die Sorgfaltspflichten des GwG effektiv wahrzunehmen.

Die REGULATORY WORKING GROUP der CRYPTO VALLEY ASSOCIATION scheint für den Begriff der dauernden Geschäftsbeziehung auf die Regelmässigkeit der Abschlüsse von Handelsgeschäften abzustellen.²¹⁶⁵ Diese Auffassung wird so- dann insb. aus datenschutzrechtlichen Erwägungen zu Recht kritisiert. Ohne- hin ist nach vorliegender Ansicht auf das Kriterium der Regelmässigkeit der Transaktionen für die Frage, ob eine dauernde Geschäftsbeziehung besteht, nicht abzustellen.

RETO LUTHIGER geht davon aus, dass ein Kundenlogin auf der Webseite einer Plattform eine dauerhafte Geschäftsbeziehung mit dem Betreiber begrün- det.²¹⁶⁶ Ähnliches lässt die KGGT verlauten, wonach Anbieter von Custodian Wallets mit ihren Kunden regelmässig eine dauernde Geschäftsbeziehung ein- gehen.²¹⁶⁷ Vorausgesetzt wird nach vorliegender Auffassung, dass der Betrei- ber der Plattform für die Nutzung seiner Dienstleistungen eine Anmeldung vorsieht, in deren Rahmen der Nutzer seine bürgerliche Identität offenlegen kann, was dem Betreiber letztlich die Wahrnehmung der GwG-Sorgfaltspflich- ten erlaubt. Die Erstellung eines Kontos beim Online Wallet-Anbieter Me- taMask, die Verknüpfung eines Hardware Wallets mit einer dezentralen Ap- plikation oder die Verwendung eines vergleichbaren Mechanismus sind demgegenüber nicht ausreichend, da der Nutzer dadurch lediglich ein Self- Hosted Wallet generiert. Solche Wallets kann der Nutzer sodann im Rahmen jeder dezentralen Applikation verwenden bzw. mit einer solchen verknüpfen, ungeachtet dessen, ob er im Einzelfall zusätzlich noch ein allfälliges Login zu erstellen hat.

Dass mit dem Abschluss einer dauernden Geschäftsbeziehung die Belastung von *Gebühren* (insb. Handelsgebühren) verbunden sind, liegt nahe. Ohnehin ist für die Aktivitäten nach Art. 4 GwV berufsmässiges Vorgehen verlangt (vgl. Art. 2 Abs. 3 GwG). Dem Aspekt der Gebührenerhebung kommt aber nach vor- liegender Auffassung aufgrund des klaren Wortlauts der Bestimmung keine ei- genständige Bedeutung, sondern höchstens Indizienwirkung zu.²¹⁶⁸ Wenn also

²¹⁶⁴ Siehe zu diesem Konzept unten, [VII](#).

²¹⁶⁵ Siehe CVA RWG, CVA's answer to the DLT Ordinance, 7–8 («transact on a repeat [...] basis»).

²¹⁶⁶ Siehe DeFi For Good, DeFi Swiss Law Regulation, Youtube, *passim*.

²¹⁶⁷ Siehe KGGT, NRA Krypto 2018, 17.

²¹⁶⁸ So aber offenbar Luthiger, IFC Review 2021, *passim* («Even the provision of partial services in the areas of payment initiation and execution or the implementation of a transaction fee that flows to the software provider/licensor are problematic.»).

Protokolle dezentraler Handelsplattformen eine Gebührenstruktur vorsehen, die bspw. Liquiditätsgebern des Protokolls oder Governance Tokeninhabern zugutekommen, kann nicht automatisch daraus geschlossen werden, dass eine dauernde Geschäftsbeziehung vorliegen muss. Die FINMA scheint jedoch dem Gebührenelement in der derzeitigen (unveröffentlichten) Aufsichtspraxis einen hohen Stellenwert zuzuschreiben.

Die vorliegende Einschätzung ist in Einklang mit der Tatsache, dass die Vorgaben in Art. 4 GwV Dienstleistungen für den Zahlungsverkehr umfassen. Rein begrifflich setzt eine Dienstleistung eine natürliche oder juristische Person voraus, welche die Dienstleistung erbringt. Ein Smart Contract oder vergleichbare Mechanismen eines «vollständig autonomen Systems» erbringen demgegenüber keine Dienstleistung im Sinne des GwG. Das Kriterium der dauernden Geschäftsbeziehung zwischen dem für eine Handelsplattform verantwortlichen Finanzintermediär und seiner Vertragspartei stösst bei dezentralen Handelsplattformen nach vorliegender Auffassung sehr rasch an seine Grenzen. Dieses Kriterium hat darum nach vorliegender Auffassung – anders als das sehr offen formulierte Kriterium der Hilfe zur Übertragung – eine *einschränkende* Wirkung auf den Geltungsbereich von Art. 4 Abs. 1 lit. b GwV.

e. Reine Vermittlungstätigkeit

Das EFD erwähnt, dass die reine Vermittlungstätigkeit nicht unter Art. 4 Abs. 1 lit. b GwV falle. Hierzu gehören Plattformen, die Käufer und Verkäufer lediglich zusammenführen und die Abwicklung der Transaktion ohne Smart Contract mit Zugriffsmöglichkeit der Handelsplattform erfolgt.²¹⁶⁹ Aus der Formulierung des EFD geht nicht eindeutig hervor, ob solche Plattformen generell ohne Smart Contract operieren oder lediglich keine Smart Contracts mit Zugriffsmöglichkeit vorsehen. Nach vorliegender Auffassung darf es aus Gründen der Technologieneutralität nicht darauf ankommen, ob Smart Contracts oder ähnliche technische Mechanismen eingesetzt werden oder nicht. In diesem Sinne üben alle dezentralen Handelsplattformen eine reine Vermittlungstätigkeit aus, wenn sie keine relevanten Admin Keys oder keine vergleichbaren effektiven Kontrollmöglichkeiten vorsehen. Im Ergebnis kann es lediglich darum gehen, Handelsplattformen dem GwG zu unterstellen, welche Tätigkeiten vornehmen, die als Finanzintermediation qualifizieren.²¹⁷⁰

²¹⁶⁹ So das EFD, Erläuterungen Verordnung DLT 2021, 23; ferner bereits Bundesrat, Bericht zu virtuellen Währungen, 16.

²¹⁷⁰ Vgl. Bundesrat, DLT-Bericht 2018, 146.

In den Fällen der reinen Vermittlungstätigkeit besteht mangels Einbezugs in die Übertragung von virtuellen Währungen von vornherein keine effektive Zugriffsmöglichkeit eines allfälligen Plattformbetreibers auf die Aufträge der Nutzer. In vielen Fällen wird es gänzlich an einem eindeutig identifizierbaren «Plattformbetreiber» fehlen. Die reine Zuordnung von Kaufs- und Verkaufsangeboten stellte bereits nach bisherigem Recht keine Finanzintermediation dar.²¹⁷¹ Das Vorliegen einer dauernden Geschäftsbeziehung wäre demgegenüber denkbar, ist aber für sich alleine für eine Unterstellung nicht ausreichend.

Im Falle von Bisq etwa werden die auszutauschenden Kryptovermögenswerte in einem Multisig Escrow zwischenverwahrt, bis die beiden beteiligten Parteien der Freigabe der Vermögenswerte zugestimmt haben. Erwähnenswert ist, dass die Bisq-Plattform ohne einen zentralen Betreiber auskommt, sodass eine Unterstellung bereits aus praktischen Gründen ausscheiden würde. Denn jeder Nutzer von Bisq «betreibt» die Plattform selbständig über einen Softwareclient.²¹⁷² Anders stellt sich vermutlich die rechtliche Situation von Local- Bitcoins dar, deren Plattform unmittelbar und in kontrollrelevanter Weise in den Escrow-Prozess involviert ist.²¹⁷³

Wenn hingegen der Anbieter eines Hosted Wallets seinen Nutzern den Handel über solche Handelsplattformen ermöglicht²¹⁷⁴ oder eine Person Kryptovermögenswerte über solche Handelsplattformen veräussert, die sie anschliessend für die Gegenpartei an eine Drittperson (z.B. eine Custodial Handelsplattform) weiterleitet, kann demgegenüber eine unterstellungspflichtige Tätigkeit vorliegen. In diesen Fällen steht allerdings nicht mehr die Unterstellung der Plattform, sondern eines auf ihr tätigen Marktteilnehmers zur Debatte.

f. Vollständig autonome Systeme vs. reine Vermittlungstätigkeit

Das EFD unterscheidet in seinen Publikationen zwischen vollständig autonomen Systemen und der reinen Vermittlungstätigkeit.²¹⁷⁵ Mit vollständig auto-

²¹⁷¹ Siehe Bundesrat, Bericht zu virtuellen Währungen, 16; SHK GwG-Schären, Art. 2 N 105 FN 165.

²¹⁷² Siehe oben, [IV.3.4.](#)

²¹⁷³ Siehe oben, [IV.3.4b.](#)

²¹⁷⁴ Vgl. FinCEN, Guidance CVC 2019, 24 FN 73.

²¹⁷⁵ Vgl. EFD, Erläuternder Bericht Verordnung DLT 2020, 16; bestätigt in EFD, Erläuterungen Verordnung DLT 2021, 23; demgegenüber noch ohne diese Abgrenzung Bundesrat, DLT-Bericht 2018, 146–147.

nomen Systemen soll wohl eine Betonung der Automatisierung des Handels über den Einsatz von Smart Contracts erfolgen; vermittelnde Plattformen scheinen hingegen die Zusammenführung der Handelsparteien hervorzuheben.

In der Praxis verschwimmen die Konturen der beiden Plattfortmtypen.²¹⁷⁶

- Systeme, die vollständig autonom sind, führen Käufer und Verkäufer zusammen, ohne dass eine entsprechende effektive Zugriffsmöglichkeit eines Dritten besteht (z.B. Uniswap). Es könnte argumentiert werden, dass die Zusammenführung über ein vorgeschaltetes Frontend geschieht. Allerdings handelt es sich dabei nur um einen Einstiegspunkt; die Zusammenführung der Parteien erfolgt innerhalb der Smart Contract-Logik.
- Plattformen, welche der reinen Vermittlungstätigkeit dienen und somit Käufer und Verkäufer lediglich zusammenführen, sind mangels effektiver Zugriffsmöglichkeit eines Dritten überwiegend autonom (z.B. Bisq). Die Autonomie wird durch den Einsatz von Smart Contracts bzw. Multisig-Adressen gewährleistet.

Die Abwicklung erfolgt sodann in beiden Fällen ausserhalb der betreffenden dezentralen Handelsplattform.

Die Unterscheidung bietet mit Blick auf dezentrale Handelsplattformen, wie sie vorliegend verstanden werden, nur einen bedingten Mehrwert. Die «Essenz» aller dezentralen Handelsplattformen liegt, wie bereits erwähnt, in der softwarebasierten Zusammenführung von Marktteilnehmern zwecks Austausches von Kryptovermögenswerten, ohne dass es für diesen Vorgang der Handlung einer Drittperson bedarf oder dass der Vorgang von der Handlung eines Dritten abhängig ist.

Das Kriterium der effektiven Zugriffsmöglichkeit ist nach den obigen Ausführungen sowohl für die Abgrenzung zwischen GwG-unterstellten Handelsplattformen und vollständig autonomen Systemen als auch zur reinen Vermittlungstätigkeit relevant.

²¹⁷⁶ Vgl. FinCEN, Guidance CVC 2019, 23–24, wo lediglich von *einem* Typus einer nichtunterstellten dezentralen Handelsplattform die Rede ist.

2.7 Bereitstellung von Liquidität über dezentrale Handelsplattform

a. Einleitung

In geldwäschereirechtlicher Hinsicht könnte sodann relevant sein, dass ein Nutzer über eine dezentrale Handelsplattform *Liquidität bereitstellt*. Dies kann etwa durch Einstellen von Aufträgen zum Geld- oder Briefkurs in einem Orderbuch oder über die Zuführung von Kryptovermögenswerten zu einem AMM-Pool geschehen. Im Vordergrund steht eine allfällige Qualifikation als Kassageschäft, was die Einhaltung der GwG-Sorgfaltspflichten nach sich ziehen würde. Nicht einschlägig scheint hingegen der Tatbestand der Geld- und Wertübertragung zu sein, setzt dieser doch ein Intermediär voraus, welche die Werte vom Absender entgegennimmt und dem Empfänger weiterleitet.²¹⁷⁷

b. Kassageschäft

Sofern die eingestellten Aufträge oder das bereitgestellte Handelspaar den Austausch von virtuellen Währungen zum Gegenstand haben (z.B. ETH-USDC), was den Handel mit Asset- und Nutzungs-Token mangels Zahlungsmittelfunktion solcher Kryptovermögenswerte grundsätzlich ausschliesst,²¹⁷⁸ könnte es sich um einen *Geldwechsel* handeln, der insb. von der neuen Bestimmung in Art. 51a GwV-FINMA bzw. der im Einzelfall anwendbaren entsprechenden SRO-Bestimmung erfasst ist. Die FINMA hat aus Risikoüberlegungen den Schwellenwert hinsichtlich der Pflicht zur Identifizierung der Vertragspartei auf 1'000 Fr. *reduziert*, wobei nach Aussage der Behörde lediglich der Geldwechsel unter die Bestimmung fallen soll. Demnach erfasst Art. 51a GwV-FINMA (Titel: «Geschäfte mit virtuellen Währungen») in der Praxis lediglich Wechselgeschäfte, d.h. den Tausch von Fiatwährungen in virtuelle Währungen und *vice versa* sowie unterschiedliche virtuelle Währungen gegeneinander.²¹⁷⁹ Für die Unterstellung eines solchen Wechselgeschäfts müssen allerdings – im Unterschied zum Geld- und Wertübertragungsgeschäft –²¹⁸⁰ die Kriterien für die berufsmässige Ausübung der Tätigkeit gegeben sein.

²¹⁷⁷ Sog. *Dreiparteienverhältnis* bzw. *-geschäft*; vgl. hierzu Bundesrat, Virtuelle Währungen, 15; SHK GwG-Schären, Art. 2 N 81, 121; OFK GwG-Wyss, Art. 2 N 27.

²¹⁷⁸ Siehe zum Begriff oben, [V.2.5a](#).

²¹⁷⁹ Siehe FINMA, Erläuterungen Ausführungsbestimmungen FIDLEG/FINIG 2020, 42.

²¹⁸⁰ Vgl. Art. 9 GwV; FINMA RS-11/1 «Tätigkeit als Finanzintermediär nach GwG», Rz. 142–147.

c. Bargeschäft

Wenn der Austausch über eine dezentrale Handelsplattform hingegen nicht ausschliesslich virtuelle Währungen beinhaltet, namentlich wenn einer der beiden auszutauschenden Vermögenswerte einen Nutzungs- oder Anlage-Token darstellt, könnte in diesem Fall immer noch allenfalls ein *Bargeschäft* vorliegen. Als Kassageschäfte gelten nach Auffassung der FINMA «alle Bargeschäfte, insbesondere der Geldwechsel, der Kauf und der Verkauf von Edelmetallen, der Verkauf von Reiseschecks, die Barliberierung von Inhaberpapieren, Kassa- und Anleiheobligationen und das Bareinlösen von Checks, sofern mit diesen Geschäften keine dauernde Geschäftsbeziehung verbunden ist» (Art. 2 lit. b GwV-FINMA). In diesem Fall würde hinsichtlich der Pflicht zur Identifizierung der Vertragspartei der Schwellenwert von 15'000 Fr. gemäss Art. 51 Abs. 1 lit. b GwV-FINMA bzw. entsprechender Bestimmung im SRO-Reglement gelten

Zu prüfen ist, ob es sich etwa bei der Bereitstellung von tokenisierten Aktien oder Anleihen über eine dezentrale Handelsplattform, die gegen den Stablecoin XCHF getauscht werden können, um ein *Bargeschäft* im Sinne der soeben erwähnten Definition handelt. Nach der Auffassung der Aufsichtscommission VSB ist für den Begriff des Kassa- bzw. Bargeschäfts nicht primär auf die Abwicklung in barer Form – im Sinne der physischen Entgegennahme bzw. Übergabe eines Vermögenswerts – abzustellen, sondern auf den Umstand, dass keine dauernde Geschäftsbeziehung besteht, weshalb lediglich eine «punktuelle Dienstleistung» erbracht wird.²¹⁸¹ Will man dieser Auslegung auch ausserhalb der GwG-Unterstellung von Banken zum Durchbruch verhelfen, was wohl angezeigt ist, so könnte die Nutzung oder Bereitstellung von Liquidität durchaus als potenziell unterstellte Wechsel- und Bargeschäfte betrachtet werden.²¹⁸²

Allerdings wäre fraglich, ob und wie ein Nutzer oder Liquiditätsgeber die Sorgfaltspflichten unter dem GwG, namentlich die Pflicht zur Identifizierung der Vertragspartei und die Pflicht zur Feststellung der wirtschaftlich berechtigten Person gemäss Art. 3-4 GwG, in praktischer Hinsicht einhalten könnte. Die Tatsache, dass die Ausführung und Abwicklung des Handels über eine dezentrale Handelsplattform überwiegend automatisiert erfolgt, spricht dafür, diese Fälle nicht als Kassageschäfte zu betrachten. Es fehlt an der technisch

²¹⁸¹ Siehe Aufsichtscommission VSB, Praxis Sorgfaltspflicht der Banken, 23-24; ferner Swiss-Banking, Kommentar VSB 20, 11; vgl. sodann bereits Botschaft GwG 1996, 1122.

²¹⁸² Ähnlich Meirich, *Decentralized Finance*, Rz. 1070-1082.

notwendigen Möglichkeit, mit der Gegenpartei, soweit eine solche überhaupt nachweisbar besteht, was eher noch im Orderbuchmodell der Fall ist, auf individueller Ebene zu interagieren und in diesem Rahmen etwa eine KYC-Prüfung der Gegenpartei durchzuführen.²¹⁸³ Will man heute hingegen diese Tätigkeiten unter das GwG stellen, so könnte daraus ein faktisches Nutzungsverbot solcher Plattformen resultieren.

Immerhin kann festgehalten werden, dass die gelegentliche Nutzung einer dezentralen Handelsplattform regelmässig die Kriterien der Berufsmässigkeit gemäss Art. 7 GwV nicht erfüllen wird.

d. Handelsgeschäft

Der Erhalt eines Liquiditätstokens (auch Pool Token), der die Gebühren des AMM-Protokolls für den Liquiditätsbereitsteller rechnerisch akkumuliert, hat Ähnlichkeiten mit einem Handelsgeschäft über «Finanzinstrumente»²¹⁸⁴ nach Art. 5 GwV.²¹⁸⁵ Allerdings fehlt es für das Vorliegen eines solchen Geschäfts an der Gegenpartei. Die Liquiditätstokens werden direkt vom Protokoll bzw. Smart Contract generiert (und durch sie auch wieder eingelöst).

Grundsätzlich ist der berufsmässige Effektenhandel auf eigene oder fremde Rechnung dem GwG unterstellt (Art. 2 Abs. 3 lit. c GwG). Nach dieser Bestimmung gelten als Effekten Wertpapier und Wertrechte. Mit anderen Worten sind auch Asset-Token erfasst. Allerdings schränkt Art. 5 Abs. 2 GwV den Anwendungsbereich wieder ein, indem lediglich Personen, welche für ihre Handelstätigkeit nach FINIG eine Bewilligung benötigen, eine geldwäschereirechtlich relevante Tätigkeit ausüben.

Zumindest für die Bereitstellung von Liquidität in den eigenen Aktien über eine dezentrale Handelsplattform ist regelmässig keine FINIG-Bewilligung erforderlich.²¹⁸⁶ Eine solche Tätigkeit sollte auch vom Volumen her im Sinne der FINMA-Praxis vernachlässigbar sein.²¹⁸⁷ Es liegt in einem solchen Fall auch

²¹⁸³ Vgl. zur Relevanz des Arguments der *faktischen Unmöglichkeit*, die Sorgfaltspflichten des GwG einzuhalten, BGer 2A.62/2007 vom 30. November 2007, E. 8; 2C_488/2018 vom 12. März 2020, E. 5.1.

²¹⁸⁴ Siehe FINMA-RS 2011/1 «Tätigkeit als Finanzintermediär nach GwG», Rz. 70.

²¹⁸⁵ Eine gewisse Ähnlichkeit besteht zum Erwerb von Kapitalmarktpapieren, wie insb. verzinslichen Obligationen; vgl. UK KSt GwG, Rz. 144–151 (betreffend Abgrenzung zum Kreditgeschäft).

²¹⁸⁶ Siehe hierzu unten, [V.5.2d](#).

²¹⁸⁷ Vgl. FINMA-RS 2011/1 «Tätigkeit als Finanzintermediär nach GwG», Rz. 83.

keine Verwaltung von Effekten und Finanzinstrumenten oder Aufbewahrung von Effekten auf *fremde* Rechnung im Sinne von Art. 6 GwV vor.

e. Bemerkungen zur Technologieneutralität von Art. 51a GwV-FINMA (Exkurs)

Als Randbemerkung ist darauf hinzuweisen, dass es sehr fraglich ist, ob die Behandlung von virtuellen Währungen durch die FINMA noch mit den Grundsätzen der Technologie- und Wettbewerbsneutralität vereinbar ist.²¹⁸⁸ Namentlich stellt die Senkung des Schwellenwerts auf 1'000 Franken in Art. 51a Abs. 1 GwV-FINMA eine deutliche Verschärfung gegenüber Kassageschäften mit Fiatwährungen dar, welche in Art. 51 GwV-FINMA geregelt sind. Diese Verschärfung ist nach vorliegender Ansicht kaum mehr mit einem technologie- und wettbewerbsneutralen Regulierungsansatz zu rechtfertigen.²¹⁸⁹ Sodann ist eine weitere Verschärfung in der Auslegung des Begriffs «miteinander verbunden» zu sehen. Die FINMA verlangt gemäss ihrer neuen Aufsichtspraxis von den einer SRO angeschlossenen Mitgliedern, dass sie alle Geschäfte mit virtuellen Währungen innerhalb eines Zeitraums von 30 Tagen (ehemals einen oder zwei Kalendertage oder 24 oder 48 Stunden) als miteinander verbunden gemäss Art. 51a Abs. 1 GwV betrachten.²¹⁹⁰ Auch diese für die Industrie überraschende Entwicklung kann schwerlich als technologie- und wettbewerbsneutral angesehen werden.²¹⁹¹

²¹⁸⁸ Im DLT-Bericht von 2018 hat der Bundesrat diesen Grundsatz für Krypto- und Fiatwährungen ausdrücklich noch hervorgehoben; siehe Bundesrat, DLT-Bericht 2018, 145. Ferner sind diese Regulierungsgrundsätze ausdrücklich in Art. 6 Abs. 3 der Verordnung zum Finanzmarktaufsichtsgesetz enthalten.

²¹⁸⁹ Gl.M. BAS, Comment on GWV-FINMA adjustment, *passim*; ferner mit zusätzlichen Hinweisen zu ungeklärten Frage der Geltung von Art. 51a GwV-FINMA für in Fiatwährung denominierte *Stablecoins* Bity SA, Diminution du seuil de vérification des opérations de change, *passim*; ferner auch Bertschinger, SZW 2020, 705, der von den Grenzen der Technologieneutralität spricht.

²¹⁹⁰ Vgl. hierzu 21 Analytics, Swiss Regulator Further Reduces Threshold for Buying Bitcoin KYC-less, *passim*.

²¹⁹¹ Fraglich ist auch, ob die von der FINMA vorgesehene knappe Implementierungsfrist von rund 45 Tagen als mit der bundesgerichtlichen Rechtsprechung zu Praxisänderungen vereinbar ist; vgl. hierzu auch Uhlmann/Stojanovic, SZW 2017, 736 m.w.H.

2.8 Wallet-Anbieter (Exkurs)

a. Hosted Wallets

Anbieter von Hosted Wallets fallen bereits nach bisherigem Recht unter das GwG. Indem sie die Private Keys ihrer Kunden sicher verwahren, haben sie die ausschliessliche und unmittelbare Verfügungsmacht über fremde Vermögenswerte. Zwischen Anbietern und Kunden besteht in der Regel eine dauerhafte Geschäftsbeziehung, welche geldwäschereichtlich relevant ist.²¹⁹² Wenn Anbieter von solchen Wallets die Überweisung von Kryptovermögenswerten im Namen und Auftrag der Vertragspartei anordnen, erbringen sie in aller Regel eine Dienstleistung für den Zahlungsverkehr nach Art. 4 Abs. 1 lit. a GwV.²¹⁹³

b. Multisig-Wallets und verschlüsselte Wallets

Die Abkehr vom Konzept der Verfügungsmacht über fremde Vermögenswerte soll neu auch für gewisse Typen von Multisig-Wallets gelten. Unter geltendem Recht war es schwierig, Anbieter von Multisig-Wallets dem GwG zu unterstellen, wenn diese lediglich über eine Minderheit der Private Keys verfügten und somit alleine, d.h. ohne die Private Keys des formellen Eigentümers der Vermögenswerte, keine Transaktionen auslösen konnten.²¹⁹⁴

Auf der Grundlage von Art. 4 Abs. 1 lit. b GwV sollen Anbieter von Wallets mit Multisig-Funktion bereits unterstellt sein, wenn die Signierung des Anbieters für eine Transaktion des Nutzers lediglich notwendig ist, obschon der Anbieter nicht über die ausschliessliche und unmittelbare Verfügungsmacht verfügt.²¹⁹⁵ Dasselbe soll für Anbieter von «Dienstleistungen zur sicheren Aufbewahrung privater Schlüssel» gelten, selbst wenn die verschlüsselten Private

²¹⁹² Vgl. Bundesrat, DLT-Bericht 2018, 28.

²¹⁹³ Siehe statt vieler Bundesrat, DLT-Bericht 2018, 145–146.

²¹⁹⁴ Dies andeutend Bundesrat, DLT-Bericht 2018, 146; ferner Botschaft DLT 2019, 271; sodann FinCEN, Guidance CVC 2019, 17; siehe hierzu Van Valkenburgh, FinCEN's new cryptocurrency guidance, *passim*.

²¹⁹⁵ So scheinbar nun auch FATF, VASP Guidance 2021, 29 («As in the definition of 'transfer', this does not mean the control must be unilateral. 'Control' can include circumstances where keys or credentials held by others are required in order to change the assets disposition, such as multi-signature processes. The existence of a multi-signature model or models in which multiple parties must use keys for a transaction to happen does not mean a particular entity does not maintain control, depending on the extent of the influence it may have over the VAs.»).

Keys nur vom Inhaber der Vermögenswerte entschlüsselt werden können und somit nur er eine Transaktion auslösen kann.²¹⁹⁶ Im letzteren Falle wird nicht einmal mehr die Notwendigkeit der Mitsignierung durch den Anbieter für eine erfolgreiche Transaktion verlangt.²¹⁹⁷ Bei diesen Wallet-Typen handelt es sich nach Auffassung des EFD weder um reine Custodial Wallets noch um reine Non-Custodial Wallets.²¹⁹⁸

Ob die neue Regelung zu Multisig-Wallets nicht nur Hosted Wallets betrifft, sondern auch Self-Hosted Wallets erfasst, geht aus den veröffentlichten Dokumenten des EFD nicht direkt hervor. Nach vorliegender Ansicht muss allerdings mindestens ein Hosted Wallet in den fraglichen Multisig-Setup involviert sein. Dies ist z.B. dann der Fall, wenn der Anbieter eines Hosted Multisig-Wallets einen von mehreren Private Keys besitzt, dessen Mitsignierung für die erfolgreiche Ausführung einer Transaktion durch den Kunden unerlässlich ist.²¹⁹⁹

c. Self-Hosted Wallets

Die Entwicklung der Software und das Angebot von *Self-Hosted Wallets* sind weiterhin nicht dem GwG unterstellt.²²⁰⁰ Denn hier handelt es sich auch bloss um die Lizenzierung einer entsprechenden Software. Die Softwarelizenzierung kann potenziell als eine dauernde Geschäftsbeziehung zwischen dem Softwareanbieter und dem Nutzer betrachtet werden.²²⁰¹ Allerdings stellt diese für sich alleine keine geldwäschereirechtlich relevante dauernde Geschäftsbeziehung dar.²²⁰²

²¹⁹⁶ Siehe EFD, Erläuternder Bericht Verordnung DLT 2020, 15; EFD, Erläuterungen Verordnung DLT 2021, 22.

²¹⁹⁷ Siehe EFD, Erläuternder Bericht Verordnung DLT 2020, 17; *sehr kritisch* zu diesen Ausführungen CVA RWG, CVA's answer to the DLT Ordinance, 8 («*Placing such services in the financial intermediation 'bucket' would be akin to designating any password management service as financial intermediaries.*»).

²¹⁹⁸ Siehe EFD, Erläuternder Bericht Verordnung DLT 2020, 15; EFD, Erläuterungen Verordnung DLT 2021, 22.

²¹⁹⁹ Vgl. FinCEN, Guidance CVC 2019, 17.

²²⁰⁰ Vgl. Bundesrat, DLT-Bericht 2018, 150; KGGT, NRA Krypto 2018, 37–38; demgegenüber wurde etwa in der UK die Unterstellung von Non-Custodial Wallets diskutiert, vgl. hierzu Weber/Baisch, SZW 2019, 152; *kritisch* diesbezüglich Coin Center, Comments on Transposition of the Fifth Money Laundering Directive, *passim*.

²²⁰¹ A.M. offenbar Bundesrat, DLT-Bericht 2018, 28 («im Gegensatz dazu»).

²²⁰² Siehe zum Begriff oben, [V.2.6d](#).

Das EFD erwähnt sodann, dass eine GwG-Unterstellung dennoch angezeigt sein könnte, wenn «Zusatzleistungen zur Auslösung und Durchführung von Zahlungen» zur Verfügung gestellt würden.²²⁰³ Nach vorliegender Lesart dieser Erläuterung stellen die Speicherung bzw. Verwahrung von Kryptovermögenswerten sowie deren Übertragung an ein anderes Wallet *keine* derartigen Zusatzleistungen dar. Zusatzleistungen müssten mit anderen Worten über diese Grundfunktionalitäten eines Self-Hosted Wallets hinausgehen. Unklar ist hingegen, worin diese Zusatzleistungen bestehen können und inwieweit der Softwareanbieter in die Leistungserbringung involviert sein muss. Vorauszusetzen ist nach vorliegender Ansicht auch hier, dass der Wallet-Anbieter die effektive Zugriffsmöglichkeit auf die Aufträge von Nutzern hat bzw. deren Dienstleistungen für die Nutzung des Angebots erforderlich sind («hilft»). Dass die Nichtunterstellung von Self-Hosted Wallets, welche Grundfunktionalitäten anbieten, nicht ausdrücklich klargestellt wurde, ist vor dem Hintergrund der dadurch für Softwareunternehmen ausgelösten Rechtsunsicherheiten sehr zu bedauern.

Reine Self-Hosted Multisig-Wallets, welche z.B. eine Person mit ihrem Ehepartner zwecks Verwahrung von gemeinsamen Vermögenswerten einsetzen, haben einerseits aus Sicht einer der beteiligten Person Ähnlichkeiten mit Hosted Multisig-Wallets. Andererseits sind ausschliesslich Self-Hosted Wallets am Multisig-Setup beteiligt, weshalb es für eine Unterstellung mangels eindeutigen Anbieters regelmässig an einer dauernden Geschäftsbeziehung fehlt (siehe hierzu oben). Zudem wird die Unterstellung unter das GwG regelmässig auch an der fehlenden Berufsmässigkeit einer allfälligen finanzintermediären Tätigkeit gemäss Art. 7 ff. GwV scheitern. Bei einem Ehepaar stellt sich sodann auch die Frage der Fremdheit der Vermögenswerte.

Schliesslich nicht erfasst vom GwG sind *Social Recovery Wallets*, die auf Basis eines Smart Contracts die Kryptovermögenswerte einer Person aufbewahren. Lediglich die berechnigte Person kann mithilfe des Signing Keys über die Vermögenswerte verfügen. Eine Mehrheit der übrigen beteiligten Personen (sog. Guardians) können lediglich den Signing Key austauschen, nachdem die berechnigte Person die Guardians dazu aufgefordert hat. Guardians haben mit anderen Worten keinen Zugriff auf die Vermögenswerte und sind auch nicht für die Mitsignierung von Transaktionen erforderlich.²²⁰⁴

²²⁰³ Vgl. EFD, Erläuterungen Verordnung DLT 2021, 11, 22.

²²⁰⁴ Diese Funktionalität bietet etwa der Wallet-Anbieter *Argent*, vgl. hierzu Lesuisse, *Argent*, *passim*.

2.9 Zwischenfazit

Es ist als Zwischenfazit festzuhalten, dass der Bundesrat mit der *kryptobezogenen* Abweichung vom Konzept der Verfügungsmacht über fremde Vermögenswerte den Finanzintermediationsbegriff weiter ausgedehnt hat. Diese Entwicklung ist zwar nicht gänzlich neu,²²⁰⁵ hat aber mit Blick auf Art. 4 GwV seinen Ursprung allein im Umstand, dass Blockchain-Technologie und darauf basierende Applikationen zur Anwendung gelangen. Das in Art. 2 Abs. 3 GwG zentrale Konzept der Kontrolle über fremde Vermögenswerte wird u.a. für «dezentrale Handelsplattformen» aufgegeben, ohne dies allerdings im Gesetz zu verankern.

Nach vorliegender Auffassung hält der Bundesrat mit Art. 4 Abs. 1 lit. b GwV dennoch an einem *ähnlich gelagerten Konzept der Kontrolle* fest. Nunmehr gelten mit Blick auf Handelsplattformen diejenigen Personen als Finanzintermediäre, welche die effektive Zugriffsmöglichkeit auf die Transaktionen von Nutzern innehaben. An die Stelle der alleinigen Verfügungsmacht eines Finanzintermediärs tritt dessen Möglichkeit, in technischer Weise auf Übertragungen von virtuellen Werten einzuwirken. Die wichtigste Ausprägung besteht wohl darin, dass eine Drittperson die Abwicklung von Übertragungen zwischen den Nutzern einer Handelsplattform über das dezentrale Netzwerk verhindern bzw. blockieren könnte. Der mit Art. 4 Abs. 1 lit. b GwV neu eingeführte «Kontrollbegriff» könnte damit durchaus Entwicklungen erfassen, die im Ergebnis vergleichbare oder ähnlich gelagerte Kontrollmöglichkeiten wie zentrale Modelle von Handelsplattformen, die über die ausschliessliche Verfügungsmacht über fremde Kryptovermögenswerte verfügen, ausüben können. Eine enge Auslegung der neuen Bestimmung in der Praxis ist dafür allerdings angezeigt: Die Existenz von Admin Keys in einer Smart Contract-basierten Handelsplattform oder einer DAO bietet nicht automatisch die erforderlichen Kontrollmöglichkeiten. Nicht jede Eingriffsmöglichkeit ist mit anderen Worten kontrollrelevant i.S. des GwG. Es muss gegebenenfalls eine Einzelfallbetrachtung vorgenommen werden. Die anwendenden Behörden können sich, anders als der Bundesrat wohl beabsichtigt, nicht einfach aus dieser Pflicht stellen.

Nach vorliegender Auffassung erfasst Art. 4 Abs. 1 lit. b GwV (in der 1. Variante ohne Verfügungsmacht) *darum lediglich Handelsplattformen, welche den Transaktionsfluss unmittelbar zulasten der Nutzer beeinflussen können*. Als relevante Vergleichsgruppe gelten zentrale Handelsplattformen mit ausschliesslicher

²²⁰⁵ Vgl. die Hinweise zur Händler- und Beraterregulierung im GwG bei Nagel, GesKR 2020, 121–122.

Verfüugungsmacht über die Vermögenswerte ihrer Kunden. Diese fallen typischerweise unter Variante 2 der Bestimmung. Mit anderen Worten ist nach vorliegender Auffassung *nicht* jede Form der Hilfe zur Übertragung unterstellungspflichtig. Der offene Wortlaut der Bestimmung ist teleologisch zu reduzieren, um dem oben erwähnten Kontrollkonzept, wie es vom Bundesrat in den Berichten erläutert wird, Rechnung zu tragen.

Nach dem Gesagten kann festgehalten werden, dass nicht alle dezentralen Handelsplattformen nach vorliegendem Verständnis unter die neue Regel fallen. Im Gegenteil ist davon auszugehen, dass die meisten dezentralen Handelsplattformen, so wie der Begriff vorliegend verstanden wird, gerade nicht von Art. 4 Abs. 1 lit. b GwV erfasst werden.

Demgegenüber würden wohl *hybride* Handelsplattformen, wie insb. IDEX und Swarm Markets, mit hoher Wahrscheinlichkeit unter die neue Regelung fallen. IDEX verfügt zwar nicht über die Private Keys und somit die Verfügungsmacht über die virtuellen Währungen ihrer Kunden. Dies ist allerdings gerade nicht mehr zwingende Voraussetzung in Art. 4 Abs. 1 lit. b GwV (1. Variante). Doch ist die Verfügbarkeit der Leistungen des Plattformbetreibers wesentlich für die Nutzung der Plattform IDEX, da die verwendeten Smart Contracts vom Plattformbetreiber kontrolliert werden.²²⁰⁶ Theoretisch ähnlich sieht die rechtliche Situation für Non-custodial P2O-Handelsplattformen, die zwar ebenfalls nicht über die Verfügungsmacht über fremde Vermögenswerte verfügen, doch im Rahmen des Austauschgeschäfts mit ihren Kunden als Gegenpartei auftreten.²²⁰⁷ Allerdings wurde diese Form der Aktivität wohl in den meisten Fällen bereits vor der Revision der Bestimmung als Geldwechsel und/oder Geld- und Wertübertragung dem Geldwäschereirecht unterstellt.²²⁰⁸

Ausdrücklich erfasst vom Wortlaut von Art. 4 Abs. 1 lit. b GwV (2. Variante) sind schliesslich (zentrale) Handelsplattformen, welche für ihre Kunden die Verfügungsmacht über virtuelle Währungen ausüben.

²²⁰⁶ Siehe zur Funktionsweise von IDEX oben, [IV.3.11b](#).

²²⁰⁷ Siehe zur Funktionsweise solcher Plattformen oben, [IV.3.3b](#).

²²⁰⁸ Vgl. Bundesrat, Bericht zu virtuellen Währungen, 15–16; FINMA, Erläuterungsbericht GwV-FINMA 2015, 11–12; Bundesrat, DLT-Bericht 2018, 147; KGGT, NRA Krypto 2018, 38; vgl. für die Tätigkeit der Money Transmission in den USA FinCEN, Guidance CVC 2019, 14–15 («P2P exchangers»), 23–24 («CVC exchanger»); ferner DOJ, Report of the Attorney General's Cyber Digital Task Force 2020, 37–38.

2.10 Teilnahme an dezentralen Netzwerken

a. Einleitung

Nachdem die obenstehenden Ausführungen sich insb. mit dezentralen Handelsplattformen als eine Ausprägung dezentraler Applikationen befasst haben, stellt sich nachfolgend noch die Frage, ob dezentrale Netzwerke bzw. die Teilnehmer solcher Netzwerke als Finanzintermediäre qualifiziert werden können. Dies ist vorliegend relevant, werden doch einige dezentrale Handelsplattformen unmittelbar auf einem dezentralen Netzwerk ausgeführt (On-Chain-Handelsplattformen) oder auf einem separaten Netzwerk, das auf einem dezentralen Netzwerk aufbaut (Layer-2-Handelsplattformen).

Es ist grundsätzlich unerheblich, ob es sich beim Finanzintermediär nach Art. 2 Abs. 3 GwG um eine natürliche oder juristische Person handelt.²²⁰⁹ Ferner ist es für die Eröffnung des räumlichen Geltungsbereichs des GwG grundsätzlich unerheblich, dass sich ein Grossteil der Netzwerkteilnehmer im Ausland befindet, solange eine Person oder eine Gruppe von Personen in der Schweiz oder von der Schweiz aus wesentliche Bestandteile der finanzintermediären Tätigkeit ausführt.²²¹⁰ Finanzmarktgesetze dürfen schliesslich nicht umgangen werden, indem man eine bestimmte regulierte Tätigkeit in ihre Einzelteile zerlegt und diese sodann von mehreren Personen als kollektive Leistung erbringen lässt. Bei Vorliegen enger wirtschaftlicher, organisatorischer, personeller oder sonstiger Verflechtungen zwischen den beteiligten Personen kann somit eine Unterstellung unter das GwG angezeigt sein.²²¹¹

b. Netzwerkteilnehmer als Gruppe?

Dezentrale Netzwerke setzen sich definitionsgemäss aus mehreren Personen zusammen. Sie besitzen keinen einzigen Standort, sondern sind typischerweise global verteilt. Dasselbe gilt auch für die von ihnen betriebene Infrastruktur (PC, Server usw.).²²¹²

Die Teilnehmer eines dezentralen Netzwerks schaffen, indem sie etwa Rechenkapazitäten zur Verfügung stellen, in gemeinschaftlicher Weise die notwendigen

²²⁰⁹ Siehe SHK GwG-Schären, Art. 2 N 60.

²²¹⁰ Vgl. zum *räumlichen Geltungsbereich* oben, [V.1.4](#).

²²¹¹ Vgl. zum *Gruppenbegriff* oben, [V.1.5](#).

²²¹² Vgl. hinsichtlich Anknüpfung am Serverstandort FATF, VASP Guidance 2021, 43–44.

Voraussetzungen für die Funktionsfähigkeit des Netzwerks. Es stellt sich darum die Frage der *gruppenmässigen* Erfassung der einzelnen Teilnehmer durch das Finanzmarktaufsichtsrecht. Nach vorliegender Auffassung fehlt es an einer zielgerichteten arbeitsteiligen Koordination der Aktivitäten der Teilnehmer in einem dezentralen Netzwerk. Das Open-Source-Protokoll, das in aller Regel den Handlungen der einzelnen Teilnehmer zugrunde liegt, genügt für sich alleine nicht als Koordinationsmechanismus im aufsichtsrechtlichen Sinne. Die Aktivitäten der Teilnehmer, etwa in Bitcoin und Ethereum, sind, wenn überhaupt, lediglich als nicht unterstellungspflichtiges «Parallelverhalten» einzustufen.²²¹³ Die Grösse und Heterogenität des Teilnehmerkreises schliesst tendenziell wirtschaftliche, organisatorische und personelle Verflechtungen zwischen den einzelnen Beteiligten aus,²²¹⁴ welche aber für den Gruppenbegriff gerade zentral sind.²²¹⁵ Zudem fehlt es an einem «Gesamtplan», welcher der Koordination der Netzwerkteilnehmer zugrunde liegen würde.²²¹⁶ Zu einem ähnlichen Ergebnis, jedoch in Bezug auf die Einordnung als Zahlungssystem gemäss Art. 81 FinfraG kommt NICOLAS JACQUEMART: Namentlich bestehe zwischen den Netzwerkteilnehmern keine vertragliche Anspruchsgrundlage und eine solche ist in aller Regel auch nicht beabsichtigt.²²¹⁷ Eine Unterstellung unter das GwG wäre zudem praktisch schwierig umzusetzen, sind die einzelnen Teilnehmer doch typischerweise über den ganzen Globus verteilt. Die Bereitstellung eines dezentralen Netzwerks durch dessen Teilnehmer kann darum nach vorliegender Ansicht und bei «faire[r] Gesamtsicht»²²¹⁸ in aller Regel nicht gruppenmässig erfasst werden.

Davon zu unterscheiden ist selbstverständlich der Fall, in dem ein Anbieter in irreführender Weise vorgibt, das von ihm initiierte System sei dezentral, er aber letztlich das System – zusammen mit anderen Personen – *kontrolliert*. Ein

²²¹³ Siehe der kürzlich ergangene BGer 2C_729/2020 vom 5. August 2021, E. 4.3.2; vgl. ferner BGer 2C_30/2011 und 2C_543/2011 vom 12. Januar 2012, E. 3.1.2; 2C_898/2010 vom 29. Juni 2011, E. 2.2.

²²¹⁴ Das Bundesverwaltungsgericht spricht im «E-Coins»-Entscheid davon, dass «derart enge» und «derart intensive» Verflechtungen bestehen müssen, so dass nur noch eine Gesamtbetrachtung den faktischen Gegebenheiten gerecht werden könne; siehe BVGer B-5769/2017 vom 21. Januar 2019, E. 3.1.

²²¹⁵ Vgl. statt vieler BGE 136 II 43, E. 4.3.1.

²²¹⁶ Siehe BGer 2C_729/2020 vom 5. August 2021, E. 5.4.3.

²²¹⁷ Siehe Jacquemart, Offene Blockchainsysteme, Rz. 430–432. Vgl. ferner die Ausführungen zum Abschluss einer Systemvereinbarung oben, [III.2.2](#).

²²¹⁸ BGer 2C_30/2011 und 2C_543/2011 vom 12. Januar 2012, E. 3.1.3; 2C_89/2010 und 2C_106/2010 vom 10. Februar 2011, E. 3.3.4.

solcher Sachverhalt lag etwa dem Verfahren gegen die als Gruppe agierenden Personen hinter der Scheinkryptowährung «E-Coins» zugrunde.²²¹⁹

c. Netzwerkteilnahme als Finanzintermediation?

Es scheint ein gewisser Konsens zu bestehen, dass die Unterstellung von dezentralen Handelsplattformen unter das Geldwäschereiregime nicht dadurch erreicht werden soll, indem der Fokus auf das *dezentrale Netzwerk* als solches verlagert wird und dieses als Ganzes für eine irgendwie geartete finanzintermediäre Tätigkeit unterstellt wird.²²²⁰ Dasselbe muss für die Teilnehmer gelten, welche das Netzwerk letztlich ausmachen.²²²¹ Sie stellen durch die Ausführung einer Software und somit die Durchsetzung der Konsensregeln das dezentrale Netzwerk bereit.²²²² Abhängig von ihrer konkreten Funktion werden Teilnehmer für die Bereitstellung von Rechenkapazitäten oder sonstigen Konsensaufgaben mit neu geschaffenen Token und den von den Nutzer bezahlten Transaktionsgebühren entschädigt. Hierzu gehören namentlich Miner bzw. Staker und Mining bzw. Staking Pools.²²²³

²²¹⁹ Siehe hierzu FINMA, Scheinkryptowährungen, *passim*; in diesem Zusammenhang BVGer B-5769/2017 vom 21. Januar 2019, E. 3.1–3.3 («Im Gegenteil habe der von der Untersuchungsbeauftragten beigezogene IT-Experte festgestellt, dass die Systemadministratoren sowohl den Algorithmus als auch die Nutzer-Guthaben jederzeit beeinflussen könnten.»); ferner das Parallelverfahren BVGer B-6413/2017 vom 21. Januar 2019.

²²²⁰ So insb. FATF, VASP Guidance 2019, 17 («[...] the FATF does not seek to regulate the technology that underlies VAs or VASP activities, but rather the natural or legal persons behind such technology or software applications that may use technology or software applications to facilitate financial activity or conduct as a business the aforementioned VA activities on behalf of another natural or legal person.»).

²²²¹ So nun explizit FATF, VASP Guidance 2021, 32 («[...] natural or legal persons that solely engage in the operation of a VA network and do not engage in or facilitate any of the activities or operations of a VASP on behalf of their customers (e.g., offering internet network services and infrastructure, offering computing resources such as cloud services and creating, validating, and broadcasting blocks of transactions) [...]»), ferner 35.

²²²² Vgl. auch FinCEN, Guidance CVC 2019, 24 («[...] a person is exempt from money transmitter status if the person only provides the delivery, communication, or network access services used by a money transmitter to support money transmission services.»).

²²²³ Siehe FATF, Draft VASP Guidance 2021, 26; vgl. hinsichtlich der geldwäschereirechtlichen Behandlung des Mining in der Schweiz Bundesrat, DLT-Bericht 2018, 148; KGGT, NRA Krypto 2018, 39, 40; ferner Grünewald, in: Weber/Thouvenin, Währungs- und geldwäschereirechtliche Fragen, 107, wonach Mining als blosser Nutzung virtueller Währungen einzuordnen ist; Müller/Reutlinger/Kaiser, EuZ 2018, 89, wonach dies für das Mining gilt, wenn es lediglich dem «privaten Eigengebrauch» dient. Vgl. hinsichtlich der geldwäschereirechtlichen Behandlung von Mining Pools unter dem US-amerikanischen Bank Secrecy Act FinCEN, Guidance CVC 2019, 28, wo unterschieden wird, ob der Betreiber eines Mining

A maiore ad minus muss dies auch für Teilnehmer gelten, die keine Rechenkapazitäten zur Konsensbildung, sondern lediglich als *Relayers* zur Bereitstellung des Netzwerks beitragen, d.h. insb. Personen, die durch Ausführung von Software einen Full Node etwa im Bitcoin Netzwerk oder einen Lightning Node auf ihrem oder einem Computer eines Dritten (z.B. eines Cloud Computing-Dienstleisters) betreiben.

Die Teilnehmer eines dezentralen Netzwerks betreiben in aller Regel lediglich eine *Infrastruktur*, die u.a. für die Übertragung von virtuellen Währungen verwendet werden kann, in technischer Hinsicht jedoch nicht auf solche Daten beschränkt ist.²²²⁴ Die Ausführung der Software dient mit anderen Worten in erster Linie der Weiterleitung von Daten, welche die unterschiedlichsten Werte abbilden können. Technisch genauer gesagt, handelt es sich dabei um Mitteilungen, die vom Absender einer Transaktion mit seinem Private Key signiert worden sind und lediglich vom Inhaber des vorbestimmten Public Keys verwertet werden kann. Obschon die oben erwähnten Teilnehmer im Falle eines Full Nodes eine vollständige Kopie der Daten anlegen, kommt ihnen mangels Kenntnis des Private Keys des Empfängers zu keinem Zeitpunkt die Verfügungsmacht über fremde Vermögenswerte zu. Durch Ausführung des Protokolls übernehmen die Netzwerkteilnehmer informationstechnisch eine mit dem Netzbetreiber vergleichbare Rolle.

Am ehesten lässt sich die Teilnahme mit den Leistungen des Telekommunikationsanbieters für Interbankenzahlungen SWIFT vergleichen,²²²⁵ alternativ mit den an einem digitalen oder mobilen Zahlungssystem beteiligten Personen, wie insb. der Betreiber eines Kreditkartennetzwerks oder der Anbieter eines Pass-Through-Wallets.²²²⁶

Zwischen den Teilnehmern eines dezentralen Netzwerks und den Nutzern einer dezentralen Applikationen besteht allerdings weder ein Kontakt noch eine sonstige spezifische Interaktion, die individuell oder kollektiv ausgehandelt werden würde. Im Gegenteil, die Teilnehmer solcher Netzwerke können gar nicht wissen, welche Personen die von ihnen bereitgestellte Infrastruktur für

Pools lediglich die Einnahmen an die Mitglieder des Pools verteilt (nicht unterstellungspflichtig) oder zusätzlich die Wallets der Mitglieder des Pools führt (unterstellungspflichtig).

²²²⁴ Siehe etwa oben, [III.4.1.](#)

²²²⁵ Ausführlich hierzu Van Valkenburgh, Bank Secrecy Act, 15–16.

²²²⁶ Vgl. hinsichtlich solcher Zahlungssysteme, die je nach Anwendungsfall auch als *Schemes* bezeichnet werden, Stengel/Weber, Digitale und mobile Zahlungssysteme, Rz. 158, 204, 422, 427, 519, 525.

die Weiterleitung ihrer Daten nutzen. Und die Nutzer sind verständlicherweise in aller Regel auch nicht bereit, freiwillig ihre Identität gegenüber allen anderen Teilnehmern offenzulegen, deren Tausende es im Bitcoin Netzwerk gibt.²²²⁷ Eine Unterstellung bietet sich darum auch aus praktischen Gründen nicht an. Anders mag die rechtliche Situation für Wallet-Anbieter aussehen, die ihren Kunden die Nutzung des Lightning Netzwerks über ein Hosted Wallet anbieten. Diese haben allerdings in praktischer Hinsicht keine Probleme, etwa ihre Kunden zu identifizieren.

Teilnehmer dezentraler Netzwerke führen letztlich eine Software aus, und in diesem Rahmen überprüfen sie die Einhaltung gewisser Protokollregeln, um die Sicherheit und Stabilität des Netzwerks zu gewährleisten, oder aber sie tragen als Miner oder Staker unmittelbar zum Konsensprozess des Netzwerks bei. Darüber hinaus kommt den Teilnehmern *bewusst* keine weitere Rolle zu.

Das EFD hält zwecks Abgrenzung des weiten Geltungsbereichs des neuen Art. 4 GwV fest, dass die Bereitstellung blosser IT-Infrastruktur, die allgemein der Datenübermittlung dient, nicht als unterstellungspflichtige Aktivität betrachtet werden könne. Konkrete Erwähnung findet der Betrieb eines Telefonnetzwerks.²²²⁸ Das Bundesgericht hat kürzlich ebenfalls deutlich gemacht, dass der reine Netzbetrieb (*in casu* durch die Swisscom), welcher lediglich als eine «zwischenengeschaltete Stelle für die Lieferung digitaler Waren und Dienstleistungen» betrachtet werden muss, noch keine unterstellungspflichtige Tätigkeit darstellt.²²²⁹

Was für die Protokolle des Internets und ähnlicher Dateninfrastrukturen gilt, muss richtigerweise auch für die Protokolle gelten, die in dezentraler Weise auf den erstgenannten Infrastrukturen ausgeführt werden. Solange die Kontrollmöglichkeit der Transaktionen durch einen einzelnen Netzwerkteilnehmer oder einer Gruppe von miteinander verbundenen Netzwerkteilnehmern marginal ist, was aber ausnahmsweise bei Minern und Stakern relevant sein kann,²²³⁰ ist nach vorliegender Auffassung dem Dezentralitätsparadigma Vor-

²²²⁷ Vgl. Coin Center, Comments on FATF Guidance, 16–18.

²²²⁸ Siehe EFD, Erläuterungen Verordnung DLT 2021, 23.

²²²⁹ Siehe BGer 2C_488.2018 vom 12. März 2020, E. 4.4.2.

²²³⁰ Vgl. die Entwicklung des US-amerikanischen Mining-Pools Marathon, der zuerst nur OFAC-konforme Blocks produziert hat, jedoch kurz darauf von diesem Vorhaben wieder abgerückt ist; vgl. hierzu Marathon Digital Holdings, Fully AML and OFAC Compliant Bitcoin, *passim*; ferner Post, Stop censoring transactions, The Block, *passim*. Siehe für weitere Informationen zu OFAC-sanktionierten Wallet-Adressen Bigart/Boone/Wilson, Lexology vom 27. März 2018, *passim*.

rang zu gewähren und somit von einer Unterstellung unter die Finanzmarkt-gesetzgebung abzusehen. An dieser Stelle ist auf das erst noch zu entwickelnde Konzept der Dezentralität hinzuweisen.²²³¹

d. Lightning Netzwerk

Das Gesagte gilt auch für Lightning Nodes, durch dessen Zahlungskanäle bitcoins vom Absender zum Empfänger «fliessen». Transaktionen über einen Zahlungskanal, der von den beiden Vertragsparteien selbst betrieben wird, sind unproblematisch, fehlt es hier ja bereits an einem Intermediär.²²³² Wenn hingegen eine Transaktion zwischen Absender und Empfänger durch mehrere Zahlungskanäle unterschiedlicher Teilnehmer geht, was in der Praxis üblich ist, so stellt sich die Frage, ob die weiterleitenden Teilnehmer das Geld- und Wertübertragungsgeschäft betreiben.

Die Teilnehmer des Lightning Netzwerks platzieren bei Kanaleröffnung Kryptovermögenswerte in einer Multisig-Adresse, um diese für Transaktionen über den Layer 2 zu blockieren. Über diese Vermögenswerte haben sie Verfügungsmacht, denn sie können jederzeit den Kanal schliessen und dadurch die «Kontobilanz» des Kanals auf dem Bitcoin Netzwerk zur Ausführung bringen. Doch handelt es sich bei den Vermögenswerten in aller Regel um *eigene* Vermögenswerte. Im Hinblick auf die Transaktionen Dritter, die wiederum ausschliesslich aus Mitteilungen bestehen, die für den Empfänger bestimmt sind, kommt den Teilnehmern des Netzwerks allerdings keine Verfügungsmacht zu. Sie leiten auch in diesem Fall lediglich die Daten anderer Teilnehmer an einen vorbestimmten Endpunkt weiter. Beim Geld- oder Wertübertragungsgeschäft nach Art. 4 Abs. 1 lit. c i.V.m. Abs. 2 GwV nimmt der Finanzintermediär hingegen die Vermögenswerte von einer Person *entgegen* und transferiert sie an eine andere Person i.d.R. an einen anderen Ort.²²³³ Dabei handelt es sich um ein sog. Dreiparteiengeschäft, während dessen Ausführung der Finanzintermediär die Verfügungsmacht über fremde Vermögenswerte erlangt.²²³⁴ Die blossen Teil-

²²³¹ Siehe unten, VII.

²²³² Jedoch könnte auch hier ein unterstellter *Geldwechsel* vorliegen, doch müssten dafür die entsprechenden Voraussetzungen erfüllt sein.

²²³³ Die FINMA unterscheidet offenbar *einschränkend* zwischen Übertragungen von der Schweiz ins Ausland und solchen auf umgekehrtem Weg; vgl. Art. 2 lit. c GwV-FINMA; ferner bereits UK KSt GwG, Rz. 173.

²²³⁴ Siehe SHK GwG-Schären, Art. 2 N 81, 121; OFK GwG-Wyss, Art. 2 N 27.

nahme am Lightning Netzwerk stellt darum nach vorliegender Auffassung kein unterstelltes Geld- und Wertübertragungsgeschäft dar.²²³⁵

Zusammenfassend kann also festgehalten werden, dass technisch betrachtet die Teilnehmer eines dezentralen Netzwerks eine protokollbasierte intermediäre Rolle wahrnehmen, was im ersten Kapitel als netzwerkbasierte Intermediation bezeichnet wurde,²²³⁶ jedoch in geldwäschereirechtlicher Hinsicht keine unterstellte Finanzintermediation vorliegt.

2.11 Softwareentwicklung

In der Literatur wird vereinzelt vorgeschlagen, die Entwickler von dezentralen Applikationen dem Geldwäschereiregime zu unterstellen.²²³⁷

Nach der FATF-Guidance vom Oktober 2021 sollen ähnliche Dienstleistungen und Risiken regulatorisch ähnlich behandelt werden.²²³⁸ Das schweizerische Geldwäschereirecht gelangt zudem hauptsächlich auf Tätigkeiten im Finanzsektor zur Anwendung.²²³⁹ Zwar wurde die ursprüngliche Erwähnung des Finanzsektors im Gesetzestitel in der Gesetzesrevision, welche seit dem 1. Januar 2016 in Kraft ist, gestrichen, doch ist das GwG angesichts der Natur der Sorgfaltspflichten in erster Linie weiterhin auf den Finanzsektor ausgerichtet.²²⁴⁰

Unter diesen Gesichtspunkten kann die Programmierung von Software sowie eine allfällige Lizenzierung kaum je als Finanzintermediation eingestuft werden. Konsequenterweise kommt die FATF zum Schluss, dass die Programmierung von Software sowie deren Lizenzierung in geldwäschereirechtlicher Hinsicht keine relevanten VASP-Aktivitäten sind.²²⁴¹ Zum selben Ergebnis kommt FinCEN in den USA.²²⁴² Diese Einschätzung wird indirekt auch in den Ausführungen des EFD zum neuen Art. 4 Abs. 1 lit. b GwV erkennbar, wonach die Entwicklung und das Anbieten von Software keine Dienstleistungen für den

²²³⁵ Ausführlich hierzu Andreotti, Teil 2, iusNet BR-KR 22.12.2022, *passim*.

²²³⁶ Siehe oben, [II.5](#).

²²³⁷ So etwa Salami, Butterworths Journal of International Banking and Financial Law 2020, 498.

²²³⁸ Siehe FATF, VASP Guidance 2021, 13.

²²³⁹ So noch explizit Botschaft GwG 1996, 1166, ferner 1115–1118

²²⁴⁰ Vgl. aber SHK GwG-Schären, Art. 2 N 4, wonach die Berücksichtigung von Händlern die expansive Tendenz der Geldwäschereiregulierung belegt.

²²⁴¹ Siehe oben, [V.2.3d.iii](#).

²²⁴² Siehe FinCEN, Guidance CVC 2019, 3, 27; vgl. hierzu *differenzierend* Van Valkenburgh, Bank Secrecy Act, 9, 14, 17–18; ferner Ox, Federal Anti-Money Laundering Regulation, *passim*.

Zahlungsverkehr darstellen. Das NRA 2024 des EJPD und fedpol nimmt beispielsweise Entwickler, die bloss eine Software zum Download anbieten, ohne mit dem Nutzer «irgendeine Geschäftsbeziehung» einzugehen, vom sachlichen Anwendungsbereich aus.²²⁴³ Einzig bei «Zusatzleistungen», wobei unklar ist, was darunter genau zu verstehen ist, könnte gegebenenfalls eine Dienstleistung für den Zahlungsverkehr vorliegen.²²⁴⁴

Nach vorliegender Ansicht stellen die Entwicklung und Lizenzierung bzw. der Verkauf von Software auch sonst keine Aktivität dar, welche als Finanzintermediation gemäss GwG qualifizieren könnte.

2.12 Fazit

a. Einleitung

Aufgrund der überragenden Bedeutung der geldwäschereirechtlichen Diskussionen für Kryptowährungen und dezentrale Systeme bietet es sich an dieser Stelle an, zu einem Fazit über die vorausgegangenen Ausführungen zu gelangen.

b. Bargeld, Inhaberaktien und virtuelle Währungen

Die Tendenz im Bereich der Verhinderung von Geldwäscherei und Terrorismusfinanzierung ist eindeutig: Vermögenswerte, die *inhaberpapierähnliche* Eigenschaften aufweisen – wie etwa Bargeld oder Inhaberaktien – und somit praktisch anonym besessen und übertragen werden können, sollen abgeschafft, eingeschränkt oder zumindest deanonymisiert werden. Der Gebrauch von Bargeld im Alltag wurde durch die Ausdehnung des persönlichen und sachlichen Geltungsbereichs des GwG eingeschränkt;²²⁴⁵ Inhaberaktien kommt heute, wo sie formell noch nicht abgeschafft wurden, aufgrund der Pflicht, sie als Bucheffekten auszugestalten und zentral zu verwahren, eine ähnliche Eigentümertransparenz wie Namenaktien zu.²²⁴⁶ Virtuelle Währun-

²²⁴³ Siehe EJPD/fedpol, NRA 2024, 33.

²²⁴⁴ Siehe oben, [V.2.8c](#).

²²⁴⁵ Vgl. Art. 8a GwG; für eine Übersicht weiterer Bestimmungen, die auf Bargeldgeschäfte zur Anwendung gelangen, siehe KGGT, NRA Bargeld 2018, 32–37.

²²⁴⁶ Vgl. Art. 622 Abs. 1^{bis} OR; ferner die Ausführungen bei Burckhardt, ex ante 2/2018, 9; Glanzmann/Spoerlé, GesKR 2018, 91–92; Knobloch, in: Müller et al., Abschaffung der In-

gen bzw. Kryptowährungen weisen dank ihrer technischen Funktionsweise ebenfalls inhaberpapierähnliche Eigenschaften auf. Sie sind allerdings im digitalen Raum zu Hause, was ihre Übertragbarkeit im Vergleich zu materialisierten Vermögenswerten deutlich vereinfacht. Die Parallele etwa zu in Wertpapieren verurkundeten Rechten kommt auch im neuen Registerwertrecht gemäss Art. 973d OR zum Ausdruck.²²⁴⁷ Demgegenüber kommt die Nach- und Rückverfolgbarkeit von kryptobasierten Transaktionen im Vergleich zu Bargeld oder Inhaberaktien der Strafverfolgung entgegen (s. hierzu unten).

c. Ausdehnung des Finanzintermediationsbegriffs

Der Bundesrat hat mit der Revision der GwV das Konzept der Verfügungsmacht über fremde Vermögenswerte weiter ausgehöhlt. Damit opfert er die eindeutigen Konturen des Finanzintermediationsbegriffs zugunsten eines nahezu beliebig ausdehnbaren neuen Finanzintermediationsbegriffes der irgendwie gearteten Kontrollmöglichkeit oder des irgendwie gearteten Einbezugs in eine Transaktion eines Nutzers.²²⁴⁸ Diese Entwicklung scheinen durch die Vorarbeiten der FATF veranlasst worden zu sein. Die FATF scheint allerdings alles andere als zufrieden mit der derzeitigen Situation in DeFi zu sein. Entsprechend soll der VASP-Begriff durch die Mitgliedsstaaten expansiv ausgelegt werden. In diesem könnte sich auch Art. 4 Abs. 1 lit. b GwV als «trojanisches Pferd», das den Weg «in die Stadtmauern» der Geldwäschereiregulierung gefunden hat, herausstellen. Im Rahmen künftiger Revisionen könnte die Bestimmung als Anlass zum weiteren Ausbau des Finanzintermediationsbegriffs genutzt werden.

Dezentrale Handelsplattformen sollen nach vorliegender Auffassung nur dann geldwäschereirechtlich erfasst werden, wenn eine Drittperson tatsächlich relevante Kontrollmöglichkeiten über eine Plattform ausüben kann. P2P-Transaktionen und Transaktionen über Plattformen, die ausschliesslich unmittelbar zwischen den beteiligten Begünstigten ablaufen, ohne dass eine Drittperson

haberaktien, 347–348; zum «Tathergang» Gericke/Kuhn, AJP 2015, *passim*; ferner zur feststellbaren Tendenz, die Anonymität des Aktionärs abzuschaffen, Egle, Anonymität, N 1127.

²²⁴⁷ Gemäss Art. 973d Abs. 2 Ziff. 1 OR muss der Gläubiger, nicht aber der Schuldner, die Verfügungsmacht über die verbrieften Rechte innehaben, damit es sich um ein Registerwertrecht handelt; vgl. hierzu Botschaft DLT 2019, 278–279 m.w.H. Dies schliesst allerdings nicht aus, dass ein Finanzintermediär ein Registerwertrecht für den Gläubiger verwaltet und verwahrt. Zudem ist auch die Emittentenverwahrung weiterhin zulässig; vgl. hierzu SBF, Circular 2021/01, 5.

²²⁴⁸ G.L.M. Stengel/Bianchi, in: Weber/Kuhn, Geldwäscherei und Terrorismusfinanzierung, Rz. 21, die davor warnen, dass das GwG «ausufernd» angewandt werden könnte.

eine effektive Zugriffsmöglichkeit auf die involvierten Vermögenswerte und Transaktionsflüsse hat, sind nach vorliegender Auffassung in geldwäschereirechtlicher Hinsicht gleich zu behandeln. Dieser Tatsache scheint die Revision von Art. 4 Abs. 1 lit. b GwV Rechnung zu tragen, zumindest wenn man der vorliegenden Auslegungsanalyse der Bestimmung folgt. Die FATF sieht demgegenüber Verschärfungen vor.

d. Handlungsmacht der Rechtsunterworfenen

Die staatliche Auferlegung von Pflichten und Verantwortung muss von der Möglichkeit der Rechtsunterworfenen abhängig gemacht werden, ob diese *objektiv* die ihnen auferlegten Pflichten erfüllen und die ihm übertragene Verantwortung tatsächlich wahrnehmen können.²²⁴⁹

Zwar verfügt jeder Teilnehmer in einem dezentralen Netzwerk insoweit über Autonomie, als er selbst bestimmen kann, welchen Konsensregeln er folgen will. Doch ist seine Autonomie auf dieses spezifische Handlungselement *beschränkt*. Die Ausübung der Autonomie hat namentlich keinen objektiv relevanten Einfluss auf das Verhalten der übrigen Netzwerkteilnehmer. Die Auferlegung von Rechtsnormen gegenüber Adressaten, allen voran Entwicklern von Software und Personen, welche deren Software ausführen, die in praktischer Hinsicht keinen Einfluss auf deren Einhaltung haben können, wäre rechtsphilosophisch und rechtsoziologisch kaum vertretbar. Ohne Handlungsmacht kann es prinzipiell keine irgendwie geartete moralisch-ethische Verantwortung geben.²²⁵⁰ Diese Handlungsmacht kann mit dem Konzept der *Agency* umschrieben werden: Kann eine Person nicht anders handeln oder hätte sie zwar anders handeln können, am Ergebnis hätte sich dennoch nichts geändert, ver-

²²⁴⁹ GLM. BAS, Comments on FATF Guidance, 4; SBF, Comments on FATF Guidance, 3.

²²⁵⁰ Vgl. etwa in *ethischer* Hinsicht Höffe et al., Lexikon der Ethik, 315, die von «Zurechnungsfähigkeit» als Voraussetzung der rechtlichen Verantwortung sprechen; in *organisations-theoretischer* Hinsicht Luhmann, Funktionen und Folgen formaler Organisation, 172–190; ferner zum Spannungsverhältnis zwischen Handlungsmacht und Verantwortung in arbeitsteiligen und korporativen Kontexten Waespi, Organisationshaftung, 114, 212; sodann im *haftungsrechtlichen* Kontext Weber, Jusletter IT vom 21. September 2017, Rz. 10; Gordon/Lutz, SZW 2020, 56; Fellmann, HAVE 2021, 110 («Haftung folge Kontrolle»); vgl. ferner Zech, in: Verhandlungen des 73. Deutschen Juristentages, Entscheidungen digitaler autonomer Systeme, A 39, A 51–A 52; schliesslich in Bezug auf die zivilrechtliche Haftung beim geteilten Netzbetrieb des Internets Weber, E-Commerce und Recht, 528.

fügt die Person über keine Agency.²²⁵¹ Zu einem ähnlichen Verantwortlichkeitskonzept gelangt man auch aufgrund einer Haftung nach dem Prinzip der Risikosphären: Demnach soll jeweils diejenige Person für einen Schaden haftbar gemacht werden können, welche die Risiken am ehesten hätte *kontrollieren* und somit den Schadenseintritt hätte *verhindern* können.²²⁵²

Der Gesetzgeber hat sich auf das Normative zu beschränken, zu dessen Einhaltung und Umsetzung die Rechtsunterworfenen faktisch fähig sind.

e. Überregulierung

Umgekehrt gilt dies aus *Praktikabilitätsgründen* auch für den Gesetzgeber, welcher die Anwendungsgeeignetheit einer Bestimmung sicherzustellen hat.²²⁵³ Die Vollzugstauglichkeit des Ansatzes der FATF, beabsichtigt die Pariser Behörde nicht die Totalüberwachung aller Marktteilnehmer durch die nationalen Aufsichtsbehörden, ist generell fraglich. Gesetze sind praxistauglich auszugestalten, was bei Missachtung allenfalls mit Blick auf das Rechtssicherheitsgebot, den Grundsatz der Verhältnismässigkeit und das Willkürverbot relevant sein kann;²²⁵⁴ ihre Anwendung hat zudem auch praktischen Anforderungen zu genügen.²²⁵⁵ Die von der FATF angestossene Regulierungskurve droht demgegenüber in eine Überregulierungswelle von Privatpersonen auszuarten.

²²⁵¹ Siehe Barnes, Understanding Agency, 9, 25–27; kritisch hinsichtlich der Kollektivität moderner Technologien am Bsp. eines Flugs nach Teneriffa Rammert, in: Passoth/Peuker/Schillmeier, Distributed agency, 103–06.

²²⁵² Vgl. insb. mit Blick auf Sachverhalte mit *autonomen Systemen* Zech, in: Verhandlungen des 73. Deutschen Juristentages, Entscheidungen digitaler autonomer Systeme, A 88–A 90, wo vom «Gleichlauf von Risikobeherrschung und Haftung» die Rede ist; ferner Lohmann, HAVE 2021, 120.

²²⁵³ Siehe Coin Center, Comments on FATF Guidance, 19–21; BA, Comments on FATF Guidance, 8; vgl. ferner Kilgus, Effektivität von Regulierung, N 32, 482; zur vergleichbaren Frage der (Un-)Wirksamkeit von Netzsperrern mit Blick auf die Durchsetzung von Urheberrechten im World Wide Web Thouvenin et al., sic! 2017, 701, 707–709; in allgemeiner Hinsicht Wyss, ZBl 2018, 19–20; vgl. demgegenüber allerdings zur Möglichkeit *symbolischer Gesetzgebung* Müller/Uhlmann, Rechtssetzungslehre, Rz. 306.

²²⁵⁴ Vgl. zu diesen Grundsätzen Müller/Uhlmann, Rechtssetzungslehre, Rz. 10, 21, 38, 61, 292; Burckhardt, Methode und System des Rechts, 251; Häfelin/Müller/Uhlmann, Allgemeines Verwaltungsrecht, Rz. 178 m.w.N.

²²⁵⁵ Vgl. zur *praxisorientierten Gesetzesauslegung* des Bundesgerichts insb. BGE 96 I 602, E. 4; 136 II 113, E. 3.3.4; 137 II 297, E. 2.3.5; 141 III 101, E. 2.9; ebenfalls hierzu Emmenegger/Tschentscher, in: BK ZGB, 2012, Art. 1 N 325–328; Meier-Hayoz, in: BK ZGB, 1962, Art. 1 N 213 («leichte Realisierbarkeit»), 325.

Der Staat würde mit solchen Rechtsnormen auch direkt gestaltend in den Markt eingreifen, was unter Gesichtspunkten von Eigentumsgarantie und Wirtschaftsfreiheit relevant sein dürfte. UDO DI FABIO spricht von der «Macht-ergreifung des öffentlichen Rechts», wenn er von der zunehmenden Expansion des Präventions- und Steuerungsstaats berichtet.²²⁵⁶ Anbieter von Dienstleistungen im Bereich von Blockchain-Technologien müssen sich darum zunehmend die Frage stellen, inwieweit sie ihr Geschäftsmodell anpassen wollen (und können), um den neuen Rahmenbedingungen bzw. den dadurch verursachten höheren Transaktionskosten zu genügen. Ob ein solcher Ergebnis erwünscht ist, ist letztlich auch eine rechtspolitische Frage, die insb. auch Fragen der Risikoversorge und der Zulassung und Förderung von Innovation miteinbeziehen sollte.²²⁵⁷

Sollten die Empfehlungen der FATF nationalstaatliches Recht werden, hätten Entwickler dezentraler Handelsplattformen wohl zwei Möglichkeiten, um einer allfälligen Unterstellung nachzukommen: Sie könnten einerseits das dezentrale Geschäftsmodell gänzlich aufzugeben, was aber wohl weitere Konsequenzen in anderen Rechtsbereichen (z.B. Bankenrecht) nach sich ziehen würde. Sie könnten andererseits versuchen, eine Gatekeeper-Funktion ihren ursprünglich frei zugänglichen dezentralen Applikationen vorzuschalten. Infrage käme dabei insb. die Einführung von Konten, die mit der Identität der Nutzer verknüpft sind. Ob dabei auf eine Blockchain-basierte Identität zurückgegriffen werden würde, kann offenbleiben.

Offensichtlich würde die Einführung einer Kontenstruktur oder dergleichen eine systemwidrige Abweichung vom heute vorherrschenden Dezentralitätsparadigma bedeuten.²²⁵⁸

²²⁵⁶ Siehe Di Fabio, Risikoentscheidung im Rechtsstaat, 450.

²²⁵⁷ Siehe zu diesem Spannungsverhältnis ausführlich Hettich, Kooperative Risikoversorge, Rz. 30–35; ferner ausdrücklich in Bezug auf Blockchain/DLT Bundesrat, DLT-Bericht 2018, 13–14.

²²⁵⁸ Vgl. BAS, Comments on FATF Guidance, 3, und SBF, Comments on FATF Guidance, 3, die jedoch davon ausgehen, dass die Umsetzung der FATF Draft Guidance die heutigen Geschäftsmodelle komplett verunmöglichen würde («The FATF's implicit assumption that DApps like Uniswap can somehow be transformed into a financial intermediary without destroying their business model is a misjudgment.»); ferner White, Use AML as an Excuse, Coin-telegraph, *passim*.

f. Wirksamkeit des heutigen Geldwäschereiregimes?

Eine allfällige weitergehende Unterstellung dezentraler Handelsplattformen unter das GwG, was nach vorliegender Auffassung allerdings nicht wünschenswert ist, sollte den inhärenten Schwächen des heutigen weltweit geltenden Geldwäschereiregimes, dessen ökonomische Kosten-Nutzen-Analyse nach Schätzungen *katastrophal* ausfällt,²²⁵⁹ vertiefte Beachtung schenken. Die negativen Konsequenzen des heutigen Regimes sind sodann mit Blick auf die finanzielle Inklusion und des De-Riskings des Finanzsektors festzustellen.²²⁶⁰ MARA WESSELING spricht schliesslich mit Blick auf empirische Daten zur Verhinderung der Terrorismusfinanzierung durch das heutige Regime von einem «Theatre of Compliance».²²⁶¹ Dass der Gesetzgeber diese Erkenntnisse zumindest berücksichtigt, ist im Lichte des Verhältnismässigkeitsprinzip geboten.²²⁶² Es ist letztlich unverständlich, weshalb der Gesetzgeber nicht auch im Bereich der Verhinderung bzw. Entdeckung (möglicher) krimineller Aktivitäten ein Kosten-Nutzen-Ansatz anwenden sollte.

²²⁵⁹ Siehe diesbezüglich Pol, *Policy Design and Practice* 2020, 81–88, ferner 77 («[...] *common responses to policy failure apply the same policy prescription, more efficiently and with renewed vigor, yet demonstrating that such efforts repeatedly produce poor outcomes has proven insufficient to break the cycle.*»), 89 («[...] *if the modern anti-money laundering paradigm is characterized by a self-reinforcing continuous loop of policy failure, with 'solutions' repeatedly 'doing more of the same' producing much the same results, and with powerful stakeholder incentives maintaining the status-quo, it will be difficult to recalibrate for better outcomes. But not impossible.*»); ferner Pol, *Journal of Financial Crime* 2018, 296 («[...] *the disruption of criminal funds hardly constitutes a rounding error in the accounts of profit-motivated criminal enterprises.*»); Findley/Nielson/Sharman, *Global Shell Games*, 173–174, sprechen von einem potemkinschen Erfolg der FATF bloss auf dem Papier; ähnlich kritisch zum Thema des Regulierungsversagens Sharman, *Money Laundry*, *passim*. Es ist allerdings eine gewisse Vorsicht geboten, denn die Datenlage in diesem Bereich ist allgemein eher schlecht, vgl. hierzu Levi/Reuter/Halliday, *Crime, Law and Social Change* 2018, *passim*.

²²⁶⁰ Siehe etwa Koker, *Journal of Money Laundering Control* 2014, insb. 291–293.

²²⁶¹ Siehe Wesseling, *European Fight against Terrorism Financing*, 188–212, wobei die vorherrschenden AML/CFT-Standards nach Auffassung der Autorin der Öffentlichkeit ein falsches Sicherheitsgefühl vermitteln («*The shortcomings of the risk-based approach – lack of transparency and accountability – are important in the light of the finding that the Third Directive has a theatrical function in reassuring citizens and financial markets but is not well suited to combating terrorism financing. In fact, detecting terrorism financing through the monitoring of clients and transactions is very complicated. The cost of terrorist acts is relatively low and decreasing, the financing of an attack does not necessarily require atypical financial behaviour and the occurrence of terrorist acts is too rare and similarities between the methods of financing are too low to establish meaningful scenarios.*»); auf ähnliche Probleme hinweisend bereits Siegel, *Die Volkswirtschaft* 11/2005, 28.

²²⁶² Vgl. BAS, *Comments on FATF Guidance*, 2.

g. Mögliche Handlungsalternativen

Alternativen zum heutigen Geldwäschereiregime sollten den technischen Besonderheiten dezentraler Systeme konsequent Rechnung tragen.²²⁶³

Einerseits darf nicht vergessen werden, dass dezentrale Netzwerke aufgrund ihres öffentlichen Registers die analytische Nachverfolgbarkeit von Finanzströmen für Strafverfolgungsbehörden deutlich vereinfacht.²²⁶⁴ Die Vorteilen werden von Behördenvertretern regelmässig bestätigt.²²⁶⁵ In eine ähnliche Richtung gehen die Vorschläge, dass staatliche Behörden selbst als (Full) Nodes an dezentralen Netzwerken teilnehmen und dadurch direkten Zugriff auf alle Daten des verteilten Registers erhalten.²²⁶⁶ In diesem Fall wären Aufsichtsbehörden weniger stark auf die heute datenverifizierenden und -vermittelnden Rollen von Finanzintermediären angewiesen.²²⁶⁷ Die BITCOIN ASSOCIATION SWITZERLAND und die SWISS BLOCKCHAIN FEDERATION fordern unter diesen Umständen zu Recht, dass der erhöhten Transparenz und somit dem tieferen Geldwäschereirisiko von (öffentlichen) Blockchains unter dem von der FATF propagierten risikoorientierten Ansatz angemessen Rechnung zu tragen ist.²²⁶⁸ Das U.S. DEPARTMENT OF THE TREASURY erachtet die Transparenz von Blockchains ebenfalls als hilfreiche Eigenschaft im Kampf gegen Kriminalität,

²²⁶³ So auch BA, Comments on FATF Guidance, 12, die zudem darauf hinweisen, dass die Entwicklung solcher «new regulatory mechanisms that can be incorporated into decentralized finance protocols» noch mehr Zeit benötige; sodann auf die *anwendungsneutrale* Regulierung von Daten in verteilten Registern hinweisend Hofert, Regulierung der Blockchains, 61.

²²⁶⁴ Vgl. die Ausführungen in Pelker/Brown/Tucker, Department of Justice Journal of Federal Law and Practice 2021, 100 («In sum, blockchain analysis is a powerful tool that can be effectively leveraged at practically any state of an investigation.»); ferner Morell/Kirshner/Schoenberger, Bitcoin's Use in Illicit Finance, 5–8; so auch Iffland/Läser, GesKR 2018, 422.

²²⁶⁵ Interessant sind etwa die Ausführungen in Shin, How DOJ Strike Force Hunts Down Cryptocurrency Criminals, Unchained Podcast, *passim*.

²²⁶⁶ Die Rede ist von einem sog. *Regulatory Node*, der sodann einen Teil von sog. *Embedded Supervision* bilden könnte; vgl. zum Regulatory Node IOSCO, Fintech Report, 64; ausführlich zu Embedded Supervision Auer, BIS Working Papers Nr. 811, Mai 2022, 3–5, wonach die Datenglaubwürdigkeit durch ökonomische Anreize sichergestellt würde; in Bezug auf *Embedded Regulation* in DeFi Zetzsche/Arner/Buckley, Journal of Financial Regulation 2020, 201–202, ferner in Bezug auf die Rolle des Regulatory Nodes 200; hinsichtlich Embedded Supervision über Stablecoins sodann Arner/Auer/Frost, BIS Working Papers Nr. 905, November 2020, 17–18.

²²⁶⁷ So Auer, BIS Working Papers Nr. 811, Mai 2022, 3.

²²⁶⁸ Siehe BAS, Comments on FATF Guidance, 5; SBF, Comments on FATF Guidance, 4; ferner auch Lipton/Cohen, International Financial Law Review 2021, *passim*.

wenn wirksame Transaction Screening Tools vorhanden sind.²²⁶⁹ Eine Möglichkeit, die bereits von gewissen DeFi-Frontends implementiert wird, ist die *Know Your Transaction* (KYT)-Methode, welche vergangene Wallet-Transaktionen vor dem Versand prüft, ohne konkret die Identität der Nutzer erfassen zu müssen.²²⁷⁰ Andererseits bestehen etwa *technische Lösungen*, die sich über die verwendeten Smart Contracts bzw. Token implementieren oder in Kryptowährungsprotokolle integrieren lassen. Hierzu gehören namentlich Access Control-Funktionen; die Rede ist auch von Permissioned Tokens oder Permissioned Pools.²²⁷¹

Schliesslich sind an dieser Stelle auch ZKP-basierte Systeme zu erwähnen, die neben der Notwendigkeit der Compliance auch das Recht auf Privatsphäre zu einem Kernanliegen machen. So ist es einem Nutzer einer Privacy-Enhancing-Technologie, wie z.B. Tornado Cash oder Zcash, bei Bedarf möglich, bloss ausgewählten Drittpersonen, wie etwa einem Finanzintermediär oder einer Behörde, den Nachweis einer einwandfreien Transaktionshistorie zu erbringen (Source of Funds).²²⁷² Um die Privatsphäre des Nutzers umfassender zu bewahren, könnte dieser an einem sog. Privacy Pool teilnehmen, der dem Nutzer gegenüber Dritten den ZKP ermöglicht, dass seine Vermögenswerte eine Verbindung zu einem Pool von unproblematischen Vermögenswerten oder aber dass sie keine Verbindung zu einem Pool von inkriminierten Vermögenswerten aufweisen, ohne jedoch der Drittperson die ganze Transaktionshistorie offenlegen zu müssen.²²⁷³

Die praktische Bedeutung solcher Alternativen hat sich bspw. im Falle des KuCoin-Hacks gezeigt, bei welchem, soweit ersichtlich, erstmals dezentrale Handelsplattformen als «Mixer» eingesetzt wurden.²²⁷⁴ Die Nachverfolgbarkeit der Austauschgeschäfte war ohne Weiteres gewährleistet und einige der betroffenen DeFi-Projekte konnten die gestohlenen Vermögenswerte blockieren, um sie später zurück an KuCoin bzw. deren Kunden zu übertragen.²²⁷⁵ Im Falle des

²²⁶⁹ Siehe U.S. Department of the Treasury, *Illicit Finance Risk*, 32–34.

²²⁷⁰ Siehe Hess, *Penn State Law Review* 2024, 55.

²²⁷¹ Siehe etwa zu Whitelisting- und Blacklisting-Funktionen oben, [IV.5.2d.ii.](#)

²²⁷² Siehe Nadler/Schär, *Federal Reserve Bank of St. Louis Review* 2023, 132–133.

²²⁷³ Siehe etwa Buterin et al., *Blockchain Privacy and Regulatory Compliance*, 1, 4; ferner zu ähnlichen Konzepten im Bereich des KYC von Kunden Boškić/Hepp, *GesKR* 2023, 217–218.

²²⁷⁴ Siehe zum Mixing-Konzept oben, [IV.5.2c.ii.](#)

²²⁷⁵ Siehe Robinson, *KuCoin and Elliptic*, *passim* («Unlike centralized exchanges, which are dead-ends when it comes to tracing the flow of funds, with DEXs everything is recorded and visible on the blockchain. Elliptic's blockchain monitoring solutions are able to trace the funds from the hack, and through DEXs. This means that Elliptic's customers are alerted if an incoming transaction has originated from the KuCoin hack, via a DEX.»)

Privacy Coins Zcash unterstützt etwa die regulierte US-amerikanische Kryptohandelsplattform Gemini Shielded Transactions, d.h. Transaktionen, deren Informationen zu den Absender- und Empfängeradressen sowie zum Betrag nicht aus dem verteilten Register ablesbar sind.²²⁷⁶ Die Plattform kann dies tun, weil sie auf die technische Möglichkeit von View Keys zurückgreifen kann, die eine selektive Publikation der Informationen erlauben.²²⁷⁷ Nicht vorzugswürdig, aber grundsätzlich technisch möglich, wäre die Etablierung geschlossener Pools in AMMs oder anderen dezentralen Handelsplattformen. Lediglich die Teilnehmer einer bestimmten Whitelist könnten somit Liquidität einbringen und diese handeln.²²⁷⁸ Dies würde offensichtlich die Dezentralität einer solchen Applikation verringern.

Technische Lösungsansätze können mit anderen Worten durchaus für Compliance mit einer neuen, technologisch adjustierten Novelle des GwG innerhalb dezentraler Systeme sorgen.²²⁷⁹

Zu erwähnen ist, dass auch die FATF technologische Lösungen für die Geldwäschereiprävention nicht *a priori* ausschließt. In ihrem Bericht von 2015 erwähnt sie explizit etwa die Verwendung von APIs, über welche Kundeninformationen ausgetauscht werden können oder der Entwicklung von eigenständigen Protokollen virtueller Währungen, welche KYC-Funktionalitäten in den Code integrieren.²²⁸⁰ Die Idee dahinter ist, dass künftig die Einhaltung der regulatorischen Vorgaben über Softwarelösungen erfolgen soll, die im Wesentlichen als Bestandteil eines DeFi-Protokolls implementiert werden.²²⁸¹ Der

²²⁷⁶ Siehe Winer, First Licensed Zcash Exchange, *passim*; ferner Team Gemini, Financial Freedom With Shielded ZEC Withdrawals, *passim*; vgl. hierzu CVA CWG, Privacy Techniques for Blockchains, 12–13.

²²⁷⁷ In Zcash können Nutzer und Finanzintermediäre die Verwendung von sog. View Keys vertraglich vereinbaren, siehe hierzu oben, [IV.5.2c.ii](#).

²²⁷⁸ Vgl. hinsichtlich der Verwendung von Permissioned Pools in einem Lending-Protokoll Aave, Arc, 3; ferner Aave, Introducing Aave Arc, *passim*.

²²⁷⁹ So auch Warren, Decentralized Exchange, *passim* m.w.H.; ausführlich hierzu Warren Compliant peer-to-peer trading, *passim*, wo der Autor eine Reihe möglicher technischer Lösungen insb. im Bereich von *Permissioned Tokens* präsentiert; ferner Ox, Extending the Ox protocol, *passim*; sodann di Angelo/Salzer, in: Xu et al., Tokens, 3; Altschuler, Stanford Journal of Blockchain Law & Policy 2022, 95, 105–111; in Bezug auf die heute praktisch unmögliche Compliance bei Herausgabe von Stablecoins Hess, AJP 2023, 946–947.

²²⁸⁰ Siehe FATF, VASP Guidance 2015, 14; ausführlich sodann FATF, New Technologies for AML/CFT, 26–35, 51–52.

²²⁸¹ Siehe etwa Reyes, Villanova Law Review 2016, 195–196, 227–231; vgl. ferner Poskriakov/Chiriaeve/Cavin, Cryptocurrency compliance and risks, *passim*

Bundesrat sieht Blockchain-Technologie zumindest als potenzielle RegTech-Lösung für den Austausch von Kundendossiers zwischen Finanzintermediären vor.²²⁸²

h. Datenschutz und Privatsphäre

Bei solchen technologischen Lösungen handelt es sich aber um ein zweischneidiges Schwert. Namentlich sind die Datenschutzinteressen der betroffenen Personen gegen das öffentliche Strafverfolgungsinteresse abzuwägen, das nach vorliegender Auffassung aus rechtsstaatlichen Gründen zugunsten der Privatsphäre der Nutzer entschieden werden sollte.²²⁸³

In diesem Zusammenhang bietet sich insb. der Einsatz dezentraler Identitätssysteme an, die den Nutzern einen hohen Grad an Persönlichkeits- und Datenschutz sowie Datensicherheit gewährleisten, indem der Nutzer seine digitale Identität(en) selbständig mithilfe eines Self-Hosted Wallets verwalten kann. Bei entsprechenden Verdachtsmomenten und der Einhaltung der strafprozessualen Voraussetzungen würde ein solcher Ansatz immer noch eine wirkungsvolle Strafverfolgung von Geldwäscherei und insb. der Vortaten zulassen. Die Herangehensweise wäre unter Gesichtspunkten verfassungsmässiger Rechte und Prinzipien geradezu geboten.²²⁸⁴ Auf das schwierige Verhältnis zwischen Datenschutz und Schutz der Privatsphäre einerseits und den umfassenden Datensammlungs- und Meldesystemen im Bereich der Geldwäschereiregulierung andererseits weist der Europäische Datenschutzausschuss (ESDA) bzw. die Vorgängerorganisation seit mindestens 2011 hin.²²⁸⁵ Der poli-

²²⁸² Siehe Bundesrat, RegTech, 9.

²²⁸³ So auch Kaiser, Privacy and Identity Issues in Financial Transactions, 582 («Anonymity is only one way in which such a strengthened protection may be offered, but it is a potent one, particularly in an online context.»).

²²⁸⁴ Siehe etwa Coin Center, Comments on FATF Guidance, insb. 9–11 («An 'expansive' approach to these highly consequential definitions is not compatible with the rule of law and individual rights in a free society.»), 30–31; ausführlich sodann Kaiser, Privacy and Identity Issues in Financial Transactions, 579 («[...] the terms of the [4th Anti-Money Laundering Directive 2015/849] utterly fail to design the anti-money laundering measures in a way which is compatible with the human rights of the customers. [...] the Directive does not respect the principle of proportionality, and is therefore incompatible with the rights to privacy and data protection.»), 581 («[...] the [anti-money laundering] measures do not allow for anonymous use of financial services, to the detriment of meaningful protection of customer privacy. Every member of society must have access to financial services, but under the framework currently in place, one must give up one's privacy in order to make use of these services.»).

²²⁸⁵ Siehe etwa Working Party, Data protection issues related to the prevention of money laundering and terrorist financing, 3–4; ferner EDPB, Letter on the protection of personal data,

tische Ton hat sich allerdings seit der Präsentation des FinTech-Aktionsplans im März 2018²²⁸⁶ sowie des Geldwäscherei-Aktionsplans im Mai 2020²²⁸⁷ durch die Europäischen Kommission deutlich verschärft:

*«If the AML-CFT legislation is not designed in a balanced and proportionate manner, that respects every individuals' fundamental rights to data protection, legal uncertainties for obliged entities will continue to exist and the AML-CFT framework would be vulnerable. Data Protection Authorities will be forced to use their powers in order to bring the activities of the obliged entities in accordance with the GDPR through corrective measures.»*²²⁸⁸

Die unmissverständlichen Aussagen²²⁸⁹ der FATF u.a. in Sachen Privacy Coins, Mixing Services und P2P-Transaktionen zwischen Self-Hosted Wallets lassen in dieser Hinsicht ebenfalls wenig Hoffnung aufkommen.²²⁹⁰ Die Vorstellung, dass ein Verbot oder die faktische Einschränkung solcher Anwendungen und von Self-Hosted Wallets Kriminelle tatsächlich daran hindern wird, Vermögenswerte zu waschen, ist überwiegend illusorisch und zeugt von einer sehr einseitigen und zudem innovations- und menschenrechtsfeindlichen Sichtweise der Pariser Behörde.²²⁹¹

Es besteht zudem wenig Einsicht, dass in einer er des um sich greifenden Digitalisierung des Ichs ein echtes Bedürfnis für den Schutz persönlicher Daten besteht. Die FATF hat in Bezug auf ein im Februar 2021 angelaufenes Projekt verlauten lassen, dass sie die unbeabsichtigten Folgen der Anwendung der

2 («[...] a fair balance has to be struck between the interest to prevent money laundering and terrorist financing, on the one hand, and the interests underlying the fundamental rights to data protection and privacy, on the other.»).

²²⁸⁶ Vgl. EC, FinTech Action plan, 2–4, 10, 16.

²²⁸⁷ Vgl. EC, Action Plan on preventing money laundering and terrorist financing, C164/25–C164/26.

²²⁸⁸ EDPB, Letter on the protection of personal data, 7.

²²⁸⁹ Vgl. etwa FATF, Draft VASP Guidance 2021, 14–16 («The ML/TF risks are more difficult to address and mitigate once the products are launched, and thus should be addressed in the design or development phase.»), 37 («Countries may consider the following non-exhaustive list of options to mitigate risks posed by P2P transactions at a national level if the ML/TF risks are unacceptably high. This includes measures that seek to bring greater visibility to P2P transactions, as well as to limit jurisdiction's exposure to P2P transactions. [...]»); ferner FATF, VASP Guidance 2021, 38–39, 45, 46.

²²⁹⁰ Siehe auch Van Valkenburgh, FinCEN's new cryptocurrency guidance, *passim*; ferner betreffend die Frage, inwieweit Softwareentwickler dazu verpflichtet werden können, Überwachungselemente bereits in einer Software zu implementieren, Coin Center, Comments on FATF Guidance, 18, 20.

²²⁹¹ Ausführlich mit Beispielen Coin Center, Comments on FATF Guidance, 27, 29–33; ferner BA, Comments on FATF Guidance, 4–5.

FATF Standards prüfen will. Darunter fallen neben Fragen des faktischen Ausschlusses legitimer Geschäftsbeziehungen aus dem Finanzsystem v.a. grundrechtliche Themen im prozeduralen Bereich.²²⁹² Allerdings erachtet die FATF die unbeabsichtigten Auswirkungen ihrer Standards lediglich als Folge einer fehlerhaften Implementierung und nicht etwa eines allfälligen *eigenen* Versagens. Es ist wohl absehbar, dass die «regulatorischen Reisen» in der Schweiz und der EU in die von der FATF vorgegebenen Richtung gehen werden. Die in der Schweiz bloss mittels einer FINMA-Aufsichtsmitteilung²²⁹³ auf Kryptotransaktionen ausgeweitete Travel Rule sowie die ursprünglich diskutierten Vorschläge in der EU sind Ausdruck dieser Haltung.²²⁹⁴

i. Risiko der Bifurkation des Finanzsystems

Die Absicht scheint darin zu bestehen, dass nicht nur die Schnittstelle zwischen traditionellem Finanzsystem und DeFi strengen Regeln unterworfen ist, sondern v.a. auch, dass die Nutzung von Kryptovermögenswerten *ausserhalb* des traditionellen Finanzintermediationssystems möglichst unattraktiv wird.²²⁹⁵

P2P-Transaktionen mit Kryptovermögenswerten sollen mit anderen Worten regulatorisch in den bestehenden Finanzintermediationsrahmen gequetscht werden. Eine solche Tendenz kann etwa daran festgestellt werden, dass zentrale Handelsplattformen damit begonnen haben, Nutzer zurückzuweisen, welche Mixing-Wallets für ihre Kryptowährungen verwenden.²²⁹⁶ Der bereits im heutigen Geldwäschereiregime verfolgte Ansatz, einen *Walled Garden* zu bauen, würde dadurch auch auf DeFi ausgedehnt. Die Erschwerung der Interaktion und somit von Geldflüssen zwischen dem traditionellen Finanzsystem und DeFi könnte allerdings gerade dazu führen, dass Kriminelle sich praktisch frei in einem staatlich unbeaufsichtigtem Bereich bewegen können.²²⁹⁷ Die Bifurkation der heutigen Finanzwelt in einen regulierten und unregulierten Teil wäre die wahrscheinliche Folge.

²²⁹² Siehe FATF, *Unintended Consequences*, 2–4, 5–6.

²²⁹³ Ebenfalls *kritisch* zu dieser Mitteilungsform aus rechtsstaatlicher Warte Kunz, Jusletter vom 7. Mai 2018, Rz. 11, 13, 86–88, 133, 151, 153.

²²⁹⁴ Vgl. EC, COM(2021) 420 final, *passim*; ferner bereits Mersch, *Virtual currencies ante portas*, *passim*.

²²⁹⁵ Vgl. auch Morris, *Europe's Hidden Agenda on Crypto Wallets*, *Coindesk*, *passim*.

²²⁹⁶ Siehe Nelson, *Binance Blockade of Wasabi Wallet*, *Coindesk*, *passim*.

²²⁹⁷ Siehe hierzu BA, *Comments on FATF Guidance*, 5.

3. Finanzmarktinfrastrukturrecht

3.1 Einleitung

Das FinfraG regelt die Organisation und den Betrieb von Finanzmarktinfrastrukturen sowie die Verhaltenspflichten der Finanzmarktteilnehmer beim Effekten- und Derivatehandel. Das Gesetz bezweckt die Gewährleistung der Funktionsfähigkeit und der Transparenz der Effekten- und Derivatemärkte, der Stabilität des Finanzsystems, des Schutzes der Finanzmarktteilnehmer sowie der Gleichbehandlung der Anleger (Art. 1 FinfraG). Hinsichtlich der bereits im alten Börsengesetz geregelten Aspekte übernimmt das FinfraG somit die Schutzzwecke von Art. 1 aBEHG. Dabei handelt es sich namentlich um die Sicherstellung der Transparenz und der Gleichbehandlung der Anleger sowie der Aufrechterhaltung der Funktionsfähigkeit der Effektenmärkte. In den übrigen Teilen des FinfraG steht primär der Schutz der Funktionsfähigkeit inkl. Systemschutz sowie der Schutz der Finanzmarktteilnehmer im Vordergrund.²²⁹⁸

3.2 Begrifflichkeiten

a. Finanzmarktinfrastruktur

Als Finanzmarktinfrastrukturen gelten gemäss Art. 2 lit. a FinfraG (i) Börsen, (ii) multilaterale Handelssysteme (MHS), (iii) zentrale Gegenparteien, (iv) Zentralverwahrer, (v) Transaktionsregister, (vi) Handelssysteme für Distributed Ledger Technology-Effekten (DLT-Handelssysteme) sowie (vii) Zahlungssysteme. Börsen und MHS firmieren sodann unter dem Oberbegriff des Handelsplatzes (Art. 26 FinfraG).

Organisierte Handelssysteme (OHS) gemäss Art. 42 FinfraG werden nicht als Finanzmarktinfrastrukturen behandelt, da sie grundsätzlich nur von Banken, Wertpapierhäusern, Börsen und MHS sowie neu DLT-Handelssystemen betrieben werden dürfen und die allgemeinen Bewilligungsvoraussetzungen und Pflichten für sie nicht gelten.²²⁹⁹

²²⁹⁸ Siehe Botschaft FinfraG 2014, 7512–7513.

²²⁹⁹ Siehe Botschaft FinfraG 2014, 7513.

b. Effekten und DLT-Effekten

Zentral für das Finanzmarktinfrastrukturrecht ist der Effektenbegriff: Als *Effekten* gelten nach Art. 2 lit. b FinfraG (sowie Art. 3 lit. b FIDLEG) vereinheitlichte und zum massenweisen Handel geeignete Wertpapiere, Wertrechte, insb. einfache Wertrechte nach Art. 973c OR und Registerwertrechte nach Art. 973d OR, sowie vereinheitlichte und zum massenweisen Handel geeignete Derivate und Bucheffekten. Vereinheitlichung und Eignung zum massenweisen Handel liegen vor, wenn Effekten in gleicher Struktur und Stückelung öffentlich angeboten oder bei mehr als 20 Kunden platziert werden, sofern sie nicht für einzelne Gegenparteien besonders geschaffen werden.²³⁰⁰ Derivate sind sodann Finanzkontrakte, deren Wert von einem oder mehreren Basiswerten abhängt und die kein Kassageschäft darstellen (Art. 2 lit. c FinfraG). Dabei handelt es sich um Finanzkontrakte, deren Preis namentlich von Vermögenswerten, wie Aktien, Obligationen, Rohstoffen und Edelmetallen, oder von Referenzwerten, wie Währungen, Zinsen und Indizes, abgeleitet wird, wobei Kassageschäfte und bestimmte Typen von Finanzkontrakten ausdrücklich vom Derivatbegriff ausgeschlossen sind.²³⁰¹ Der Begriff der Bucheffekte richtet sich nach dem Bucheffektengesetz.²³⁰² Nach der Terminologie der FINMA handelt es sich bei Token, die unter den Effektenbegriff fallen und in der Praxis in aller Regel in Form von (Register-)Wertrechten, ausnahmsweise aber auch als Derivate ausgestaltet werden, um Anlage-Token.²³⁰³ Nicht erfasst sind der Handel mit Rohstoffen, Edelmetallen und Devisen bzw. Währungen, soweit es sich um Kassageschäfte handelt, da es sich bei den gehandelten Vermögenswerten nicht um Effekten handelt.²³⁰⁴

Es ist an dieser Stelle allerdings darauf hinzuweisen, dass der sachliche Geltungsbereich gewisser Finanzmarktinfrastrukturen auch bereits an das Vorliegen von *Finanzinstrumenten* anknüpft.²³⁰⁵ Kryptowährungen bzw. (reine) Zahlungs-Token qualifizieren jedoch mangels einer Beteiligungs- oder For-

²³⁰⁰ Art. 2 Abs. 1 FinfraV.

²³⁰¹ Art. 2 Abs. 2–4 FinfraV.

²³⁰² Siehe Art. 3 BEG.

²³⁰³ Siehe FINMA, Wegleitung ICOs, 4–5; ferner Bundesrat, DLT-Bericht 2018, 100–101; ausführlich hierzu MacCabe, Anlage-Tokens, Rz. 120–124; zu Recht kritisch, da ein rechtsstaatlich fragwürdiges Abweichen vom gesetzlichen Effektenbegriff vorliegt, Mauchle, GesKR 2022, 184.

²³⁰⁴ Vgl. das inzwischen aufgehobene FINMA-RS 08/5 «Effektenhändler», Rz. 38; ferner BSK FINMAG/FinfraG-Daeniker/Waller, Art. 2 lit. b FinfraG N 13; SK FinfraG-Favre/Kramer, Art. 2 lit. b N 19.

²³⁰⁵ Siehe insb. Art. 42 FinfraG (OHS) und Art. 61 FinfraG (Zentralverwahrer).

derungskomponente nicht als Finanzinstrumente.²³⁰⁶ Dasselbe gilt zumindest dann für Nutzungs-Token, wenn sie lediglich den Zugang zu einer digitalen Dienstleistung vermitteln, welche über ein dezentrales Netzwerk zugänglich gemacht wird.²³⁰⁷

DLT-Effekten bilden sodann einen Unterfall innerhalb des Effektenbegriffs: Bei DLT-Effekten handelt es sich laut Art. 2 lit. b^{bis} FinfraG um Effekten in Form von Registerwertrechten (Art. 973d OR) oder in Form von anderen Wertrechten (z.B. nach ausländischem Recht), die in verteilten elektronischen Registern gehalten werden und die mittels technischer Verfahren den Gläubigern, nicht aber dem Schuldner, die Verfügungsmacht über das Wertrecht vermitteln.²³⁰⁸ Mit anderen Worten ist – analog zum zivilrechtlichen Registerwertrechtsbegriff –²³⁰⁹ auch für DLT-Effekten in aufsichtsrechtlicher Hinsicht begriffswesentlich, dass der Gläubiger die Verfügungsmacht über das Recht innehat. Damit DLT-Effekten den Effektenbegriff erfüllen, haben sie schliesslich einen für den Finanzmarkt anlagetypischen Charakter aufzuweisen, wie er insb. bei Aktien, Obligationen und derivativen Finanzinstrumenten vorliegt.²³¹⁰ Zur Beurteilung, ob dies der Fall ist, soll weiterhin auf die FINMA-Praxis zu Anlage-Token abgestellt werden. Reine Zahlungs- und Nutzungs-Token qualifizieren mangels Effektenqualität somit nicht als DLT-Effekten.²³¹¹ Da DLT-Effekten als Effekten gelten, stellen sie i.d.R. auch Finanzinstrumente nach Art. 3 lit. a FIDLEG dar.

²³⁰⁶ Siehe etwa Abegglen/Andreotti, GesKR 2020, 46; Luthiger/Kuhn, in: Weber/Kuhn, Aufsichtsrechtliche Rahmenbedingungen, Rz. 55; SK FIDLEG-Favre, Art. 3 lit. a und b N 15. Dies ist jedoch in aller Regel anders bei *Stablecoins*, welche von einem Emittenten herausgegeben werden; vgl. hierzu FINMA, Ergänzung Wegleitung ICOs, 2, 7.

²³⁰⁷ So wohl auch Bundesrat, DLT-Bericht 2018, 123; Luthiger/Kuhn, in: Weber/Kuhn, Aufsichtsrechtliche Rahmenbedingungen, Rz. 55; siehe ferner SK FIDLEG-Favre, Art. 3 lit. a und b N 13, wonach *Nutzungs-Token*, soweit darin Rechte abgebildet sind, die gegenüber einem Emittenten oder Dritten ausgeübt werden können, als Finanzinstrumente qualifizieren; nunmehr wie vorliegend BVGer B-4185/2020 vom 16. Januar 2024, E. 4.2.2.

²³⁰⁸ Siehe Botschaft DLT 2019, 309; weitergehend Kramer/Meier, GesKR 2020, 75.

²³⁰⁹ Art. 973d Abs. 2 Ziff. 1 OR.

²³¹⁰ Siehe Kuhn, in: Weber/Kuhn, Taxonomie, Rz. 27; Kramer/Meier, GesKR 2020, 74.

²³¹¹ Siehe Botschaft DLT 2019, 262–263, 309.

3.3 Dezentrale Handelsplattformen als DLT-Handelssysteme?

a. Vorbemerkung

Mit Blick auf dezentrale Handelsplattformen ist zu untersuchen, ob diese insb. als *DLT-Handelssysteme* gemäss Art. 73a FinfraG qualifizieren, verknüpfen sie doch ähnlich wie diese die Funktionen mehrerer Finanzmarktinfrastrukturen miteinander. Konkret handelt es sich dabei neben der Handels(abschluss)funktion, die etwa von einer Börse, eines MHS oder OHS erbracht wird, um diejenige des Clearing und Settlement. Letztere Funktionen werden in traditionellen Märkten von einem Zentralverwahrer in seiner Funktion als Effektenabwicklungssystem im Sinne von Art. 61 Abs. 3 FinfraG und von einem Zahlungssystem im Sinne von Art. 81 FinfraG übernommen. Nicht relevant ist demgegenüber vorliegend die zentrale Verwahrungsfunktionen von Zentralverwahrern im Sinne von Art. 61 Abs. 2 FinfraG, da die Nutzer dezentraler Handelsplattformen die Private Keys ihrer Vermögenswerte gerade selbst aufzubewahren haben.

b. DLT-Handelssysteme

i. Begriff und Konzept

Als DLT-Handelssystem gilt seit dem 1. August 2021 gemäss Art. 73a FinfraG eine gewerbsmässig betriebene Einrichtung zum multilateralen Handel von DLT-Effekten, die den gleichzeitigen Austausch von Angeboten unter mehreren Teilnehmern sowie den Vertragsabschluss nach nichtdiskretionären Regeln bezweckt und mindestens *eine* der folgenden Voraussetzungen erfüllt:

- a. Sie lässt Teilnehmer nach Art. 73c Abs. 1 lit. e FinfraG zu.
- b. Sie verwahrt DLT-Effekten gestützt auf einheitliche Regeln und Verfahren zentral.
- c. Sie rechnet und wickelt Geschäfte mit DLT-Effekten gestützt auf einheitliche Regeln und Verfahren ab.

Diese Voraussetzungen dienen letztlich der Abgrenzung gegenüber traditionellen Handelsplätzen.²³¹²

²³¹² Siehe Botschaft DLT 2019, 311.

Eine *erste Besonderheit* des DLT-Handelssystems ist in der Konvergenz von Handels- und Nachhandelsinfrastrukturen zu sehen. Der Bundesrat spricht von «*einheitlicher Finanzmarktinfrastruktur*».²³¹³ SONJA MAIRE und ARIE GERSZT sprechen von der Loslösung von einem Silo-basierten Verständnis der Finanzmarktinfrastrukturen hin zu einem «*holistischen Ansatz*».²³¹⁴ DLT-Handelssysteme können die heute von Handelsplätzen (multilateraler Handel), Zentralverwahren (Verwahrung, Abrechnung und Abwicklung von DLT-Effekten) und Zahlungssystemen (Abrechnung und Abwicklung von Zahlungsverpflichtungen) übernommenen Funktionen in einer einzigen Rechtseinheit vereinen. Eine Vereinigung dieser Funktionen ist hingegen keine zwingende Bedingung für den Betrieb eines DLT-Handelssystems. In der Praxis steht einem Betreiber eine Vielzahl von Kombinationsmöglichkeiten zentralerer und dezentralerer Strukturen offen.²³¹⁵

Demgegenüber ist DLT-Handelssystemen aus Risikoüberlegungen die Rolle einer zentralen Gegenpartei als Gegenpartei vorenthalten.²³¹⁶ Zudem ist dem Betreiber der Abschluss von Handelsgeschäften als Gegenpartei verboten.²³¹⁷

Eine *zweite Besonderheit* liegt in der Durchbrechung des althergebrachten Finanzintermediationsmodells, wonach lediglich regulierte und beaufsichtigte Marktteilnehmer unmittelbar Zugang zu einer Finanzmarktinfrastruktur erhalten.²³¹⁸ DLT-Handelssysteme können, müssen aber nicht, *natürliche und juristische Personen* als Teilnehmer zulassen, sofern diese erklären, in eigenem Namen und auf eigene Rechnung teilzunehmen (Art. 73c Abs. 1 lit. e FinfraG). Dies sei namentlich, so der Bundesrat, aus GwG-Gründen geboten.²³¹⁹ Solche Personen ohne Intermediärfunktion werden in Art. 58b FinfraV als «*private Teilnehmer*» bezeichnet. Das DLT-Handelssystem erlässt gemäss Art. 73c Abs. 5 FinfraG ein Reglement über die Zulassung sowie die Pflichten und den Ausschluss von Teilnehmern und beachtet dabei insb. den Grundsatz der

²³¹³ Siehe Botschaft DLT 2019, 272, 310–311.

²³¹⁴ Siehe Maire/Gerszt, in: Reutter/Werlen, DLT-Vorlage des Bundesrates, 142.

²³¹⁵ Skeptisch bezüglich der Frage, wie weit Dezentralität in der Praxis tatsächlich umgesetzt werden kann, Eggen/Sillaber, Jusletter vom 11. Mai 2020, Rz. 12, 14, 17, 32, 50; weniger skeptisch hingegen Weber, in: Weber/Kuhn, Handel mit digitalen Aktiven, Rz. 43.

²³¹⁶ Siehe Botschaft DLT 2019, 311.

²³¹⁷ Siehe Botschaft DLT 2019, 312.

²³¹⁸ Siehe Botschaft DLT 2019, 272; ferner Abegglen/Andreotti, GesKR 2020, 37 m.w.H.; vgl. demgegenüber die Kritik der SIX in EFD, Ergebnisbericht Vernehmlassung DLT 2019, 14; zurückhaltend Eggen/Sillaber, Jusletter vom 11. Mai 2020, Rz. 9, 14, 17, 50.

²³¹⁹ Siehe Botschaft DLT 2019, 312.

Gleichbehandlung.²³²⁰ Der Betreiber überwacht die Einhaltung des Reglements und ergreift bei Verstössen die vertraglich vorgesehenen Sanktionen.²³²¹

Dem DLT-Handelssystem werden sodann zum Schutz privater Teilnehmer «Informationspflichten» auferlegt, wie etwa die Bereitstellung von unter FIDLEG erstellten Prospekten und Basisinformationsblättern zu den betreffenden DLT-Effekten. Ferner haben sie private Teilnehmer über die Governance und die technischen Risiken, wie namentlich die Verlustrisiken, des verwendeten verteilten elektronischen Registers (z.B. Ethereum oder Corda) zu informieren.²³²² Diese Pflichten scheinen in diesem Umfang geboten, weil privaten Teilnehmer bei direkter Teilnahme am DLT-Handelssystem der üblicherweise vorhandene «Filter» des Wertpapierhauses fehlt. Die Vor- und Nachhandelstransparenz für DLT-Effekten und die Nachhandelstransparenz für weitere Vermögenswerte sind zudem gewährleistet.²³²³

Andererseits trifft die Teilnehmer eines DLT-Handelssystems eine Informationspflicht gemäss Art. 73c Abs. 2 FinfraG: Teilnehmer mit Sitz in der Schweiz müssen der FINMA alle Auskünfte erteilen und alle Unterlagen herausgeben, die sie zur Erfüllung ihrer Aufgaben benötigt. Das DLT-Handelssystem muss sicherstellen, dass ihm Teilnehmer mit Sitz im Ausland entsprechende Auskünfte erteilen und Unterlagen herausgeben, wenn die FINMA es anordnet. Demgegenüber sind private Teilnehmer von der Aufzeichnungs- und Meldepflicht nach Art. 38–39 FinfraG ausgenommen.²³²⁴

ii. Bemerkungen zur Technologieneutralität von Art. 73a ff. FinfraG

Nach vorliegender Ansicht handelt es sich beim neuen Bewilligungsregime entgegen der Auffassung des Bundesrates nicht um eine Abweichung vom Grundsatz der Technologieneutralität.²³²⁵ Die Absicht, technologieneutrale Regulierung erlassen zu wollen, scheint im Wesentlichen auf einer grundsätzlich falschen Annahme der Behörden zu beruhen. Denn hinter jedem Reglungsakt steckt ein impliziter Entscheid, eine Technologie einerseits recht-

²³²⁰ Vgl. ferner Art. 58e FinfraV.

²³²¹ Art. 73c Abs. 6 FinfraG.

²³²² Art. 73e Abs. 1 FinfraG i.V.m. Art. 58i Abs. 1 und 2 FinfraV.

²³²³ Art. 73b lit. c FinfraG i.V.m. Art. 58c Abs. 1 FinfraV; Art. 73e Abs. 1 FinfraG i.V.m. Art. 58i Abs. 3 FinfraV.

²³²⁴ Art. 58d Abs. 1 FinfraV.

²³²⁵ Siehe Botschaft DLT 2019, 272; EFD, Erläuternder Bericht DLT-Vernehmlassungsvorlage 2019, 25; Bundesrat, DLT-Bericht 2018, 114.

lich zu erfassen und sodann in einer gewissen Weise zu ordnen oder aber die Technologie rechtlich nicht zu erfassen.²³²⁶ Ein solcher Entscheid beinhaltet *per se* eine technologiespezifische Wertung der sie treffenden Behörde.

Die bisherige Regel in Art. 10 Abs. 1 FinfraG etwa, wonach Finanzmarktinfrastrukturen von unterschiedlichen juristischen Personen zu betreiben sind, stellte vor der Revision ein faktisches Verbot des Einsatzes von DLT- und Blockchain-Technologien für solche Aktivitäten dar. Genauso verhält es sich mit dem Ausschluss nichtunterstellter Personen vom Handel an einem Handelsplatz (siehe sogleich unten). Damit wurden jeweils gesetzgeberische Entscheide zugunsten der Finanzintermediation getroffen, die allenfalls in ihrer Wertung legitim, auf jeden Fall aber nicht technologieneutral sind.

Die Öffnung der Gesetzgebung für neue Technologien – allenfalls unter Berücksichtigung der Chancen und Risiken von Innovation –²³²⁷ trägt demgegenüber im Grundsatz einer technologieneutralen Herangehensweise von Regulierung besser Rechnung als die Beibehaltung des Status quo.²³²⁸ Auch eine verfassungsmässige Betrachtungsweise des Finanzmarktrechts, die u.a. dem Grundsatz der rechtsgleichen und wettbewerbsneutralen Behandlung der Marktteilnehmer auch «in die andere Richtung» Rechnung trägt, muss zu diesem Schluss führen.

c. Funktionale Parallelen und Unterschiede zwischen dezentralen Handelsplattformen und DLT-Handelssystemen

Handelsplätzen, Handelssystemen und Handelsplattformen, ob den Finanzmarkterlassen unterstellt oder nicht, ist grundsätzlich gemeinsam, dass sie den Austausch von Angeboten über standardisierte Vermögenswerte, wobei namentlich Preis und Menge die relevanten Verhandlungsgegenstände dar-

²³²⁶ Ähnlich mit Blick auf die faktischen Rahmenbedingungen bei Einführung des Bucheffektengesetzes Kuhn/Weber, in: Weber/Kuhn, Einleitung, Rz. 21.

²³²⁷ Siehe etwa Hettich, Kooperative Risikovorsorge, Rz. 31 («Die Bewahrung der Chancen auf Innovationen und der Chancen aus Innovationen sind aber ein wesentlicher Faktor bei der Gestaltung von Risikoregulierung. Der Einbezug dieser Chancen ist vordringlich Aufgabe des formellen Gesetzgebers.»).

²³²⁸ Dies anerkennend Bundesrat, DLT-Bericht 2018, 14 («auch heute schon nicht technologieneutral ausgestaltet»).

stellen, und dabei die Zusammenführung von Angebot und Nachfrage, d.h. den Vertragsabschluss, ermöglichen. Es besteht somit primäre eine *funktionale* Nähe zwischen unterschiedlichen Plattfortmptypen.

DLT-Handelssysteme haben sodann sehr viele Ähnlichkeiten mit *traditionellen* Finanzmarktinfrastrukturen und besonders Handelsplätzen und Zentralverwahrern. Dies wird etwa auch am Angebot der SDX hinsichtlich Kotierung, Handel, Abwicklung und Verwahrung von tokenisierten Vermögenswerten ersichtlich: Dabei erfolgen Handel, Abwicklung und Verwahrung (in Form von Bucheffekten) über die Permissioned Blockchain Corda. Gleichzeitig verfügen die beteiligten Gesellschaften weiterhin über traditionelle Bewilligungen als Börse (SDX Trading AG) und Zentralverwahrerin (SDX Digital Exchange AG).²³²⁹

Offensichtlich ist, dass DLT-Handelssysteme wie traditionelle Finanzmarktinfrastrukturen auf dem personalen und institutionellen Intermediationsmodell basieren. Hinter solchen Infrastrukturen steht mit anderen Worten ein in der Schweiz domizilierter Betreiber, der in irgendeiner Form in den Austauschprozess von DLT-Effekten involviert ist.²³³⁰ Die finanzmarktrechtlichen Anforderungen an DLT-Handelssysteme sind sodann überwiegend den Anforderungen an Handelsplätze nachgebildet, soweit letztere nicht unmittelbar oder sinngemäss auf DLT-Handelssysteme zur Anwendung gelangen.²³³¹ Sie fallen selbst für «kleine DLT-Handelssysteme» streng aus, für welche die in Art. 73f FinfraG vorgesehenen Erleichterungen gelten.²³³² Der Bundesrat will dadurch im Wesentlichen eine Gleichbehandlung mit etablierten Finanzmarktinfrastrukturen erreichen.²³³³ Aufgrund der Tatsache, dass DLT-Handelssysteme mehrere, bisher voneinander unabhängige Finanzmarktinfrastrukturen, namentlich die Funktionen eines Zentralverwahrers, zusammenführen können, ist jedoch davon auszugehen, dass die Anforderungen je nach Ausgestaltung des DLT-Handelssystems deutlich höher ausfallen als bei einem traditionellen Handelsplatz.²³³⁴

²³²⁹ Siehe FINMA, Börse und Zentralverwahrer für Handel mit Token, *passim*; ferner hierzu m.w.H. Morscher/Staub, in: Gericke, Tokenisierung von Effekten, 219–220.

²³³⁰ Vgl. etwa Weber, SZW 2021, 453; ferner Eggen/Sillaber, Jusletter vom 11. Mai 2020, Rz. 19.

²³³¹ Siehe EFD, Erläuterungen Verordnung DLT 2021, 11, 25.

²³³² So etwa SBF, Circular 2020/01, 7; Weber, in: Weber/Kuhn, Handel mit digitalen Aktiven, Rz. 101, der darum von der «Notwendigkeit» spricht, alternative Handelsplätze unterhalb der vom FinfraG vorgegebenen Schwellen zuzulassen; Weber, SZW 2021, 453, 460.

²³³³ Siehe Botschaft DLT 2019, 316.

²³³⁴ Vgl. betreffend den *zusätzlichen* Anforderungen an die zentrale Verwahrung, Abrechnung und Abwicklung von DLT-Effekten Art. 73e Abs. 2 FinfraG.

Ferner weisen DLT-Handelssysteme auch gewisse Parallelen zu *dezentralen* Handelsplattformen auf. Nach Art. 58g Abs. 1 FinfraV können DLT-Effekten vom DLT-Handelssystem zugelassen werden, wenn das «verteilte elektronische Register» mindestens die Anforderungen nach Artikel 973d Abs. 2 OR erfüllt.²³³⁵ Namentlich können DLT-Handelssysteme neben eigenen und proprietären Systemen, wie etwa eine private bzw. permissioned Blockchain, welches von bestimmbar Personen betrieben wird,²³³⁶ auch öffentliche Blockchains als verteiltes elektronisches Register nutzen. Dafür bieten sich etwa die Blockchains von Bitcoin oder Ethereum an. In diesem Fall ist der Betreiber des DLT-Handelssystems nicht auch der (System-)Betreiber des verteilten elektronischen Registers.²³³⁷ Ein solcher existiert bei dezentralen Netzwerken gerade nicht. HARALD BÄRTSCHI geht davon aus, dass die Bestimmungen zum DLT-Handelssystem auf Strukturen ausgerichtet sind, wie sie bei private und permissioned Blockchains vorkommen.²³³⁸ Tatsächlich ist für die Praxis davon auszugehen, dass ein Auseinanderfallen von Kontrolle und Verantwortlichkeit mit allzu hohen operationellen Risiken für den Betreiber verbunden sein dürfte.²³³⁹

Ein DLT-Handelssystem, das für gewisse Funktionen dennoch an eine *öffentliche* Blockchain anknüpft, würde wohl in erster Linie eine Benutzeroberfläche mit Handelsfunktionalitäten, allenfalls ein Orderbuch und einen Matching-Algorithmus sowie ein System zur Verarbeitung von Marktdaten betreiben. Handelsgeschäfte in DLT-Effekten würden demgegenüber – z.B. unter Zuhilfenahme eines Smart Contracts – ausschliesslich über das mit dem Handelssystem verbundene dezentrale Netzwerk abgewickelt werden. *Hybride Systeme*, die proprietäre und öffentliche Komponenten miteinander verknüpfen, lassen sich somit unter dem neuen Bewilligungsregime umsetzen.²³⁴⁰ *Hybride*

²³³⁵ Zu den Anforderungen an solche Wertrechtregister siehe unten, [V.3.6b](#).

²³³⁶ Vgl. für das *Project Helvetia* u.a. der SNB, das auf der privaten permissioned DLT-Plattform Corda läuft, BIS/SIX/SNB, *Project Helvetia*, 23, 37.

²³³⁷ Vgl. die Ausführungen in EFD, Erläuterungen Verordnung DLT 2021, 26, 30–31, 33; hinsichtlich der in diesem Fall anwendbaren *Prüfungspflicht* des Betreibers eines DLT-Handelssystems Art. 73d Abs. 3 FinfraG i.V.m. Art. 58g Abs. 2 FinfraV; ferner hinsichtlich der *Segregierung* der zugelassenen DLT-Effekten Art. 58j Abs. 2 FinfraV; siehe auch die Ausführungen in FINMA, *Wegleitung für Gesuche betreffend Bewilligung als DLT-Handelssystem*, 6.

²³³⁸ Siehe Bärtschi, in: Jung/Krauskopf/Cramer, *Digitaler Wandel*, 9; ebenso Weber, SZW 2021, 456.

²³³⁹ Ähnlich Weber, Jusletter vom 13. Juni 2022, Rz. 28–30.

²³⁴⁰ GLM. Kramer/Oser/Meier, Jusletter vom 6. Mai 2019, Rz. 110, wonach etwa das Orderbuch zentral geführt werden könne; ebenso Eggen/Sillaber, Jusletter vom 11. Mai 2020, Rz. 19; ferner auch Weber, SZW 2021, 454; sodann in Bezug auf ein zentralisiertes Matching von Kundenaufträgen OFK FinfraG/BEG-Vogel/Heiz/Luthiger, Art. 26 FinfraG N 12; MME,

Handelsplattformen, wie etwa das in der vorliegenden Arbeit untersuchte Angebot von IDEX,²³⁴¹ in denen das Orderbuch zentral geführt sowie im Rahmen der Ausführung von Handelsaufträgen insb. das Matching zentral oder semi-dezentral erfolgen, könnten demnach als DLT-Handelssysteme qualifizieren.

Im Gegensatz zu dezentralen Handelsplattformen steht es einem DLT-Handelssystem offen, neben dem Handel, der Abrechnung und Abwicklung von Geschäften über DLT-Effekten diese für die Teilnehmer *zentral* zu verwahren und für sie unverzinsliche Abwicklungskonten in Buchgeld oder Kryptowährungen zu führen.²³⁴² Nutzer von dezentralen Handelsplattformen verwalten und verwahren ihre Kryptovermögenswerte demgegenüber typischerweise in einem Self-Hosted Wallet und greifen direkt über diese auf die dezentralen Applikationen zu.

Das Bewilligungskleid des DLT-Handelssystems steht demgegenüber Handelssystemen, an denen keine DLT-Effekten gehandelt werden, nicht offen.²³⁴³ Anders formuliert bedürfen solche Systeme keiner Bewilligung nach Art. 73a ff. FinfraG. Es ist jedoch nicht ausgeschlossen, dass an DLT-Handelssystemen im Sinne von Nebendienstleistungen zusätzlich zu DLT-Effekten auch Nichteffekten gehandelt werden können (z.B. Kryptowährungen bzw. Zahlungs-Token und Nutzungs-Token gemäss Praxis der FINMA).²³⁴⁴ Daraus folgt, dass Plattformen, über welche Token, die nicht als Finanzinstrumente qualifizieren, gehandelt werden können, generell nicht dem FinfraG unterstellt sind.

Die nachfolgenden Ausführungen gehen vertieft auf die rechtlichen Unterschiede zwischen dezentrale Handelsplattformen und DLT-Handelssystemen ein:

Stellungnahme, 27, wo unterschiedliche zentralisierte Funktionen abgegrenzt werden; Weber, in: Arpagaus/Stadler/Werlen, Ausgabe von und Handel mit digitalen Wertrechten, Rz. 2462 («extensive Auslegung»); Weber, DLT-Handelsplattformen, 109–110.

²³⁴¹ Siehe oben, [IV.3.11](#).

²³⁴² Siehe zu letzterem Punkt Kramer/Oser/Meier, Jusletter vom 6. Mai 2019, Rz. 111; ebenso Weber, SZW 2021, 454; sodann nunmehr zur Ausnahme vom Einlagebegriff für Abwicklungskonti in *Fiatwährung* Art. 5 Abs. 3 lit. c Ziff. 2 BankV; sodann für Abwicklungskonti in *kryptobasierten Vermögenswerten bzw. Kryptowährungen* Art. 5a Abs. 2 lit. a Ziff. 2 BankV; vgl. hierzu EFD, Erläuterungen Verordnung DLT 2021, 17–18.

²³⁴³ Siehe Botschaft DLT 2019, 311.

²³⁴⁴ Art. 73d Abs. 2 FinfraG i.V.m. Art. 58f FinfraV.

d. Abgrenzung zu DLT-Handelssystemen

i. Kein Handelssystem

Dezentrale Handelsplattformen können potenziell derart konzipiert sein, dass sie in rechtlicher Hinsicht nicht einmal ein Handelssystem im Sinne des FinfraG darstellen. Der Begriff taucht im Gesetz an mehreren Orten auf, wird aber nicht definiert.

Die FINMA stellt – mit Blick auf die Einordnung von Systemen als OHS – grundsätzlich darauf ab, ob ein einheitliches Regelwerk vorliegt und der *Vertragschluss* innerhalb des Regelwerks erfolgt. Demgegenüber kommt es für das Vorliegen eines Handelssystems nicht darauf an, ob der Vertrag innerhalb oder ausserhalb des Regelwerks *abgewickelt* wird.²³⁴⁵ Wenn ein Angebot gestellt wird und der Vertrag durch Annahme des Angebotes *innerhalb des Regelwerks* zustande kommen kann, liegt nach Auffassung der FINMA ein Handelssystem vor.²³⁴⁶ Während das Vorliegen eines technischen Systems ein Anhaltspunkt für das Vorliegen eines Handelssystems ist, genügt bereits das Bestehen eines Regelwerks im vorliegend verstandenen Sinne.²³⁴⁷ Systeme, deren Handelstätigkeit nicht auf der Grundlage eines besonderen Regelwerks beruhen, wie etwa der Telefonhandel, das E-Banking oder der Handel über Chat-Kanäle, qualifizieren jedoch nicht als Handelssystem.²³⁴⁸

Systeme, welche z.B. die Kauf- und Verkaufsinteressen von Marktteilnehmern lediglich *bekanntmachen* (sog. Bulletin Boards), sind nach dem Gesagten keine Handelssysteme.²³⁴⁹ Bulletin Boards dienen demgegenüber Marktteilnehmern als Preis- bzw. Kursinformationssysteme.²³⁵⁰ Die Marktteilnehmer haben in diesem Fall sodann individuell die Vertragsbedingungen auszuhandeln und den Vertrag manuell abzuschliessen. Dies kann etwa per E-Mail oder über andere Kommunikationskanäle erfolgen.²³⁵¹ Das Matching erfolgt mit anderen Worten durch die Parteien selbst, und zwar ausserhalb eines einheitlichen

²³⁴⁵ Siehe FINMA-RS 18/1 «Organisierte Handelssysteme», Rz. 7–9.

²³⁴⁶ Siehe FINMA-RS 18/1 «Organisierte Handelssysteme», Rz. 11.

²³⁴⁷ Siehe FINMA-RS 18/1 «Organisierte Handelssysteme», Rz. 8; vgl. auch SK FinfraG-Favre/Kramer, Art. 42 N 19.

²³⁴⁸ Siehe FINMA, Anhörungsbericht Rundschreiben 2018/1, 8.

²³⁴⁹ Vgl. FINMA-RS 18/1 «Organisierte Handelssysteme», Rz. 10.

²³⁵⁰ Siehe zum Begriff Bühler, OTC-Handel mit nichtkotierten Aktien, N 299, der sodann zwischen aktiven und passiven Bulletin Boards unterscheidet.

²³⁵¹ Vgl. hinsichtlich *manueller* Eingaben BSK FINMAG/FinfraG-Studer/Vollenweider, Art. 42 FinfraG N 12 a.E.

Regelwerks. Schliesslich findet die Abwicklung entweder direkt zwischen den Parteien statt oder über eine Drittplattform, welche nicht mit derjenigen identisch ist, welche das Bulletin Board betreibt.

Dezentrale Handelsplattformen, wie etwa Bisq, funktionieren im Wesentlichen nach dieser Logik. Die Nutzungsbedingungen der Software solcher Plattformen, soweit solche überhaupt existieren und ihnen verbindliche Rechtswirkung zukommt, stellen sodann regelmässig kein ausreichendes Regelwerk eines Handelssystems dar.²³⁵² Die Handelsaktivitäten auf einer solchen Plattform erscheinen demgegenüber vielmehr *ad hoc* bzw. spontan ausgeführt.²³⁵³ Grundsätzlich gleich verhält es sich mit webbasierten Benutzeroberflächen (z.B. <https://app.uniswap.org/>), die über eine entsprechende API lediglich an Smart Contracts anknüpfen. Auch solche Webseiten, welche den Marktteilnehmern Handelsinformationen, wie namentlich Preise, zur Verfügung stellen, üben nach vorliegender Ansicht i.d.R. die Funktion eines Bulletin Boards aus.

Ebenfalls nicht als Handelssysteme qualifizieren nach Auffassung der FINMA Einrichtungen, die lediglich potentielle Kauf- und Verkaufsinteressen bündeln und durch das System an den Ausführungsort weiterleiten.²³⁵⁴ Smart Contract-basierte Aggregatoren, welche die Nutzeraufträge über ihre Benutzeroberfläche erfassen und sodann über Smart Contracts zur Ausführung an dezentrale Handelsplattformen weiterleiten, stellen darum auch keine Handelssysteme dar. Demgegenüber ist bei verteilten RFQ-Systemen, wie etwa Ox, tendenziell vom Vorliegen eines Handelssystems auszugehen. Obschon der Nutzer die vom Relayer im Orderbuch aufbereiteten Nutzeraufträge selbst anzunehmen hat, erfolgt der Vertragsabschluss mit der Gegenpartei innerhalb des Funktionslogik des eingesetzten Smart Contracts, was je nach Auslegung des Begriffs als das Regelwerk eines Handelssystems betrachtet werden kann.²³⁵⁵

²³⁵² Vgl. zum Begriff FINMA-RS 18/1 «Organisierte Handelssysteme», Rz. 7 («Das Regelwerk enthält die Grundsätze zur Ausführung der Nutzeraufträge, den Handelsabläufen sowie die Handelszeiten.»); so auch SK FINMAG/FinfraG-Studer/Vollenweider, Art. 42 N 16 bezüglich der allgemeinen Bedingungen eines E-Banking-Zugangs oder einer Vereinbarung über die Nutzung eines Chat-Kanals.

²³⁵³ Siehe FINMA-RS 18/1 «Organisierte Handelssysteme», Rz. 7 («Ein System, das ausschliesslich spontanen, zeitlich nicht im Voraus geplanten (*ad hoc*) Handel nach nicht im Voraus definierten Regeln vorsieht, ist von der OHS Regulierung nicht erfasst.»).

²³⁵⁴ Siehe FINMA-RS 18/1 «Organisierte Handelssysteme», Rz. 10; ferner auch SK FinfraG-Favre/Kramer, Art. 42 N 21.

²³⁵⁵ Vgl. FINMA-RS 18/1 «Organisierte Handelssysteme», Rz. 12.

ii. Kein OHS (Exkurs)

Allerdings ist der Begriff des Regelwerks nicht in der Weise zu verstehen, dass eine dezentrale Handelsplattform ein OHS im Sinne von Art. 42 FinfraG darstellen könnte. OHS verfügen über unmittelbar und klar identifizierbare Betreiber des Handelssystems. Sein Betrieb ist prudenziell regulierten und beaufsichtigten Finanzintermediären vorbehalten. Diese setzen nicht nur das Regelwerk fest, sondern gehen unter Einbezug des Regelwerks auch Verträge mit den Benutzern des OHS ein. Der Einhaltung des Regelwerks müssen sowohl Betreiber als auch Benutzer zustimmen und es muss beide verpflichten.²³⁵⁶

Nutzer von dezentralen Handelsplattformen können demgegenüber *mangels Betreibers* keine relevanten Rechtsbeziehungen mit der dezentralen Handelsplattform eingehen. Wenn überhaupt, liegt eine rechtliche Beziehung höchstens mit den Entwicklern der Software vor, wobei in den diesbezüglichen Softwarelizenzierungsbedingungen kaum der Regelungsinhalt und die Regelungstiefe von Regelwerken eines OHS gesehen werden kann. Die allfälligen Vertragsabschlüsse mit anderen Nutzern sind in diesem Zusammenhang nicht weiter relevant. Dies gilt selbst dann, wenn es sich beim betreffenden Nutzer um einen Liquiditätsgeber handelt, der den Eigenhandel oder das Market Making nach Art. 41 FINIG betreibt.²³⁵⁷ Solche Tätigkeiten sind gerade nicht von der OHS-Regulierung erfasst.²³⁵⁸

Hinsichtlich Handelsaktivitäten am OHS verfügt der Betreiber – im Gegensatz zu den Nutzern oder Entwicklern einer dezentralen Handelsplattform – sodann über genügend Kontrolle über die Abläufe, sodass der Gesetzgeber ihm ohne Weiteres eine Reihe von Pflichten auferlegen kann.²³⁵⁹

iii. Multilateraler Handel nach nichtdiskretionären Regeln

Im Falle der untersuchten dezentralen Handelsplattformen ist sodann vielfach offen, ob diese überhaupt einen multilateralen Handel und den Vertragsab-

²³⁵⁶ Siehe FINMA-RS 18/1 «Organisierte Handelssysteme», Rz. 7.

²³⁵⁷ Zur Frage des Wertpapierhandels siehe unten, [V.5.2.](#)

²³⁵⁸ Vgl. FINMA, Anhörungsbericht Rundschreiben 2018/1, 11–12; BSK FINMAG/FinfraG-Studer/Vollenweider, Art. 42 FinfraG N 30; bereits Schären/Dobrauz-Saldapenna/Liebi, SZW 2016, 198; ausführlich Humbel, GesKR 2021, 33–34.

²³⁵⁹ Vgl. Art. 44–46 FinfraG, Art. 39–43 FinfraV, FINMA-RS 18/1 «Organisierte Handelssysteme», Rz. 26–42.

schluss nach nichtdiskretionären Regeln ermöglichen. Dies wäre jedoch für das Vorliegen eines DLT-Handelssystems zwingend.

Als *multilateral* gilt der Handel, der die Interessen einer Vielzahl von Teilnehmern am Kauf und Verkauf von Effekten, DLT-Effekten oder anderen Finanzinstrumenten innerhalb des Handelssystems zu einem Vertragsabschluss zusammenführt.²³⁶⁰ Ab drei aktiven Teilnehmern wird grundsätzlich von einer Vielzahl gesprochen.²³⁶¹ Anders als im bilateralen Handel, bei welchem der Betreiber bzw. die Einrichtung ein bestimmtes Angebot nur einem bestimmten Handelsteilnehmer unterbreitet und in der Folge zur Vertragspartei wird,²³⁶² können im multilateralen Handel mehrere Handelsteilnehmer gleichzeitig auf ein bestimmtes Angebot eintreten. Der Eintritt einer zentralen Gegenpartei in die Rechtsgeschäfte zwischen Erwerber und Veräusserer ist dabei unerheblich.²³⁶³ Als *nichtdiskretionär* gelten Regeln, die dem Betreiber bei der Zusammenführung von Angeboten keinen Ermessensspielraum einräumen.²³⁶⁴ Wenn der Betreiber bzw. die Einrichtung in irgendeiner Form ein Ermessen hat, handelt es sich um diskretionäres Matching.²³⁶⁵ Anders als Handelsplätze und DLT-Handelssysteme können die Betreiber eines OHS die Aufträge von Benutzern einerseits bilateral ausführen und andererseits diskretionär zusammenführen.²³⁶⁶

Die Multilateralität des Handels ist auf dezentralen Handelsplattformen in der Regel gegeben. Mehrere Nutzer haben regelmässig gleichzeitig die Möglichkeit, die Angebote anderer Nutzer anzunehmen. Dies ist unabhängig davon, ob im Einzelfall das Orderbuch- oder AMM-Modell gilt. Bilateraler Handel ist mangels Betreibers systembedingt ausgeschlossen.²³⁶⁷ In der Praxis erfolgt

²³⁶⁰ Vgl. Art. 58a i.V.m. 22 FinfraV.

²³⁶¹ Vgl. FINMA-RS 18/1 «Organisierte Handelssysteme», Rz. 20, 23; ferner BSK FINMAG/FinfraG-Daeniker/Waller, Art. 26 FinfraG N 9 a.E.; BSK FINMAG/FinfraG-Studer/Vollenweider, Art. 42 FinfraG N 29; kritisch zu den unterschiedlichen Begriffsverständnissen der Multilateralität Bühler, OTC-Handel mit nichtkотиerten Aktien, N 519–528.

²³⁶² Noch unklar hingegen Botschaft FinfraG 2014, 7539–7540; demgegenüber FINMA-RS 18/1 «Organisierte Handelssysteme», Rz. 23; ferner BSK FINMAG/FinfraG-Daeniker/Waller, Art. 26 FinfraG N 33; SK FinfraG-Favre/Kramer, Art. 42 N 27; Schären/Dobrauz-Saldapenna/Liebi, SZW 2016, 198–199.

²³⁶³ Siehe Botschaft FinfraG 2014, 7531.

²³⁶⁴ Vgl. Art. 58a i.V.m. 23 FinfraV.

²³⁶⁵ Siehe Botschaft FinfraG 2014, 7539.

²³⁶⁶ Siehe Art. 42 lit. a und c FinfraG; ferner 43 FinfraV, FINMA-RS 18/1 «Organisierte Handelssysteme», Rz. 17, wobei dem Betreiber eines OHS in mehrfacher Hinsicht Ermessensspielraum zukommen kann.

²³⁶⁷ Im Vergleich dazu ist dem Betreiber eines DLT-Handelssystems der vertragliche Abschluss von Gegenparteigeschäften rechtlich verboten.

die Zusammenführung von Aufträgen in einem nichtdiskretionären Matching-System in aller Regel automatisiert oder zumindest ausschliesslich nach den vorbestimmten Regeln des Systems.²³⁶⁸ In dezentralen Handelsplattformen, in denen Nutzer die Aufträge manuell zusammenführen, ist darum von einem diskretionären Matching auszugehen (z.B. bei Bisq, EtherDelta und 0x). Diese Art von Diskretionarität ist untypisch, da es durch die Nutzer selbst erfolgt.²³⁶⁹ Über eine Vielzahl von dezentralen Handelsplattformen erfolgt das Matching allerdings protokollbedingt vollautomatisch und damit nichtdiskretionär (z.B. Uniswap und Serum).²³⁷⁰ Nichtdiskretionäres Matching ist damit im Orderbuchmodell regelmässig gegeben, im AMM-Modell, das auf Smart Contracts beruht, hingegen zwingend der Fall.

Im Ergebnis können dezentrale Handelsplattformen wie DLT-Handelssysteme den multilateralen Handel nach nichtdiskretionären Matching-Regeln anbieten. Allerdings passen die Bestimmungen des FinfraG nicht direkt auf die Mechanik dezentraler Handelsplattformen, gehen sie doch davon aus, dass die Frage des Matchings sich daran entscheidet, ob ein Betreiber bzw. eine Einrichtung über Ermessen verfügt oder nicht (siehe zu diesen beiden Punkten sogleich).

iv. Kein Betreiber

Der Bundesrat vertritt in seinen Publikationen ausdrücklich die Auffassung, dass ein Spektrum an Finanzmarktinfrastrukturen im Handelsbereich existiert: *«Die vorgeschlagenen Anpassungen des FinfraG fokussieren auf den vom Bundesrat identifizierten dringlichsten Handlungsbedarf im Finanzmarktinfrastrukturrecht, namentlich auf zentral und zum Teil dezentral erbrachte Finanzmarktinfrastrukturdienstleistungen mit DLT-basierten Effekten.»*²³⁷¹ Er kommt zum Schluss, dass Handelsplattformen bei genügender Dezentralisierung gerade nicht von der neuen Bewilligungskategorie erfasst sein sollen.²³⁷² Zur Be-

²³⁶⁸ Vgl. FINMA-RS 18/1 «Organisierte Handelssysteme», Rz. 16; ferner SK FinfraG-Schott/Winkler, Art. 26 N 27.

²³⁶⁹ Vgl. zu einer ähnlich gelagerten Frage des Ermessens der Benutzer im OHS-Bereich Humbel, GesKR 2021, 28–29 m.w.H.

²³⁷⁰ GLM. Bundesrat, DLT-Bericht 2018, 106–107; ferner Humbel, GesKR 2021, 39 a.E. («inhärent nichtdiskretionäre Natur»); wohl auch Jutzi/Abbühl, Fintech und DLT, Rz 536, die jedoch in Rz. 534 noch davon sprechen, dass «Nichthandelsplätze» kein Matching aufweisen können.

²³⁷¹ Siehe Botschaft DLT 2019, 273; so bereits Bundesrat, DLT-Bericht 2018, 105–106, 115–116.

²³⁷² Vgl. Botschaft DLT 2019, 273 («vollständig dezentrale ‘Finanzmarktinfrastrukturen’»); ferner Eggen/Sillaber, Jusletter vom 11. Mai 2020, Rz. 19, die davon sprechen, dass die Regulierung bei vollkommener Dezentralität «obsolet» wäre.

gründung wird angeführt, dass es in diesen Fällen an einem unmittelbaren²³⁷³ und klar identifizierbaren Betreiber fehlt.²³⁷⁴ STEFAN KRAMER und URS MEIER sprechen in diesem Fall von «Organismen».²³⁷⁵ FEDOR POSKRIAKOV setzt voraus, dass niemand für das Funktionieren der Handelsplattform verantwortlich ist. Eine solche Verantwortlichkeit liegt etwa bei der Möglichkeit der Betreiberin vor, eine relevante Kontrolle über den Inhalt des Orderbuchs (z.B. durch die Stornierung von Aufträgen) sowie über den Handelsabschluss zwischen den Nutzern und dessen Abwicklung auszuüben.²³⁷⁶ Auch die Möglichkeiten, den Zugang zur Handelsplattform einzuschränken und die Zulassung von Token zum Handel zu regeln, implizieren eine relevante Verantwortlichkeit.²³⁷⁷

Die Analyse in der Botschaft verdient der Zustimmung: Einerseits verfügen dezentrale Handelsplattformen über keine Betreiberin oder eine sonstige verantwortliche Person, welche die Plattform *unmittelbar* kontrollieren bzw. eine relevante Eingriffsmöglichkeit aufweisen könnte.²³⁷⁸ Andererseits ist die Gruppe der involvierten Personen so gross, dass eine *klare Identifikation* ihrer Identitäten oder Domizile praktisch ausgeschlossen ist.²³⁷⁹ Die Funktionslogik dezentraler Handelsplattform, wie etwa von Uniswap, wird letztlich von den unzähligen Teilnehmern des dezentralen Netzwerks (z.B. Ethereum) ausgeführt.

v. Keine Einrichtung

Eng verwandt mit der Betreibereigenschaft scheint der Begriff der *Einrichtung* zu sein, der in Art. 73a FinfraG verwendet wird. Das Gesetz bezeichnet auch andere Finanzmarktinfrastrukturen als Einrichtungen.²³⁸⁰ Der Begriff wurde ferner bereits im aBEHG verwendet, namentlich für Börsen und börsenähnli-

²³⁷³ So bereits EFD, Erläuternder Bericht DLT-Vernehmlassungsvorlage 2019, 26.

²³⁷⁴ Siehe Botschaft DLT 2019, 273; vgl. ferner aus dem Blickwinkel des Marktverhaltensrechts Remund/Wyss, GesKR 2023, 35–36.

²³⁷⁵ Kramer/Meier, GesKR 2020, 75 FN 156.

²³⁷⁶ Siehe Poskriakov, in: Richa/Canapa, *Conservation et négoce de cryptoactifs*, 120 («*implique également que personne ne soit responsable pour l'exploitation de l'organisation de négociation*»), 121; ferner FINMA, Jahresbericht 2021, 20, die von keinen «kontrollierenden Betreiber» spricht.

²³⁷⁷ Siehe SBF, Circular 2020/01, 9.

²³⁷⁸ Vgl. in diesem Zusammenhang auch BuA TVTG 2019, 101.

²³⁷⁹ So auch Kramer/Oser/Meier, Jusletter vom 6. Mai 2019, Rz. 107; ferner Kramer/Meier, GesKR 2020, 75; Luthiger/Kuhn, in: Weber/Kuhn, *Aufsichtsrechtliche Rahmenbedingungen*, Rz. 74–75.

²³⁸⁰ Vgl. u.a. Handelsplätze (Art. 26), OHS (Art. 42), zentrale Gegenpartei (Art. 48), Zentralverwahrer (Art. 61), Transaktionsregister (Art. 74), Zahlungssystem (Art. 81).

che Einrichtungen.²³⁸¹ Die Materialien zum alten Recht lassen den Schluss zu, dass mit dem Einrichtungsbegriff eine physische Präsenz und gewisse technische Infrastruktur für den Handel verbunden ist.²³⁸² In der Literatur wird sodann die Meinung vertreten, dass eine Einrichtung ein gewisses Mass an zentraler Organisation, zentraler technischer Infrastruktur oder ein Mindestmass an Infrastruktur voraussetzt.²³⁸³

Dezentrale Handelsplattform weisen demgegenüber keiner dieser Eigenschaften auf.²³⁸⁴ Ein gewisses Mass an logischer Zentralisierung kann zwar insofern vorliegen, als dass in vielen Fällen hinter einer Plattform ein Hauptentwicklungsteam samt allfälliger rechtlicher Strukturen existiert (z.B. Uniswap Labs bzw. Universal Navigation Inc. hinter Uniswap). Doch schlägt diese Form der logischen Zentralisierung nicht auf die dezentrale Handelsplattform selbst durch.²³⁸⁵ Falls demgegenüber eine Gruppe von Personen die wesentlichen Komponenten einer Plattform (d.h. Handel, Ausführung und Abwicklung) kontrollieren kann, indem bspw. der Handel über einen zentralen Server abläuft, so handelt es sich nach vorliegender Auffassung gar nicht erst um eine dezentrale Handelsplattform.²³⁸⁶

vi. Keine Gewerbsmässigkeit

Eine dezentrale Handelsplattform fällt sodann nicht in den Geltungsbereich der neuen Bestimmungen zu DLT-Handelssystemen, wenn es sich nicht um eine gewerbsmässig betriebene Einrichtung gemäss Art. 73a Abs. 1 FinfraG handelt.²³⁸⁷ Gewerbsmässigkeit liegt vor, wenn eine selbstständige, auf dauernden Erwerb ausgerichtete wirtschaftliche Tätigkeit vorliegt (Art. 73a Abs. 2 FinfraG).

²³⁸¹ Art. 2 lit. b und Art. 3 Abs. 4 aBEHG.

²³⁸² Siehe Botschaft BEHG 1993, 1386, 1396, 1398, 1399.

²³⁸³ Siehe Maire/Gerszt, in: Reutter/Werlen, DLT-Vorlage des Bundesrates, 146; Kramer/Oser/Meier, Jusletter vom 6. Mai 2019, Rz. 109 FN 160; Kramer/Meier, GesKR 2020, 76 FN 160; in Bezug auf Zahlungssysteme sodann SK FinfraG-Hess/Kalbermatter/Weiss Voigt, Art. 81 N 30, und BSK FINMAG/FinfraG-Bahar/Stupp, Art. 81 FinfraG N 2.

²³⁸⁴ Ähnlich mit Blick auf dezentrale Netzwerke Iffland/Ben Hattar, CapLaw-2020-05, *passim* («The nodes are the building blocks of the distributed ledger, but they are not an organization, and due to the decentralized logic of DLT, they cannot be deemed to be constituent parts of a broader organization.»).

²³⁸⁵ GLM. Weber, in: Weber/Kuhn, Handel mit digitalen Aktiven, Rz. 110, wobei der Autor die abweichende Terminologie des Bundesrates verwendet; ferner Jutzi/Abbühl, Fintech und DLT, Rz. 533.

²³⁸⁶ Siehe hierzu auch unten, VII.4.2a.iii.

²³⁸⁷ Siehe EFD, Erläuterungen Verordnung DLT 2021, 27.

Dezentrale Handelsplattformen können nach vorliegender Auffassung nicht als eine *gewerbsmässig* betriebene Einrichtung betrachtet werden. Dieses Argument hängt einerseits mit dem ersten zusammen, wonach keine unmittelbare und klar identifizierbare Betreibergesellschaft besteht. Der Gewerbsmässigkeitsbegriff setzt nach vorliegender Auffassung notwendigerweise eine eindeutig identifizierbare Person oder eine Gruppe von eindeutig identifizierbaren Personen voraus, welche mit dem Betrieb der Handelsplattform eine wirtschaftliche Tätigkeit verfolgen. In der Praxis erbringt allerdings eine Vielzahl von Personen verschiedene Teilkomponenten, welche zur Gesamtfunktionsweise einer dezentralen Handelsplattform beitragen: Die Entwickler eines Smart Contracts besorgen die Programmierung der Funktionalitäten der Plattform. Die Liquiditätsgeber ermöglichen den Handel von Kryptovermögenswerten über die Plattform. Die Inhaber von Governance Token beeinflussen die Weiterentwicklung der Plattform. Die dezentrale Handelsplattform selbst wird mit anderen Worten von einer Vielzahl von Personen unterhalten, die gegebenenfalls *ihrerseits* gewerbsmässig handeln.

Interessanterweise ist das DLT-Handelssystem die einzige Finanzmarktinfrastuktur, für welche gewerbsmässiges Vorgehen vorausgesetzt wird. Dieser Einschub erfolgte aufgrund der Kritik an der «Schwerfälligkeit» des neuen Bewilligungsregimes in der Vernehmlassung.²³⁸⁸ Die Gewerbsmässigkeit wird sodann in Art. 58b FinfraV konkretisiert. Ein DLT-Handelssystem übt seine Tätigkeit demnach gewerbsmässig aus, wenn es (i) damit pro Kalenderjahr einen Bruttoertrag von mehr als 50'000 Franken erzielt, (ii) pro Kalenderjahr mit mehr als 20 Teilnehmern, die als nicht regulierte und beaufsichtigte Personen qualifizieren, oder mit mindestens einem Teilnehmer nach Art. 73c Abs. 1 lit. a–d FinfraG Geschäftsbeziehungen unterhält, was wohl wie im Geldwäschereirecht eine dauernde Kundenbeziehung voraussetzt,²³⁸⁹ oder (iii) unbeschränkte Verfügungsmacht über fremde DLT-Effekten hat, die zu einem beliebigen Zeitpunkt 5 Millionen Franken überschreiten.

Die Bestimmung erinnert an die Regelung der Berufsmässigkeit in Art. 7 GwV bzw. der Gewerbsmässigkeit in Art. 19 FINIV. Während die Bestimmung ohne Zweifel die Rechtssicherheit erhöht, schränkt sie den Gewerbsmässigkeitsbegriff stark ein.

²³⁸⁸ Siehe Botschaft DLT 2019, 311 a.E.; ausführlich hierzu EFD, Ergebnisbericht Vernehmlassung DLT 2019, 13–14.

²³⁸⁹ Wohl zustimmend SBF, Circular 2020/01, 11 («A relevant ongoing business relationship is given when the operator indefinitely holds assets on behalf of a client for the purpose of trading or when there is another ongoing business relationship that concerns the trading.»).

vii. Fazit

Angesichts der klaren rechtstatsächlichen Unterschiede zwischen dezentralen Handelsplattformen und DLT-Handelssystemen im Sinne von Art. 73a ff. FinfraG kann festgehalten werden, dass dezentrale Handelsplattformen in aller Regel nicht als DLT-Handelssysteme qualifizieren.

3.4 Emittenten-betriebene Handelslösungen (Exkurs)

Eine Handelslösung basierend auf Smart Contracts kann schliesslich durch den *Emittenten* von DLT-Effekten selbst betrieben werden. Dies kann er vor dem Hintergrund tun, einen Sekundärmarkt für seine eigenen tokenisierten Aktien oder Anleihen zu schaffen.²³⁹⁰

In erster Linie kann ein Emittent eine *multilaterale* Handelslösung für Erwerber und Veräusserer seiner DLT-Effekten betreiben. Bei entsprechender Ausgestaltung fehlt es an der Gewerbsmässigkeit des Betriebs eines DLT-Handelsystems im Sinne von Art. 73a ff. FinfraG. Dies ist insb. dann der Fall, wenn der Betreiber den Nutzern keine oder nur geringfügige Handelsgebühren auferlegt und keinen übermässigen Spread vereinnahmt. Die Handelsgeschäfte werden sodann typischerweise *ad hoc*, d.h. ohne dauernde Kundenbeziehung, zwischen den Nutzern des Smart Contracts abgeschlossen. Mit Blick auf das Kriterium der unbefristeten Verfügungsmacht sollte der Betreiber des DLT-Handelsystems in den verwendeten Smart Contracts Admin Keys vermeiden, welche ihm potenziell Zugriff auf Vermögenswerte über dem Grenzwert von 5 Millionen Franken gewähren.²³⁹¹

Ferner kann der Emittent von DLT-Effekten auch eine Handelslösung betreiben, gemäss welcher er selbst Vertragspartei der Handelsgeschäfte wird. Es handelt sich dabei trotz *Bilateralität* der Handelsgeschäfte nicht um ein OHS, wenn es an einem einheitlichen Regelwerk fehlt,²³⁹² wovon bei *ad hoc*-getätigten Handelsabschlüssen der Nutzer auszugehen ist.²³⁹³ Wo der Emittent Ver-

²³⁹⁰ Vgl. zu den unterschiedlichen Formen Emittenten-betriebener Märkte SBF, Circular 2020/01, 10–11, 11–12, 16; Weber, in: Weber/Kuhn, Handel mit digitalen Aktiven, Rz. 113–114. Allerdings warnt WEBER, dass die Rechtsunsicherheit «im Moment noch recht gross» ist; siehe Weber, SZW 2021, 453.

²³⁹¹ Siehe SBF, Circular 2020/01, 11.

²³⁹² Siehe zu diesem Erfordernis oben, [V.3.3d.ii.](#)

²³⁹³ Siehe SBF, Circular 2020/01, 11, 16.

tragspartei von Handelsgeschäften ist, muss er allerdings die Voraussetzungen an die Unterstellung des Eigenhändlers und Market Makers nach FINIG beachten.²³⁹⁴

Selbstredend steht es einem Emittenten auch offen, für Käufer und Verkäufer seiner eigenen DLT-Effekten eine Matching-Plattform zu betreiben, die aufsichtsrechtlich regelmässig lediglich als Bulletin Board qualifizieren würde.

Da der Betreiber in diesen Fällen eindeutig identifizierbar ist, handelt es sich nicht um eine dezentrale Handelsplattform nach vorliegendem Verständnis.

3.5 DLT-basierte Derivate und «Privacy Coins» (Exkurs)

Der Gesetzgeber hat dem Bundesrat in Art. 73d Abs. 3 FinfraG die Möglichkeit eingeräumt, vorzusehen, dass DLT-Effekten an DLT-Handelssystemen nur zugelassen werden dürfen, wenn sie bestimmte Mindestanforderungen namentlich hinsichtlich deren Integrität und Publizität erfüllen. Damit wird in erster Linie auf die in Art. 973d Abs. 2 OR enthaltenen Mindestanforderungen an das Wertrechtregister verwiesen. Ferner kann der Bundesrat zum Schutz von Finanzmarktteilnehmern, der Stabilität oder der Integrität des Finanzsystems DLT-Effekten und weitere Vermögenswerte bezeichnen, die an DLT-Handelssystemen nicht zugelassen werden dürfen. Mit dieser Bestimmung hatte der Gesetzgeber primär als DLT-Effekten ausgestaltete Derivate sowie als Kryptowährungen bzw. Zahlungs-Token ausgestaltete Privacy Coins im Auge.²³⁹⁵

Der Bundesrat hat in Art. 58f Abs. 3 FinfraV von der Kompetenzdelegation Gebrauch gemacht. DLT-Effekten und weitere Vermögenswerte, welche die Umsetzung der Anforderungen des GwG erheblich erschweren oder die Stabilität und die Integrität des Finanzsystems beeinträchtigen könnten, dürfen nicht zum Handel an einem DLT-Handelssystem zugelassen werden. Das EFD verweist explizit auf die Ausführungen der FATF zu sog. «Anonymity-Enhanced Cryptocurrencies (AECs)» in deren Guidance vom Juni 2019.²³⁹⁶ Die FINMA kann schliesslich diese DLT-Effekten und Vermögenswerte näher umschreiben. Die Schweizer Behörden haben sich damit der grundsätzlichen Kritik der FATF an Privacy Coins angeschlossen. Die Zulassung solcher Vermögens-

²³⁹⁴ Siehe hierzu unten, [V.5.2d](#).

²³⁹⁵ Siehe Botschaft DLT 2019, 314.

²³⁹⁶ Siehe EFD, Erläuterungen Verordnung DLT 2021, 29 FN 16.

werte sei «grundsätzlich abzulehnen».²³⁹⁷ Damit soll nunmehr das Geldwäschereirecht direkt auf das Finanzmarktinfrastrekturrecht ausstrahlen, was unter Berücksichtigung der unterschiedlichen Zielsetzungen der Erlasse sowie aufgrund der Vernachlässigung von Anliegen des Daten- und Privatsphärenschutzes zu bedauern ist.²³⁹⁸

Demgegenüber sollen gemäss Art. 58f Abs. 2 FinfraV DLT-basierte Derivate zum Handel zugelassen werden können, wenn sie weder Zeitwert- noch Hebelkomponente aufweisen. Davon sollen insb. Zertifikate im Sinne von Art. 3 lit. a Ziff. 4 FIDLEG erfasst sein.²³⁹⁹

Im Gegensatz zu DLT-Handelssystemen können DLT-basierte Derivate und Privacy Coins, wie etwa Zcash und Monero, über dezentrale Handelsplattformen grundsätzlich frei gehandelt werden.

3.6 Liquiditätsgeber als Anbieter eines Wertrechtereisters (Exkurs)

a. Registerwertrechte

Seit dem 1. Februar 2021 besteht die Möglichkeit, elektronisch registrierte Rechte mit Wertpapierwirkungen, d.h. Legitimations-, Transport- und Verkehrsschutzfunktion, herauszugeben. Damit kommt ihnen wie physischen Wertpapieren – im Gegensatz zu den einfachen Wertrechten –²⁴⁰⁰ Wertpapiercharakter zu. Die so geschaffenen Rechte werden gemäss Art. 973d ff. OR als Registerwertrechte bezeichnet. Festzuhalten ist allerdings, dass Registerwertrechte entgegen der unglücklichen Bezeichnung und Legaldefinition in Art. 973d Abs. 1 OR selbst gerade

²³⁹⁷ So EFD, Erläuterungen Verordnung DLT 2021, 29; kritisch, was ein Besitz- und Handelsverbot von Privacy Coins unter österreichischem Verfassungsrecht angeht, Hospes et al., in: Schweighofer et al., Grundrechtliche Grenzen von Verboten, 574–576.

²³⁹⁸ Dies feststellend CVA RWG, CVA's answer to the DLT Ordinance, 9 («Privacy coins are not the problem as such and shall be authorized as encryption and anonymity is not the issue under AML, non-compliance is. At the opposite, anonymisation in general is a great tool to comply with data protection issues on the blockchain.»).

²³⁹⁹ Siehe EFD, Erläuterungen Verordnung DLT 2021, 29; kritisch zur Einschränkung bei Derivaten Weber, in: Weber/Kuhn, Handel mit digitalen Aktiven, Rz. 70.

²⁴⁰⁰ Siehe hierzu BSK Wertpapierrecht-Pöschel/Maizar, Art. 973c OR N 29.

nicht Rechte sind, sondern lediglich als Gefäss bzw. Kleid oder Informationsträger für solche dienen.²⁴⁰¹

Im Unterschied zu den traditionellen Wertrechten und Bucheffekten kommen Registerwertrechte grundsätzlich ohne personale und institutionelle Intermediation aus.²⁴⁰² Voraussetzung ist, dass die Rechte in einem elektronischen Register, welches bestimmten Anforderungen genügt, abgebildet werden und die Parteien, welche durch das Recht berechtigt und verpflichtet werden, dieser Registrierung zugestimmt haben.²⁴⁰³ Es braucht damit eine Art wertpapierrechtlichen Begebungsvertrag.²⁴⁰⁴ Einem solchen Begebungsvertrag ist der Abschluss einer Registrierungsvereinbarung zwischen Schuldner und Gläubiger gleichzustellen.²⁴⁰⁵ Für die Registrierungsvereinbarung ist keine bestimmte Form vorgesehen. So kann die Registrierung etwa in Ausgabebedingungen, Anleihebedingungen und Allgemeinen Geschäftsbedingungen (AGB), in einer Statutenbestimmung oder in Zeichnungsscheinen vorgesehen sein.²⁴⁰⁶ Alle Rechte, die bis anhin in Wertpapieren verbrieft werden konnten, können als Registerwertrechte ausgestaltet werden. Dies umfasst neben Anlage-Token auch Nutzungs-Token, welche zivilrechtlich häufig Forderungen gegenüber dem Emittenten darstellen, sowie Stablecoins, soweit ihnen ebenfalls eine Forderung zugrunde liegt.²⁴⁰⁷

b. Wertrechtregister

Mit der Einführung von Registerwertrechten in Art. 973d ff. OR wurde auch das Konzept des Wertrechtregisters eingeführt. In einer möglichst technologieoffenen²⁴⁰⁸ Formulierung definiert der Gesetzgeber über Abs. 2 von Art. 973d OR die Anforderungen an ein solches Register:

²⁴⁰¹ Siehe ferner Zellweger-Gutknecht/Monnerat, in: Omlor/Möslein/Grundmann, Schweizerisches Registerwertrecht, 9, die sich darum für den Begriff der *Wertregistrierung* aussprechen; ferner Eggen/Stengel, GesKR 2020, 208 («verkörpern»). Der Bundesrat spricht generell vom (qualifizierten) Kleid; siehe Botschaft DLT 2019, 275–278.

²⁴⁰² Vgl. Weber, SZW 2021, 451; Kramer/Meier, GesKR 2020, 62; Stengel, in: Reutter/Werlen, Blockchain/Distributed Ledger Technology, 147.

²⁴⁰³ Siehe Botschaft DLT 2019, 276.

²⁴⁰⁴ Siehe hierzu Meier-Hayoz/von der Crone, Wertpapierrecht, N 263, 269–270.

²⁴⁰⁵ Siehe Botschaft DLT 2019, 276.

²⁴⁰⁶ Siehe Botschaft DLT 2019, 276; Kramer/Meier, GesKR 2020, 66; SBF, Circular 2021/01, 8,11–12.

²⁴⁰⁷ Ausführlich Botschaft DLT 2019, 276–277; vgl. ferner zur zivilrechtlichen Einordnung von Stablecoins FINMA, Ergänzung Wegleitung ICOs, 2.

²⁴⁰⁸ Siehe diesbezüglich die Kritik am Vorentwurf Kuhn et al., Jusletter IT vom 23. Mai 2019, Rz. 6–13, 44; ferner Wyss, Jusletter vom 1. Juli 2019, Rz. 48.

1. Es vermittelt den Gläubigern, nicht aber dem Schuldner, mittels technischer Verfahren die Verfügungsmacht über ihre Rechte.
2. Seine Integrität ist geschützt, indem es durch angemessene technische und organisatorische Massnahmen, wie die gemeinsame Verwaltung durch mehrere voneinander unabhängige Beteiligte, gegen unbefugte Veränderungen geschützt ist.
3. Der Inhalt der Rechte, die Funktionsweise des Registers und die Registrierungsvereinbarung sind im Register oder in damit verknüpften Begleitdaten festgehalten.
4. Die Gläubiger können die sie betreffenden Informationen und Registerinträge einsehen sowie die Integrität des sie betreffenden Registerinhalts ohne Zutun Dritter überprüfen.

Der Schuldner hat sodann gemäss Art. 973d Abs. 3 OR sicherzustellen, dass das Wertrechteregister dessen Zweck entsprechend organisiert ist. Insb. ist sicherzustellen, dass das Register jederzeit gemäss Registrierungsvereinbarung funktioniert.

In Bezug auf *dezentrale Systeme* ist nach vorliegender Ansicht konzeptionell strikt zwischen dem verteilten Register (d.h. i.d.R. der Blockchain) und dem eigentlichen Wertrechteregister (d.h. den Smart Contracts oder dergleichen) zu unterscheiden.²⁴⁰⁹ Bereits nach der früheren Praxis zu den gemäss ERC-20-Standard tokenisierten Aktien in Form von (einfachen) Wertrechten nach Art. 973c OR wurde nach wohl überwiegender Auffassung im Smart Contract ein verteilt geführtes, elektronisches Wertrechtbuch gesehen.²⁴¹⁰ Diese Differenzierung ist auch darum angezeigt, weil Kryptowährungen, die in Form von nativen Token lediglich im verteilten Register eines dezentralen Netzwerks «registriert» sind, gerade nicht als Registerwertrechte erfasst sind.²⁴¹¹

²⁴⁰⁹ So auch SBF, Circular 2021/01, 4, wo zwischen «infrastructure layer» und «register layer» unterschieden wird. Vgl. ferner etwa Iffland/Läser, GesKR 2018, 420; von der Crone/Monsch/Meisser, GesKR 2019, 9; sodann bereits Hess/Lienhard, Jusletter vom 4. Dezember 2017, Rz. 3 («Die entsprechenden [Handels]prozesse laufen via Code im jeweiligen Smart Contract ab, welcher wiederum auf der Blockchain läuft.»); weniger eindeutig Botschaft DLT 2019, 274, 279–282, 289–290, wobei je nach Erläuterung von Registertechnologie, Wertrechteregister, verteiltes elektronisches Register, Register, DLT-System, System, Blockchain oder Smart Contracts die Rede ist.

²⁴¹⁰ Siehe etwa Weber/Iacangelo, Jusletter IT vom 24. Mai 2018, Rz. 29; von der Crone/Kessler/Angstmann, SJZ 2018, 342; so wohl auch von der Crone/Derungs, SZW 2019, 4–7.

²⁴¹¹ Siehe Botschaft DLT 2019, 277; kritisch Kuhn, in: Weber/Kuhn, Digitale Aktiven im schweizerischen Privatrecht, Rz. 96; ausführlich zur Unterscheidung zwischen Native und Non-Native Tokens Eggen, AJP 2018, 561–565.

Der Schuldner des im Registerwertrecht verkörperten Rechts selbst «führt» das Wertrechtereister,²⁴¹² wobei freilich die Verfügungsmacht über das Recht beim Gläubiger verbleiben muss (vgl. Art. 973d Abs. 2 Ziff. 2 OR). Zudem kann der Schuldner eines Registerwertrechts lediglich bei Smart Contracts und dergleichen die ihm vom Gesetz auferlegte Organisationsverantwortung wahrnehmen (vgl. Art. 973d Abs. 3 OR).²⁴¹³ Dies wird etwa gut ersichtlich an der Notwendigkeit des Schuldners, im Rahmen eines Kraftloserklärungsverfahrens nach Art. 973h OR bis zu einem gewissen Grad intervenieren zu können. Auf die konkrete Funktionsweise eines dezentralen Netzwerks, wie insb. den Konsens der Netzwerkteilnehmer, hat der Schuldner hingegen ohnehin keinen oder lediglich einen vernachlässigbaren Einfluss.

Im Ergebnis übernimmt das jeweilige Wertrechtereister die Funktion, die mit einem Handelsregister oder Grundbuch oder aber – bei dezentraler Betrachtung – mit einem lückenlosen Indossament vergleichbar ist.²⁴¹⁴

c. Anbietereigenschaft

Die Registerwertrechte und deren Tokeninhaber werden im Smart Contract erfasst, der in der Praxis auch als *Token Contract* bezeichnet wird, und dieser wird sodann im verteilten Register des dezentralen Netzwerks abgespeichert. Wenn eine Aktiengesellschaft mit anderen Worten ein Registerwertrecht (z.B. zwecks Verbriefung ihrer Namenaktien) herausgeben möchte, hat der Verwaltungsrat der Gesellschaft nicht nur das dezentrale Netzwerk, sondern insb. auch den Smart Contract zu bestimmen, welcher für die Emission und Übertragung der tokenisierten Aktien als Register dient. Vor dem Hintergrund der Begebung der Aktien als Registerwertrechte schliesst die Gesellschaft mit ihren bestehenden und künftigen Aktionären eine Registrierungsvereinbarung ab, welche allerdings auch in Form einer Statutenbestimmung vorgesehen werden kann.²⁴¹⁵

Demgegenüber sind in der Praxis Liquiditätsgeber, welche etwa ein Handelspaar bestehend aus Kryptovermögenswerten in einem AMM-Pool bereitstellen, nur ausnahmsweise auch die *Anbieter eines Wertrechtereisters* gemäss Art. 973d OR für die gehandelten Registerwertrechte. Dies ist namentlich dann

²⁴¹² So auch Kuhn, in: Weber/Kuhn, Digitale Aktiven im schweizerischen Privatrecht, Rz. 51.

²⁴¹³ Siehe Botschaft DLT 2019, 283–284, 289–290 («die Wahl des Registers selbst massgeblich in der Hand»).

²⁴¹⁴ So Weber, SZW 2021, 452 m.w.N.

²⁴¹⁵ So bereits von der Crone/Monsch/Meisser, GesKR 2019, 9.

der Fall, wenn eine Gesellschaft, die ihre Aktien wertpapierrechtlich in Form von Registerwertrechten ausgestaltet hat, gleichzeitig auch einen Sekundärmarkt für ihre Beteiligungsrechte über einen Smart Contract einer dezentralen Handelsplattform begründen möchte. Die Sicherstellung der Einhaltung der Pflichten nach Art. 973d ff. und insb. die Haftung nach Art. 973i OR treffen darum in aller Regel den Liquiditätsgeber von Kryptovermögenswerten nur dann, wenn er gleichzeitig auch Schuldner der in den Registerwertrechten verkündeten Rechte ist.²⁴¹⁶ Es gilt darum zwischen den beiden unterschiedlichen Smart Contracts zu unterscheiden:²⁴¹⁷ Der für die Emission der tokenisierten Werte verwendete Token Contract ist vom Smart Contract zu unterscheiden, welcher eine Person zwecks Austausch von Kryptovermögenswerten erstellt. Dies ist gut daran zu erkennen, dass ein Austausch von Kryptovermögenswerten technisch zuerst zu einem Update der Tokenbilanz im Smart Contract führt, infolgedessen sodann die Tokenbilanzen der Tokeninhaber im Smart Contract, der für die Emission der Registerwertrechte verwendet wurde, aktualisiert wird. Der Token Contract wird in diesem Fall i.d.R. als Inhaber der sich im AMM-Pool befindenden Vermögenswerte ausgewiesen.

Der Vollständigkeit halber sei erwähnt, dass Registerwertrechte nach Art. 973d ff. OR grundsätzlich auch über Layer-2-Protokolle herausgegeben und übertragen werden können. Dafür haben Wertrechtereister, die auf dem Layer-2-Protokoll (z.B. ZK-Rollup) basieren, ebenfalls den Anforderungen von Art. 973d Abs. 2 OR zu genügen. Dies sollte ohnehin nur wenige Probleme bereiten, wenn das zugrundeliegende dezentrale Netzwerk (z.B. Ethereum) als regelmässiger Abwicklungsmechanismus verwendet wird.²⁴¹⁸ Der Vorteil der Herausgabe von Registerwertrechten über ein Layer-2-Netzwerk ist,²⁴¹⁹ dass

²⁴¹⁶ Vgl. den Hinweis bei Weber, SJZ 2021, 680, 682–683, wonach solche Angebote in der Praxis bereits bestehen und nicht in jedem Fall *Parallelität* zwischen dem Anbieter eines Wertrechtereisters und dem Anbieter einer «DLT-Handelsplattform» bestehen muss.

²⁴¹⁷ Die Unterscheidung ist im Grundsatz auch in Art. 973f Abs. 2 Ziff. 2 OR angelegt, wonach sich die Unwiderruflichkeit einer Verfügung über ein Registerwertrecht entweder aus den Regeln des Wertrechtereisters oder aber «eines anderen[sic!] Handelssystems» ergibt.

²⁴¹⁸ Es handelt sich in diesen Fällen nicht um *Off-chain-Transaktionen* ausserhalb des verteilten elektronischen Registers und Wertrechtereisters, wie sie etwa durch Übertragung des Token innerhalb von privaten Datenbanken eines Intermediärs oder durch die unmittelbare physische Übergabe des Private Keys vorkommen können; vgl. hierzu auch Kuhn, in: Weber/Kuhn, Digitale Aktiven im schweizerischen Privatrecht, Rz. 119; von der Crone/Derungs, SZW 2019, 14–15.

²⁴¹⁹ Bei den derart gehandelten Rechten handelt es sich ebenfalls um Registerwertrechte, soweit sie *direkt* auf dem Layer 2 herausgegeben worden sind, weshalb in diesem Fall nicht bloss ein *Derivat* eines Registerwertrechts vorliegt; vgl. demgegenüber zur Derivatethe-

der Emittent von den Skalierungslösungen solcher Netzwerke profitieren kann und die Registerwertrechte über dezentrale Handelsplattformen, die auf demselben Layer-2-Protokoll beruhen (z.B. Loopring), gehandelt werden können.

3.7 Dezentrale Handelsplattformen als Zentralverwahrer?

a. Parallelen zu dezentralen Handelsplattformen

Als Zentralverwahrer gilt der Betreiber einer zentralen Verwahrungsstelle oder eines Effektenabwicklungssystems (Art. 61 Abs. 1 FinfraG). Als zentrale Verwahrungsstelle gilt eine Einrichtung, die gestützt auf einheitliche Regeln und Verfahren Effekten und andere Finanzinstrumente zentral verwahrt (Art. 61 Abs. 2 FinfraG). Als Effektenabwicklungssystem gilt sodann eine Einrichtung, die gestützt auf einheitliche Regeln und Verfahren, Geschäfte mit Effekten und anderen Finanzinstrumenten abrechnet und abwickelt (Art. 61 Abs. 3 FinfraG).

Vorliegend von Interesse ist lediglich die Funktion des *Effektenabwicklungssystems*; demgegenüber ist die zentrale Verwahrung von Effekten und anderen Finanzinstrumenten durch dezentrale Handelsplattformen sachlogisch ausgeschlossen.²⁴²⁰ Ferner findet auch keine Effektenregistrierung, d.h. die erstmalige Verbuchung von Effekten im Effektingiro, über dezentrale Handelsplattformen statt.²⁴²¹ Darüber hinaus gilt auch eine Einrichtung als Effektenabwicklungssystem, welche nur Abrechnungs- oder nur Abwicklungsschritte ausführt.²⁴²²

Im DLT-Bericht von 2018 hat der Bundesrat festgehalten, dass es denkbar sei, dass Blockchain-basierte Konzepte als Effektenabwicklungssysteme im Sinne des FinfraG qualifizieren. Namentlich wird erwähnt, dass bspw. die Aktivität der Abwicklung und Verwahrung von Token mit Effektenqualität über Smart Contracts als Abrechnung und Abwicklung gestützt auf einheitliche Regeln und Verfahren eingestuft werden könnte.²⁴²³ Diese Aussagen erfolgten vor

matik bei Off-chain-Transaktionen in privaten, internen Registern eines Intermediärs von der Crone/Baumgartner, SZW 2020, 361–362.

²⁴²⁰ Vgl. zur ähnlich gelagerten Frage hinsichtlich des dezentralen Netzwerks Jacquemart, Offene Blockchainsysteme, Rz. 440.

²⁴²¹ Vgl. zu dieser Funktion SK FinfraG–Costantini, Art. 61 N 15–16, 58.

²⁴²² Siehe Botschaft FinfraG 2014, 7548.

²⁴²³ Siehe Bundesrat, DLT-Bericht 2018, 112–113.

dem Hintergrund, die Einführung des DLT-Handelssystems als Alternative zu den bisherigen Bewilligungskategorien des Handelsplatzes und des Zentralverwahrers vorzuschlagen.

Es stellt sich die Frage nach der Abgrenzung dezentraler Handelsplattformen zum (zentralisierten) Effektenabwicklungssystem im Sinne von Art. 61 Abs. 3 FinfraG:

b. Dezentrale Abrechnung und Abwicklung

In dezentralen Handelsplattformen werden Abrechnung und Abwicklung von unterschiedlichen Komponenten des dezentralen Systems ausgeführt: Typischerweise bildet die Abrechnung Teil der Smart Contract-Logik. Dazu gehört insb. die Erfassung der Transaktionsdaten sowie die Abstimmung der beiden Transaktions-Legs (vgl. Art. 2 lit. g FinfraG). Daran anschliessend erfolgt die Abwicklung des Handelsgeschäfts durch die Teilnehmer des dezentralen Netzwerks (Atomic Settlement).

In der Literatur wird vor dem Hintergrund, dass kein traditionelles Settlement Risk besteht, zu Recht argumentiert, dass der Abwicklungsbegriff des FinfraG für die atomistische Abwicklung von Handelsgeschäften ungeeignet ist.²⁴²⁴ Analoges gilt nach vorliegender Ansicht auch für den Abrechnungsbegriff des FinfraG. Namentlich stellt ein Eintrag im verteilten Register gleichzeitig die Abrechnung und Abwicklung eines Handelsabschlusses dar.²⁴²⁵ WEBER geht ebenfalls davon aus, dass die Simultanausführung von Effekten- und Geldseite keinen Fall von Abrechnung und Abwicklung mehr darstellt, sodass die Verwendung von Smart Contract-basierten Abwicklungssystemen für sich alleine den Geltungsbereich von Art. 73a Abs. 1 FinfraG nicht eröffnen würde.²⁴²⁶ Dies ist überzeugend und gilt umso mehr für dezentrale Handelsplattformen.

c. Kein Betreiber, keine Einrichtung

Es kann auf die bereits zu DLT-Handelssystemen gemachten Ausführungen verwiesen werden, wonach dezentrale Handelsplattformen weder über einen Betreiber verfügen noch eine Einrichtung im Sinne des Gesetzes darstellen.²⁴²⁷

²⁴²⁴ Siehe SBF, Circular 2020/01, 8.

²⁴²⁵ Vgl. auch Bundesrat, DLT-Bericht 2018, 39.

²⁴²⁶ Siehe Weber, in: Weber/Kuhn, Handel mit digitalen Aktiven, Rz. 136; ferner Weber, SZW 2021, 458 m.w.H.

²⁴²⁷ Siehe oben, [V.3.3d.iv](#) und [V.3.3d.v](#). Gl.M. Jutzi/Abbühl, Fintech und DLT, Rz. 538.

3.8 Anbieter eines Wertrechtereisters als Effektenabwicklungssystem (Exkurs)

Während der Begriff des Effektenabwicklungssystems, wie oben gezeigt, sehr offen formuliert ist und potenziell die unterschiedlichsten Technologien erfasst, qualifizieren Anbieter eines Wertrechtereisters, über welches Personen dessen Registerwertrechte übertragen können, nicht als solches. Solange der Anbieter des Registers nicht unmittelbar in die Abrechnungs- und Abwicklungsschritte von Transaktionen involviert ist, fehlt es nach vorliegender Ansicht an den für das Vorliegen eines Effektenabwicklungssystems notwendigen Aktivitäten. Das blosse Erstellen eines Smart Contracts durch eine Person und deren eingeschränkte Möglichkeit, die Ausführungslogik des Smart Contracts in Einklang mit Art. 973d Abs. 2 Ziff. 1 OR zu beeinflussen,²⁴²⁸ qualifiziert mit anderen Worten nicht als Betrieb eines Effektenabwicklungssystems.²⁴²⁹

Sodann ist diese Aktivität auch nicht als Betrieb eines DLT-Handelssystems zu betrachten, wenn der Anbieter des Wertrechtereisters die Smart Contracts lediglich für den nichtgewerbsmässigen Handel (z.B. in Bezug auf die eigenen Aktien) verwendet.

²⁴²⁸ Siehe hierzu oben, [V.3.6b](#).

²⁴²⁹ So auch Iffland/Ben Hattar, CapLaw-2020-05, *passim*, die richtigerweise auf die Abwicklungsleistungen des dezentralen Netzwerks hinweisen.

4. Bankenrecht

4.1 Einleitung

Natürliche und juristische Personen, die nicht dem BankG unterstehen, dürfen keine Publikumseinlagen gewerbsmässig entgegennehmen (Art. 1 Abs. 2 BankG). Zweck der Verbotsnorm ist in erster Linie der Schutz der Einleger vor dem Verlust der von ihnen eingebrachten Einlagen insb. im Konkurs des Intermediärs.²⁴³⁰ Seit der Revision der BankV (vgl. aArt. 2a BankV) wird nicht mehr nur auf die Entgegennahme von Fremdmitteln zur Finanzierung Dritter abgestellt, sondern im Regelfall wird bloss noch die Passivseite der Unternehmensbilanz betrachtet.²⁴³¹ Im Zentrum steht demnach das bankenmässige Passivgeschäft, ohne dass es für die Unterstellungsfrage auf die Ausübung des Aktivgeschäfts ankommen würde.²⁴³² Ferner sollen die Bestimmungen des Bankenrechts – wie inzwischen allgemein üblich in der Finanzmarktgesetzgebung (vgl. Art. 4 FINMAG) – auch dem Funktionsschutz dienen.²⁴³³

FinTech-Geschäftsmodelle können in den Anwendungsbereich des BankG fallen, obschon sie regelmässig kein klassisches Bankgeschäft, d.h. Zinsdifferenzgeschäft samt Fristentransformation, betreiben.²⁴³⁴ Darunter fallen etwa Aktivitäten in den Bereichen des Crowdfundings und Zahlungsverkehrs.²⁴³⁵ Auf

²⁴³⁰ Vgl. aus den *Materialien* Botschaft BankG 1934, 178–179, 187; Botschaft BankG 1970, 1145; Botschaft FINMAG 2006, 2859; ferner aus der *Rechtsprechung* des Bundesgerichts BGE 97 I 84, E. 3a; 99 Ib 104, E. 5; 103 Ib 350, E. 7a; 105 Ib 348, E. 10c; 106 Ib 357, E. 2c; 108 Ib 78, E. 3; 108 Ib 270, E. 2d; 108 Ib 513, E. 5baa; 116 Ib 193, E. 2b; 121 II 147, E. 3a; sodann aus der *Literatur* BSK BankG–Müller, Einleitung N 19; BSK BankG–Bahar/Stupp, Art. 1 N 1; schliesslich ausführlich Burghof/Rudolph, Bankenaufsicht, 19–22.

²⁴³¹ Ausführlich Hess, Geltungsbereich der bewilligungspflichtigen Tätigkeiten, Rz. 193 m.w.N. 692, 696, der korrekterweise jedoch nicht mehr von Passivgeschäften, sondern von «Verwahrungsgeschäften» spricht, um auch ausserbilanziell gehaltene sammelverwahrte kryptobasierte Vermögenswerte im Sinne von Art. 5a BankV zu erfassen; kritisch mit Blick auf die FinTech-Bewilligung gemäss Art. 1b BankG Staub, iusNet BR-KR 27.04.2023, *passim*.

²⁴³² Vgl. BGer 2C_345/2015 vom 29. März 2016, E. 6.5.

²⁴³³ Siehe bereits EBK, Jahresbericht 1989, 13–14; ferner Botschaft FINMAG 2006, 2859; sodann BGE 111 Ib 126, E. 2a; 126 II 111, E. 3b; in *allgemeiner* Hinsicht BGE 135 II 356, E. 3.1; 131 II 306, E. 3.1.2; 130 II 351, E. 2.2.

²⁴³⁴ Siehe Bundesrat, DLT-Bericht 2018, 90, 95; ausführlich EFD, Erläuternder Bericht Vernehmlassungsvorlage FinTech 2017, 16–17, 20; ferner Leimgruber/Flückiger, Jusletter vom 6. November 2017, Rz. 4–5, 26–27.

²⁴³⁵ Vgl. etwa die Ausführungen des Bundesgerichts zu innovativen Zahlungssystemen BGer 2C_345/2015 vom 24. November 2015, E. 4.2 («Geschäften mit Einlagencharakter»).

diese Geschäftsmodelle hat der Bundesrat per 1. August 2017 durch eine Revision der BankV reagiert, indem er einerseits die Abwicklungsfrist für Abwicklungskonten auf 60 Tage ausgedehnt und andererseits eine Sandbox für innovative Geschäftsmodelle geschaffen hat.²⁴³⁶

4.2 Entgegennahme von Publikumseinlagen oder sammelverwahrten kryptobasierten Vermögenswerten

a. Publikumseinlagen

i. Im Allgemeinen

Als *Bank* gilt insb. eine Person, die hauptsächlich im Finanzbereich tätig ist und gewerbsmässig Publikumseinlagen von mehr als 100 Millionen Franken entgegennimmt oder sich öffentlich dafür empfiehlt oder gewerbsmässig Publikumseinlagen bis zu 100 Millionen Franken entgegennimmt oder sich öffentlich dafür empfiehlt und diese Publikumseinlagen anlegt oder verzinst (Art. 1a lit. a und b BankG).

Demgegenüber gilt als *Person nach Art. 1b BankG* jede Person, die gewerbsmässig Publikumseinlagen von bis zu 100 Millionen Franken entgegennimmt oder sich öffentlich dafür empfiehlt *und* diese Publikumseinlagen weder anlegt noch verzinst (Art. 1b Abs. 1 BankG). Gemeinhin wird bei dieser auf den 1. Januar 2019 eingeführten neuen Bewilligungskategorie von «FinTech-Bewilligung» oder «Banklizenz Light» gesprochen.²⁴³⁷ Das Bewilligungsgefäss für Personen nach Art. 1b Bank findet sich bereits wieder im Gesetzgebungsprozess.²⁴³⁸ Neben den identifizierten Schwächen insb. im Bereich der Aussonderung von – notabene – Publikumseinlagen muss die Entwicklung auch vor dem Hintergrund der europarechtlichen MiCAR gesehen werden, die ein Spezialregime für Anbieter von Dienstleistungen in Bezug auf Kryptowerte eingeführt hat. MiCAR tritt neben bestehende Richtlinien wie MiFID II (Finanzinstrumente) und die E-Geld-Richtlinie (elektronisches Geld).²⁴³⁹

²⁴³⁶ Art. 6 Abs. 2 und Art. 5 Abs. 3 lit. c BankV.

²⁴³⁷ Vgl. EFD, Erläuterungen FinTech 2018, *passim*.

²⁴³⁸ Siehe Bundesrat, Evaluation BankG, 5–6.

²⁴³⁹ Siehe Tobler, EuZ 04/2023, E5–E6, E13–E14; Bürgi/Kremer, iusNet BR-KR 25.08.2022, *passim*; ferner Contratto, CapLaw-2023-38, *passim*.

Vorbehaltlich der Anwendbarkeit einer Ausnahme gelten als *Publikumseinlagen* alle Verbindlichkeiten gegenüber Kunden (Art. 5 Abs. 1 BankV).²⁴⁴⁰ Als Verbindlichkeiten qualifizieren in erster Linie Gelder bzw. Geldmittel mit Fremdmittelcharakter.²⁴⁴¹ Das Bundesgericht erachtet als zentrales Element des Einlagebegriffs den Umstand, dass die Person, die vorab eine Geldleistung empfängt, auf eigene Rechnung eine Verpflichtung zur Rückzahlung eingeht.²⁴⁴² Eine Erweiterung dieser Regel kann in der Qualifizierung von vertraglich vereinbarten Zinszahlungen an den Einleger als Einlagen gesehen werden.²⁴⁴³ Bei der Beurteilung wendet das Bundesgericht eine wirtschaftliche Betrachtungsweise an.²⁴⁴⁴ *Gewerbsmässig* im Sinne des BankG handelt, wer dauernd mehr als 20 Publikumseinlagen entgegennimmt oder sich öffentlich zur Entgegennahme von Publikumseinlagen empfiehlt, selbst wenn daraus weniger als 20 Einlagen resultieren (Art. 6 Abs. 1 BankV).

Im BankG selbst werden die Auflage von Anleihen sowie Wertpapierhäuser nach FINIG, die den Effektenhandel betreiben, und Vermögensverwalter, Notare und Geschäftsagenten, welche die Gelder ihrer Kunden verwalten, von der Unterstellung unter das Gesetz *ausgenommen*, soweit diese keinen Bankbetrieb führen (Art. 1 Abs. 2 und 3 BankG). Der Bundesrat sieht sodann eine abschliessende²⁴⁴⁵ Liste von Ausnahmen in der BankV vor, die einerseits an den Publikumsbegriff und andererseits an den Einlagebegriff sowie an den Begriff der Gewerbsmässigkeit anknüpfen.²⁴⁴⁶ Hintergrund der Ausnahmen ist ein verringertes Bedürfnis nach aufsichtsrechtlichem Einlegerschutz.²⁴⁴⁷

²⁴⁴⁰ Siehe auch FINMA-RS 08/3 «Publikumseinlagen bei Nichtbanken», Rz. 10.

²⁴⁴¹ Vgl. Schönknecht, GesKR 2016, 309–310, der in erster Linie zwischen Darlehens-, Hinterlegungs- (*depositum irregulare*) und Treuhandverhältnissen unterscheidet; ferner Zogg, recht 1/2020, 4–5; Zellweger–Gutknecht/Seiler, in: Maume/Maute/Fromberger, Switzerland, 482.

²⁴⁴² Siehe hierzu BGE 132 II 382, E. 6.3.1; 136 II 43, E. 4.2; ausführlich BGer 2C_345/2015 vom 29. März 2016, E. 6.3–6.5 m.w.N.; 2C_89/2010 und 2C_106/2010 vom 10. Februar 2011, E. 3.1 (nicht publiziert in BGE 137 II 284); 2C_671/2014 vom 18. Dezember 2014, E. 2.1; 2C_929/2010 vom 13. April 2011, E. 2.1 («für eigene Rechnung»); 2A.218/1999 und 2A.219/1999 vom 5. Januar 2000, E. 3b/bb («[teilweise] Auszahlung ihrer Guthaben»).

²⁴⁴³ So BGer 2C_345/2015 vom 29. März 2016, E. 7.4.3.

²⁴⁴⁴ Vgl. BGer 2C_352/2016 vom 9. Dezember 2016, E. 3.3.

²⁴⁴⁵ Siehe EFD, Erläuternder Bericht Vernehmlassungsvorlage FinTech 2017, 13.

²⁴⁴⁶ Art. 1 Abs. 2 BankG i.V.m. Art. 5–6 BankV.

²⁴⁴⁷ So BGer 2C_345/2015 vom 29. März 2016, E. 8.2.

ii. Virtuelle Währungen im Besonderen

Virtuelle Währungen (bzw. Kryptowährungen), denen definitionsgemäss die Geldfunktion zukommt,²⁴⁴⁸ können nach überwiegend vertretener Ansicht als bankenrechtliche Einlagen qualifizieren.²⁴⁴⁹ In der Folge sind Geschäftsmodelle, die mit virtuellen Währungen in Berührung kommen, für ihre Tätigkeiten allenfalls auf eine Bankbewilligung angewiesen.²⁴⁵⁰

Als wesentliche Merkmale für die Entgegennahme von Publikumseinlagen in Form von *virtuellen Währungen* gelten, dass (i) der Kunde nicht jederzeit ohne Mitwirkung des Intermediärs über die virtuelle Währung verfügen kann, (ii) der Intermediär eine Auszahlungsverpflichtung gegenüber dem Kunden hat und (iii) die entgegengenommene virtuelle Währung im Konkursfall in die Konkursmasse des Intermediärs fallen würde.²⁴⁵¹ Die Qualifikation als bankenrechtliche relevante Einlage hängt somit von der im Einzelfall gewählten technischen Verwahrungslösung ab. So war nach bisheriger FINMA-Praxis «unter engen Voraussetzungen» keine Bankbewilligung erforderlich, wenn die Guthaben in virtueller Währung ausschliesslich zur sicheren Verwahrung auf das (Hosted bzw. Custodial) Wallet des Anbieters übertragen werden und diese virtuellen Währungseinheiten gesondert pro Kunde auf der Blockchain verwahrt und zu jedem Zeitpunkt dem einzelnen Kunden zugeordnet werden können.²⁴⁵²

²⁴⁴⁸ Siehe oben, [V.2.5a](#).

²⁴⁴⁹ So bereits Bundesrat, Bericht zu virtuellen Währungen, 13; EFD, Erläuternder Bericht Vernehmlassungsvorlage FinTech 2017, 15; FINMA, Erläuterungsbericht GwV-FINMA 2015, 2; ferner zu Meinungen in der Literatur Schönknecht, GesKR 2016, 308–309, der voraussetzt, dass die Einlage entweder breit als Zahlungsmittel einsetzbar ist oder aber ohne Weiteres in staatliche Währungen gewechselt werden kann; Maurenbrecher/Meier, Jusletter vom 4. Dezember 2017, Rz. 30; Reiser, AJP 2018, 815, die voraussetzt, dass es sich um ein liquides Zahlungsmittel handelt; ferner Hess/Spielmann, in: Reutter/Werlen, Digitalisierte Werte, 180; bereits Bärtschi/Meisser, in: Weber/Thouvenin, Virtuelle Währungen, 130; zurückhaltend Hari, GesKR 2017, 460.

²⁴⁵⁰ Vgl. jedoch Hauser-Spühler, Innovation vs. Regulation, Rz. 139–143, welche die Anwendbarkeit des Einlagebegriffs auf Wallet-basierte Geschäftsmodelle grundsätzlich infrage stellt, was für sie letztlich eine Frage des Legalitätsprinzips ist.

²⁴⁵¹ Siehe EFD, Erläuternder Bericht Vernehmlassungsvorlage FinTech 2017, 15; Bundesrat, DLT-Bericht 2018, 91.

²⁴⁵² Siehe FINMA, Erläuterungsbericht GwV-FINMA 2015, 2; diesbezüglich kritisch bereits Graham-Siegenthaler/Furrer, Jusletter vom 8. Mai 2017, Rz. 80–86, welche unter gewissen Umständen die Nutzung eines «internal ledger» des Wallet-Anbieters als ausreichend betrachten.

Der Einlagebegriff ist mit Blick auf Handelsplattformen regelmässig erfüllt, wenn der Betreiber einer solchen Plattform virtuelle Währungen auf seinem eigenen Wallet zwecks vorübergehender Aufbewahrung oder zwecks künftigen Kaufs und Verkaufs von Kryptovermögenswerten samt buchmässiger Führung von Konten für den Kunden entgegennimmt.²⁴⁵³ Diese Umstände sind bei zentralen Handelsplattformen typischerweise aufgrund der Verwendung von Hosted Wallets gegeben. Hier führt der Plattformbetreiber die von den Kunden eingebrachten virtuellen Währungen in einer von ihm kontrollierten «Sammel-Wallet» zusammen, um den Kunden den Handel von Kryptovermögenswerten über seine Plattform zu ermöglichen. In diesem Fall kommt dem Intermediär die ausschliessliche Verfügungsmacht über die eingebrachten virtuellen Währungen zu. Der Kunde trägt in der Folge das Konkursrisiko des Intermediärs.

b. Sammelverwahrte kryptobasierte Vermögenswerte

Im Rahmen der DLT-Revision, deren zweiter Teil am 1. August 2021 in Kraft trat, wurde die Bewilligungskategorie nach Art. 1b BankG auf die Entgegennahme – und, richtigerweise, auch Verwahrung – von kryptobasierten Vermögenswerten *ausgeweitet*.

Der für den sachlichen Geltungsbereich des BankG massgebliche Begriff der kryptobasierten Vermögenswerte wird in Art. 5a Abs. 1 BankV definiert: Kryptobasierte Vermögenswerte sind demnach Vermögenswerte nach Art. 16 Ziff. 1^{bis} lit. b BankG (sog. *sammelverwahrte kryptobasierte Vermögenswerte*), die tatsächlich oder nach der Absicht des Organisators oder Herausgebers in einem erheblichen Umfang als Zahlungsmittel für den Erwerb von Waren oder Dienstleistungen oder der Geld- oder Wertübertragung dienen. Es handelt sich hierbei also um sammelverwahrte Kryptowährungen bzw. Zahlungstoken. Davon zu unterscheiden ist die Frage der Aus- bzw. Absonderbarkeit der kryptobasierten Vermögenswerte (unabhängig von der Token-Klassifizierung) im Konkurs der Bank bzw. der Person nach Art. 1b BankG; Diese richtet sich ausschliesslich nach den Voraussetzungen in Art. 16 Ziff. 1^{bis} i.V.m. Art. 37d BankG.

²⁴⁵³ Vgl. etwa Bundesrat, Bericht zu virtuellen Währungen, 13–14; EFD, Erläuternder Bericht Vernehmlassungsvorlage FinTech 2017, 15 FN 21; ferner Botschaft DLT 2019, 268; FINMA, Erläuterungsbericht GwV-FINMA 2015, 2.

Solche sammelverwahrte kryptobasierte Vermögenswerte dürfen weder angelegt noch verzinst werden. Sie werden somit wie Publikumseinlagen, welche von FinTech-Unternehmen entgegengenommen werden, behandelt.²⁴⁵⁴ Das Aktiv- bzw. Eigengeschäft mit diesen Vermögenswerten ist damit ausgeschlossen. Diese Vorgabe wäre etwa verletzt, wenn ein Wallet-Anbieter die kryptobasierten Vermögenswerte im eigenen Namen auf eigene Rechnung im Kapitalmarkt anlegen würde.²⁴⁵⁵ Demgegenüber ist es möglich, auf Rechnung des Kunden Anlagen zu tätigen.²⁴⁵⁶ Die Detailbestimmungen zur Form der Verwahrung sind in Art. 14f BankV festgelegt.

Sammelverwahrte kryptobasierte Vermögenswerte im Sinne von Art. 16 Ziff. 1^{bis} lit. b BankG sind im Konkurs des Intermediärs aussonderbar bzw. absonderbar und qualifizieren deshalb gerade *nicht* als Publikumseinlagen.²⁴⁵⁷ Die Absonderung setzt allerdings voraus, dass der Intermediär vertraglich die Pflicht übernimmt, die sammelverwahrten kryptobasierten für die Kunden jederzeit bereitzuhalten, und dass die Vermögenswerte einer Gemeinschaft von Kunden i.d.R. in einem internen Register, wie etwa einem Kernbankensystem, zugeordnet sind und daraus ersichtlich ist, welcher Anteil am Gemeinschaftsvermögen dem einzelnen Kunden zusteht. Sind die Vermögenswerte demgegenüber nicht den Kunden zuordenbar, liegen keine Depotwerte im Sinne von Art. 16 Ziff. 1^{bis} BankG, sondern bloss Publikumseinlagen vor.

Das EFD will mit der Erweiterung des bankgesetzlichen Unterstellungsraumes verhindern, dass Personen sammelverwahrte Kryptowährungen bzw. Zahlungs-Token in unbeschränktem Umfang bewilligungsfrei entgegennehmen und verwahren können.²⁴⁵⁸ Als Gründe führt das EFD Überlegungen einerseits zur Marktintegrität (betrügerisches Verhalten, Reputation) und andererseits zur Technologieneutralität an.²⁴⁵⁹ Namentlich hatte die FINMA anlässlich der

²⁴⁵⁴ Umstritten ist, ob sich aus der Formulierung von Art. 1b Abs. 1 BankG eine *Unterstellungslücke* für Geschäftsmodelle ergibt, die kryptobasierte Vermögenswerte entgegennehmen oder sich öffentlich dafür empfehlen *und diese Vermögenswerte verzinsen*; siehe hierzu namentlich Kunz, Jusletter vom 14. Dezember 2020, Rz. 5.

²⁴⁵⁵ Vgl. EFD, Erläuterungen FinTech 2018, 6.

²⁴⁵⁶ Siehe hinsichtlich der Zulässigkeit des *Stakings* von Kryptovermögenswerten auf Rechnung (und Risiko) des Kunden eines Intermediärs in Proof-of-Stake-Protokollen Schärli/Meisser/Luthiger, Jusletter IT vom 30. September 2021, Rz. 43–49. Mit dem Custodial Staking ist sodann auch keine Verzinsung der Kundevermögen verbunden; vgl. hierzu Andreotti/Zimmermann/Prantl, GesKR 2023, 352.

²⁴⁵⁷ Selbstredend war die Entgegennahme von Kryptowährungen bzw. Zahlungs-Token in Form von *Publikumseinlagen* bereits unter altem Recht bewilligungspflichtig.

²⁴⁵⁸ Siehe Botschaft DLT 2019, 247, 268–269, 301–302.

²⁴⁵⁹ Siehe Botschaft DLT 2019, 268–269.

Ausarbeitung der Vorlage ihre grossen Bedenken am neuen Art. 242a SchKG (siehe unten) geäussert.²⁴⁶⁰ Korrekt ist, dass die Vermischung bzw. Sammelbuchung traditioneller Geldeinheiten, d.h. von Bargeld²⁴⁶¹ und Bankbuchgeld, typischerweise die bankenrechtliche Bewilligungspflicht auslöst. Eine Gleichbehandlung von Fiat- und kryptobasierten Zahlungsmitteln könnte sich darum aufdrängen.²⁴⁶² Dass die Unterstellung aufgrund des Betrugs- und Veruntreuungsrisikos zu erfolgen habe, wie der Bundesrat in der Botschaft ausführte,²⁴⁶³ überzeugt demgegenüber nicht. Kryptovermögenswerte konnten bereits nach der alten FINMA-Aufsichtspraxis ohne Bewilligung entgegengenommen werden, solange sie im Konkurs des betrügerisch handelnden Intermediärs rein theoretisch aussonderbar waren.

Damit knüpft der Geltungsbereich des BankG erstmals nicht mehr ausschliesslich an den Einlagebegriff an. Darüber hinaus weist die konkursrechtliche Behandlung der entgegengenommenen Vermögenswerte keine Indizienwirkung mehr auf. Nunmehr ist neu auch die Sammelverwahrung von Kryptovermögenswerten, die tatsächlich eine Geld- bzw. Zahlungsmittelfunktion übernehmen, dem BankG unterstellt.²⁴⁶⁴ Es handelt sich bei der bewilligungspflichtigen Sammelverwahrung von kryptobasierten Vermögenswerten um eine Unterkategorie der FinTech-Bewilligung. Hingegen gilt anders als bei Publikumseinlagen der Schwellenwert von 100 Millionen Franken für kryptobasierte Vermögenswerte gemäss Wortlaut von Art. 1b Abs. 1 BankG nicht. Umstritten ist schliesslich, ob trotz der Sonderregelung in Art. 5a Abs. 2 BankV die weiteren Ausnahmen vom Publikumseinlagenbegriff in Art. 5 Abs. 2 und 3 BankV auch für sammelverwahrte Zahlungs-Token gelten.²⁴⁶⁵

Die FINMA kann schliesslich gestützt auf Art. 4^{sexies} BankG im Einzelfall einen Höchstbetrag für kryptobasierte Vermögenswerte festlegen, welche eine

²⁴⁶⁰ So Siehe Botschaft DLT 2019, 246–247.

²⁴⁶¹ Vgl. in diesem Zusammenhang Art. 481 Abs. 1 und 2 OR und Art. 727 ZGB.

²⁴⁶² Vgl. Botschaft DLT 2019, 246–247 («[...] Kryptowährungen [...] rechtlich gleich erfasst [...] wie staatliche Währungen»), 268–269, 302 («Vergleichbarkeit mit Fiat-Geld»); EFD, Erläuterungen Verordnung DLT 2021, 17.

²⁴⁶³ Siehe Botschaft DLT 2019, 268.

²⁴⁶⁴ Vgl. in diesem Zusammenhang Tränkle, in: Reutter/Werlen, Blockchain, 159; Kramer/Wyss, in: Weber/Kuhn, Verwahrung, Rz. 20–21; zum Begriff Zellweger-Gutknecht/Weber, Jusletter vom 11. Januar 2021, Rz. 17–18, 33 («Kryptozahlungsmittel»).

²⁴⁶⁵ Vgl. Kramer/Wyss, in: Weber/Kuhn, Verwahrung, Rz. 21; ferner Zellweger-Gutknecht/Weber, Jusletter vom 11. Januar 2021, Rz. 35 FN 60.

Bank²⁴⁶⁶ als Depotwerte für Depotkunden, d.h. *ausserhalb* ihrer Bilanz hält,²⁴⁶⁷ wenn dies aufgrund der mit dem Geschäft verbundenen Risiken als geboten erscheint. Soweit sie Kryptovermögenswerte auf der Bilanz hält, sind die einschlägigen Eigenmittelvorschriften zu beachten.²⁴⁶⁸

c. Individuell verwahrte kryptobasierte Vermögenswerte

Weiterhin bewilligungsfrei ist dagegen die Entgegennahme von den Kunden individuell zuordenbaren Depotwerten im Sinne von Art. 16 Ziff. 1^{bis} lit. a BankG.²⁴⁶⁹ Nach dem Gesagten löst einzig die Entgegennahme von kryptobasierten Vermögenswerten die neue FinTech-Bewilligungspflicht aus, wenn es sich bei ihnen um lediglich gemeinschaftlich zuordenbare Depotwerte im Sinne von Art. 16 Ziff. 1^{bis} lit. b BankG handelt.²⁴⁷⁰

4.3 Aus- und Absonderbarkeit im Konkurs (Exkurs)

a. Aussonderbarkeit nach Art. 242 SchKG

Ob Publikumseinlagen entgegengenommen werden, hängt nach Auffassung des Bundesrates wesentlich von der konkursrechtlichen Frage der Aussonderung ab.²⁴⁷¹ *Aussonderbarkeit indiziert mit anderen Worten Bewilligungsfreiheit*

²⁴⁶⁶ Nach eindeutigen Wortlaut müsste diese Bestimmung nur auf Banken im Sinne von Art. 1a BankG und gerade nicht auf Personen mit einer FinTech-Bewilligung zur Anwendung gelangen; *a.A.* aber Botschaft DLT 2019, 269 («von einer Bank oder einer Person nach Artikel 1b BankG»).

²⁴⁶⁷ Siehe Botschaft DLT 2019, 302.

²⁴⁶⁸ Vgl. BIS/BCBS, Prudential treatment of cryptoasset exposures, 3–4 *e contrario*, ferner 5 («[...] the term 'exposure' includes on- or off-balance sheet amounts [of a bank] that give rise to credit, market, operational and/or liquidity risks [...] the operational risk requirements [...] are also applicable to banks' crypto asset activities, such as custodial services involving the safekeeping or administration of client cryptoassets on a segregated basis, that do not generally give rise to credit, market or liquidity requirements.»).

²⁴⁶⁹ Diesbezüglich *zurückhaltend* Jaccard, Jusletter vom 25. Oktober 2021, Rz. 24–25.

²⁴⁷⁰ Siehe EFD, Erläuterungen Verordnung DLT 2021, 17; ferner hierzu Schärli/Meisser/Luthiger, Jusletter IT vom 30. September 2021, Rz. 57–58.

²⁴⁷¹ Vgl. Bundesrat, DLT-Bericht 2018, 97 («Soweit nämlich Token in einer Insolvenz aus der Konkursmasse ausgesondert werden können, sind diese aus bankenrechtlichen Gesichtspunkten nicht als Einlagen zu qualifizieren und führen entsprechend auch nicht zu einer Bewilligungspflicht als Bank.»); ferner die Meinung der FINMA wiedergebend Botschaft DLT 2019, 246 («starke sachlogische Wechselwirkung»); ebenso Reiser, AJP 2018, 815; Bun-

bzw. *Nichtunterstellung*. Von diesem «Prinzip» scheint man sich nun aber mit der Einführung der FinTech-Bewilligung für sammelverwahrte, aber grundsätzlich aussonderbare kryptobasierte Vermögenswerte verabschiedet zu haben.²⁴⁷²

Praxisrelevant ist die Zuordnung von Kryptovermögenswerten im Konkurs einer Person, *wenn* die wirtschaftliche Berechtigung an den Vermögenswerten und die Verfügungsmacht bzw. Kontrolle über sie *auseinanderfallen*. Die konkreten Bedingungen des Auseinanderfallens sind grundsätzlich in der vertraglichen Dokumentation zwischen Kunde und Intermediär stipuliert.

Ein Auseinanderfallen kann namentlich im Rahmen der Fremdverwahrung von Kryptovermögenswerten durch Wallet-Anbieter der Fall sein. Vor der Revision des SchKG im August 2021 hat die Literatur ausführlich diskutiert, ob²⁴⁷³ und unter welchen Bedingungen Kryptovermögenswerte im Konkurs des Wallet-Anbieters gestützt auf Art. 242 Abs. 1 SchKG aussonderbar sind. Die wohl überwiegend vertretene Ansicht ging in Anlehnung an die bundesgerichtliche Rechtsprechung zum Mitgewahrsam an Sachen davon aus, dass lediglich Sachen, über welche der Konkursit die «ausschliessliche tatsächliche Verfügungsgewalt» hat, in die Konkursmasse fallen, weshalb sie vom wirtschaftlich Berechtigten auf dem Klageweg ausgesondert werden können.²⁴⁷⁴ Sachen, die sich in Mitgewahrsam des Konkursiten *und* des wirtschaftlich Berechtigten befinden, hat die Konkursverwaltung demgegenüber mithilfe der Admassierungsklage zur Masse zu ziehen (Art. 242 Abs. 3 SchKG).

Nach dieser Auffassung fallen lediglich Kryptovermögenswerte in die Konkursmasse des Wallet-Anbieters, wenn dieser über *sämtliche* relevanten Private Keys und somit unmittelbar über die Vermögenswerte verfügen kann, wohingegen der Kunde keinen eigenen Zugriff auf die Vermögenswerte hat.²⁴⁷⁵ Bei bloss geteilter Verfügungsmacht fallen die Vermögenswerte also nicht

desrat, Bericht Anpassungen BankG, 6, wonach eine neue Bewilligungskategorie, welche die Aussonderung von (treuhänderisch verwahrten) Fiatgeldern von Kunden vorsieht, aufgrund des Einlagenbegriffs nicht mehr im BankG zu regeln wäre; *skeptisch* demgegenüber, was diese Gleichsetzung anbelangt, Maurenbrecher/Meier, Jusletter vom 4. Dezember 2017, Rz. 36.

²⁴⁷² Siehe oben, [V.4.2b](#).

²⁴⁷³ Grundsätzlich *verneinend* Piller, AJP 2017, 1437, ausser es handelt sich um ein (körperliches) Hardware-Wallet im Gewahrsam des Konkursiten.

²⁴⁷⁴ Vgl. BGE 110 III 87, E. 2a m.w.N.

²⁴⁷⁵ Siehe Bundesrat, DLT-Bericht 2018, 70; ferner Kramer/Wyss, in: Weber/Kuhn, Verwahrung, Rz. 36; Schärli/Meisser/Luthiger, Jusletter IT vom 30. September 2021, Rz. 16 und insb. auch die dortige FN 15.

in die Masse des Wallet-Anbieters.²⁴⁷⁶ Nach dieser Ansicht sind bspw. auch Vermögenswerte in Multisig-Lösungen «konkursfest». Die Konkursverwaltung muss solche Vermögenswerte an den wirtschaftlich Berechtigten herausgeben, ohne dass dieser den Klageweg zu beschreiten hat.²⁴⁷⁷

Wie der Bundesrat ausführt, steht dem wirtschaftlich Berechtigten ein Vorgehen nach Art. 242 SchKG nur bei dinglichen Rechten zu. Soweit der wirtschaftlich Berechtigte weiterhin über das Eigentum an der Sache, die sich im Besitz des Konkursiten befindet (z.B. aufgrund eines *depositum regulare*), verfügt, so steht ihm als Hinterleger ein Aussonderungsrecht im Konkurs des Aufbewahrers zu.²⁴⁷⁸ Soweit hingegen der Konkursit – z.B. im Rahmen eines fiduziarischen Rechtsverhältnisses – Eigentum an der Sache erwirbt, kann der wirtschaftlich Berechtigte allenfalls einen obligatorischen Rückforderungsanspruch gegen ihn bzw. die Masse geltend machen. Demgegenüber hat er bei rein obligatorischen Rechten, vorbehaltlich einer abweichenden gesetzlichen Regelung (z.B. Art. 401 Abs. 1 und 3 OR),²⁴⁷⁹ lediglich einen Anspruch auf quotenmässige Erfüllung der Forderung.²⁴⁸⁰ Dies ist etwa der Fall bei bankenrechtlichen Publikumseinlagen, die als virtuelle Währungen in einem Hosted Wallet des Intermediärs mit den Eigenschaften eines Sammelkontos zusammengeführt werden.

²⁴⁷⁶ Siehe Hauser-Spühler/Meisser, *digma* 2018, 11–12, die allerdings noch *weitergehen*, indem sie ausführen, dass dies u.U. selbst bei «alleinige[m] Gewahrsam des Schuldners» bzw. Konkursiten gelten könne (vgl. in diesem Zusammenhang auch Hauser-Spühler, *Innovation vs. Regulation*, Rz. 131 [*«Entgegen der mutmasslichen Meinung der FINMA [...] sind Bitcoins immer auf der Blockchain gespeichert und bleiben auch im Konkursfall aussondert.»*]); ferner wohl auch Maurenbrecher/Meier, *Jusletter* vom 4. Dezember 2017, Rz. 26, die zwar zuerst davon sprechen, dass ein Kunde «alleine Zugriff auf die Private Keys» hat, doch ausdrücklich auch Formen des Mitgewahrsams genügen lassen; ferner Meisser/Meisser/Kogens, *Jusletter IT* vom 24. Mai 2018, Rz. 44, die für die Zuordnung zum Vermögen allerdings nicht auf die Verfügungsmacht abstellen, sondern das *Verfügungsrecht* an den Vermögenswerten als ausschlaggebend betrachten; Graham-Siegenthaler/Furrer, *Jusletter* vom 8. Mai 2017, Rz. 97; sodann auch Hari, *GesKR* 2017, 464–467; schliesslich auch CVA RWG, *Custody of Crypto Assets*, 5 («not sufficient to consider securities as deposited *stricto sensu* under civil law»).

²⁴⁷⁷ Art. 51 KOV.

²⁴⁷⁸ Vgl. auch Art. 641 Abs. 2 ZGB.

²⁴⁷⁹ Vgl. diesbezüglich Zogg, *AJP* 2020, 980, 984, wonach der obligatorische Ablieferungsanspruch des Auftraggebers nach Art. 400 Abs. 1 OR gewissermassen «verdinglicht» wird.

²⁴⁸⁰ Zum Ganzen Bundesrat, *DLT-Bericht* 2018, 71.

Da Kryptovermögenswerte trotz ihrer datenmässigen²⁴⁸¹ Abbildung in einem verteilten Register *Ähnlichkeiten mit Sachen* im zivilrechtlichen Sinne aufweisen, wurde in der Literatur bereits früh gefordert, dass sie durch direkte oder sinngemässe Anwendung oder aber durch Lückenfüllung von Art. 242 SchKG ebenfalls Gegenstand der konkursrechtlichen Aussonderung sein können.²⁴⁸² Die Diskussionen rund um die Sachqualität von Kryptowährungen war darum in erster Linie konkursrechtlich motiviert. Im Wesentlichen wird vertreten, dass Kryptovermögenswerte aussonderbar sind, wenn sie den einzelnen wirtschaftlich Berechtigten (individuell) zugeordnet werden können.²⁴⁸³ Die Zu-

²⁴⁸¹ Allerdings stellen lediglich die Private und Public Keys, die Wallet-Adressen sowie die in den Blöcken abgebildeten Transaktionsdaten in informationstheoretischer Hinsicht digitale Daten dar und nicht die Kryptovermögenswerte selbst, die rein fiktiv sind; vgl. hierzu in Bezug auf Bitcoins Meisser/Meisser/Kogens, Jusletter IT vom 24. Mai 2018, Rz. 3 m.w.H.; ebenso Kogens/Montanari, SZW 2021, 462; wohl auch Omlor, ZHR 2019, 308; Enz, Kryptowährungen, N 398, jedoch sodann unklar in N 401-403 («Wertdaten»); vgl. zum Konzept der Wertdaten Zellweger-Gutknecht, in: Fox/Green, Right Regulatory Regime, N 4.82.

²⁴⁸² Siehe bereits Bärtschi/Meisser, in: Weber/Thouvenin, Virtuelle Währungen, 130; sodann Eckert, SJZ 2016, 272, wonach aussonderbares Eigentum an digitalen Daten, namentlich Bitcoins, begründet werden könne; Graham-Siegenthaler/Furrer, Jusletter vom 8. Mai 2017, Rz. 78-96, die grundsätzlich die Begründung von Eigentumsrechten an Kryptovermögenswerten u.a. in Analogie zu Bucheffekten als Vermögensobjekte *sui generis* befürworten; Maurenbrecher/Meier, Jusletter vom 4. Dezember 2017, Rz. 26-27; Meisser/Meisser/Kogens, Jusletter IT vom 24. Mai 2018, Rz. 15, 48-53, die sich dafür aussprechen, dass bitcoins als Vermögenswerte *sui generis* gelten, weshalb sich eine analoge Anwendung von Art. 242 SchKG rechtfertige; Hauser-Spühler/Meisser, digma 2018, 11-12; Reiser, AJP 2018, 816-817; Seiler/Seiler, *sui-generis* 2018, Rz. 31, wobei auch diese Autoren die unmittelbare Begründung von Eigentumsrechten an Kryptowährungen bejahen; ähnlich mit Blick auf die analoge Anwendung sachenrechtlicher Prinzipien Kogens/Luchsinger Gähwiler, Jusletter vom 17. Dezember 2018, Rz. 8 («rivalisierende, fiktive, unkörperliche Gegenstände *sui generis*»), 10 («absolutes Recht besonderer Art»); sodann wohl auch Enz, Kryptowährungen, N 617-626; ferner in diesem Zusammenhang Jutzi/Abbühl, Fintech und DLT, Rz. 110-127, 133, die Token generell als Gegenstand eines absoluten Rechts betrachten und darum im Grundsatz unter Art. 713 ff. ZGB subsumieren; *offenlassend* Schönknecht, GesKR 2016, 309-310; Hürlimann-Kaup, AJP 2018, 1449; ferner Hürlimann-Kaup, in: Emmenegger, 151; *ablehnend, aber differenzierend* hinsichtlich der Zweckmässigkeit des Sachenrechts für gewisse Fragen Meyer, Crypto Tokens, N 465-477; wohl *ablehnend* Gobat, AJP 2016, 1098-1099 («[...] le droit objectif ne confère, du moins pour l'heure, aucun statut et aucune protection.»); vgl. schliesslich für das deutsche Recht Omlor, ZHR 2019, 308.

²⁴⁸³ So etwa Hauser-Spühler/Meisser, digma 2018, 11-12; Reiser, AJP 2018, 816-817; Graham-Siegenthaler/Furrer, Jusletter vom 8. Mai 2017, Rz. 64, 79, 85, 109; implizit wohl auch Meisser/Meisser/Kogens, Jusletter IT vom 24. Mai 2018, Rz. 17-18, 44, 52, welche zwischen Verfügungsmacht über die Vermögenswerte und Verfügungsrecht bzw. -befugnis an den Vermögenswerten unterscheiden. Das Verfügungsrecht richte sich in erster Linie nach der konkreten vertraglichen Abmachung zwischen Wallet-Provider und Kunde und sei für die

ordnung muss je nach Auffassung unmittelbar über die Blockchain erfolgen oder aber kann sich bloss auf ein vom Intermediär geführtes internes Buch bzw. Register stützen.

b. Aussonderbarkeit nach Art. 242a SchKG

Aus Gründen der Rechtssicherheit für u.a. die Verwahrungsindustrie hat der Bundesrat sich für die Einführung einer neuen Bestimmung im SchKG entschieden. Art. 242a SchKG gewährt Kunden von Wallet-Anbietern einen gesetzlichen Anspruch auf Herausgabe «kryptobasierter Vermögenswerte». Der Anspruch erfolgt nach Ansicht des Bundesrates entweder aus dem Gedanken der sachenrechtlichen (Art. 641 Abs. 2 ZGB) oder aber der auftragsrechtlichen (Art. 401 Abs. 3 OR) Aussonderung.²⁴⁸⁴ Kann der Kunde selber über den Vermögenswert verfügen, namentlich weil er Zugriff auf den Private Key hat, so ist eine Herausgabe nicht erforderlich; kann die Konkursverwaltung nicht eigenständig über die Vermögenswerte zugunsten des wirtschaftlich Berechtigten verfügen, so ist eine Herausgabe nicht möglich. Allenfalls kommt in diesem Fall der neue Art. 242b Abs. 1 SchKG zur Anwendung, welcher einer Person, die eine gesetzliche oder vertragliche Berechtigung an den Daten nachweist, einen Anspruch auf Zugang zu diesen vom Konkursiten auf seinen Servern abgespeicherten Daten zusteht.²⁴⁸⁵

In Bezug auf tokenisierte Finanzinstrumente ergibt sich die Aussonderung so- dann bereits aufgrund der materiell-rechtlichen Position des Rechteinhabers (z.B. in seiner Funktion als Aktionär oder Obligationär).²⁴⁸⁶

Der Vorentwurf eines neuen Art. 242a SchKG sah noch vor, dass die individuelle Zuordnung über das verteilte Register zu erfolgen habe, eine rein interne kontenmässige Zuordnung demgegenüber ungenügend sei, was bis anhing der

Zuordnung der Vermögenswerte zu den einzelnen Vermögen massgeblich; ferner Reiser/ Wyss, SZW 2018, 173–174 («pro Nutzer individualisiert und segregiert verwahrt»).

²⁴⁸⁴ Siehe Botschaft DLT 2019, 265, 291–292; ferner Zogg, recht 2019, 120, der das Aussonderungsrecht begrüsst, aber von einem *Novum* spricht, da der Bundesrat davon ausgeht, dass es bitcoins und vergleichbaren «Native Token» an Rechtsobjektsqualität mangelt.

²⁴⁸⁵ Siehe Botschaft DLT 2019, 292; ferner zu diesem Anspruch auf Zugang zu Daten gemäss Art. 242b SchKG ausführlich Botschaft DLT 2019, 295–296.

²⁴⁸⁶ Siehe hierzu Kramer/Wyss, in: Weber/Kuhn, Verwahrung, Rz. 42 m.w.N.

Praxis der FINMA entsprach.²⁴⁸⁷ Dies hätte dazu geführt, dass lediglich die direkt in der Blockchain abgebildeten Vermögenspositionen in Form von Wallet-Adressen von der Aussonderung profitiert hätten.

Der neu eingeführte Art. 242a SchKG sieht in Abs. 2 demgegenüber vor, dass der Anspruch begründet ist, wenn der Gemeinschuldner sich dazu verpflichtet hat, die «kryptobasierten Vermögenswerte» für den Dritten jederzeit bereitzuhalten – d.h. damit keine Aktiv- bzw. Eigengeschäfte²⁴⁸⁸ zu betreiben, was nach Auffassung des Bundesrates zur Entgegennahme von Publikumseinlagen führen würde –²⁴⁸⁹ und diese dem Dritten individuell zugeordnet sind oder aber einer Gemeinschaft zugeordnet sind und dabei ersichtlich ist, welcher Anteil am Gemeinschaftsvermögen dem Dritten zusteht. Kryptobasierte Vermögenswerte auf Sammelkonten sind somit auch «konkursfest» (was allerdings, wie gesehen, nicht mehr indikativ für die Bewilligungspflicht nach BankG ist). Anders als noch im Vorentwurf der Vernehmlassung folgt daraus, dass es nicht mehr notwendig ist, dass die Kryptovermögenswerte eines Kunden unmittelbar über die Wallet-Adresse im *verteilten Register* eines dezentralen Netzwerks individualisiert werden können (on-chain).²⁴⁹⁰ Die Individualisierung bzw. die Zuordnung von Vermögenswerten zu einer Gemeinschaft kann nunmehr auch in einem Register oder über eine entsprechende Kontenstruktur des Intermediärs geschehen (off-chain).²⁴⁹¹ Es ist nach dem Gesagten somit zu rechnen, dass die bisherige Aufsichtspraxis der FINMA zum BankG damit ein Ende findet.

²⁴⁸⁷ Siehe EFD, Erläuternder Bericht DLT-Vernehmlassungsvorlage 2019, 38–39; vgl. auch Bundesrat, DLT-Bericht 2018, 73.

²⁴⁸⁸ Dabei handelt es sich um Geschäfte *im Namen und auf Rechnung* des Wallet-Anbieters; vgl. hierzu oben, [V.4.2b](#).

²⁴⁸⁹ Siehe Botschaft DLT 2019, 266, 292–293; ferner Kramer/Meier, GesKR 2020, 73; Kramer/Wyss, in: Weber/Kuhn, Verwahrung, Rz. 40 («keine Weiterausleihung»); schliesslich mit Blick auf *Staking-Protokolle* Schärli/Meisser/Luthiger, Jusletter IT vom 30. September 2021, Rz. 19–22, 27–29 («Entscheidend ist demnach einzig, dass die Vermögenswerte jederzeit vorliegen und nicht etwa, dass sie jederzeit bewegt werden können.»); ausführlich zum Thema: SBF, Zirkular 2023/01, Fassung vom 5. September 2023, 16–22; Andreotti/Zimmermann/Prantl, GesKR 2023, 338–347; CVA RWG, Staking, 8–10; nunmehr auch FINMA-Aufsichtsmittelteilung 08/2023; noch *abw.* Obrecht, Vortrag EIZ 2023, 21.

²⁴⁹⁰ Siehe Botschaft DLT 2019, 293; vgl. zur diesbezüglich Kritik in der Vernehmlassung EFD, Ergebnisbericht Vernehmlassung DLT 2019, 10; ferner zu den von der FINMA *geäusserten Bedenken* gegenüber der nunmehr übernommenen Regelung Botschaft DLT 2019, 246–247.

²⁴⁹¹ Ausführlich Botschaft DLT 2019, 293; ferner Schärli/Meisser/Luthiger, Jusletter IT vom 30. September 2021, Rz. 24–26; CVA RWG, Custody of Crypto Assets, 7.

c. Absonderbarkeit nach Art. 16 i.V.m. 37d BankG

Wohingegen nicht Einlagen entgegengenommen werden, kann es sich bankeninsolvenzrechtlich um *absonderbare Depotwerte* im Sinne von Art. 16 i.V.m. 37d BankG handeln.

Dabei handelt es sich um eine *lex specialis* zu Art. 242–242a SchKG.²⁴⁹² Zu den Depotwerten gehören bewegliche Sachen und Effekten der Depotkunden, für Rechnung der Depotkunden fiduziarisch gehaltene bewegliche Sachen, Effekten und Forderungen sowie frei verfügbare Lieferansprüche der Bank gegenüber Dritten aus Kassageschäften, abgelaufenen Termingeschäften, Deckungsgeschäften oder Emissionen für Rechnung der Depotkunden. Depotwerte sind nach Art. 37d BankG im Konkurs der Bank absonderbar, d.h., sie werden von Amtes wegen ausgesondert.²⁴⁹³

Die DLT-Revision führte zu einer im Vergleich mit Art. 242a SchKG analogen Ergänzung von Art. 16 BankG. Kryptobasierte *Vermögenswerte*, selbst wenn sie sich als Depotwerte in Sammelverwahrung befinden,²⁴⁹⁴ werden entsprechend von Amtes wegen nach Art. 37d BankG aus dem Konkurs der Bank abgesondert. Gewissermassen analog können nunmehr auch sammelverwahrte kryptobasierte Vermögenswerte nach Art. 16 Ziff. 1^{bis} lit. b i.V.m. 37d BankG abgesondert werden. Soweit tokenisierte Vermögenswerte DLT-Effekten i.S. des FinfraG darstellen, kommt eine Absonderung bereits gestützt auf Art. 16 Ziff. 1 i.V.m. 37d BankG infrage.²⁴⁹⁵

Diese bankeninsolvenzrechtlichen Absonderungsregeln gelten sinngemäss auch für Fondsleitungen und Wertpapierhäuser nach FINIG sowie Finanzmarktinfrastrukturen nach FinfraG.²⁴⁹⁶

d. Fazit

Die Aussonderungs- und Absonderungsregeln gemäss Art. 242a SchKG und Art. 16 Ziff. 1^{bis} i.V.m. 37d BankG sollen nach Absicht des Gesetzgebers aus Kun-

²⁴⁹² Vgl. Art. 34 Abs. 2 BankG; Botschaft DLT 2019, 268, 291; ferner Pulver/Schott, in: Sprecher, Insolvenzrecht für Banken und Effektenhändler, 240–242.

²⁴⁹³ Vgl. Bertschinger, AJP 1995, 432 m.w.N.; ferner zu den Gründen des Absonderungsregimes Jaeger/Hautle, AJP 2009, 400.

²⁴⁹⁴ Vgl. zur Kritik am Vorentwurf, der die Sammelverwahrung noch nicht mitberücksichtigte, EFD, Ergebnisbericht Vernehmlassung DLT 2019, 11–12.

²⁴⁹⁵ Siehe Botschaft DLT 2019, 303; Kramer/Wyss, in: Weber/Kuhn, Verwahrung, Rz. 46.

²⁴⁹⁶ Vgl. Art. 67 FINIG bzw. Art. 88 FinfraG.

denschutzgründen unabhängig davon gelten, ob der Intermediär die Vermögenswerte für den Kunden individuell verwahrt oder sammelverwahrt oder ob er sie für den Kunden auf oder ausserhalb seiner Bilanz hält, solange es sich nicht um Publikumseinlagen handelt. Entscheidend ist demgegenüber vielmehr, dass sich der Intermediär dazu bereit erklärt, die geschuldete Anzahl an Einheiten des Vermögenswerts für den Kunden ständig verfügbar zu halten.²⁴⁹⁷

4.4 Keine Entgegennahme von Publikumseinlagen oder kryptobasierten Vermögenswerten durch dezentrale Handelsplattformen

Ein zentraler Bestandteil der Funktionsweise einer dezentralen Handelsplattform ist der Einsatz von Self-Hosted Wallets. Mit anderen Worten behalten die Nutzer der Plattform grundsätzlich bis zum erfolgreichen Austauschgeschäft die Kontrolle über ihre Kryptovermögenswerte. Eine Drittperson, welche in irgendeiner Form in die Verwahrung involviert sein könnte, existiert grundsätzlich nicht. Auch kann das Kollektiv der Netzwerkteilnehmer nicht als Einlagenschuldner konstruiert werden.²⁴⁹⁸

Entsprechend stellt sich die Frage gar nicht erst, ob eine Drittperson «Verbindlichkeiten gegenüber Kundinnen und Kunden» gemäss Art. 5 Abs. 1 BankV begründet hat. Eine Verbindlichkeit kann auch nicht zwischen den an einem Austauschgeschäft beteiligten Parteien konstruiert werden, soweit eine solche Gegenpartei überhaupt besteht.²⁴⁹⁹ Keine eigentliche Gegenpartei existiert etwa, wenn das Handelsgeschäft gegen den Pool eines Smart Contracts abgewickelt wird. Sodann würde der als Zweiparteiengeschäft geltende und Zugum-Zug abgewinkelte Geldwechsel ohnehin nicht als unterstellungspflichtiges Bankgeschäft qualifizieren.²⁵⁰⁰ Es können mit anderen Worten grundsätzlich gar keine Publikumseinlagen vorliegen. Auch die Frage nach der Aus- bzw. Absonderung von Kryptovermögenswerten im Konkurs des Aufbewahrers stellt sich somit nicht.²⁵⁰¹

²⁴⁹⁷ So Botschaft DLT 2019, 247, 303.

²⁴⁹⁸ Siehe Jacquemart, Offene Blockchainsysteme, Rz. 442.

²⁴⁹⁹ Vgl. Art. 5 Abs. 3 lit. a BankV.

²⁵⁰⁰ Vgl. BGer 2A.218/1999 und 2A.219/1999 vom 5. Januar 2000, E. 3b/bb.

²⁵⁰¹ Vgl. Hürlimann-Kaup, AJP 2018, 1449, wobei die Autorin zwischen «Private Wallet» und «Direct Account» unterscheidet, was nach vorliegender Auffassung keine relevante Abgrenzung darstellt.

In der Praxis werden teilweise Smart Contracts eingesetzt, die Kryptovermögenswerte zwecks Ausführung und Abwicklung eines Austauschgeschäfts vorübergehend halten. Dies ist etwa der Fall bei Plattformen wie EtherDelta. Smart Contracts solcher Art implementieren eine Form von «Abwicklungs- oder Rückzahlungsfunktionalität», weshalb sie «Berührungspunkte mit dem Bankenrecht» aufweisen können.²⁵⁰² Die Situation ist vergleichbar mit den «idealtypischen» Crowdfunding-Plattformen, welche lediglich die Mittel zwischen Darlehensgeber und Darlehensnehmer vermitteln.²⁵⁰³ Allerdings kommt vorliegend hinzu, dass Softwarecode den Betreiber der Crowdfunding-Plattform ersetzt. Software alleine kann allerdings nicht dem auf personale und institutionelle Intermediation beruhenden Bankenrecht unterstellt werden.

Zudem kann im Fall von EtherDelta ausschliesslich diejenige Person, welche den entsprechenden Private Key hat, die von einem Smart Contract gehaltenen Vermögenswerte wieder aus dem Smart Contract zurückziehen. Weder der Smart Contract noch eine Drittperson (z.B. der Entwickler der Plattform) können dagegen über die Vermögenswerte verfügen; sie können somit gar nicht erst eine Verpflichtung zur Rückzahlung im Sinne der Rechtsprechung des Bundesgericht eingehen. Die Situation gleich somit eher dem Schliessfachgeschäft einer Bank als dem klassischen bilanzdifferenten Banktätigkeit. In letzterem Rahmen erhält die Bank nicht nur die ausschliessliche Verfügungsmacht bzw. Besitz über die eingebrachten Vermögenswerte, sondern erwirbt auch das Eigentum an ihnen. Die Entgegennahme von Vermögenswerten im Rahmen eines Schrankfachvertrages erfüllt demgegenüber den Einlagebegriff nicht, da die Bank rechtlich betrachtet keine Verfügungsmacht bzw. Sachherrschaft über den Schrankfachinhalt erlangt.²⁵⁰⁴

Ein Bedürfnis nach Schutz der Nutzer vor dem Konkurs einer Person besteht im Rahmen der Nutzung dezentraler Handelsplattformen mangels Intermediationstätigkeit grundsätzlich nicht.²⁵⁰⁵ Die Vermögenswerte bleiben jederzeit

²⁵⁰² Siehe FINMA, Jahresbericht 2018, 32.

²⁵⁰³ Siehe hierzu Hettich, GesKR 2013, 393; Kunz, Jusletter vom 25. August 2014, Rz. 34; sodann FINMA, Faktenblatt Crowdfunding, 1 («Der Betrieb von Crowdfunding-Plattformen, bei welchen die Gelder direkt von den Projektfinanzierern an die Projektentwickler fliessen, unterliegt grundsätzlich keiner finanzmarktrechtlichen Bewilligungspflicht.»).

²⁵⁰⁴ Vgl. zum Eigentumsübergang Schönknecht, GesKR 2016, 309–310; ausführlich Kleiner/Müller, in: Zobl et al., Kommentar BankG, Art. 16 N 9; BSK BankG-Hess/Zbinden, Art. 16 N 13.

²⁵⁰⁵ Vgl. zur Frage der Unterstellung einer intermediären Tätigkeit in einem P2P-Zahlungssystem unter das BankG BGer 2C_345/2015 vom 29. März 2016, E. 8.1 und 8.3.2.1.

den einzelnen Nutzern individuell und unmittelbar über den Smart Contract bzw. das verteilte Register zuordenbar, womit selbst den strengerer Anforderungen der alten FINMA-Praxis Genüge getan wäre.²⁵⁰⁶

Das bisher Gesagte gilt grundsätzlich auch für kryptobasierte Vermögenswerte. Das vorübergehende Halten von *kryptobasierten Vermögenswerten* in einem Smart Contract könnte gegebenenfalls aber dann bankenrechtlich relevant sein, wenn der Smart Contract in massgeblicher Weise von einer Drittperson kontrolliert würde.²⁵⁰⁷ Problematisch könnte namentlich die Situation sein, in welcher eine Drittperson über Admin Keys verfügt, welche ihr die Verfügungsmacht über die im Smart Contract abgelegten Vermögenswerte der Nutzer einräumen. Ein gesteigertes Betrugs- und Veruntreuungsrisiko bestünde ferner, wenn die Drittperson sich gegenüber den Nutzern des Smart Contracts nicht verbindlich dazu bereit erklären würde, die Vermögenswerte für sie *jederzeit* bereitzuhalten. Solche Konstellationen sind bei dezentralen Handelsplattformen aber typischerweise gerade nicht gegeben. Ungeachtet dessen stellt sich aber auch die Frage, ob Token, die von einem Smart Contract gehalten werden, tatsächlich als «sammelverwahrt» im Sinne von Art. 5a Abs. 1 BankV i.V.m. Art. 16 Ziff. 1^{bis} lit. b BankG gelten können, was mit Blick auf die Unterstellung unter das BankG zentral ist (s. oben). Vorbehalten bleibt schliesslich auch die Abwicklungsausnahme für Kundenkonten in Art. 5a Abs. 2 lit. a BankV.

Anders stellte sich die rechtliche Situation im Falle der zentralisierten digitalen Währung E-Coins dar: Die FINMA leitete gegen drei juristische Personen ein Enforcementverfahren wegen Verstosses gegen das Bankengesetz ein, nachdem die beteiligten Personen zusammen eine internetbasierte Handelsplattform für die Ausgabe, den Austausch und die Übertragung der von ihnen kontrollierten Währungseinheiten betrieben hatten. Hier mangelte es den Besitzern von E-Coins an der Möglichkeit, ohne Mitwirkung der Emittenten über die «Token» zu verfügen.²⁵⁰⁸

²⁵⁰⁶ Siehe zu diesem Erfordernis oben, [V.4.2a.ii.](#)

²⁵⁰⁷ Demgegenüber handelt es sich in diesen Fällen nicht um Publikumseinlagen, solange die Nutzer ihrerseits weiterhin durch Zugriff auf den Smart Contract ihre Vermögenswerte zurückziehen können. In diesem Sinne besteht zwischen den Konzepten der «Kontrolle» und der «Publikumseinlage» ein enger Zusammenhang; vgl. auch CVA RWG, Custody of Crypto Assets, 5.

²⁵⁰⁸ Siehe FINMA, Scheinkryptowährungen, 1; ausführlich zum Sachverhalt BVGer B-5769/2017 vom 21. Januar 2019, E. 3.1; BVGer B-6413/2017 vom 21. Januar 2019, E. 5.1.

Eine vergleichbare Diskussion wird in den USA mit Blick auf die einzelstaatlichen Gesetze betreffend Zulassung von Personen geführt, welche das Geld- und Wertübertragungsgeschäft für ihre Kunden durchführen (*State Money Transmission Licenses*). Diese Gesetze weisen aufsichtsrechtliche Regeln auf, welche – ähnlich wie das schweizerische Bankenrecht – in erster Linie dem Schutz von Konsumenten vor Verlusten dienen.²⁵⁰⁹ Im Wesentlichen qualifizieren gemäss diesen Regeln als Money Transmitters Unternehmen, welche Vermögenswerte von Kunden annehmen und diese allenfalls an Dritte weiterleiten, wobei sie in diesem Rahmen Kontrolle über die Vermögenswerte erlangen, oder diese gegen andere Vermögenswerte tauschen.²⁵¹⁰ Dabei fokussiert sich die Diskussion u.a. auf die Rolle von Teilnehmern im Lightning Netzwerk.²⁵¹¹ COIN CENTER argumentiert etwa, dass dort, wo Drittpersonen keine alleinige Verfügungsmacht bzw. Kontrolle über die Vermögenswerte der an einer Transaktion beteiligten Personen innehaben, kein Bedürfnis für die Anwendbarkeit solcher Gesetze besteht.²⁵¹² Auch gemäss dieser sehr ähnlichen Sichtweise fallen dezentrale Handelsplattformen – genauso wie Non-Custodial Wallet-Anbieter und Teilnehmer am Bitcoin oder Lightning Netzwerk –²⁵¹³ nicht in den Anwendungsbereich der Bankenregulierung.

²⁵⁰⁹ Siehe CSBS, Model Regulatory Framework, 10; ferner Santori, Money Transmission, *passim*.

²⁵¹⁰ Siehe Van Valkenburgh, Need for a Federal Alternative to State Money Transmission Licensing, 6.

²⁵¹¹ Siehe Agrawal, Lightning network nodes and money transmission licensing, *passim*.

²⁵¹² Siehe Van Valkenburgh, Uniform Law Commission, *passim* («Under the ULC model act, that gray area is totally eliminated. It is clearly spelled out that licensure is only required of companies that have control of a customer's cryptocurrency, with control defined as the 'power to execute unilaterally or prevent indefinitely a virtual currency transaction.'»); ausführlich hierzu ULC, Uniform Regulation of Virtual-Currency Businesses Act, *passim*; zustimmend Miraz/Donald, ICISDM 2019: Proceedings of the 2019 3rd International Conference on Information System and Data Mining 2019, 187.

²⁵¹³ Ausführlich zu Lightning Andreotti, Teil 2, iusNet BR-KR 22.12.2022, *passim*. Der im November 2020 in den USA propagierte STABLE Act, der vorschreibt, dass Stablecoins nur von Banken herausgegeben werden dürfen, würde je nach Interpretation des weiten Wortlauts auch Full Node-Betreiber in Ethereum und in anderen dezentralen Netzwerken für illegal erklären; vgl. hierzu Van Valkenburgh, STABLE Act, *passim*.

5. Finanzinstitutsrecht

5.1 Einleitung

Der Handel mit *Effekten* ist unter gewissen Umständen prudenziell beaufsichtigten Personen vorbehalten (Art. 5 Abs. 1 i.V.m. Art. 2 Abs. 1 lit. e FINIG). Diese werden seit der Einführung des Finanzinstitutsgesetzes (FINIG) sowie der dazugehörigen Finanzinstitutsverordnung (FINIV) nicht mehr als Effektenhändler²⁵¹⁴, sondern als Wertpapierhäuser bezeichnet.

Zweck des FINIG – wie bereits im BEHG und KAG – sind der Schutz von Anleger sowie Kunden von Finanzinstituten und die Gewährleistung der Funktionsfähigkeit des Finanzmarkts (Art. 1 Abs. 2 FINIG).²⁵¹⁵ Nach Auffassung des Gesetzgebers legt das FINIG die Anforderungen an Finanzinstitute fest, die im Rahmen ihrer Geschäftstätigkeit Vermögenswerte von Drittpersonen anlegen und verwalten.²⁵¹⁶ Im Zentrum steht dabei weniger der – bankengesetzliche – Schutz vor dem Risiko einer Insolvenz oder Illiquidität der Gegenpartei als vielmehr der Schutz des Kunden vor Übervorteilung und Missbräuchen durch den Vertragspartner und allenfalls der Schutz des Anlegers vor unlauterem Verhalten von Emittenten und anderen Marktteilnehmern.²⁵¹⁷

5.2 Effektenhandel

a. Im Allgemeinen

Als dem FINIG unterstellte Finanzinstitute gelten u.a. Wertpapierhäuser (Art. 2 Abs. 1 lit. e FINIG).

²⁵¹⁴ Vgl. insb. Art. 2 lit. d aBEHG und Art. 2–3 aBEHV.

²⁵¹⁵ Siehe Botschaft BEHG 1993, 1381–1382; Botschaft FINMAG 2006, 2859; vgl. ferner den Wortlaut von Art. 1 aBEHG; sodann BVGer B-1215/2009 vom 9. November 2010, E. 4.2.6.2; Zobl, in: Hertig et al., Kommentar BEHG, Art. 1 N 12–24; OFK BEHG-Weber, Art. 1 N 2–6; BSK BEHG/FINMAG-Watter, Art. 1 BEHG N 9, 14, der allerdings den Hauptfokus des BEHG im Anlegerschutz sieht; BSK KAG-Winzeler, Art. 1 N 13–15.

²⁵¹⁶ Siehe Botschaft FIDLEG/FINIG 2015, 9017.

²⁵¹⁷ Siehe Botschaft BEHG 1993, 1381–1382.

Als Wertpapierhaus gelten nach Art. 41 FINIG Personen, die gewerbsmässig in eigenem Namen für Rechnung von Kunden Effekten handeln und direkt oder indirekt für mehr als 20 Kunden Konten führen oder Effekten aufbewahren (*Kundenhändler*).²⁵¹⁸ Personen, die gewerbsmässig für eigene Rechnung kurzfristig mit Effekten handeln, hauptsächlich auf dem Finanzmarkt tätig sind und dadurch die Funktionsfähigkeit des Finanzmarkts gefährden könnten, sind nur erfasst, sofern ihre Effektenhandelsgeschäfte ein Gesamtvolumen von fünf Milliarden Franken pro Kalenderjahr in der Schweiz überschreiten (*Eigenhändler*).²⁵¹⁹ Ferner gelten als Eigenhändler Personen, die als Mitglied eines Handelsplatzes tätig sind oder ein organisiertes Handelssystem betreiben.²⁵²⁰ Sodann sind auch Personen bewilligungspflichtig, die gewerbsmässig für eigene Rechnung kurzfristig mit Effekten handeln und öffentlich dauernd oder auf Anfrage Kurse für einzelne Effekten stellen (*Market Maker*).²⁵²¹

Mit Blick auf den Primärmarkt ist schliesslich Art. 12 FINIG relevant. Die Bestimmung legt fest, dass Personen eine Bewilligung als Wertpapierhaus – oder Bank – bedürfen, wenn sie gewerbsmässig Effekten, die von Drittpersonen ausgegeben werden, übernehmen und auf dem Primärmarkt öffentlich anbieten (*Emissionshaus*) oder gewerbsmässig Derivate in Form von Effekten schaffen und auf dem Primärmarkt öffentlich anbieten (*Derivathaus*). Solche Personen müssen ausserdem «hauptsächlich im Finanzbereich» tätig sein. Ob ein öffentliches Angebot vorliegt, bestimmt sich nach den entsprechenden Bestimmungen im FIDLEG.²⁵²² Art. 12 FINIG betrifft lediglich Primärmarktgeschäfte, weshalb die Bestimmung für den Handel von Kryptovermögenswerten nicht im Mittelpunkt steht.²⁵²³

Anders als das Wertpapierhaus knüpfen Vermögensverwalter und Verwalter von Kollektivvermögen nach Art. 17 Abs. 1 bzw. Art. 24 FINIG an den Begriff des Vermögenswerts an. Es müssen mit anderen Worten weder Effekten noch Finanzinstrumente nach FIDLEG vorliegen, so dass bereits die gewerbsmässige Vermögensverwaltung von Kryptowährungen und Zahlungs-Token dem FINIG unterstellt sein dürfte, sofern diesen der Charakter einer Finanzanlage zukommt.²⁵²⁴

²⁵¹⁸ Art. 41 lit. a FINIG i.V.m. Art. 65 Abs. 1 FINIV.

²⁵¹⁹ Art. 41 lit. b Ziff. 1 FINIG i.V.m. Art. 65 Abs. 4 FINIV.

²⁵²⁰ Art. 41 lit. b Ziff. 2 und 3 FINIG.

²⁵²¹ Art. 41 lit. c FINIG i.V.m. Art. 65 Abs. 6 FINIV.

²⁵²² Art. 14 Abs. 1 FINIV.

²⁵²³ Vgl. Bundesrat, DLT-Bericht 2018, 100.

²⁵²⁴ Siehe Bundesrat, DLT-Bericht 2018, 119; ferner zum Begriff des Vermögenswerts Botschaft FIDLEG/FINIG 2015, 8943.

b. Kein Effektenhandel durch dezentrale Handelsplattformen

Das Gesetz knüpft an den Begriff des Finanzinstituts gemäss Art. 2 Abs. 1 FINIG an. Geschützt werden sollen in erster Linie die Kunden (und Gläubiger) eines Finanzinstituts, aber auch die Anleger von kollektiven Kapitalanlagen im Vermögensverwaltungsgeschäft eines Verwalters von Kollektivvermögen oder einer Fondsleitung.²⁵²⁵ Damit liegt dem FINIG offensichtlich das Konzept der personalen und institutionellen Intermediation zugrunde. Kontroll- und Vertrauensrisiken sind für die Anwendung des FINIG entsprechend vorauszusetzen.

Zwingend für das Vorliegen eines unterstellten Kundenhandels ist, dass es sich bei den gehandelten Kryptovermögenswerten um *Effekten* handelt. Zu den Begriffen der Effekte und der DLT-Effekte sei auf die bereits gemachten Ausführungen verwiesen.²⁵²⁶

Über eine dezentrale Handelsplattform lassen sich Token, die als Effekten qualifizieren, handeln. Inzwischen sind tatsächlich tokenisierte Aktien von einigen Schweizer Gesellschaften über Uniswap und andere Plattformen handelbar.²⁵²⁷ Eine dezentrale Handelsplattform ist dabei in aller Regel nicht in der Funktion eines Wertpapierhauses tätig. Namentlich fungiert sie nicht als Kundenhändlerin der unterschiedlichen Nutzer, wie es regelmässig bei der Internalisierung von Kundenaufträgen durch einen Finanzintermediär der Fall ist.²⁵²⁸ Es kann somit nicht davon gesprochen werden, dass die Plattform in eigenem Namen auf Rechnung der von ihr vertretenen Nutzer auftritt, wobei diese das wirtschaftliche Risiko der von der Plattform getätigten oder in Auftrag gegebenen Effektengeschäfte selbst tragen.²⁵²⁹ Zwischen der Plattform und dem Kunden kann gerade kein vertragliches Verhältnis bestehen, das in traditionellen Märkten typischerweise als Kommissionsgeschäft qualifiziert.²⁵³⁰ Dies ist dort gut ersichtlich, wo Nutzer einer dezentralen Handelsplattform ihre Gegenpartei selbst auszuwählen haben. Dies gilt sodann auch für Plattformen mit automatisiertem Matching.

²⁵²⁵ Siehe Botschaft FIDLEG/FINIG 2015, 9017.

²⁵²⁶ Siehe oben, [V.3.2b](#).

²⁵²⁷ Vgl. etwa die Aufstellung auf <https://aktionariat.com/>.

²⁵²⁸ Siehe Zobl/Kramer, Kapitalmarktrecht, Rz. 1225, 1234; BSK OR I-Lenz/von Planta, Art. 436 N 2; Abegglen/Andreotti, GesKR 2020, 38, 52.

²⁵²⁹ Siehe hierzu das inzwischen aufgehobene FINMA-RS 08/5 «Effektenhändler», Rz. 50.

²⁵³⁰ Vgl. hierzu etwa BGE 133 III 221, E. 5.1; ferner Abegglen/Andreotti, GesKR 2020, 37 m.w.N.

Schliesslich kann auch nicht davon gesprochen werden, dass die Plattform im Sinne von Art. 44 Abs. 1 lit. a und b FINIG Konten für die Nutzer führt oder deren Effekten aufbewahrt. Die Verwahrung der Anlage-Token erfolgt entweder über ein Self-Hosted Wallet des Nutzers (z.B. MetaMask) oder über das Hosted Wallet eines Kundenhändlers (siehe sogleich).

c. Kundenhändler

Eine dezentrale Handelsplattform ist demgegenüber analog zu traditionellen Handelsplattformen ein Ort, wo *Kundenhändler* gewerbsmässig in eigenem Namen für Rechnung von Kunden Kryptovermögenswerte, die als Effekten qualifizieren, handeln können. Diese Personen fallen bei Vorliegen der übrigen Bedingungen ohne Weiteres unter das FINIG,²⁵³¹ denn der Begriff des Kundenhändlers unterscheidet nicht nach der Art der Plattform, über welche die Effekten gehandelt werden (wenn auch aufgrund des Effektenbegriffs in erster Linie Börsen, MHS, DLT-Handelssysteme und OHS infrage kommen).

Die Kunden des Wertpapierhauses sind in diesem Fall analog zur indirekten Teilnahme an einem Handelsplatz lediglich indirekte Nutzer einer DeFi-Applikation. Kein unterstellungspflichtiger Kundeneffektenhandel stellt jedoch die reine Verwahrung von Anlage-Token dar, die Rücküberweisung durch den Verwahrer an den Kunden oder im Grundsatz auch die Weiterleitung durch den Verwahrer an einen Dritten im Namen des Kunden.²⁵³²

d. Market Maker

Offen ist, ob Nutzer, welche der Plattform Liquidität zuführen, bei Vorliegen der entsprechenden Bedingungen als *Market Maker* qualifizieren können. Voraussetzung dafür ist, dass eine Person (i) gewerbsmässig für eigene Rechnung (ii) kurzfristig mit Effekten handelt und (iii) öffentlich dauernd oder auf Anfrage Kurse für einzelne Effekten stellt. Dabei unterscheiden Gesetz und Praxis grundsätzlich nicht, ob die Effekten von Dritten oder vom Market Maker selbst ausgegeben werden oder ob der Market Maker direkten Zugang zum betreffenden Handelssystem hat.²⁵³³

²⁵³¹ So auch Bundesrat, DLT-Bericht 2018, 121.

²⁵³² Siehe Bundesrat, DLT-Bericht 2018, 121.

²⁵³³ Siehe Wicki, Market Making eigener Aktien, 32.

Gemäss Art. 65 Abs. 6 FINIV stellt eine Person Kurse *öffentlich*, wenn sie nach Art. 3 lit. g und h FIDLEG Teil eines Angebots sind, das sich an das Publikum richtet. Nach Art. 3 Abs. 7 FIDLEV hat sich ein solches Angebot an einen unbegrenzten Personenkreis zu richten, damit es als öffentlich gilt. Bei dezentralen Handelsplattformen, die über eine webbasierte Benutzeroberfläche im Internet frei zugänglich sind, ist regelmässig von einem öffentlichen Angebot im Sinne der oben erwähnten Bestimmung auszugehen.²⁵³⁴ Denkbar ist, dass ein Market Maker auf einer Handelsplattform aktiv ist, welche lediglich einen begrenzten Personenkreis zum Handel zulässt, weshalb die Kursstellung des Market Makers als nicht öffentlich gilt.²⁵³⁵ Offen ist allerdings, ob in diesem Fall noch von einer dezentralen Handelsplattform gesprochen werden kann.

Andererseits muss der Market Maker die Tätigkeit *gewerbsmässig* ausüben. Das Kriterium der Gewerbsmässigkeit ist gegeben, wenn eine selbstständige, auf dauernden Erwerb ausgerichtete wirtschaftliche Tätigkeit vorliegt (Art. 3 FINIG). Klar ist, dass ein Liquiditätsgeber, der keine Handelsgebühren vereinbart oder keinen sonstigen Ertrag aus dem Spread generiert, mangels Gewerbsmässigkeit keine unterstellungspflichtige Tätigkeit ausübt. So kann ein Emittent seine eigenen Aktien bewilligungsfrei über eine entsprechende dezentrale Handelsplattform anbieten, solange mit der Tätigkeit keine oder aber im Vergleich zur Haupttätigkeit des Emittenten bloss geringfügige Einnahmen verbunden sind.²⁵³⁶ Dies ist in Einklang mit der kapitalmarktrechtlichen Praxis, wonach ein Emittent, der zudem die aktienrechtlichen Vorschriften²⁵³⁷ und Marktverhaltensregeln²⁵³⁸ einzuhalten hat, bewilligungsfrei seine eigenen Aktien am Sekundärmarkt handeln kann, weil er dadurch die Liquidität am Markt zu erhöhen beabsichtigt.²⁵³⁹

²⁵³⁴ Siehe zum Angebotsbegriff unten, [V.6.3a](#).

²⁵³⁵ Vgl. diesbezüglich etwa Thurman, *Permissioned Pool*, Cointelegraph, *passim*; vgl. ausführlich zum Konzept von Permissioned Pools Aave, Arc, 3; ferner Aave, *Introducing Aave Arc*, *passim*.

²⁵³⁶ GLM. SBF, Circular 2020/01, 13 («This criterion [professional capacity] is not met, and hence no licensing requirement applies, if market making is undertaken merely in an ancillary, supportive capacity and does not constitute an independent business line aimed at generating income on a regular basis.»), 12; ferner Weber, in: Weber/Kuhn, *Handel mit digitalen Aktiven*, Rz. 125.

²⁵³⁷ Siehe Art. 659–659b OR hinsichtlich Erwerb und Halten eigener Aktien.

²⁵³⁸ Art. 143 und 155 FinfraG.

²⁵³⁹ Siehe Hertig/Schuppisser, in: Hertig et al., *Kommentar BEHG*, Art. 2 lit. b N 32; FINMA-Mitteilung 52 (2013), *passim*; vgl. ferner Böckli, *Schweizer Aktienrecht*, 5. Aufl., § 4 Rz. 80 (offenbar aber noch grosszügiger Böckli, *Schweizer Aktienrecht*, 4. Aufl., § 4 Rz. 382); von der Crone, *Aktienrecht*, § 13 N 559; Handschin, in: ZK OR, Art. 659–659b N 49; a.M. offen-

Nachfolgend ist allerdings ein Vorbehalt anzubringen: Einige der untersuchten dezentralen Handelsplattformen sehen zwecks Incentivierung der Liquiditätsaufbringung eine Handelsgebühr oder dergleichen vor, welche den Bereitstellern der Liquidität automatisch gutgeschrieben wird. Ein Liquiditätsgeber auf Uniswap erhält die Handelsgebühr etwa in Form von Liquiditätstoken, welche bei Beendigung der Bereitstellung automatisch in die Token des betreffenden Pools konvertiert und an den Liquiditätsgeber ausbezahlt werden. Geringfügige Einnahmen im Vergleich zur Haupttätigkeit des Emittenten sind nach vorliegender Auffassung noch vertretbar, handelt es sich beim Incentivierungsmechanismus doch um eine technische Komponente, auf welche der Liquiditätsbereitsteller oft keinen direkten Einfluss nehmen kann. Der Emittent könnte sodann den verdienten Spread auch an die Nutzer der Handelsplattform zurückübertragen. Protokolle könnten schliesslich ohne Weiteres auf einen solchen Mechanismus verzichten.²⁵⁴⁰

Demgegenüber unproblematisch dürften Handelslösungen sein, welche der Emittent selbst auf seiner Webseite betreibt, wie insb. ein *Share Dispenser*, und in dessen Rahmen er bilaterale Austauschgeschäfte abschliesst.²⁵⁴¹ Hier hat der Emittent als Betreiber der Handelslösung sowie als Gegenpartei aller Transaktionen die Möglichkeit, gänzlich auf Handelsgebühren zu verzichten.

Die ursprüngliche Motivation für die Unterstellung von Market Makern unter das Börsengesetz scheint mit Blick auf dezentrale Handelsplattformen nicht mehr gleichermassen gegeben zu sein: Historisch wurden Market Maker – als besondere Ausprägung des Eigenhändlers – primär aus Funktionsschutzgründen dem BEHG unterstellt, namentlich weil sie bedeutende Effekturnumsätze realisieren und aufgrund ihrer Tätigkeit für die Integrität und Funktionsfähigkeit einer Börse zentral sind.²⁵⁴² Offensichtlich ist, dass Liquiditätsgeber mit ihrer Tätigkeit nicht bloss die langfristig orientierte Verwaltung ihres eigenen Vermögens und somit ausschliesslich einen Anlagezweck verfolgen.²⁵⁴³ Im Ge-

bar Arter/Jörg, AJP 2001, 55 FN 32, die nicht ausschliessen, dass *unterstelltes* Market Making bei Angebot und Kursstellung über eine Webseite vorliegen könnte.

²⁵⁴⁰ In Uniswap wäre dafür offenbar ein Governance-Entscheid der DAO notwendig; vgl. Adams et al., Uniswap v3, 3. Alternativ könnte auch der Softwarecode von Uniswap geforked werden.

²⁵⁴¹ Dies ist etwa möglich mit dem *BrokerBot* der Aktionariat AG; vgl. Aktionariat, *Brokerbot*, *passim*. Der *Share Dispenser* wurde ursprünglich von Alethena entwickelt; vgl. Alethena, *Share-Dispenser-ServiceHunter*, GitHub, *passim*.

²⁵⁴² Vgl. Botschaft BEHG 1993, 1381–1382, 1397.

²⁵⁴³ Vgl. hierzu FINMA-RS 08/5 «Effekthändler», Rz. 19; Roth, in: Hertig et al., Kommentar BEHG, Art. 2 lit. d N 12; OFK BEHG-Weber, Art. 2 lit. d N 13; OFK FIDLEG/FINIG-Vogel/Heiz/Luthiger, Art. 41 FINIG N 22.

genteil beabsichtigen Liquiditätsgeber gerade die laufende Stellung von Geld- und Briefkursen, woraus sich je nach Protokoll ein Gewinn für sie ergeben kann. Allerdings erfolgt ihre Tätigkeit anders als diejenige von Market Makern auf traditionellen Handelsplätzen, welche sich regelmässig vertraglich zu diesem Verhalten verpflichten (z.B. gegenüber einem börsenkotierten Emittenten), in aller Regel auf rein freiwilliger Basis.²⁵⁴⁴ Ein Rückzug aus dem Markt ist jederzeit möglich und kann rechtlich auch nur bedingt eingeschränkt werden. Ausserdem können traditionelle Market Maker über die Grösse des Spreads ihr Risiko beschränken, was im AMM-Modell für viele Handelspaare nicht möglich zu sein scheint.²⁵⁴⁵ Die Motivation hinter der Liquiditätsbereitstellung über eine dezentrale Handelsplattform kann sehr unterschiedlicher Natur sein, wie etwa die Schaffung eines Sekundärmarktes durch den Emittenten für seine illiquiden Titel.

Fraglich ist schliesslich, ob die Tätigkeit von Liquiditätsgebern tatsächlich immer *kurzfristiger* Natur ist: Der Begriff der Kurzfristigkeit bezieht sich nach Auffassung der FINMA zum ehemaligen Börsengesetz auf das mit dem Erwerb von Effekten verfolgte Ziel, nämlich deren aktive Bewirtschaftung, um innerhalb kurzer Fristen aus Veränderungen von Kursen oder Zinsen Gewinne zu erzielen.²⁵⁴⁶ Zumindest in den meisten Ausprägungen des AMM-Modells fehlt es allerdings an einer aktiven Bewirtschaftung des Handelspaares.²⁵⁴⁷ Die konkrete Preisstellung ist der Berechnungsformel des Protokolls überlassen bzw. abhängig von der Effektivität von Arbitragestrategien anderer Marktteilnehmer. Ein Vorbehalt könnte allerdings dann gelten, wenn der Liquiditätsgeber mit Effektenhandelsgeschäften mehr als 5 Mrd. Schweizer Franken Handelsvolumen pro Kalenderjahr in der Schweiz generiert, womit er bei Vorliegen der übrigen Bedingungen als bewilligungspflichtiger *Eigenhändler* qualifizieren könnte. In diesem Fall würde es keines technischen Market Makings bedürfen. Allerdings setzt Art. 41 lit. b FINIG auch in diesem Fall die Kurzfristigkeit der Effektenhandels voraus.

Noch am ehesten mit traditionellem Market Making vergleichbar ist darum die Liquiditätsstellung über eine Plattform mit Orderbuch. Dasselbe gilt bei Kursstellung auf Anfrage, wie es typischerweise im auftragsgesteuerten RFQ-Modell von Kyber Network oder Ox der Fall ist. In diesen Fällen kontrahieren

²⁵⁴⁴ Vgl. die Auffassung der FINMA eines idealtypischen Market Makers BGer 2C_315/2020, E. 7.3.4; ferner zum Market Making Zobl/Kramer, Kapitalmarktrecht, Rz. 1100.

²⁵⁴⁵ Siehe etwa die Untersuchung in Heimbach/Wang/Wattenhofer, Behavior of Liquidity Providers, 7–9, welche nach Pool-Kategorien differenzieren.

²⁵⁴⁶ Vgl. FINMA-RS 08/5 «Effektenhändler», Rz. 44 i.V.m. 22.

²⁵⁴⁷ GLM. SBF, Circular 2020/01, 13, 16; a.M. Meirich, Decentralized Finance, Rz. 1053–1069.

die beteiligten Parteien direkt miteinander. Demgegenüber ist die direkte Interaktion der Handelspartner beim Market Making im AMM-Modell technisch ausgeschlossen. Aus Anlegerschutzgründen besteht folglich in diesem Fall kein Bedürfnis für eine Unterstellung unter das FINIG.²⁵⁴⁸ Zumindest in Bezug auf Liquiditätsgeber, welche über dezentrale Handelsplattformen mit solchen Matching-Mechanismen tätig sind, wäre es nach dem Gesagten wünschenswert, dass diese Personen *de lege ferenda* ausdrücklich nicht als Market Maker gemäss Art. 41 lit. c FINIG qualifizieren.

e. Initial Decentralized Exchange Offering (IDO)

Bei *Initial Exchange Offerings* (IEOs) handelt es sich nach allgemeiner Auffassung um die Durchführung eines ICOs oder STOs *direkt* über eine Kryptohandelsplattform. Dabei unterstützt der Betreiber der Plattform den Emittenten des Token im Rahmen der Emission und Platzierung der Token bei den Kunden der Plattform sowie allenfalls im Rahmen des Handels der Token auf der Plattform.²⁵⁴⁹ Emittenten führen IEOs typischerweise über zentrale Kryptohandelsplattformen zwecks Kapitalaufnahme oder Crowdfunding eines Projekts durch.²⁵⁵⁰ Es handelt sich dabei um Primärmarktgeschäfte.

Initial Decentralized Exchange Offerings bzw. Initial DEX Offerings (IDOs) können als Weiterentwicklung des IEO-Emissionsmodells betrachtet werden. In solchen Fällen lanciert ein Emittent seinen Token (z.B. eine Aktie) direkt über eine dezentrale Handelsplattform.²⁵⁵¹ Im Falle einer Aktienemission könnte dies bspw. durch originäre Zeichnung der Aktien im Rahmen einer Kapitalerhöhung erfolgen,²⁵⁵² welche sodann im eigenen Namen auf eigene Rechnung über einen Liquiditätspool zum Verkauf bereitgestellt werden.²⁵⁵³ Die Verwendung eines Auktionsmechanismus mit einheitlichem Markträumungspreis könnte sich besonders gut für die Markteinführung von Aktien eignen. Dies würde allen künftigen Aktionären ermöglichen, die Beteiligung zum selben Preis zu erwerben.²⁵⁵⁴ Bei einem IDO über eine dezentrale Handelsplattform

²⁵⁴⁸ Vgl. zum Anlegerschutz beim Market Making Roth, in: Hertig et al., Kommentar BEHG, Art. 2 lit. d N 14 m.w.H.

²⁵⁴⁹ Siehe strategy&/PwC/CVA, 6th ICO / STO Report, 2.

²⁵⁵⁰ Siehe etwa Bitfinex, Bitfinex Token Sales, *passim*.

²⁵⁵¹ Vgl. zum Konzept Harvey/Ramachandran/Santoro, DeFi, 62.

²⁵⁵² Zur Zulässigkeit der *originären* Zeichnung eigener Aktien durch die Gesellschaft BSK OR II-Lenz, Art. 659 N 4 m.w.N.; ferner Handschin, in: ZK OR, Art. 659-659b N 25.

²⁵⁵³ Siehe für ein Bsp. über Uniswap UMA, Initial Uniswap Listing, Medium, *passim*.

²⁵⁵⁴ Siehe zum Niederländischen Auktionsmodell sowie zum Frequent-Batch-Auction-Modell oben, [IV.4.2c](#).

ist lediglich der Emittent auf der einen und die Tokenerwerber auf der anderen Seite involviert. Es fehlt an einem eindeutig identifizierbaren Betreiber der Plattform. In diesem Sinne stellen IDOs durch Emittenten eine neue Gestaltungsmöglichkeit der aufsichtsrechtlich grundsätzlich nicht unterstellten Eigen- bzw. Selbstemission dar.²⁵⁵⁵

Offen ist allerdings, ob es sich aufgrund des vorab getätigten originären Erwerbs der Aktien durch die Gesellschaft überhaupt noch um ein Primärmarktgeschäft handelt. In Anlehnung an die Lehrmeinungen zur Festübernahme und anschließenden Platzierung von Effekten im Publikum sollten IDOs, denen ein originärer Erwerb durch den Emittenten vorausgeht, dem Primärmarkt zugeordnet werden.²⁵⁵⁶ Dies kann sich entsprechend auf die Prospektpflicht nach FIDLEG auswirken (s. unten). Ausnahmen von einer bewilligungsfreien Emission bestehen sodann bei Festübernahmen von Effekten durch Banken oder Wertpapierhäuser vom Emittenten (Art. 12 lit. a FINIG) sowie bei der Schaffung von Derivaten in Form von Effekten und deren Emission auf dem Primärmarkt (Art. 12 lit. b FINIG).

²⁵⁵⁵ Vgl. BGE 136 II 43, E. 7.3.1; BGer 2C_571/2018 vom 30. April 2019, E. 4.3; ferner FINMA, Wegleitung ICOs, 5.

²⁵⁵⁶ Vgl. zur Festübernahme durch Emissionshäuser BSK OR II-Zindel/Isler, Art. 650 N 31-32b m.w.N.; ferner Zobl/Kramer, Kapitalmarktrecht, Rz. 1109 m.w.N.

6. Finanzdienstleistungsrecht

6.1 Einleitung

Das Finanzdienstleistungsgesetz (FIDLEG) und die Finanzdienstleistungsverordnung (FIDLEV) bezwecken gemäss Art. 1 FIDLEG den Schutz der Kunden von Finanzdienstleistern sowie die Schaffung vergleichbarer Bedingungen für das Erbringen von Finanzdienstleistungen durch die Finanzdienstleister. Dazu legen sie die Anforderungen für die getreue, sorgfältige und transparente Erbringung von Finanzdienstleistungen fest und regelt das Anbieten von Finanzinstrumenten. Sie sollen dadurch zur Stärkung des Ansehens und der Wettbewerbsfähigkeit des Finanzplatzes Schweiz beitragen.

Es geht mit anderen Worten darum, dass Personen, wenn sie in Kontakt mit einem Finanzdienstleister treten, vor den in der traditionellen Finanzintermediation verbreiteten Informationsasymmetrien und teils endemischen Interessenkonflikten geschützt werden. Dies soll durch die Auferlegung von Verhaltensregeln und besonders kundenbezogenen Informationspflichten am Point of Sale erreicht werden (Art. 7 ff. FIDLEG).²⁵⁵⁷ Entsprechend handelt es sich nicht um Anleger-, sondern *Kundenschutz*.²⁵⁵⁸ Ferner bestehen Regeln zur Veröffentlichung marktbezogener Informationen in Form eines Prospekts oder eines Basisinformationsblatts (Art. 35 ff. FIDLEG). Im Gegensatz zu den Verhaltensregeln geht es dabei primär um die Schaffung allokalionseffizienter Transparenz gegenüber potenziellen Investoren, damit diese in Kenntnis aller wesentlichen Tatsachen ihre Anlageentscheidungen treffen können.²⁵⁵⁹ Neben Primärmarkttransaktionen betreffen diese Pflichten auch Sekundärmarkttransaktionen von Effekten, bei denen der Emittent nicht zwingend mitzuwirken hat.²⁵⁶⁰

²⁵⁵⁷ Siehe Botschaft FIDLEG/FINIG 2015, 8919, 9084.

²⁵⁵⁸ Siehe SK FIDLEG-Winkler, Art. 1 N 24, wonach die Anleger als Bezüger von Finanzdienstleistungen geschützt werden sollen; ferner hierzu BSK FIDLEG/FINIG-Watter, Art. 1 FIDLEG N 5-7.

²⁵⁵⁹ Siehe Botschaft FIDLEG/FINIG 2015, 9084; SK FIDLEG-Bösch/Leisinger, Art. 35 N 5; BSK FIDLEG/FINIG-Bahar/Weber, Art. 35 FIDLEG N 2, 5; vgl. auch die unter altem Recht ergangenen BGE 120 IV 122, E. 4d.bb; 112 II 172, E. I.2.a); sodann Zobl/Kramer, Kapitalmarktrecht, Rz. 98, 1106; Klöhn, ZHR 2013, 358; ferner Ruffner, Ökonomische Grundlagen, 429; Eggen, SZW 2010, 207.

²⁵⁶⁰ Die Personen des Anbieters und Emittenten können in diesen Fällen auseinanderfallen (vgl. Art. 35 Abs. 2 FIDLEG; ferner Art. 36 Abs. 2 und 4 FIDLEG); vgl. zu *Sekundärmarkttransaktionen* Rehm/Werlen, in: Reutter/Werlen, Paradigmenwechsel, 67-68.

Die kundenbezogenen Verhaltenspflichten sind anders als die marktbezogenen Transparenzpflichten systembedingt um die Existenz von Finanzintermediären aufgebaut.²⁵⁶¹ Beide Regelungskomplexe gehen im Grundsatz zu Recht von einem mündigen und selbstverantwortlichen Anleger aus.²⁵⁶²

Ähnlich wie das GwG, handelt es sich doch bei beiden Gesetzen um sektorenübergreifende Erlasse, sind der persönliche und sachliche Geltungsbereich des FIDLEG sehr breit gefasst.²⁵⁶³ Die Breite des *sachlichen* Geltungsbereichs ist besonders gut erkennbar an der Finanzdienstleistung des Erwerbs oder der Veräusserung von Finanzinstrumenten im Sinne von Art. 3 lit. c Ziff. 1 FIDLEG, deren Anwendungsbereich im FIDLEV nochmals ausgeweitet wird.²⁵⁶⁴ Letztlich verbindet allerdings alle Typen von Finanzdienstleistungen gemäss Art. 3 lit. c FIDLEG der Umstand, dass sie auf den Erwerb, das Halten oder die Veräusserung von Finanzinstrumenten *ausgerichtet* sind; dies gilt insb. auch für die Vermögensverwaltung oder Anlageberatung.

In *persönlicher* Hinsicht sind dem Gesetz Finanzdienstleister, Kundenberater sowie Ersteller und Anbieter von Finanzinstrumenten unterstellt (Art. 2 Abs. 1 FIDLEG). Als *Finanzdienstleister* gelten Personen, die gewerbsmässig Finanzdienstleistungen in der Schweiz oder für Kunden in der Schweiz erbringen, wobei Gewerbsmässigkeit gegeben ist, wenn eine selbstständige, auf dauernden Erwerb ausgerichtete wirtschaftliche Tätigkeit vorliegt (Art. 3 lit. d FIDLEG). Als *Kundenberater* gelten sodann natürliche Personen, die im Namen eines Finanzdienstleisters oder selbst als Finanzdienstleister Finanzdienstleis-

²⁵⁶¹ Vgl. allerdings Bösch, SZW 2018, 455–456, wonach das Informations- bzw. Offenlegungsparadigma nach und nach von einem *Intermediärspadigma* sowie paternalistischen Ansätzen «bedrängt» wird, ferner 457–458.

²⁵⁶² Siehe Botschaft FIDLEG/FINIG 2015, 8940–8941 («ausreichender Informationsfluss»), 8985; so hinsichtlich strukturierter Produkte bereits FINMA, FINMA-Vertriebsbericht 2010, 47–48; ausführlich zu Produktverboten Andreotti, Produktverbote, *passim*; vgl. zu den *unterschiedlichen Anlegerleitbildern*, die in der Vertriebs- bzw. Produktregulierung zur Anwendung gelangen, Contratto, in: Sethe et al., Anlegerleitbild, 78–83; kritisch zum im FIDLEG gewählten Ansatz Baisch, in: Grosz/Grünwald, Basisinformationsblatt, 306–308 m.w.H., 322–323; schliesslich relativierend aufgrund der neueingeführten Kundensegmentierungspflicht in Art. 4 FIDLEG Sethe, in: Emmenegger, Kundensegmentierung, 215.

²⁵⁶³ Siehe Botschaft FIDLEG/FINIG 2015, 8946; SK FIDLEG-Sethe/Aggteleky, Art. 3 lit. c N 20 («weit auszulegen»); ferner Abegglen/Andreotti, GesKR 2020, 43.

²⁵⁶⁴ Art. 3 Abs. 2 FIDLEV; siehe hierzu EFD, Erläuterungen FIDLEV/FINIV/AOV 2019, 19 («Der Begriff umfasst von seinem Sinn und Zweck her insbesondere auch jene Tätigkeiten gegenüber einer bestimmten Kundschaft, die im Vorfeld des förmlichen Erwerbs oder der Veräusserung von Finanzinstrumenten erkennbar und spezifisch auf den Erwerb oder den Verkauf eines Finanzinstruments ausgerichtet sind, bei denen aber noch keine transaktionsbezogene Beratung vorliegt.»).

tungen erbringen (Art. 3 lit. e FIDLEG). *Emittenten* sind ferner Personen, die Effekten begeben oder zu begeben beabsichtigen (Art. 3 lit. f FIDLEG). Keine gesetzliche Legaldefinition besteht für den *Anbieter*. Demgegenüber wird allerdings das Angebot als jede Einladung zum Erwerb eines Finanzinstruments, die ausreichende Informationen über die Angebotsbedingungen und das Finanzinstrument selber enthält, definiert. Ein Angebot ist öffentlich, wenn es an das Publikum gerichtet ist (Art. 3 lit. g und h FIDLEG). Schliesslich sind *Ersteller* Personen, die ein Finanzinstrument erstellen oder Änderungen an einem bestehenden Finanzinstrument, einschliesslich Änderungen seines Risiko- und Renditeprofils oder der mit einer Anlage in das Finanzinstrument verbundenen Kosten, vornehmen (Art. 3 lit. i FIDLEG).

Zu klären ist vorliegend, ob dezentrale Handelsplattformen selbst oder Personen, die im Kontext solcher Plattformen aktiv sind, eine unterstellungspflichtige Tätigkeit ausüben.

6.2 Erbringen einer Finanzdienstleistung

a. Im Allgemeinen

Als *Finanzdienstleistungen* gelten gemäss Art. 3 lit. c FIDLEG die folgenden für Kunden erbrachten Tätigkeiten: der Erwerb oder die Veräusserung von Finanzinstrumenten (Ziff. 1), die Annahme und Übermittlung von Aufträgen, die Finanzinstrumente zum Gegenstand haben (Ziff. 2), die Verwaltung von Finanzinstrumenten (Vermögensverwaltung) (Ziff. 3), die Erteilung von persönlichen Empfehlungen, die sich auf Geschäfte mit Finanzinstrumenten beziehen (Anlageberatung) (Ziff. 4) und die Gewährung von Krediten für die Durchführung von Geschäften mit Finanzinstrumenten (Ziff. 5). Art. 3 Abs. 2 und 3 FIDLEG enthalten sodann genauere Umschreibungen oder aber Ausnahmen vom gesetzlichen Finanzdienstleistungsbegriff.

b. Kein Erbringen einer Finanzdienstleistung durch dezentrale Handelsplattformen

Ohne Weiteres wird aus den eingangs erwähnten Begriffsdefinitionen ersichtlich, dass auch das FIDLEG eine personale bzw. institutionelle Anknüpfung vornimmt. Personen sind gemäss dem Einleitungssatz von Art. 2 Abs. 1 FIDLEG «unabhängig von der Rechtsform» dem Gesetz unterstellt. Infrage kommen natürliche Personen (auch in Form von Einzelunternehmen), Personengesell-

schaften oder juristische Personen.²⁵⁶⁵ Damit steht auch im Finanzdienstleistungsrecht grundsätzlich die finanzintermediär tätige Person im Zentrum. Wie bereits erwähnt, führt die auf personale und institutionelle Intermediation ausgerichtete Gesetzgebung dazu, dass dezentrale Handelsplattformen grundsätzlich nicht in den Geltungsbereich der Finanzmarktgesetze fallen.

Zum Vergleich: Die Betreiber von Finanzmarktinfrastrukturen sind in ihren Kernaktivitäten grundsätzlich ebenfalls nicht dem FIDLEG unterstellt. Dies gilt selbst für zentrale Gegenparteien, welche zwischen den Gegenparteien eines Effktengeschäfts oder eines anderen Kontrakts über Finanzinstrumente tritt und somit als Käufer für jeden Verkäufer und als Verkäufer für jeden Käufer fungiert (Art. 48 FinfraG). Die zentrale Gegenpartei übernimmt mit anderen Worten das Gegenparteirisiko für die an einem Austauschgeschäft beteiligten Parteien.²⁵⁶⁶ Dabei handelt es sich hierbei um nichtunterstellte Gegenparteiengeschäfte der zentralen Gegenpartei, die nicht als Erwerb oder Veräusserung von Finanzinstrumenten für einen Kunden gelten (Art. 3 lit. c Ziff. 1 FIDLEG).²⁵⁶⁷ Zentrale Gegenparteien erbringen zudem in aller Regel – zumindest dort, wo sie an einem Handelsplatz tätig sind –²⁵⁶⁸ ausschliesslich Dienstleistungen gegenüber institutionellen Kunden im Sinne von Art. 4 Abs. 4 FIDLEG, auf welche die Verhaltenspflichten des zweiten Kapitels des Gesetzes zudem ohnehin keine Anwendung fänden.²⁵⁶⁹

Wenn das FIDLEG grundsätzlich nicht auf traditionelle Finanzmarktinfrastrukturen zur Anwendung gelangt, muss dies umso mehr auch für dezentrale Handelsplattformen gelten. Über solche Plattformen interagieren die Nutzer ohne Beteiligung eines Finanzdienstleisters bzw. Plattformbetreibers unmittelbar und ausschliesslich mithilfe von Self-Hosted Wallets. Eine Benachteiligung der Nutzer durch einen Finanzintermediär ist systembedingt ausgeschlossen. Die Anwendung von Regeln zur Verringerung von Informationsasymmetrien zwischen Kunden und Finanzdienstleistern und die Vermeidung von Interessenkonflikten machen somit nur bedingt Sinn.²⁵⁷⁰ Der Code der Plattform, sofern er in den relevanten Punkten fehlerfrei ist, macht genau das, was er vorgibt zu tun. Dies beinhaltet auch die Ausführung von Nutzeraufträgen in bestmöglicher Weise, die traditionell mit der Best Execution-Pflicht des Fi-

²⁵⁶⁵ Vgl. etwa Art. 18 Abs. 1, 25, 33 Abs. 1 und 42 FINIG; Art. 1 Abs. 1 BankG, Art. 14a BankV.

²⁵⁶⁶ Siehe BSK FINMAG/FinfraG-Bahar/Gurtner, Art. 48 FinfraG N 2; ferner Hess, AJP 2004, 692, 695.

²⁵⁶⁷ Ausführlich hierzu Abegglen/Andreotti, GesKR 2020, 39, 44, 46, 56.

²⁵⁶⁸ Vgl. für den Kreis der Teilnehmer an einem Handelsplatz Art. 34 Abs. 2 FinfraG.

²⁵⁶⁹ Art. 20 Abs. 1 FIDLEG.

²⁵⁷⁰ Vgl. Art. 25–27 FIDLEG.

nanzdienstleisters sichergestellt wird.²⁵⁷¹ Dezentrale Handelsplattformen können im Prinzip als die Verkörperung des «ehrlichen Maklers» verstanden werden.²⁵⁷²

Der Bundesrat vertritt die Auffassung, dass ein DLT-Handelssystem abhängig von der im Einzelfall erbrachten Tätigkeit als Finanzdienstleister gelten könne.²⁵⁷³ Dies ist wenig überraschend, können DLT-Handelssysteme doch auch private Teilnehmer zum Handel zulassen. In Art. 58i FinfraV werden DLT-Handelssystemen, die private Teilnehmer zum Handel zulassen, sodann bestimmte Informationspflichten auferlegt, die Ähnlichkeiten mit FIDLEG-Pflichten aufweisen. Dazu gehört etwa die Bereitstellung der i.d.R. vom Emittenten erstellten Prospekte oder Basisinformationsblätter zu den am DLT-Handelssystem zugelassenen DLT-Effekten.

c. Nutzung einer dezentralen Handelsplattform

Nutzer dezentraler Handelsplattformen haben sich demgegenüber selbst über die Funktionsweise der auszutauschenden Finanzinstrumente sowie deren Risiken zu informieren, wobei die generelle Informationssituation in der Praxis mangels gesetzlicher²⁵⁷⁴ oder vertraglicher²⁵⁷⁵ Informationspflichten oft nicht zufriedenstellend ist. Ferner kommt es nicht zur Prüfung der Angemessenheit oder Eignung eines Finanzinstruments im Einzelfall, so dass Nutzer ohne Weiteres auch Kryptovermögenswerte erwerben können, die sie weder verstehen («Kenntnisse und Erfahrungen») noch deren Risiken zu tragen sie fähig oder bereit sind (Risikofähigkeit und -bereitschaft). Die Situation scheint allerdings nicht allzu stark vom traditionellen Setup abzuweichen, schuldet ein Finanzdienstleister doch auch bei blosser Ausführung oder Übermittlung von Kundenaufträgen keine Angemessenheits- oder Eignungsprüfung (sog. Execution-Only-Geschäfte).²⁵⁷⁶

²⁵⁷¹ Vgl. ausführlich zu Art. 18 FIDLEG Abegglen/Andreotti, GesKR 2020, *passim*.

²⁵⁷² Vgl. zu diesem Bild Engert, AcP 2018, 311.

²⁵⁷³ Siehe Botschaft DLT 2019, 312 a.A.; vgl. ferner zur Kritik in der Vernehmlassung EFD, Ergebnisbericht Vernehmlassung DLT 2019, 15.

²⁵⁷⁴ Vgl. demgegenüber Art. 8 Abs. 1 lit. d FIDLEG und Art. 73e Abs. 1 FinfraG i.V.m. Art. 58i FinfraV.

²⁵⁷⁵ Vgl. Art. 394 ff. OR.

²⁵⁷⁶ Art. 13 Abs. 1 FIDLEG; vgl. hierzu und insb. auch zur auftragsrechtliche Seite Schmid, in: Emmenegger, Execution-only-Geschäfte, 225–230, 231.

Ferner wäre unklar, *wem* solche oder ähnliche Informations- und Prüfungspflichten mangels eindeutige identifizierbarer Betreiber oder sonstiger Personen im Kontext einer dezentralen Handelsplattform überhaupt auferlegt werden könnten. Demgegenüber gewährleistet die Transparenz verteilter Register, dass abgewickelte Handelsgeschäfte nachträglich leicht überprüft werden können (z.B. hinsichtlich der Ausführungskosten).²⁵⁷⁷

d. Betrieb einer Handelsplattform als Finanzdienstleistung (Exkurs)

Die Auferlegung von Pflichten scheint dort unproblematisch, wo ein Betreiber einer Handelsplattform existiert, der etwa seine eigenen Bestände für die Abwicklung von Austauschgeschäften ohne direktes Matching der Nutzer einsetzt.²⁵⁷⁸ Nach vorliegender Auffassung handelt es sich hierbei entweder um zentrale Handelsplattformen oder aber um Non-custodial P2O-Handelsplattformen. In diesen Fällen erbringt der Betreiber regelmässig Finanzdienstleistungen für Kunden im Sinne des FIDLEG, namentlich der Erwerb oder die Veräusserung von Finanzinstrumenten (Art. 3 lit. c Ziff. 1) und, bei Weiterleitung des Auftrages an eine andere Handelsplattform oder einen anderen Finanzintermediär durch den Betreiber, die Annahme und Übermittlung von Aufträgen, die Finanzinstrumente zum Gegenstand haben (Art. 3 lit. c Ziff. 2). Analoges gilt für die Unterstellung des Geschäfts der Krypto-Brokerage unter das FIDLEG.²⁵⁷⁹

Sodann könnte auch ein Smart Contract-basierter Aggregator unter das FIDLEG fallen, zumindest wenn dieser gewisse Order-Routing-Komponenten zentral auf seinem Server ausführt (off-chain). Es könnte sich namentlich um einen Fall der Annahme und Übermittlung von Aufträgen, die Finanzinstrumente zum Gegenstand haben, handeln.

Ferner soll auch auf die Frage eingegangen werden, ob ein allfälliger Betreiber einer Plattform, die ausschliesslich auf die Vermittlungstätigkeit ausgerichtet ist, d.h. Erwerber und Veräusserer lediglich zusammenführt und diese die Abwicklung über ihre Self-Hosted Wallets selbst vornehmen, als Finanzdienst-

²⁵⁷⁷ Vgl. zur Relevanz von Dokumentations- und Rechenschaftspflichten im traditionellen Kontext Sethe/Seiler, in: Waldburger et al., 432, sodann aber relativierend 454, wo auf den kaum auszugleichenden Informationsvorsprung des Finanzdienstleisters hingewiesen wird.

²⁵⁷⁸ Siehe Bundesrat, DLT-Bericht 2018, 125 («Krypto-Handelsplattformen»).

²⁵⁷⁹ Siehe Bundesrat, DLT-Bericht 2018, 126 («Krypto-Brokerage»).

leister qualifizieren könnte. Einerseits ist festzuhalten, dass der Bundesrat einen weiten Finanzdienstleistungsbegriff, soweit es den Erwerb oder die Veräußerung von Finanzinstrumenten betrifft, zu vertreten scheint, der insb. auch gewisse Formen der Vermittlung erfassen kann.²⁵⁸⁰ Der Einschub wurde sodann aufgrund breiter Kritik in der Vernehmlassung gestrichen, allerdings mit dem Hinweis, dass «[der Begriff] nun nicht zu weit aber auch nicht zu eng gefasst ist [...]».²⁵⁸¹

Nach vorliegender Auffassung ist die hier interessierende Vermittlungstätigkeit einer Handelsplattform nicht mit der Vermittlung bzw. dem Vertrieb von Finanzinstrumenten und insb. Anteilen an kollektiven Kapitalanlagen gleichzusetzen. Dies wird daran gut erkennbar, dass der Bundesrat mit dem Einschub den im alten Kollektivanlagenrecht verbreiteten Vertriebsbegriff *de facto* ins FIDLEG übernehmen wollte.²⁵⁸² Dezentrale Handelsplattformen vermitteln demgegenüber lediglich die Interessen von Käufern und Verkäufern an einem Abschluss eines Austauschgeschäfts. Es besteht gerade kein Bezug auf ein spezifisches Finanzinstrument, soweit ein solches überhaupt vorliegt.

e. Nutzung einer dezentralen Handelsplattform über einen Finanzdienstleister

Nutzer können andererseits Austauschgeschäfte über dezentrale Handelsplattformen nicht selbst, sondern als *Kunden* eines Finanzintermediärs vornehmen. In diesem Fall interagieren sie mit den Plattformen typischerweise über das Hosted Wallet des Finanzintermediärs. Das FIDLEG gelangt zur Anwendung, wenn die übrigen gesetzlichen Voraussetzungen erfüllt sind. Dies ist insb. der Fall, wenn der Finanzdienstleister im eigenen Namen auf Rechnung des Kunden Vermögenswerte handelt, die nicht zwingend als Effekten, aber zumindest als Finanzinstrumente zu qualifizieren haben. In diesen Fällen erbringt der Finanzdienstleister regelmässig Finanzdienstleistungen für Kunden im Sinne des FIDLEG, namentlich der Erwerb oder die Veräußerung von Finanzinstrumenten (Art. 3 lit. c Ziff. 1) und bei Weiterleitung des Auftrages an

²⁵⁸⁰ Siehe EFD, Erläuternder Bericht FIDLEV/FINIV/AOV 2018, 18 («Der Begriff muss insbesondere auch jene Tätigkeiten umfassen, die – wie etwa die Vermittlung [bzw. der Vertrieb] – spezifisch auf den Erwerb oder den Verkauf eines Finanzinstruments ausgerichtet sind, bei denen aber noch keine transaktionsbezogene Beratung vorliegt.»).

²⁵⁸¹ EFD/SIF, Änderungen an FIDLEV/FINIV/AOV, 1.

²⁵⁸² Vgl. zum Hintergrund EFD, Erläuternder Bericht FIDLEV/FINIV/AOV 2018, 18–19.

einen anderen Finanzintermediär die Annahme und Übermittlung von Aufträgen, die Finanzinstrumente zum Gegenstand haben (Art. 3 lit. c Ziff. 2).²⁵⁸³

Der Finanzdienstleister muss die Verhaltenspflichten des FIDLEG am Point of Sale gegenüber den Kunden einhalten, wenn es sich bei den Kryptovermögenswerten um *Finanzinstrumente* handelt. Kryptowährungen bzw. (reine) Zahlungs-Token sowie Nutzungs-Token stellen im Gegensatz zu Anlage-Token grundsätzlich keine Finanzinstrumente nach FIDLEG dar.²⁵⁸⁴ Dienstleistungen im Zusammenhang mit diesen Tokenkategorien qualifizieren entsprechend nicht als Finanzdienstleistungen im Sinne des FIDLEG. Eine Ausnahme besteht dort, wo Zahlungs-Token als Einlagen entgegengenommen werden, wenn deren Rückzahlungswert oder Zins risiko- oder kursabhängig ist, ausgenommen solche, deren Zins an einen Zinsindex gebunden ist.²⁵⁸⁵ Demgegenüber gelten reguläre Einlagen, mit welchen Forderungen aus einem Konto- oder Depotvertrag auf Auszahlung oder physische Lieferung namentlich von Fremdwährungen, Festgeldern oder Edelmetallen verbunden sind, nicht als Finanzinstrumente.²⁵⁸⁶ Hierzu sind auch Einlagen auf Kryptowährungen bzw. Zahlungs-Token zu zählen.

f. Bereitstellung von Liquidität über eine dezentrale Handelsplattform

Offen ist, ob in der Bereitstellung von Liquidität über eine dezentrale Handelsplattform, z.B. dadurch, dass regelmässig Aufträge zum Geld- oder Briefkurs in ein Orderbuch gestellt werden oder einem AMM-Pool Liquidität zugeführt wird, die Erbringung der Finanzdienstleistung des Erwerbs oder der Veräusserung von Finanzinstrumenten gegenüber den anderen Nutzern einer solchen Plattform gesehen werden könnte.

Eine solche Tätigkeit ist je nach Ausgangslage entweder dem Primärmarkt oder dem Sekundärmarkt zuzuordnen: Hat die bereitgestellte Liquidität ihren Ursprung in der Emission eines Tokens, so ist die Tätigkeit des Emittenten dem *Primärmarkt* zuzurechnen. Ist die Liquidität demgegenüber Teil des Han-

²⁵⁸³ Vgl. SK FIDLEG-Sethe/Aggteleky, Art. 3 lit. c N 22 («sämtliche Finanzdienstleistungen, die keine Beratungskomponente aufweisen und dem Anleger den Zugang zu Finanzinstrumenten eröffnen»).

²⁵⁸⁴ Siehe Bundesrat, DLT-Bericht 2018, 123; Luthiger/Kuhn, in: Weber/Kuhn, Aufsichtsrechtliche Rahmenbedingungen, Rz. 55; Abegglen/Andreotti, GesKR 2020, 46.

²⁵⁸⁵ Art. 3 lit. a Ziff. 6 FIDLEG.

²⁵⁸⁶ Art. 3 Abs. 1 FIDLEV.

delsbestandes einer Person, wozu auch der Emittent selbst gehören kann, so handelt es sich um ein *Sekundärmarktgeschäft*.

Als Erwerb oder Veräußerung von Finanzinstrumenten im Sinne von Art. 3 lit. c Ziff. 1 FIDLEG gilt «jede direkt an bestimmte Kundinnen und Kunden gerichtete Tätigkeit, die spezifisch auf den Erwerb oder die Veräußerung eines Finanzinstruments abzielt» (Art. 3 Abs. 2 FIDLEG). Der Fokus ist dabei, um den Finanzdienstleistungsbegriff nicht ausufern zu lassen,²⁵⁸⁷ auf die qualifizierenden Adjektive «direkt», «bestimmt» und «spezifisch» zu legen. Bei der Bereitstellung von Liquidität über eine dezentrale Handelsplattform handelt es sich nach vorliegender Auffassung in aller Regel noch nicht um eine Finanzdienstleistung: Der Liquiditätsgeber übt namentlich keine Tätigkeit aus, die *direkt an bestimmte Kunden* gerichtet ist. Er weiss im Zeitpunkt der Bereitstellung weder, ob sein Angebot überhaupt nachgefragt wird (*direkt*), noch, wer letztlich Handelsgeschäfte über die Plattform ausführen wird (*bestimmte Kunden*). Er selbst stellt lediglich Liquidität ein, die Ausführung eines Handelsgeschäfts wird demgegenüber einseitig von der Gegenpartei, soweit eine solche eindeutig feststellbar ist, bestimmt und im Übrigen vollständig autonom durch den Smart Contract oder einen ähnlichen Mechanismus abgewickelt. Gegebenenfalls muss das Vorliegen eines öffentlichen Angebots geprüft werden.²⁵⁸⁸ ROLF SETHE und TOBIAS AGGTELEKY setzen entsprechend in Abgrenzung zu Geschäften über traditionelle Handelsplätze für das Vorliegen einer Finanzdienstleistung voraus, dass zwischen den Parteien eine *individualisierte Rechtsbeziehung* besteht.²⁵⁸⁹ Zwar sind nach Auffassung des Bundesrates auch rein faktische Beziehungen zu einem Kunden für das Vorliegen einer Finanzdienstleistung ausreichend,²⁵⁹⁰ doch wird in der Praxis zivilrechtlich regelmässig ein Auftrag oder auftragsähnliches Rechtsverhältnis zwischen Finanzdienstleister und Kunde bestehen. Konkret muss der Finanzdienstleister im Interesse des Kunden tätig werden, damit es sich um eine Finanzdienstleistung *für* einen Kunden im Sinne von Art. 3 lit. c Einleitungssatz FIDLEG handelt.²⁵⁹¹ An einer individualisierten Beziehung, welche zudem einen Inter-

²⁵⁸⁷ Vgl. zur diesbezüglich Kritik in der Vernehmlassung EFD, Ergebnisbericht Vernehmlassungsverfahren FIDLEG/FINIV/AOV 2019, 8 («unzulässige Ausweitung auf Tätigkeiten im Vorfeld von Finanzdienstleistungen»); ferner bereits EFD, Bericht Vernehmlassungsergebnisse FIDLEG/FINIG 2015, 14–15.

²⁵⁸⁸ Siehe hierzu unten, [V.6.3b](#).

²⁵⁸⁹ Siehe SK FIDLEG–Sethe/Aggteleky, Art. 3 lit. c N 18, ferner N 72.

²⁵⁹⁰ Siehe Botschaft FIDLEG/FINIG 2015, 8948; a.M. wohl Isler/Eckert, GesKR 2021, 43–44.

²⁵⁹¹ Siehe Isler/Eckert, GesKR 2021, 43; OFK FIDLEG/FINIG, Art. 3 FIDLEG N 60, 66; vgl. ferner mit Blick auf die Best-Execution-Pflicht in Art. 18 FIDLEG Abegglen/Andreotti, GesKR 2020, 46; BSK FIDLEG/FINIG–Rayroux, Art. 3 lit. c FIDLEG N 18; differenzierend SK FID-

essenwahrungs- bzw. Dienstleistungscharakter aufweist, wird es bei blosser Bereitstellung von Liquidität über eine dezentrale Handelsplattform allerdings regelmässig fehlen.²⁵⁹²

Funktionell können Konstellationen mit Smart Contracts mit der Platzierung von Finanzinstrumenten oder anderen Vermögenswerten verglichen werden (vgl. Art. 3 Abs. 3 lit. b FIDLEV),²⁵⁹³ wobei die technische Platzierung bei den Nutzern, unabhängig davon, ob diese den Primär- oder Sekundärmarkt betrifft, nicht durch den Liquiditätsgeber selbst, sondern durch den Smart Contract erfolgt. Software kann allerdings nicht als Finanzdienstleister qualifizieren. Eine unterstellungsrelevante Beziehung zwischen dem Liquiditätsgeber und einem Nutzer der Plattform konstruieren zu wollen, würde nach dem Gesagten den Finanzdienstleistungsbegriff überdehnen. Dies ist allerdings auch nicht nötig, denn ein Vergleich mit traditionellen Märkten verdeutlicht, dass die an einem Austauschgeschäft beteiligten Parteien in diesem Fall auch keine Finanzdienstleistungen im technischen Sinne erbringen (wollen).²⁵⁹⁴

Im AMM-Modell muss ein Nutzer nicht einmal die Preiskonditionen des Liquiditätsgebers akzeptieren, wird doch der Preis nach einer vorbestimmten mathematischen Formel berechnet.²⁵⁹⁵ Eine Benachteiligung des Nutzers durch den Liquiditätsgeber, die den Kundenschutz rechtfertigen würde, ist technisch ausgeschlossen. Schliesslich kann der zeitliche Abstand zwischen der Bereitstellung von Liquidität und der konkreten Ausführung eines Handelsgeschäfts im Einzelfall sehr gross ausfallen. Mit anderen Worten wird es auch aus diesem Grund regelmässig an der *Direktheit* der Tätigkeit fehlen. Die Bereitstellung von Liquidität im Orderbuch- oder AMM-Modell stellt demnach keine Finanzdienstleistung im Sinne des FIDLEG dar.

LEG-Sethe/Aggteleky, Art. 3 lit. c N 29–56, wobei die Autoren in erster Linie darauf abstellen, ob das fragliche Geschäft auf einem Kundenauftrag beruht (N 38).

²⁵⁹² So auch Weber, SJZ 2021, 682, der für «dezentrale DLT-Handelsplattformen» vom Abschluss eines Kaufvertrags ausgeht, wobei der Autor in seinen Ausführungen davon ausgeht, dass ein Plattformbetreiber existiert und in diesem Rahmen als Vermittler tätig wird.

²⁵⁹³ Siehe zu dieser Tätigkeit EFD, Erläuterungen FIDLEV/FINIV/AOV 2019, 19–20, wonach sie das «vorgelagerte Verhältnis» zwischen dem Finanzdienstleister und dem Emittenten eines Finanzinstruments bzw. dessen Eignern betrifft.

²⁵⁹⁴ Vgl. zum Umstand, dass die Gegenpartei eines Wertpapierhauses in der Praxis regelmässig ein anderes Wertpapierhaus bzw. im Börsenhandel eine zentrale Gegenpartei ist, Costantini, SJZ 2013, 26; Zobl/Kramer, Kapitalmarktrecht, Rz. 1242–1243; ferner hinsichtlich Gegenparteigeschäfte Abegglen/Andreotti, GesKR 2020, 44, 46.

²⁵⁹⁵ Siehe oben, [IV.3.7b](#) und [IV.4.2a](#).

Ohnehin würde dies dort gelten, wo der Emittent eines Finanzinstruments selbst die Liquidität zur Verfügung stellt – unabhängig davon, ob sein Handeln dem Primär- oder Sekundärmarkt zuzurechnen ist. In diesem Fall kann der Nutzer gar nicht erst erwarten, dass der Emittent eine Finanzdienstleistung für einen Kunden im Sinne des FIDLEG erbringen will.²⁵⁹⁶ Wenn überhaupt, liegt einer solchen Tätigkeit zivilrechtlich höchstens ein Kauf- oder Tauschgeschäft zwischen Emittent und Gegenpartei zugrunde. Fraglich ist auch das Kriterium der Gewerbsmässigkeit einer solchen Aktivität, wenn es sich bei den tokenisierten Finanzinstrumenten um Aktien oder Anleihen des Emittenten handelt, die er zwecks Finanzierung seiner Geschäftstätigkeit ausgibt.²⁵⁹⁷ Emittenten unterstehen somit nicht den Verhaltenspflichten des FIDLEG, wenn sie Liquidität für ihre eigenen Titel über eine dezentrale Handelsplattform zur Verfügung stellen. Dies gilt grundsätzlich unabhängig davon, ob die zur Verfügung gestellten Titel aus einer Emission oder aber aus dem Eigenbestand des Emittenten stammen. Eine derartige Einschränkung des persönlichen Geltungsbereichs des FIDLEG ist auch darum gerechtfertigt, weil aus den Materialien nicht ersichtlich ist, dass der Gesetzgeber die Verhaltenspflichten auf Emittenten und deren Eigen- bzw. Selbstemissionen ausdehnen wollte, die vor Einführung von FIDLEG finanzmarktrechtlich nach einvernehmlicher Ansicht nicht erfasst waren.²⁵⁹⁸ So führte etwa die

²⁵⁹⁶ A.M. SK FIDLEG-Sethe/Aggteleky, Art. 3 lit. c N 71, die Eigenemissionen als Finanzdienstleistungen qualifizieren, jedoch davon ausgehen, dass es bei solchen Emissionen durch Gesellschaften «ohne Bankstatus» an der Gewerbsmässigkeit fehle (siehe auch SK FIDLEG-Sethe/Aggteleky, Art. 3 lit. d N 70). Die Botschaft des Bundesrates ist diesbezüglich zweideutig, vgl. Botschaft FIDLEG/FINIG 2015, 8946 («Erfasst werden einerseits alle Tätigkeiten, die zum Erwerb eines Finanzinstruments durch eine Kundin oder einen Kunden führen können. Darunter fallen der Erwerb und die Veräusserung von Finanzinstrumenten auf Rechnung von Kundinnen und Kunden, unabhängig davon, ob die Finanzinstrumente von Dritten erworben werden oder vom Finanzdienstleister selbst geschaffen, platziert oder auf dem Sekundärmarkt veräussert werden.»).

²⁵⁹⁷ GL.M. Abegglen/Andreotti, GesKR 2020, 44 FN 100; Kuhn, in: Weber/Kuhn, Primärmarktregulierung, Rz. 6-7; ferner Bösch, SZW 2018, 461, der erwähnt, dass eine Unterstellung von Emittenten unter die FIDLEG-Verhaltenspflichten zum «absurden» Resultat führen würde, dass Emittenten einer Registrierungspflicht als Kundenberater unterstehen würden.

²⁵⁹⁸ Vgl. etwa die Aussage zur historischen Kontinuität in der Gesetzeslage in Botschaft FIDLEG/FINIG 2015, 8929 («Mit der vorgeschlagenen Vorlage kann die Schweiz eine moderne, funktionsübergreifende sowie verständliche Finanzmarktregulierung schaffen. An die Stelle der bisherigen Regulierung, basierend auf sektorspezifischen Erlassen, soll eine Regulierung treten, die im Grundsatz für alle Institute und Aktivitäten gilt. So müssten sich alle Finanzdienstleister an die gleichen Verhaltensregeln halten. Dies führt zu einer Vereinfachung und eine Vereinheitlichung der historisch gewachsenen Gesetze.»).

Eigenemission von Effekten nur ausnahmsweise zur Unterstellung des Emittenten unter das alte Börsengesetz und in der Folge zur Anwendbarkeit der Verhaltenspflichten in Art. 11 aBEHG.²⁵⁹⁹

g. Vertragsrechtliche Bemerkungen (Exkurs)

Es ist fraglich, ob die Nutzer einer dezentralen Handelsplattform überhaupt in jeder Konstellation in eine *vertragliche* Beziehung miteinander treten.²⁶⁰⁰

Im traditionellen Kontext werden in den Orders, die in ein Orderbuch eines Handelssystems eingestellt werden, rechtsverbindliche Willensäußerungen im Sinne von Art. 1 OR gesehen. Dabei werden die sich deckenden Orders in aller Regel automatisch vom System zum Zweck des Vertragsschlusses zusammengeführt.²⁶⁰¹ Die Beantwortung der eingangs gestellten Frage scheint damit vom konkreten Matching-Modell der fraglichen dezentralen Handelsplattform abhängig zu sein. Dabei ist zu beachten, dass die praktische Bedeutung von Angebot und Annahme als vertragsrechtliche Konzepte bei Verwendung von Smart Contracts in den Hintergrund tritt.²⁶⁰² Dasselbe könnte in Ausnahmefällen selbst für den Rechtsbindungswillen der in einen Austausch involvierten Personen gelten.

Generell kann zwischen Smart Contracts, die «code-only» sind und solchen, die zur Ausführung und Durchsetzung von traditionellen textbasierten Verträgen eingesetzt werden («ancillary»), unterschieden werden.²⁶⁰³ Für DEX ist grundsätzlich erstere Kategorie von Interesse, denn angesichts der relativ tiefen Komplexität von Austauschgeschäften kommen die Parteien i.d.R. nicht zusammen, um separate Vertragsbedingungen auszuhandeln (z.B. per E-Mail) und nur selten ziehen sie etwa die Dokumentation des Softwarecodes der DEX als Vertragsbestandteil ausdrücklich mit ein. Die Dokumentation des Codes

²⁵⁹⁹ Vgl. BGE 136 II 43, E. 7.3.1; BGer 2C_571/2018 vom 30. April 2019, E. 4.3; ferner FINMA, Wegleitung ICOs, 5.

²⁶⁰⁰ Grundsätzlich davon ausgehend Eggen, AJP 2017, 8–9, die von Distributed Ledgers als «Matchingsystemen für Willenserklärungen» spricht; ebenfalls Essebie/Wyss, Jusletter vom 24. April 2017, Rz. 40.

²⁶⁰¹ Siehe etwa von Hall, GesKR 2015, 499 m.w.H.; ferner Zobl/Kramer, Kapitalmarktrecht, Rz. 911.

²⁶⁰² Siehe Jaccard/Toral, in: Richa/Canapa, Smart contracts, 10, welche die Bedeutung von Angebote und Annahme als rein theoretisches Anliegen betrachten; ähnlich wohl Weber, SZW 2021, 455, der von der *vertragsähnlichen* Abmachung beim Einsatz von Smart Contracts spricht.

²⁶⁰³ Zur Unterscheidung ausführlich Levi/Lipton, Harvard Law School Forum on Corporate Governance 2018, *passim*.

der Plattform kann aber u.U. zur Auslegung des gemeinsamen Verständnisses des Rechtsgeschäfts und der Willen der Parteien beigezogen werden. Vom Zustandekommen einer Vertragsbeziehung ist ohne Weiteres bei Matching-Modellen auszugehen, bei welchen der Nutzer seine Gegenpartei manuell auszuwählen hat (z.B. Bisq). Hier liegen dem manuellen Matching elektronisch übermittelte, ausdrückliche oder konkludente Willensäußerungen in Form von Angebot und Annahme zugrunde. Für das Orderbuchmodell ist ebenfalls generell vom Abschluss eines Vertrages auszugehen: Wenn ein Nutzer bspw. seine Vermögenswerte zwecks Auftragserstellung vorab im Smart Contract deponiert und sodann einen Auftrag ins Orderbuch einstellt (so z.B. bei Ether-Delta), ist darin ein Angebot des Liquiditätsgebers bzw. Makers zum Abschluss eines Kaufvertrages zu erkennen. Nutzer bzw. Taker können dessen Angebot akzeptieren, indem sie die Order durch Ausführung auf der Blockchain annehmen, worin ein Realakzept oder sonstiges konkludentes Verhalten gesehen werden kann.²⁶⁰⁴ In diesem Fall sind die den Willensäußerungen beider Parteien entsprechenden Vertragsbedingungen bereits im zur Ausführung vorgesehenen Code des Smart Contracts abgebildet.²⁶⁰⁵

Im AMM-Modell ist die Rechtslage indessen weniger eindeutig: In der Bereitstellung von Liquidität in einem Pool kann eine konkludente Willensäußerung ähnlich zu einer Realofferte gesehen werden.²⁶⁰⁶ Der Einsatz von Liquiditätspools verunmöglicht allerdings die eindeutige Zuordnung der an einem konkreten Handelsgeschäft beteiligten Parteien. Dies liegt daran, dass i.d.R. nicht nur eine Person, sondern mehrere Personen gleichzeitig und zu unterschiedlichen Teilen Liquidität in Form von Token einbringen. Der Nutzer der Plattform weiss darum im Einzelfall nicht, mit welcher Partei bzw. mit welchen Gegenparteien er ein Austauschgeschäft abschliesst, was in obligationenrechtlicher Hinsicht ein Problem darstellen könnte.²⁶⁰⁷ Dass die Parteien hingegen, wenn überhaupt, nur anhand ihrer Wallet-Adresse identifizierbar sind, ist vorbehalten-

²⁶⁰⁴ Vgl. zum Realakzept Müller, in: BK OR, Art. 3 N 124, mit Blick auf Smart Contracts sodann N 38.

²⁶⁰⁵ Ausführlich zum *On-chain-Vertragsschluss* Müller, ZBJV 2019, 342-343; ferner Ernst, ZSR 2018 II, 79, welcher aus dem *Vertrauensprinzip* die rechtliche Verbindlichkeit der Programmverwendung durch die Nutzer herleitet; sodann auch Carron/Botteron, in: Carron/Müller, Contrats intelligents, 27-29.

²⁶⁰⁶ Vgl. zur Realofferte Müller, in: BK OR, Art. 3 N 41.

²⁶⁰⁷ Siehe zur *Identifikation der Vertragspartei* als objektiv wesentlicher Punkt des Vertrages Müller, in: BK OR, Art. 2 N 15 a.E.; sodann Schwenzer/Fountoulakis, Obligationenrecht, § 29 N 29.03; Guhl/Koller, Schweizerisches Obligationenrecht, § 13 N 8 m.w.H. auf die bundesgerichtliche Rechtsprechung; demgegenüber offenbar weniger streng Huguenin, Obligationenrecht, Rz. 258-259.

lich zwingender gesetzlicher Anforderungen an den Vertragsschluss²⁶⁰⁸ nicht grundsätzlich ein Hindernis für das Zustandekommen eines Vertrages.²⁶⁰⁹ Es könnte argumentiert werden, dass der Smart Contract – ähnlich einer zentralen Gegenpartei im traditionellen Wertpapierhandelskontext –²⁶¹⁰ selbst Vertragspartei wird, da der Nutzer unmittelbar ausschliesslich mit dem Smart Contract interagiert. Dies ist jedoch *de lege lata* mangels Rechtsfähigkeit von Computerprogrammen kein gangbarer Weg.²⁶¹¹

Die Bestimmbarkeit der Vertragsparteien ist nach vorliegender Auffassung im AMM-Modell primär ein praktisches Problem.²⁶¹² Trotz der fehlenden Bestimmbarkeit der Gegenpartei ist in der Tendenz von einem Vertragsschluss auszugehen.²⁶¹³ Angesichts der Bedeutung des Handelsgeschäfts für die beteiligten Nutzer liegt ein Vertragsschluss grundsätzlich nahe.²⁶¹⁴ Dies ist ferner aus den folgenden beiden Gründen der Fall: *Erstens* entspricht der rechtsverbindliche Austausch von Kryptovermögenswerten in aller Regel dem klaren Willen der Parteien, wenn sie für den Austausch eine dezentrale Handelsplattform in Anspruch nehmen. Handlungs-, Geltungs- und Rechtsfolgewille liegen somit bei den Parteien bis zu einem gewissen Umfang vor.²⁶¹⁵ Dies trifft besonders auf Liquiditätsgeber zu, die im Hinblick auf das eigentliche Austauschgeschäft keine weitere Handlung mehr vorzunehmen haben. Ihre konkludenten

²⁶⁰⁸ Z.B. bei Handlungsunfähigkeit der Gegenpartei gemäss Art. 17 ZGB; siehe hierzu etwa Müller/Seiler, AJP 2019, 323–324; differenzierend Gyr, Jusletter IT vom 30. Juni 2022, Rz. 23–27.

²⁶⁰⁹ GLM. von der Crone/Kessler/Angstmann, SJZ 2018, 341; SLTA, Regulatory Task Force Report 2018, 44; a.M. Jaccard, Jusletter IT vom 23. November 2017, Rz. 83; scheinbar auch Müller, ZBJV 2019, 344; siehe zur Anonymität im elektronischen Rechtsverkehr ferner Weber, E-Commerce und Recht, 348.

²⁶¹⁰ Vgl. Zobl/Kramer, Kapitalmarktrecht, Rz. 912, 1319–1320.

²⁶¹¹ Siehe Bundesrat, DLT-Bericht 2018, 85–86 m.w.N.; vgl. hierzu etwa Teubner, AcP 2018, 160–163; Zobel/Lysakowski, digma 2019, *passim*.

²⁶¹² Vgl. auch Weber, Jusletter vom 4. Dezember 2017, Rz. 20, der darin ebenfalls primär ein praktisches Problem zu erkennen scheint; ähnlich Kaulartz/Heckmann, CR 2016, 620.

²⁶¹³ GLM. wohl Weber, sic! 2018, 293, der davon auszugehen scheint, dass trotz der Zurechnungsprobleme Willenserklärungen letztlich unter zwei Personen auszutauschen sind; wohl offenlassend Glarner/Meyer, Jusletter vom 4. Dezember 2017, Rz. 20; a.M., jedoch in Bezug auf das ähnlich gelagerte Verhältnis zwischen Nutzer und Miner Meyer/Schuppli, recht 2017, 212–214, die von einer Auslobung durch den Nutzer im Sinne von Art. 8 Abs. 1 OR ausgehen; ferner hierzu Meyer, Crypto Tokens, N 227–228.

²⁶¹⁴ Das Bundesgericht stellt für die Abgrenzung der Gefälligkeit vom Vertrag u.a. auf die rechtliche und wirtschaftliche Bedeutung der Leistungen für die beteiligten Personen ab; vgl. BGE 116 II 695, E. 2 bb).

²⁶¹⁵ Die «Willens- und Wissenserklärungen» des Smart Contracts sind in der Folge grundsätzlich den Parteien *zuzurechnen*; vgl. Furrer, Anwaltsrevue 2018, 106–109; *ausführlich* zu den unterschiedlichen Willenstypen Müller, in: BK OR, Art. 1 N 15.

Willensäusserungen können als ein verbindliches, computercodemässig bedingtes Angebot *ad incertas personas* qualifiziert werden.²⁶¹⁶ Die Bereitstellung von Liquidität in einem Pool wäre somit als eine (konkludente) verbindliche Offerte zu betrachten, die sich an einen unbegrenzten Personenkreis richtet. Alternativ könnte in der Bereitstellungshandlung bloss eine *invitatio ad offerendum* (ohne Abschlusswillen) gesehen werden, die jedoch von einer antizipiert-bedingten Annahmeerklärung begleitet wird.²⁶¹⁷ Die Annahme der Offerte bzw. die Möglichkeit, ein Angebot zu unterbreiten, stünde grundsätzlich jedem Nutzer bis zum Rückzug der Liquidität aus dem Pool offen. Zweitens vollzieht der Smart Contract – bei Aggregatoren können es auch eine Mehrzahl von Smart Contracts sein – im vorliegenden Fall lediglich den von den Parteien beabsichtigten Austausch von Vermögenswerten.²⁶¹⁸ Die Funktionsweise des Smart Contracts soll nicht dem Lauf der Dinge gemäss dem bereits initialisierten Willen der Parteien im Wege stehen. Die Automatisierung von bereits abgegebenen Willenserklärungen durch den Smart Contract, die letztlich zum Vertragsabschluss führen,²⁶¹⁹ ist mit anderen Worten den beteiligten Parteien *zuzurechnen*.²⁶²⁰

Beim Handelsmodell einer AMM stellt sich dennoch aufgrund des *fortgeschrittenen Autonomie- und Anonymitätsgrades* solcher Plattformen die Frage, ob überhaupt noch ein Vertrag zustande kommt. Es scheint nicht ausgeschlossen, dass es unter gewissen Umständen vollständig an einem vertraglichen Rechtsbindungswillen der beteiligten Personen fehlt; in diesem Fall verlassen sich die beteiligten Personen *vollständig* auf die soziotechnische Funktionalität des de-

²⁶¹⁶ Zum Konzept Kollmann, Wertpapierhandelssysteme, 245–247.

²⁶¹⁷ Eine vergleichbare Situation ergibt sich bei Vertragsschlüssen im Rahmen von Internet-auktionen; vgl. etwa BGer 4A_58/2008 vom 28. April 2008, E. 3, wonach der Vertrag mit einer E-Mail an den Höchstbietenden, die den Zuschlag nach Art. 229 Abs. 2 OR darstellt, zustande kommt. Denkbar ist jedoch auch, dass die Plattform die Zuschlagsmitteilung für den Veräusserer automatisiert versendet. Der Autor dankt Frau Prof. Zellweger-Gutknecht für den Hinweis.

²⁶¹⁸ Siehe zum *Vollzugselement* des Smart Contracts insb. Kaulartz/Heckmann, CR 2016, 618–619, 621; Weber, sic! 2018, 292; Müller, in: BK OR, Art. 1 N 420; *differenzierend* Trüeb, in: Grolimund et al., Smart Contracts, 725.

²⁶¹⁹ Vgl. betreffend *Einordnung* der Erklärung eines autonomen Software-Agenten als Willenserklärung des Nutzers der Software Cornelius, MMR 2002, 355; ferner Sester, Informatik Spektrum 2004, 317; Weber, E-Commerce und Recht, 340 m.w.N.

²⁶²⁰ So auch Möslin, ZHR 2019, 270–274; Kollmann, Wertpapierhandelssysteme, 249–252; Müller, ZBJV 2019, 346; Gyr, Jusletter IT vom 30. Juni 2022, Rz. 40–47; ferner allgemein Gauch et al., Obligationenrecht AT, Rz. 300.

zentralen Systems.²⁶²¹ Es läge somit nur noch ein faktisches Verhältnis zwischen den beteiligten Nutzern vor.

Davon zu unterscheiden ist eine allfällige Vertragsbeziehung zwischen dem Entwickler einer Software und dessen Nutzern. In der reinen Nutzung von Open-Source-Software ist nach vorliegender Auffassung in aller Regel kein Vertragsabschluss zu erkennen.²⁶²² Mit anderen Worten begründen der Download und die Ausführung von Software, die etwa das Erstellen eines Liquiditätspools erlaubt, kein Vertragsverhältnis. Vorbehalten bleiben die besonderen Bedingungen der einzelnen Softwarelizenzen im Open-Source-Bereich.

In der Lehre ist schliesslich umstritten, ob *Verfügungen über Registerwertrechte* zivilrechtlich dem Kausalitäts- oder dem Abstraktionsprinzip folgen.²⁶²³ Nach vorliegender Ansicht ist dem Abstraktionsprinzip der Vorzug zu geben. Sollte es zu Mängeln im Verpflichtungsgeschäft kommen, so soll die Situation nach vorliegender Ansicht nach bereicherungsrechtlichen Regeln gelöst werden. Das Abstraktionsprinzip trägt besser dem Umstand Rechnung, dass Transaktionen in verteilten Registern dezentraler Netzwerke grundsätzlich unabänderlich sind. Die Dezentralität des Netzwerks verunmöglicht die Rückabwicklung von Transaktionen, deren Verpflichtungsgeschäfte unwirksam geworden sind.²⁶²⁴ Ob demgegenüber auf Verfügungen über Registerwertrechte über permissioned Blockchains das Kausalitätsprinzip zur Anwendung gelangen soll, kann hier offenbleiben (und könnte allenfalls vom Willen der Beteiligten abhängig gemacht werden).

²⁶²¹ Ähnlich Omlor, ZHR 2019, 327–329, der für Blockchain-Transaktionen von einem blossen *Realakt* ausgeht, der keinen Konsens zwischen Veräusserer und Erwerber erfordert; ferner zum in der Praxis regelmässig fehlenden Rechtsbindungswillen der Teilnehmer von DAOs, Meyer, AJP 2023, 327–328, 338 («nicht vorschnell bejaht»); Maurenbrecher/Leisinger, SJZ 2022, 707–708; von einem Vertragsschluss ausgehend hingegen Meirich, Decentralized Finance, Rz. 943.

²⁶²² So auch Meyer/Schuppli, recht 2017, 210–212 hinsichtlich Verhältnis zwischen Protokollentwickler und Nutzer einer Client Software; vgl. jedoch zur Haftungsfrage beim Einsatz von Smart Contracts von Dritten Eggen, in: Emmenegger et al., Smart Contracts, 171–173.

²⁶²³ Für das *Kausalitätsprinzip*: Botschaft DLT 2019, 186; Kramer/Oser/Meier, Jusletter vom 6. Mai 2019, Rz. 28; wohl auch Wyss, Jusletter vom 1. Juli 2019, Rz. 69, 71–72, wobei der Autor die Möglichkeit einer privatautonomen Regelung offenlässt; demgegenüber für das *Abstraktionsprinzip*: Kuhn/Stengel/Meisser/Weber, Jusletter vom 23. Mai 2019, Rz. 43; offenbar *vermittelnd* aufgrund des Gutglaubensschutzes bei Geltung des Kausalitätsprinzips Weber, SZW 2021, 459.

²⁶²⁴ So etwa BuA TVTG 2019, 69 («Das Kausalitätsprinzip würde hier zu einem Auseinanderklaffen zwischen nomineller Rechtslage und faktischen, auf dem VT-System dokumentierten und praktisch unveränderlichen Verhältnissen führen.»), 191–197.

h. Softwareentwicklung

Die reine Softwareentwicklung ist dem FIDLEG nicht unterstellt, da es sich dabei nicht um eine Finanzdienstleistung nach Art. 3 lit. c FIDLEG handelt. Dies gilt selbst dann, wenn die Token, die infolge der Ausführung der Software geschaffen werden (z.B. Liquiditätstoken oder Governance Token), als Finanzinstrumente qualifizieren würden.²⁶²⁵ Dies gilt im Grundsatz auch für das FINIG, das teils direkt an «Tätigkeiten» anknüpft, die dem FIDLEG unterstellt sind (so z.B. Art. 17 Abs. 1 FINIG).²⁶²⁶

6.3 Anbieten von Finanzinstrumenten

a. Im Allgemeinen

Anknüpfungspunkte für die Prospektpflicht gemäss Art. 35 Abs. 1 FIDLEG ist *einerseits* die Unterbreitung eines öffentlichen Angebot zum Erwerb von Effekten in der Schweiz und *andererseits* das Ersuchen um Zulassung von Effekten zum Handel auf einem Handelsplatz nach Art. 26 lit. a FinfraG.

Von der Finanzdienstleistung ist strikt der Begriff des Angebots zu unterscheiden. In der Praxis geht das (öffentliche) Angebot, dem seinerseits typischerweise Werbung nach Art. 68 FIDLEG i.V.m. Art. 95 FIDLEV vorausgeht, der Erbringung einer Finanzdienstleistung chronologisch regelmässig, aber nicht zwingend voraus.²⁶²⁷

Ein Angebot im Sinne von Art. 3 lit. g FIDLEG ist jede Einladung zum Erwerb eines Finanzinstruments, die ausreichende Informationen über die Angebotsbedingungen und das Finanzinstrument selber enthält. Demnach liegt ein Angebot bei einer Kommunikation jeglicher Art vor, die ausreichende Informationen über die Angebotsbedingungen und das Finanzinstrument enthält und üblicherweise darauf abzielt, auf ein bestimmtes Finanzinstrument aufmerksam zu machen und dieses zu veräussern (Art. 3. Abs. 5 FIDLEV). Ein solches

²⁶²⁵ Vgl. Bundesrat, DLT-Bericht 2018, 124–125.

²⁶²⁶ Vgl. aber zum Risiko von Lücken zwischen FIDLEG und FINIG bereits Bärtschi, SZW 2014, 475–477.

²⁶²⁷ Vgl. EFD, Erläuterungen FIDLEV/FINIV/AOV 2019, 21; SK FIDLEG-Bösch/Leisinger, Art. 3 lit. f–i N 14; ausführlich zu Abgrenzungsfragen Isler/Eckert, GesKR 2021, 48–49, 52–53; ferner in Bezug auf das Anbieten von *kollektiven Kapitalanlagen* Abegglen/Wettstein, SZW 2018, 137.

Angebot ist öffentlich gemäss Art. 3 lit. h FIDLEG, wenn es sich um ein an ein Publikum gerichtetes Angebot handelt, d.h. sich an einen unbegrenzten Personenkreis richtet (Art. 3 Abs. 7 FIDLEV).²⁶²⁸

Die Literatur zum Prospektrecht schliesst aus diesen ähnlich formulierten Legaldefinitionen, dass der Angebotsbegriff gewisse Mindestanforderungen zu erfüllen hat, d.h. insb. die Kommunikation der *essentialia negotii* des Vertrages, wie namentlich das Kaufobjekt und den Kaufpreis bzw. Preisrahmen, zu umfassen hat.²⁶²⁹ In diesem Sinne spricht das EFD in seinen Erläuterungen von der privatrechtlich relevanten Offerte oder wenigstens der Einladung zur Offertstellung.²⁶³⁰ Auf die Form bzw. Modalität der Willenserklärung oder -bekundung kommt es nicht an; auch eine konkludente Erklärung, z.B. in Form einer Realofferte, kann ein Angebot im Sinne des FIDLEG darstellen.²⁶³¹ Als Angebot gilt demnach nur ein Handeln, das *final* auf einen Investitionsentscheid eines Anlegers ausgerichtet ist, was im Einzelfall nach dem Vertrauensprinzip aus Publikumssicht zu beurteilen ist.²⁶³²

b. Bereitstellung von Liquidität über dezentrale Handelsplattformen

Die zweite Variante in Art. 35 Abs. 1 FIDLEG betreffend Zulassung von Effekten zu einem (Schweizer) Handelsplatz kommt im Falle des Handels von Anlage-Tokens über eine dezentrale Handelsplattform offensichtlich nicht infrage.²⁶³³ Abgesehen davon, dass die Bedingungen des im Einzelfall eingesetzten Smart Contracts (z.B. der ERC-20-Standard) einzuhalten sind, bestehen auf dezentralen Handelsplattformen – anders als auf traditionellen Handelsplätzen –²⁶³⁴

²⁶²⁸ Vgl. diesbezüglich auch SK FIDLEG-Bösch/Leisinger, Art. 3 lit. f-i N 23–24; ferner zur eigenständigen Bedeutung des Begriffs der Öffentlichkeit im Prospektrecht Spillmann/Giger, GesKR 2019, 186–188.

²⁶²⁹ Siehe etwa Spillmann/Giger, GesKR 2019, 185; Bösch, ZSR 2016 I, 85–86, wonach sich der Angebotsbegriff des FIDLEG an den bestehenden Rechtsnormen in Art. 652a und Art. 1156 OR orientiert; Spillmann/Meyer, in: Reutter/Werlen, Prospektregelung, 13–14; Schleiffer/Schärli, GesKR 2018, 2–3; ferner Bösch, in: Weber et al., Neues Prospektrecht, 498; kritisch Courvoisier, SZW 2020, 308, der lediglich eine Einladung zur Offertstellung voraussetzt, ohne dass zwingend die *essentialia negotii* vorzuliegen haben.

²⁶³⁰ Siehe EFD, Erläuterungen FIDLEV/FINIV/AOV 2019, 20.

²⁶³¹ Siehe SK FIDLEG-Bösch/Leisinger, Art. 3 lit. f-i N 10.

²⁶³² Siehe EFD, Erläuterungen FIDLEV/FINIV/AOV 2019, 20–21; ferner SK FIDLEG-Bösch/Leisinger, Art. 3 lit. f-i N 15, die Bestimmbarkeit des Finanzinstruments voraussetzen.

²⁶³³ Vgl. zum Begriff des Handelsplatzes oben, [V.3.2a](#).

²⁶³⁴ Vgl. Art. 35–36 FinfraG.

grundsätzlich keine Zulassungsbedingungen. Dies ist auf die Teilnahme- und Nutzungsoffenheit solcher Protokolle zurückzuführen.²⁶³⁵ In diesem Sinne macht es mehr Sinn, von der *Bereitstellung von Liquidität* bezüglich eines Anlage-Tokens als von Zulassung (und schon gar nicht von Kotierung) zu sprechen.

Die *erste Variante* der Unterbreitung eines öffentlichen Angebot zum Erwerb von Effekten ist demgegenüber genauer zu untersuchen: Zu denken ist etwa an einen Emittenten von tokenisierten Aktien oder Anleihen,²⁶³⁶ welcher auf einer dezentralen Handelsplattform, wie etwa Uniswap, Liquidität sowohl bezüglich des Anlage-Tokens als auch bezüglich eines Stablecoins zur Verfügung stellt.

Offen ist, ob die *bloße* Bereitstellung von Liquidität bereits eine ausreichende Kommunikation der obigen Art darstellt und somit die Prospektpflicht nach Art. 35 Abs. 1 FIDLEG auslöst. Dies ist zu verneinen, wenn der Liquiditätsgeber neben der Bereitstellung von Liquidität über eine dezentrale Handelsplattform keine angebotsspezifischen Kommunikationsbemühungen unternimmt. Allerdings wird zumindest der Emittent einer von ihm bereitgestellten Effekte regelmässig über einen Kanal öffentlich kommunizieren wollen, dass eine solche Austauschmöglichkeit für den von ihm herausgegebenen Anlage-Token besteht. Falls er dies etwa über eine frei zugängliche Webseite tut, d.h. die Informationen bewusst an einen unbegrenzten Personenkreis richtet, und die darin enthaltenen Informationen über die Angebotsbedingungen und die Effekte ausreichend sind, liegt nach vorliegender Auffassung ein öffentliches Angebot dar, das vorbehaltlich einer Ausnahme gemäss Art. 36–37 FIDLEG die Prospektpflicht auslöst.

Ein öffentliches Angebot liegt hingegen nicht vor, wenn der Smart Contract über einen Registry Contract eine Whitelist implementiert, welche den Erwerb der Anlage-Tokens auf bestimmte Wallet-Adressen einschränkt. In diesem Fall richtet sich der Emittent mit der Bereitstellung von Liquidität über die dezentrale Handelsplattform gerade nicht an einen unbegrenzten Personenkreis.²⁶³⁷

²⁶³⁵ Siehe oben, [III.2.3.](#)

²⁶³⁶ Vgl. in diesem Zusammenhang SBF, Circular 2019/01, *passim*.

²⁶³⁷ Nach Art. 36 Abs. 1 lit. b FIDLEG ist ohnehin kein Prospekt zu veröffentlichen, wenn das «öffentliche Angebot» sich an weniger als 500 Anleger richtet.

Abschliessend zu erwähnen ist, dass das öffentliche Angebot gemäss Art. 35 Abs. 1 FIDLEG «in der Schweiz» unterbreitet werden muss.²⁶³⁸ Aus der Tatsache, dass der Handel über dezentrale Handelsplattformen global ist – zumindest, wenn das Frontend zu den Smart Contracts für jedermann frei zugänglich ist –,²⁶³⁹ könnte geschlossen werden, dass dieses Kriterium ohne Weiteres zu bejahen ist. Die FINMA stellte im Rahmen der Einordnung des Vertriebs von kollektiven Kapitalanlagen in der Schweiz darauf ab, ob Indizien in ihrer Gesamtwirkung einen Bezug zur Schweiz herstellen.²⁶⁴⁰ Nach Aussage des EFD ist davon auszugehen, dass diese Praxis auch unter dem FIDLEG weiterhin von Relevanz ist.²⁶⁴¹ Die blosser Erreichbarkeit eines Frontends oder die Möglichkeit, eine Software über eine Webseite herunterzuladen, genügen mit anderen Worten nicht, um von einem in der Schweiz unterbreiteten öffentlichen Angebot auszugehen. Allenfalls relevant kann zudem auch sein, ob der Liquiditätsgeber im Rahmen seiner Kommunikation, etwa über seine Webseite, gewisse territoriale und personale Einschränkungen hinsichtlich des von ihm unterbreiteten Angebots vornimmt.²⁶⁴² MATTHIAS COURVOISIER geht weiter, wenn er ein *direktes* Adressieren von Anlegern in der Schweiz verlangt. Er führt zur Begründung aus, dass der ehemalige Vertriebsbegriff der FINMA deutlich weiter geht als der neue Angebotsbegriff unter FIDLEG.²⁶⁴³

c. Publikation von Informationen durch Frontend-Betreiber

Abschliessend sei erwähnt, dass die namentliche Nennung, Bekanntmachung oder Publikation von bspw. Preisen zu Finanzinstrumenten und deren Kursentwicklungen oder die blosser Zurverfügungstellung von faktischen Informationen zu Finanzinstrumenten nicht als Angebote im Sinne von Art. 3 lit. g FIDLEG qualifizieren.²⁶⁴⁴ Dies befreit insb. die Betreiber von Frontends zu de-

²⁶³⁸ Vgl. hierzu Spillmann/Giger, GesKR 2019, 190.

²⁶³⁹ Vgl. demgegenüber das von einigen Frontends implementierte *Geoblocking* basierend auf der IP-Adresse des Webseitenbesuchers; vgl. etwa Bancor, Service Restrictions, *passim*.

²⁶⁴⁰ Siehe das inzwischen aufgehobenen FINMA-RS 13/9 «Vertrieb kollektiver Kapitalanlagen», Rz. 68–74.

²⁶⁴¹ Siehe EFD, Erläuterungen FIDLEV/FINIV/AOV 2019, 21–22; so auch SK FIDLEG-Bösch/Leisinger, Art. 35 N 10.

²⁶⁴² Siehe hinsichtlich Disclaimer und Zugangsbeschränkung der Webseite FINMA-RS 13/9 «Vertrieb kollektiver Kapitalanlagen», Rz. 76–79.

²⁶⁴³ Siehe Courvoisier, SZW 2020, 310; *differenzierend* Abegglen/Wettstein, SZW 2018, 133–135.

²⁶⁴⁴ Art. 3 Abs. 3 lit. b und c FIDLEV; vgl. ausführlich hierzu EFD, Erläuterungen FIDLEV/FINIV/AOV 2019, 22.

zentralen Handelsplattformen und insb. von Webseiten, welche in aggregierter Form Handelsinformationen zusammenführen, von einer allfälligen Prospektpflicht unter Schweizer Recht.

Unklar ist allerdings, ob der Betreiber eines solchen Frontends ein Angebot macht, wenn er über die «Plattform» zusätzlich auch den direkten Kauf der angezeigten Finanzinstrumente erlaubt.²⁶⁴⁵ Ob das Bereitstellen von Informationen und Unterlagen zu Finanzinstrumenten auf einer Plattform als Angebot gilt oder nicht, ist nach Auffassung des EFD nach den Umständen, insb. nach der konkreten Ausgestaltung der Information und der Plattform, zu entscheiden.²⁶⁴⁶ RENÉ BÖSCH und BENJAMIN LEISINGER gehen davon aus, dass kein Angebot auf einer Plattform vorliegt, die lediglich zu Informationszwecken genutzt oder bereitgestellt wird. Dies gelte selbst dann, wenn die Nutzer der Plattform ein Kaufinteresse bei den (externen) Finanzdienstleistern anmelden oder etwa direkt auf der Plattform einen Kaufauftrag eingehen können.²⁶⁴⁷

Der Erwerb und die Veräusserung von Kryptovermögenswerten über solche Webseiten stellt in den meisten Fällen zwar gerade der eigentliche Betriebszweck dar. Allerdings sind die Frontends lediglich *Schnittstellen* zu den eigentlichen Plattformen. Sie fungieren primär als «Publikationsfenster» für die Handelsinformationen der dezentralen Handelsplattformen. Sie sind nach vorliegender Auffassung zu weit vom eigentlichen Angebot entfernt, soweit ein solches überhaupt vorliegt, und vom darauffolgenden Erwerbs- bzw. Veräusserungsgeschäft, in welches sie in keiner Art und Weise involviert sind. Dies zeigt sich auch daran, dass die von ihnen publizierten Informationen sich typischerweise auf eine Vielzahl von Kryptovermögenswerten beziehen. Der Betreiber eines Frontends will in vertrauenstheoretischer Hinsicht gerade nicht spezifisch auf ein «bestimmtes Finanzinstrument» im Sinne von Art. 3 Abs. 5 lit. b FIDLEG aufmerksam machen, um «dieses zu veräussern».²⁶⁴⁸ Selbstredend stellt sich zudem auch hier die oben erwähnte Thematik des territorialen Geltungsbereichs von Art. 35 FIDLEG.

²⁶⁴⁵ So EFD, Erläuternder Bericht FIDLEG/FINIV/AOV 2018, 20.

²⁶⁴⁶ Siehe hierzu EFD, Erläuterungen FIDLEG/FINIV/AOV 2019, 21.

²⁶⁴⁷ Siehe SK FIDLEG-Bösch/Leisinger, Art. 3 lit. f-i N 10.

²⁶⁴⁸ Vgl. auch Spillmann/Giger, GesKR 2019, 189–190; ferner SK FIDLEG-Bösch/Leisinger, Art. 3 lit. f-i N 11, die auch ausdrückliche Hinweise der Plattform, dass es sich nicht um ein Angebot handelt, genügen lassen; ebenso BSK FIDLEG/FINIG-Bahar/Weber, Art. 3 lit. g FIDLEG N 17.

7. Zusammenfassung Kapitel V

Das vorliegende Kapitel wendet sich der Einordnung dezentraler Handelsplattformen in das geltende Schweizer Finanzmarktrecht zu:

Im *ersten Abschnitt* werden die rechtlichen Grundlagen erarbeitet, die im späteren Verlauf der Arbeit von Relevanz sind. Aufgrund der Globalität und Multilateralität dezentraler Systeme handelt es sich dabei um wirtschaftskollisionsrechtliche Aspekte, das Konzept des Finanzintermediärs als Anknüpfungspunkt in Binnenverhältnissen, aber auch bei Sachverhalten mit ausländischem Bezug und das finanzmarktrechtliche Konzept der arbeitsteilig vorgehenden Gruppe.

Der *zweite Abschnitt* wendet sich sodann dem Geldwäschereirecht zu. In den meisten aktuellen Diskussionen werden dezentrale Systeme und Kryptovermögenswerte v.a. aus geldwäschereirechtlicher Sicht untersucht. Dabei zeigt sich, dass in der Literatur keine einheitliche Meinung darüber besteht, wie gross das Geldwäschereirisiko im Zusammenhang mit Kryptovermögenswerten tatsächlich ist. Als heute überwiegend relevantes Anknüpfungskriterium im Geldwäschereirecht gilt der Begriff der Finanzintermediation (vgl. Art. 2 Abs. 3 GwG). Dieser Begriff ist nach vorliegender Ansicht so auszulegen, dass er grundsätzlich ausschliesslich die Intermediation fremder Vermögenswerte im Finanzsektor betrifft. Das konkrete Geldwäschereirisiko einer unter diesen Tatbestand fallenden finanzintermediären Tätigkeit ist gegebenenfalls als Korrektiv einzusetzen, um risikoarme Aktivitäten von der Unterstellung auszunehmen.

Sodann erfolgt ein Unterabschnitt, der sich genauer mit dezentralen Handelsplattformen im Geldwäschereirecht auseinandersetzt. Im Vordergrund steht dabei die Frage, ob bei dezentralen Handelsplattformen überhaupt von einer finanzintermediären Tätigkeit gesprochen werden kann. Mangels alleiniger Verfügungsmacht über fremde Vermögenswerte durch eine Person, welche mit den Nutzern der Plattform nicht identisch ist, kommt dies in der Regel nicht in Betracht. Eine Analyse des kürzlich eingeführten Art. 4 Abs. 1 lit. b GwV zeigt hingegen, dass der Bundesrat vom vorherrschenden Finanzintermediationsbegriff bewusst abweicht, um gewisse Formen des Austausches von virtuellen Währungen zu erfassen, die bisher kaum oder nicht unter den Finanzintermediationsbegriff subsumiert werden konnten. Er verzichtet namentlich auf das Kriterium der alleinigen Verfügungsmacht über fremde Ver-

mögenswerte. Neu gelten Aktivitäten der Hilfe zur Übertragung von virtuellen Währungen als eine unterstellte Dienstleistung für den Zahlungsverkehr, soweit eine dauernde Geschäftsbeziehung zwischen dem Plattformbetreiber und seinen Kunden besteht. Dezentrale Handelsplattformen sollen nach vorliegender Auffassung nur dann geldwäschereirechtlich erfasst werden, wenn eine Drittperson tatsächlich relevante Kontrollmöglichkeiten über eine Plattform ausüben kann. P2P-Transaktionen und Transaktionen über Plattformen, die ausschliesslich unmittelbar zwischen den beteiligten Begünstigten ablaufen, ohne dass eine Drittperson die effektive Zugriffsmöglichkeit auf die involvierten Vermögenswerte und Transaktionsflüsse hat, sind nach vorliegender Auffassung in geldwäschereirechtlicher Hinsicht gleich zu behandeln und somit nicht zu unterstellen.

Ferner wird die Aktivität der Bereitstellung von Liquidität über dezentrale Handelsplattformen genauer untersucht. Solche Geschäfte können im Falle virtueller Währungen als unterstellte Wechselgeschäfte eingestuft werden. Diesbezüglich zeigen sich Probleme der GwG-Compliance. Die Gegenparteien beim Handel von Kryptovermögenswerten über dezentrale Handelsplattformen sind oft nicht namentlich bekannt und entsprechend kann ein Liquiditätsbereitsteller die Sorgfaltspflichten nicht einhalten, soweit sie auf ihn zur Anwendung gelangen. In einem Exkurs werden sodann die Auswirkungen von Art. 4 Abs. 1 lit. b GwV auf die unterschiedlichen Wallet-Typen analysiert. Dabei zeigt sich, dass v.a. in Bezug auf Multisig-Wallets und Self-Hosted Wallets Rechtsunsicherheiten bestehen.

Anschliessend beschäftigt sich ein Unterabschnitt mit dem Thema der FATF-Empfehlungen. Es zeigt sich insb. in der jüngsten Guidance vom Oktober 2021 zu VAs und VASPs, dass eine deutliche Ausdehnung der unterstellten Aktivitäten propagiert wird. Ein ausgedehnter VASP-Begriff könnte insb. auch einige Typen dezentraler Handelsplattformen regulatorisch erfassen. Zwar ist die FATF-Guidance lediglich Teil der Empfehlungen und somit unverbindlich,²⁶⁴⁹ doch sind die politischen Wirkungen auf das nationalstaatliche Recht bekanntlich sehr ausgeprägt.

Sodann wird die Teilnahme an dezentralen Netzwerken aus geldwäschereirechtlicher Sicht analysiert. Dabei zeigt sich, dass etwa Consensus Nodes (Miner bzw. Staker), Full Nodes oder Teilnehmer des Lightning Netzwerks nicht

²⁶⁴⁹ Siehe etwa FATF, VASP Guidance 2021, 13; vgl. hierzu Abegg/Bärtschi, in: Abegg/Bärtschi/Dietrich, § 2 Rz. 247.

dem GwG unterstellt sind. Zum gleichen Ergebnis kommt die Arbeit in Bezug auf die Entwicklung von Software, welche im Rahmen von DeFi-Anwendungen eingesetzt wird.

Der zweite Abschnitt endet ausnahmsweise mit einem Fazit, welche auf die mannigfaltigen Spannungsverhältnisse im heutigen Geldwäschereiregime hinweist. In erster Linie geht es um die feststellbare Tendenz, alle möglichen Erscheinungsformen des DeFi-Marktes in das vorherrschende Finanzintermediationsmodell hineindrängen zu wollen. Gleichzeitig wird insb. die Wirksamkeit des heutigen Regimes hinterfragt. Im Gegenzug werden alternative Ansätze zur Diskussion gestellt, welche allerdings einen schwierigen Balanceakt zwischen den berechtigten Interessen der Nutzer dezentraler Applikationen am Schutz ihrer persönlichen Daten, ihrer Privatsphäre und ihrer Persönlichkeitsrechte einerseits und legitimen Strafverfolgungsinteressen andererseits vornehmen muss. Bei Verfolgung des von der FATF vorgezeichneten Wegs würde die Bifurkation des heutigen Finanzsystems drohen.

Im *dritten* Abschnitt werden dezentrale Handelsplattformen aus der Perspektive des Finanzmarktinfrastrukturrechts untersucht. Nach Klärung einiger Begrifflichkeiten befasst sich ein Unterabschnitt mit der Frage, ob dezentrale Handelsplattformen als DLT-Handelssysteme im Sinne von Art. 73a ff. FinfraG qualifizieren können. Dabei werden die funktionalen Parallelen und Unterschiede herausgearbeitet. Ein wesentlicher Teil beschäftigt sich mit der rechtlichen Abgrenzung dezentraler Handelsplattformen zu DLT-Handelssystemen. Dabei zeigt sich, dass für viele Typen dezentraler Handelsplattformen nicht von einem Handelssystem im Sinne des FinfraG gesprochen werden kann. Zudem mangelt es systembedingt an einem Betreiber, welcher eine Einrichtung im rechtlichen Sinne betreibt. Schliesslich erfüllen dezentrale Handelsplattform aus Sicht der Plattform auch nicht den Gewerbmässigkeitsbegriff. Nach einem kurzen Fazit widmen sich eigenständige Unterabschnitte unterschiedlichen Fragestellungen, die sich im Kontext dezentraler Handelsplattformen stellen. Dabei handelt es sich insb. um die Frage, inwieweit Emittenten eigene Smart Contract-basierte Handelslösungen betreiben können, ohne vom FinfraG erfasst zu sein, und ob Liquiditätsgeber als Anbieter eines Wertrechtereigisters im Sinne von Art. 973d ff. OR gelten können, was in der Praxis in aller Regel zu verneinen ist.

Ein weiterer Unterabschnitt untersucht sodann die Frage, ob dezentrale Handelsplattformen als Zentralverwahrer qualifizieren können. Dies wird grundsätzlich verneint, obschon Smart Contract-basierte Plattformen ansatzweise Ähnlichkeiten mit Effektenabwicklungssystemen aufweisen.

Der *vierte* Abschnitt beschäftigt sich sodann mit dem Bankenrecht. Im Zentrum stehen die Tätigkeiten der Entgegennahme von Publikumseinlagen und die Entgegennahme und Verwahrung von kryptobasierten Vermögenswerten. Nach eingehender Auseinandersetzung mit den Begrifflichkeiten und einem ausführlichen Exkurs zur Aus- und Absonderungsfähigkeit von Kryptovermögenswerten im Konkurs eines Intermediärs kommt die Arbeit zum Schluss, dass dezentrale Handelsplattformen in aller Regel weder Publikumseinlagen entgegennehmen noch kryptobasierte Vermögenswerte im Sinne des Gesetzes entgegennehmen und verwahren.

Im *fünften* Abschnitt steht das Finanzinstitutsrecht im Fokus. Anschliessend an allgemeine Ausführungen zum Effektenhandel kommt die Arbeit zum Schluss, dass dezentrale Handelsplattformen selbst nicht in den Effektenhandel involviert sind. Demgegenüber können Nutzer der Plattform als Kundenhändler oder Market Maker bzw. Eigenhändler qualifizieren. Gerade mit Blick auf das Market Making stellen sich einige Abgrenzungsfragen, welche in der Praxis im Einzelfall zu klären sind. Typischerweise ist aber beim AMM-Modell nicht von Market Making im Sinne des FINIG auszugehen. Sodann geht der Abschnitt auch auf das Konzept des Initial Decentralized Exchange Offerings ein, gemäss welchem ein Emittent seine Token direkt über eine dezentrale Handelsplattform herausgibt und/oder zum Handel anbietet. Zumindest Eigen- bzw. Selbstemissionen dürften aus Sicht des FINIG nicht relevant sein.

Das Kapitel endet mit einem *sechsten* Abschnitt zum Finanzdienstleistungsrecht. Die erste Haupttätigkeit unter dem FIDLEG ist das Erbringen einer Finanzdienstleistung. Dabei kommen einmal mehr verschiedene Aktivitäten im Kontext dezentraler Handelsplattformen als potenziell regulierte Finanzdienstleistungen infrage. Klar ist, dass dezentrale Handelsplattform selbst nicht als Finanzdienstleister zu qualifizieren sind. Nutzer dezentraler Handelsplattformen sind mangels eines Intermediationsverhältnisses ferner weniger schutzbedürftig. Anders stellt sich die Situation dar, wenn die Kunden eines Finanzdienstleisters eine dezentrale Handelsplattform indirekt in Anspruch nehmen. In diesem Fall greift das FIDLEG in aller Regel, soweit es sich um den Erwerb oder die Veräusserung von Finanzinstrumenten handelt. Schwierig abzugrenzen ist sodann die Frage, ob und unter welchen Umständen die Bereitstellung von Liquidität über eine dezentrale Handelsplattform als Finanzdienstleistung qualifiziert. Dabei spielt auch die vertragsrechtliche Dimension des Austauschgeschäftes eine Rolle. Die reine Softwareentwicklung ist schliesslich dem FIDLEG nicht unterstellt, da es sich dabei nicht um eine Finanzdienstleistung handelt.

Der zweite Unterabschnitt zum FIDLEG beschäftigt sich mit dem Anbieten von Finanzinstrumenten über dezentrale Handelsplattformen. Potenziell prospektpflichtig ist eine Person, welche einer dezentralen Handelsplattform, die öffentlich zugänglich ist, Liquidität zuführt. Oft wird in diesem Fall ein öffentliches Angebot zum Erwerb vorliegen, soweit es sich bei den Kryptovermögenswerten um Effekten handelt. Demgegenüber löst die Publikation von handelsbezogenen Informationen durch Frontend-Betreiber, welche auch den Erwerb und die Veräußerung von Kryptovermögenswerten ermöglichen, in aller Regel noch keine Prospektpflicht aus.

VI. Ansätze für die Regulierung dezentraler Handelsplattformen

Many policy prescriptions [...] advocate oversimplified, idealized institutions – paradoxically, almost ‘institution-free’ institutions

– Elinor Ostrom²⁶⁵⁰

1. Herausforderungen für Aufsicht und Regulierung

1.1 Herausforderungen

Dezentrale Systeme fordern das Finanzmarktrecht heraus. Sie lassen sich nicht ohne Weiteres in das vorherrschende Regulierungsmodell, welche an die Finanzintermediation anknüpft, einordnen. In mehrerer Hinsicht stellen sich dabei Probleme:

- konzeptionelle und terminologische Schwierigkeiten;
- Infragestellung der Geltungs- und Anwendungshoheit bestehender Regeln bei transnationalen Sachverhalten;
- praktische Herausforderungen im Rahmen der Anwendbarkeit und Durchsetzbarkeit bestehender Regeln;
- Fehlen eindeutiger Verantwortlichkeiten für Aktivitäten und/oder deren Folgen.

Unzählige wissenschaftliche Beiträge, Berichte und amtliche Stellungnahmen weisen auf die erwähnten Schwierigkeiten in der Regulierung und Aufsicht hin.²⁶⁵¹ Die Rede ist von der fehlenden oder eingeschränkten Regulierbarkeit

²⁶⁵⁰ Ostrom, *Governing the Commons*, 22.

²⁶⁵¹ Siehe statt vieler Shcherbak, *European Journal of Legal Studies* 2014, 78; FATE, *New Technologies for AML/CFT*, 26; FSB, *Crypto-assets*, 6 («crypto-asset platforms»); IMF, *Crypto Ecosystem*, 46; Nabilou, *International Journal of Law and Information Technology* 2019, 278–279; Bärtschi/Hirschi, *SZW* 2017, 790; Jacquemart, *Offene Blockchainsysteme*, Rz. 593 m.w.N.; Cohen/Angelovska-Wilson/Strong, *Decentralized Finance*, *passim*; Clements,

der von der Technologie möglich gemachten Aktivitäten (*regulability*).²⁶⁵² Die damit einhergehenden Schwierigkeiten wirken sich selbsttendend auf den regulatorischen Anleger- und Funktionsschutz aus; sie bedeuten jedoch nicht zwingend ein tieferes Schutzniveau im Finanzmarkt. Aufgrund der mit dezentralen Systemen verbundenen Risiken ist den Interessen an einem angemessenen Schutz der Nutzer solcher Protokolle und des Gesamtmarktes Rechnung zu tragen.

Als aufsichtsrechtlich gravierendstes Problem der Regulability wird die Verantwortlichkeitsfrage bezeichnet.²⁶⁵³ *Worin besteht die relevante Aktivität? Übt eine bestimmte Person oder eine bestimmte Gruppe von Personen die beobachtbaren Aktivitäten aus? Wo sind diese Personen ansässig? Was sind ihre bürgerlichen Identitäten?*²⁶⁵⁴ Diese Fragen lassen sich allerdings bei einer Vielzahl beteiligter und involvierter Personen und semiautonomem Computer, die lediglich in einer faktischen Beziehung zueinanderstehen, nicht mehr ohne Weiteres beantworten.²⁶⁵⁵ Denn man könnte argumentieren, dass DeFi-Anwendungen überall und gleichzeitig nirgendwo sind; sie sind überall dort, wo Netzwerkteilnehmer sind, und gleichzeitig ist keiner ihrer Beitrag genügend massgeblich, um einen eindeutigen Anknüpfungspunkt zu bestimmen. Die Transnationalität globaler Netzwerke verschärft zudem den Umstand, dass das Recht weiterhin in erster Linie Binnensachverhalte regelt und die Rechtsordnung jenseits der Grenzen regelmässig auch ihre eigenen Grenzen findet.²⁶⁵⁶ Ganz anders verhält es sich mit Computercode.

Banking and Finance Law Review 2021, 23 («Uniswap uses open source code; therefore, the possibility for copycat decentralized crypto exchanges, outside of securities regulatory jurisdiction is endless.»), 27; Kerkemeyer, ZGR 2020, 677–678, 685; Paech, The Modern Law Review 2017, 1085, 1101–1102; EP, Cryptocurrencies and blockchain, 77 («very hard to regulate»); EP, Crypto-assets, 52; Hofert, Regulierung der Blockchains, 53, 57; Omarova, Journal of Financial Regulation 2020, 94; Maurenbrecher/Leisinger, SJZ 2022, 710–711; Humbel/Eckert, GesKR 2023, 18–21; Zetzsche et al., Remaining regulatory challenges, 50–51, welche die spieltheoretischen Erwägungen der Teilnehmer, sich nicht an die Regeln zu halten, betonen. Unklar ist allerdings, welche Regeln im Einzelfall gelten würden.

²⁶⁵² Siehe Takanashi et al., Stanford Journal of Blockchain Law & Policy 2020, 9.

²⁶⁵³ So etwa Cohen/Angelovska-Wilson/Strong, Decentralized Finance, *passim*; ferner Bundesrat, Digital Finance, 14.

²⁶⁵⁴ Ähnlich bereits für das Internet Lessig, Laws of cyberspace, 19–20.

²⁶⁵⁵ Siehe etwa WEF, Decentralized Finance, 18, 21–22; Jutzi/Abbühl, Fintech und DLT, Rz. 510, 1343; ferner die Hinweise in FATF, VASP Guidance 2021, 27–28, 33; ausführlich zur Frage der Verantwortlichkeit aus Sicht der CFTC sodann Quintenz, Remarks at GITEX, *passim*.

²⁶⁵⁶ Vgl. Senn, ZSR 2015 I, 509–510 («Die Komplexität der globalen Beziehungen und die Vielfalt der rechtlichen Vorschriften, die durch Dezentralisierung und Fragmentierung gekennzeichnet sind, müssen gesteuert werden. In einer dezentralen und fragmentierten Welt gibt es verschiedene Formen der staatlichen und privaten sowie transnationalen Regulierungen, was

Sozial skalierende Netzwerke und Applikationen, die den ganzen Globus umspannen, scheinen zudem auch für die anderen Rechtsgebiete unüberwindbare Hürden aufzustellen. Deliktisch und strafrechtliche Ansprüche kommen oftmals an den Grenzen des Territoriums zum Erliegen, wie die Erfahrungen mit dem The DAO-Hackerangriff zeigen. Diese nüchtern zu betrachtenden Tatsachen lassen sich nicht einfach «wegregulieren».

Die schweizerischen Behörden haben denn auch die Grenzen der Regulierung dezentraler Systeme bereits früh (an)erkannt: *«Die Tatsache, dass Bitcoins kaum von zentralen Stellen verwaltet werden und somit keine Ansprechpartner für Strafverfolgungsbehörden existieren, erschwert die effiziente Aufklärung von Straftaten sowie die konsequente Einziehung von Vermögenswerten. Ausserdem kennt der Bitcoin als dezentrales Zahlungssystem keine Grenzen, und kann folglich nicht zu einem Hoheitsgebiet zugeordnet werden.»*²⁶⁵⁷ HESTER PEIRCE, Kommissionsmitglied der US-amerikanischen Wertpapieraufsichtsbehörde, bringt die Herausforderungen ebenfalls auf den Punkt: *«Our whole rulebook is built around the notion that you've got these intermediaries. So when you take them out of the picture our job as regulators becomes very difficult[.]»*²⁶⁵⁸ Sodann schreibt die OECD mit Blick auf dezentrale Handelsplattformen in einem Bericht von 2020: *«The absence of single point that can be held responsible for the operation of the exchange/trading platform makes regulatory compliance and the enforcement of regulation difficult in decentralised exchanges/trading platforms.»*²⁶⁵⁹

Ein eindrückliches Praxisbeispiel aus dem Bereich dezentraler Handelsplattformen für diese neuen Realitäten ist das Verfahren der SEC gegen den Gründer von EtherDelta. Obschon Coburn der Betrieb der Plattform in der Unterlassungsanordnung untersagt wurde und er, soweit ersichtlich, dieser Anordnung nachgekommen ist, existieren die Smart Contracts weiterhin auf der Ethereum Blockchain.²⁶⁶⁰ In diesem Zusammenhang ist erwähnenswert,

dazu führt, dass das Expertenwissen, die Macht und die Kontrolle nicht mehr bei einem Akteur zentralisiert sind. Sie sind vielmehr verstreut und kein Akteur kann den Anspruch erheben, über das gesamte Wissen und die gesamte Macht zu verfügen oder alles kontrollieren zu können.»).

²⁶⁵⁷ Bundesrat, Virtuelle Währungen, 27; ferner Bundesrat, DLT-Bericht 2018, 115–116; Bottschaft DLT 2019, 273.

²⁶⁵⁸ Zitiert in Wolfson, New convos for regulators, *passim*.

²⁶⁵⁹ OECD, Tokenisation and Implications for Financial Markets, 30.

²⁶⁶⁰ Siehe für die Adresse des Smart Contracts <https://etherscan.io/address/0x4aea7cf559f67cedcad07e12ae6bc00f07e8cf65>; dies ebenfalls anerkennend Quintenz, Remarks at GITEX, *passim* («[e]nforcing CFTC regulations against [smart contract developers] does not

jedoch wenig überraschend,²⁶⁶¹ dass ausschliesslich der Betreiber ins Visier genommen wurde, obwohl er bereits einige Zeit davor die Plattform an eine Drittperson verkauft hatte, welche die Plattform mutmasslich seither betreibt.²⁶⁶² An dieser Realität dezentraler Systeme konnte auch die wohl mächtigste Finanzmarktaufsichtsbehörde der Welt nichts ändern.

1.2 Codebeispiel

Die Dezentralität gewisser Typen dezentraler Handelsplattformen kann eindrücklich am verwendeten Quellcode veranschaulicht werden. Ein Beispiel: Der Code eines Smart Contracts, der vom Schweizer Unternehmen Mt Pelerin Group AG entwickelt wurde, erlaubt den uneingeschränkten Austausch von Kryptovermögenswerten zwischen zwei Personen über die Ethereum Blockchain.²⁶⁶³ Zurückgegriffen wird auf ein On-chain-Orderbuch mit integrierter Matching-Engine. Der Code umfasst gut 1'000 Zeilen in der Programmiersprache Solidity.²⁶⁶⁴ Mt Pelerin Group AG ist in keiner Weise in den Austausch involviert.

1.3 Fazit

Die Gründe für die oben erwähnten Herausforderungen sind schnell festzumachen: Dezentrale Systeme sind global agierende, computergesteuerte Softwareprogramme, die grundsätzlich von jedermann von überall auf der Welt verwendet werden können. Die einzigen Voraussetzungen sind ausschliesslich technischer Natur, namentlich ein Internetzugang und ein Gerät, um die entsprechenden Applikationen auszuführen.

Die Regeln des heutigen Finanzmarktrechts sind demgegenüber in einer Zeit der Ubiquität der Finanzintermediation und territorialer Begrenzungen entstanden. Daran ändern auch die Globalisierung und Digitalisierung der Finanzmärkte nichts. Die Anwendbarkeit und Durchsetzbarkeit der Regeln beruhen auf der Tatsache, dass die für eine unterstellte Aktivität verantwortliche Person feststellbar ist und zumindest theoretisch den Behörden zugeführt wer-

immediately stop the activity from occurring, because individual users could continue to use the software [...]»).

²⁶⁶¹ Siehe CleanApp, Individual Liability, *passim*.

²⁶⁶² Siehe hierzu oben, [IV.3.6a](#).

²⁶⁶³ Die Adresse lautet: 0x38B7EC49EC1369209fB273fD7e21bFe9D159dC83.

²⁶⁶⁴ Siehe Mt Pelerin, bridge-v2, GitHub, *passim*.

den kann. In dezentralen Systemen muss demgegenüber eine Person weder ihre Identität offenlegen noch müssen die Folgen einer Aktivität zwingend auf menschliches Handeln zurückgeführt werden.

Die vorliegende Arbeit vertritt dezidiert die Auffassung, dass das heutige Finanzintermediationsmodell *nicht* ausgedient hat. Im Gegenteil soll es vollumfänglich und ohne grosse Anpassungen auf die an dezentralen Systemen beteiligten Personen zur Anwendung gelangen, *falls* diese von den entsprechenden persönlichen, sachlichen, räumlichen und zeitlichen Geltungsbereichen erfasst sind.²⁶⁶⁵ In weiten Teilen hat der Bundesrat dieser Aufforderung bereits nachgelegt.²⁶⁶⁶

Gleichzeitig wird vorliegend aber auch entschieden die Ansicht vertreten, dass die Regeln der Finanzintermediation für dezentrale Phänomene ungeeignet sind, ja sogar schädlich sein können. Die Schädlichkeit bezieht sich dabei insb. auf die potenzielle Innovationsfeindlichkeit von Regulierung und Aufsicht, indem diese dezentralen Systemen ihren Finanzintermediationsansatz zu überstülpen versuchen.²⁶⁶⁷ Im Ergebnis ist damit eine *teilweise Abkehr vom Finanzintermediationsmodell* heutiger Regulierung verbunden.

Die Arbeit plädiert demgegenüber dafür, abzuklären, mit welchen *anderen* Mitteln Anleger (besser: Nutzer) und die Funktionsfähigkeit der Märkte geschützt werden können. Anlegerschutz scheint in erster Linie darum relevant zu sein, da Dezentralität die Verantwortung vermehrt auf die Nutzer verlagert. Funktionsschutz könnte demgegenüber dann angezeigt sein, wenn traditionelle Märkte von unerwünschten Auswirkungen dezentraler Systeme betroffen sind. Die vorliegende Arbeit vertritt die Auffassung, dass markt- und technologienahe Instrumente eingesetzt werden sollten, deren Erlass zudem die beteiligten Akteure eng einzubinden hat.²⁶⁶⁸ Vorab soll allerdings der Frage nachgegangen werden, weshalb ein Technologieverbot als Regulierungsinstrument nicht in Frage kommt.

²⁶⁶⁵ Vgl. Jacquemart, Offene Blockchainsysteme, Rz. 596, welcher die Regulierung der Finanzintermediäre als «am praktikabelsten» bezeichnet; hinsichtlich Verhinderung der Geldwäscherei sodann Hofert, Regulierung der Blockchains, 62

²⁶⁶⁶ Siehe statt vieler Bundesrat, DLT-Bericht 2018, 9–11, wo zusammenfassend die grundsätzliche Ausrichtung des Rechts auf die bestehenden Finanzmarktakteure bestätigt wird.

²⁶⁶⁷ Ebenfalls *skeptisch* Altschuler, Stanford Journal of Blockchain Law & Policy 2022, *passim*; hinsichtlich der Übernahme der Wertpapierregulierung Brummer, Stanford Journal of Blockchain Law & Policy 2022, 146–151; Humbel, GesKR 2022, 25.

²⁶⁶⁸ Vgl. in diesem Zusammenhang Boehme-Neßler, NJW 2017, 3037, der für eine *grundsätzliche Neuerfindung des Rechts* unter Berücksichtigung von Software und Technologie plädiert.

2. Unmöglichkeit eines Technologieverbots

2.1 Vorbemerkungen

Angesichts der konzeptionellen und praktischen Schwierigkeiten des Finanzmarktrechts im Umgang mit dezentralen Systemen stellt sich die Frage, wie der Gesetzgeber angemessen reagieren könnte. In Frage käme – notabene als Extremmassnahme – der Erlass eines *Technologieverbots*.²⁶⁶⁹ Ein Verbot verschiedener Aktivitäten im Kontext dezentraler Systeme hätte erwartungsgemäss einen gewissen Einfluss auf das Verhalten der betreffenden Personen. Allerdings ist zu beachten, dass ein Technologieverbot in erster Linie unter grundrechtlichen Gesichtspunkten problematisch sein dürfte.²⁶⁷⁰ Davon zu unterscheiden ist sodann der Umstand, dass ein Verbot mit relativ einfachen Mitteln umgangen werden könnte und zu einer globalen Regulierungsarbitrage führen dürfte.²⁶⁷¹

2.2 Nutzung dezentraler Systeme

a. Meinungs- und Informationsfreiheit

Im Kern erlauben die Protokolle dezentraler Systeme die Errichtung von *Kommunikationsnetzwerken*. Nach bundesgerichtlicher und EGMR-Rechtsprechung umfasst der sachliche Schutzbereich der Meinungs- und Informationsfreiheit gemäss Art. 16 BV bzw. Art. 10 Abs. 1 EMRK die Gesamtheit der Mitteilungen menschlichen Denkens und alle möglichen Kommunikationsformen.²⁶⁷² Dass diese für die Offlinewelt geschaffenen Grund- bzw. Freiheits-

²⁶⁶⁹ Vgl. zum Technologie- bzw. Technikverbot als *Extremform* der Regulierung von neuen Technologien Errass, Sicherheit & Recht 2016, 77; ferner Hettich, Kooperative Risikoversorge, Rz. 288.

²⁶⁷⁰ Vgl. zur Finanzinnovation auch Möslein, in: Möslein, Finanzinnovation und Rechtsordnung, 33–34, 35–36, der zudem auf die Möglichkeit der Regulierungsarbitrage hinweist.

²⁶⁷¹ Vgl. ausführlich zum Verbot, als Netzwerkteilnehmer eine Software auszuführen, Jacquemart, Offene Blockchainsysteme, Rz. 540–544, sodann zum Verbot, Software zu entwickeln, Rz. 549, und schliesslich zum Nutzungsverbot Rz. 561–565.

²⁶⁷² Siehe BGE 127 I 145, E. 4b; 144 I 126, E. 4.1; 137 I 209, E. 4.2; vgl. ferner BGE 138 II 346, E. 10.5 («Google Street View»); ferner betreffend eine Übersicht der EGMR-Rechtsprechung zu

rechte auch auf internetbasierte Kommunikation zur Anwendung gelangen, ist heute unbestritten.²⁶⁷³

Die Kommunikationsform von Mitteilungen in dezentralen Systemen ist internet- und somit datenbasiert. Im Fall einer einfachen Transaktion teilt eine Person durch Veröffentlichung eines mit ihrem Private Key signierten Datenpakets dem gesamten Netzwerk mit, dass der Inhaber des im Datenpaket mit-signierten Public Keys die exklusive Verfügungsmöglichkeit über den dezentral abgespeicherten Datensatz haben soll. Mitteilungen müssen dabei nicht ausschliesslich Zahlungsmittelfunktion ausüben. Sie können darüber hinaus beliebigen Inhalts sein, da Transaktionen die Übermittlung von *Metadaten* erlauben. Mit dem *Colored Coin*-Protokoll etwa lassen sich über die Bitcoin Blockchain Datenpakete übertragen, die mit jeglichen Arten von (externen) Vermögenswerten oder sonstigen Informationen verknüpft sind.²⁶⁷⁴ Ferner lassen sich mithilfe von IPFS-Hashes dezentral abgespeicherte Datensätze über ein verteiltes Register eines dezentralen Netzwerks verbreiten.²⁶⁷⁵ Welcher Natur die mittels Hash referenzierten Datensätze sind, ist grundsätzlich nicht erkennbar, allerdings *könnte* es sich bspw. eine politische Aussage handeln.

Für Aussenstehende ist folglich oft nicht klar, welcher Natur die Informationen sind, die Nutzer miteinander teilen. Nun besteht allerdings keine Notwendigkeit, den Inhalt internetbasierter Kommunikation gegenüber Drittpersonen offenzulegen. Denn Meinungsfreiheit und das Recht auf Schutz der Privatsphäre sind eng miteinander verbunden.²⁶⁷⁶ In der Nutzung von dezentralen Systemen kann aufgrund des Gesagten ohne Weiteres eine Mitteilung menschlichen Denkens gesehen werden, welche grundsätzlich in den Gel-

Art. 10 EMRK Hertig Randall, SRIEL 2016, 236–239; schliesslich aus der Perspektive des 1. Zusatzartikel der US-amerikanischen Verfassung Wales/Ovelmen, University of Miami Law Review 2019, insb. 252–265.

²⁶⁷³ Siehe mit Blick auf Art. 19 Allgemeine Erklärung der Menschenrechte (AEMR) sowie Art. 19 Abs. 1 und 2 Internationaler Pakt über bürgerliche und politische Rechte (UNO Pakt II) UN, Human rights on the Internet, 2; ferner UN, Report of the Special Rapporteur, 6–9; ferner Human Rights Committee, Freedoms of opinion and expression, 3; sodann ferner hinsichtlich der *Charta der Menschenrechte und Prinzipien im Internet* der UNO IGF, Charter of human rights and principles for the internet, 16.

²⁶⁷⁴ Siehe etwa Rosenfeld, Colored Coins, 1–3; ferner Open Assets, open-assets-protocol, *passim*; vgl. hierzu auch Bundesrat, DLT-Bericht 2018, 24.

²⁶⁷⁵ Siehe etwa ARTICLE 19, Blockchain and freedom of expression, 27.

²⁶⁷⁶ Siehe etwa MacKinnon et al., Fostering Freedom Online, 13, 24, 37–39; IGF, Charter of human rights and principles for the internet, 18; *ausführlich* hinsichtlich der Nutzung von Verschlüsselungssoftware Tien, Berkeley Technology Law Journal 2000, 672.

tungsbereich der erwähnten Rechte fallen.²⁶⁷⁷ Der grundrechtliche Kerngehalt der Meinungs- und Informationsfreiheit wäre darum nach vorliegender Auffassung durch den Erlass eines Technologieverbots verletzt (vgl. Art. 36 Abs. 4 BV).

Dies gilt umso mehr, als dezentrale Systeme zunehmend auch *ausserhalb* des Finanzbereichs von Bedeutung sind (z.B. für digitale Identitäten, Kunst, Gaming, Social Media und Abstimmungen über Prognosemärkte oder im Rahmen der Governance eines Protokolls).²⁶⁷⁸ Die offene Natur von Blockchains erlaubt sodann unmittelbar die Verwendung des verteilten Registers als Plattform für Meinungsäusserungen oder aber wenigstens für Handlungen, mit welchen eine Person ein ähnliches Ziel verfolgen kann (z.B. eine Spende an eine politische Organisation, wie etwa Wikileaks²⁶⁷⁹). Namentlich werden Transaktionen bzw. deren Metadaten auf Bitcoin und Ethereum, aber auch auf eigens dafür programmierten Protokollen regelmässig als Speicher- und Vertriebsmedium für politische Texte verwendet, um sie vor drohender staatlicher Zensur zu schützen.²⁶⁸⁰ Freilich lässt sich in einem offenen, globalen Netzwerk nicht verhindern, dass auch illegale Daten im verteilten Register abgespeichert werden, wobei die Illegalität des Inhalts oftmals von Jurisdiktion zu Jurisdiktion anders beurteilt wird.²⁶⁸¹

b. Vertragsfreiheit und Privatautonomie

Ferner würde ein Technologieverbot wohl auch die *Vertragsfreiheit* der Nutzer von Computerprotokollen als Teilaspekt der Eigentumsgarantie in Art. 26 BV und der Wirtschaftsfreiheit in Art. 27 BV, aber auch des Rechts auf persönliche Freiheit in Art. 10 Abs. 2 BV der verletzen.

Grundprinzip der Privatrechtsordnung ist die Privatautonomie, die im Schuldrecht ihren Ausdruck in der Vertragsfreiheit findet. Diese beinhaltet die Abschlussfreiheit, die Partnerwahlfreiheit, die Inhaltsfreiheit, die Formfreiheit

²⁶⁷⁷ Allgemein zu diesem Thema Weber, E-Commerce und Recht, 548–549 («Platzierung von Inhalten auf einem globalen Netzwerk»); ferner aus Sicht des deutschen Rechts Jülicher/Röttgen, InTeR 2018, 16 m.w.N.

²⁶⁷⁸ Auf diese Thematik hinweisend Hofert, Regulierung der Blockchains, 59–61.

²⁶⁷⁹ Siehe etwa Matonis, WikiLeaks Bypasses Financial Blockade, Forbes, *passim*.

²⁶⁸⁰ Siehe etwa Singh, Circumvent Censorship in China, Slate, *passim*; ferner Hui, Hong Kongers are using blockchain archives, Quartz, *passim*.

²⁶⁸¹ Auf dieses *Spannungsverhältnis* hinweisend etwa De Gregorio, in: Pollicino/De Gregorio, Blockchain and freedom of expression, *passim*.

und die Aufhebungsfreiheit.²⁶⁸² Die staatliche Verhinderung bestimmter Rechtsgeschäfte etwa aufgrund des Inhalts, der Form oder der beteiligten Parteien betrifft sensible Bereiche von Art. 27 BV.²⁶⁸³ Ein Technologieverbot beträfe namentlich die Wahl, Verträge über den Austausch von Kryptovermögenswerten über ein dezentrales Netzwerk und/oder einen Smart Contract abzuschliessen und auszuführen bzw. durchzusetzen. Konkret würde dies bedeuten, dass die Parteien in ihrer umfassenden Gestaltungsfreiheit in Bezug auf die Möglichkeit eines computergestützten Vertragsschlusses, eine in Form von Computercode ausgedrückte Vertragsform, den u.U. pseudonymen Vertragspartner und den technisch durchsetzbaren Vertragsinhalt behindert würden.²⁶⁸⁴ Ein Verbot der Nutzung dezentraler Systeme würde damit aller Voraussicht nach durch Aushöhlung der Vertragsfreiheit den Kerngehalt der Wirtschaftsfreiheit und allf. weitere Grundrechte betreffen.²⁶⁸⁵

Demgegenüber kann aus dem Recht auf persönliche Freiheit nach vorliegender Ansicht kein (positives) Recht auf Zugang zum Internet und zu technischen Protokollen, die darauf basieren, abgeleitet werden.²⁶⁸⁶

Schliesslich könnte auch die Konsumfreiheit als (umstrittener) Teilaspekt der Wirtschaftsfreiheit in Art. 27 BV gegen ein Verbot der Nutzung von Computerprotokollen angeführt werden.²⁶⁸⁷ Wo allerdings ein Nutzer solche Protokolle geschäftsmässig verwendet (z.B. in der Funktion als Market Maker), ist es grundsätzlich nicht erforderlich, sich auf die Konsumfreiheit zu berufen.

2.3 Teilnahme an dezentralen Systemen

In der *Teilnahme* an einem verteilten Netzwerk kann neben der Ausübung des Rechts auf persönliche Freiheit und der Wirtschaftsfreiheit insb. auch die Wahrnehmung der Rechte aus der Vereinigungsfreiheit gemäss Art. 23 BV ge-

²⁶⁸² Siehe insb. BGE 129 III 35, E. 6.1; ausführlich Vallender, in: SGK BV, Art. 27 N 44 m.w.N.; zu Art. 10 Abs. 2 BV BSK BV-Tschentscher, Art. 10 N 38 m.w.N.

²⁶⁸³ Siehe BSK BV-Uhlmann, Art. 27 N 13.

²⁶⁸⁴ Siehe Möslin, ZHR 2019, 266–268; ferner Omlor, ZHR 2019, 336, der unter deutschem Recht Zweifel an der grundrechtlichen Zulässigkeit hat.

²⁶⁸⁵ Vgl. Vallender, in: SGK BV, Art. 27 N 45 m.w.N., 57.

²⁶⁸⁶ Siehe zur Diskussion insb. im deutschen Verfassungsrecht Haux, Digitale Allmende, 134–141.

²⁶⁸⁷ Vgl. zur Konsumfreiheit Vallender, in: SGK BV, Art. 27 N 8; BSK BV-Uhlmann, Art. 27 N 18; ferner BSK BV-Tschentscher, Art. 10 N 38, welcher die Konsumfreiheit als Teilgehalt des Rechts auf persönliche Freiheit betrachtet; *ablehnend* BGE 102 Ia 104, E. 7.

sehen werden. Demnach hat jede Person das Recht, Vereinigungen zu bilden, Vereinigungen beizutreten oder anzugehören und sich an den Tätigkeiten von Vereinigungen zu beteiligen (Art. 23 Abs. 2 BV).

Eine Vereinigung im Sinne der Verfassungsbestimmung stellt einen Zusammenschluss von natürlichen oder juristischen Personen von gewisser Dauer und minimaler Organisation mit dem Ziel dar, einen gemeinsamen Zweck zu erfüllen. Ob lediglich ideelle oder auch wirtschaftliche Vereinigungszwecke zulässig sind, ist umstritten.²⁶⁸⁸ Angesichts der überragenden Bedeutung des Internets für die soziale Kommunikation sollten auch online agierende Gemeinschaften den Vereinigungsbegriff erfüllen können.²⁶⁸⁹

Die Betreiber von Full Nodes, aber auch Miner und Staker verwalten in gemeinschaftlicher Weise ein Netzwerk u.a. für den Austausch von Kryptovermögenswerten. Als Grundlage dieser Form von Vereinigung dient ihnen das Protokoll des Netzwerks. Fraglich ist, ob bereits derart lose Computernetzwerke eine Vereinigung darstellen. Angesichts der Bedeutung dezentraler Systeme als potenziell neue Organisationsform globaler Gemeinschaften sollte es nicht *a priori* ausgeschlossen sein, dass etwa in der Teilnahme von Personen an einem Netzwerk als Full Nodes eine Vereinigung im Sinne von Art. 23 Abs. 2 BV gesehen werden kann.

2.4 Programmierung und Veröffentlichung von Software

Die *Programmierung und Veröffentlichung von Computercode* könnte sodann in den Genuss der Meinungsäusserungsfreiheit kommen. Soweit ersichtlich, ist diese Frage in der Schweiz bisher nicht höchststrichterlich beurteilt worden. Da es allerdings nach der Rechtsprechung des Bundesgerichts und des EGMR nicht auf die Form der Kommunikation ankommt und grundsätzlich jede Mitteilung menschlichen Denkens erfasst ist, soll nach vorliegender Ansicht auch Computercode in den sachlichen Schutzbereich von Art. 16 BV fallen. Dies ist insb. dann zu bejahen, wenn der programmierte Code letztlich den politischen bzw. ideologischen Willen des Programmierers zum Ausdruck bringt. In diesem Fall wäre der Computercode, der als Quellcode menschenlesbar ist, verfassungsrechtlich im Wesentlichen einer Buchpublikation gleichgestellt.

²⁶⁸⁸ Siehe Errass, in: SGK BV, Art. 23 N 6–10; ferner BSK BV-Schiess-Rütimann, Art. 23 N 8–9.

²⁶⁸⁹ Vgl. etwa UN, Report of the Special Rapporteur on the rights to freedom of peaceful assembly and of association, 20; IGF, Charter of human rights and principles for the internet, 17.

Praktisch relevanter, zumindest für Softwareentwickler in der Schweiz,²⁶⁹⁰ ist wohl allerdings die Tatsache, dass die berufsmässige Ausübung der Entwicklung von Computercode in aller Regel durch die Wirtschaftsfreiheit gemäss Art. 27 BV geschützt wird. Zu erwähnen ist in diesem Zusammenhang insb. der Teilgehalt der Berufsausübungsfreiheit.²⁶⁹¹ Dabei dürfte es keine Rolle spielen, ob ein Entwickler ein Protokoll als gemeinsamen Standard oder aber eine konkrete Anwendung auf Basis des Protokolls, wie z.B. eine bestimmte dezentrale Applikation, entwickelt.

In den USA ist die Diskussion, ob Software «protected speech» darstellt, nunmehr wieder in vollem Gange: Ausgelöst wurde dies durch die OFAC-Sanktionierung des Anonymisierungsprotokolls *Tornado Cash*.²⁶⁹² In der Folge kam es im August 2023 zur strafrechtlichen Anklage von zwei Gründern und Programmierern des Protokolls. Ihnen wird vorgeworfen, mit dem Protokoll u.a. ein registrierungspflichtiges «Money Transmission Business» betrieben zu haben. Es liege ein Verstoß gegen den Bank Secrecy Act vor, denn die beiden Angeklagten hätten im relevanten Zeitraum die Kontrolle über gewisse Elemente von Tornado Cash ausgeübt, namentlich über (i) die Benutzeroberfläche, welche die Kommunikation mit den Smart Contracts des Protokolls vereinfachte, (ii) die GitHub-Webseite des Protokolls, auf welcher der Code und dessen Dokumentation verfügbar gemacht wurde, und (iii) eine Zeit lang einen Teil oder

²⁶⁹⁰ Siehe demgegenüber zur lebhaft geführten Diskussion in den USA zur Frage, ob Computercode «protected speech» und Softwareentwicklung somit verfassungsrechtlich geschützt ist, Van Valkenburgh, *Electronic Cash*, 32–45; hinsichtlich des EtherDelta-Falls m.w.H. sodann EFF, *Constitutional Questions*, *passim*; Yakubowski, *Is Bitcoin Protected as Speech Under the 1st Amendment?*, *Cointelegraph*, *passim*; ferner Richards, *Apple's Mistake*, *Technology Review*, *passim*.

²⁶⁹¹ Siehe hierzu etwa BGE 137 I 167, E. 3.1 («toute activité économique privée»); 116 Ia 237, E. 2d («freie Wahl und Ausübung eines Berufs»); 128 I 92, E. 2a; 128 I 19, E. 4c («protegge ogni attività economica privata esercitata a titolo professionale, volta al conseguimento di un guadagno o di un reddito»); BGER 2P.55/2003 vom 3. Juli 2003, E. 4.3.2 («freie wirtschaftliche Betätigung in umfassendem Sinn»); ausführlich hierzu sodann Vallender, in: SGK BV, Art. 27 N 9–27; vgl. auch Errass, *Sicherheit & Recht* 2016, 77.

²⁶⁹² U.S. Department of the Treasury, *Tornado Cash Sanctions*, *passim*. Die Sanktionen von OFAC wurden in der Folge gleich *doppelt* angefochten: Im *ersten* Verfahren entschied ein Gericht u.a., dass Tornado Cash eine sanktionierbare «Entity» darstellt, die sich aus den Gründern, Entwicklern und der dazugehörigen DAO zusammensetzt (vgl. U.S. District Court for the Western District of Texas Austin Division, *Van Loon et al. vs. Department of Treasury et al.*, 13–16). In einem *zweiten* ähnlichen Verfahren entschied ein Gericht u.a., dass die OFAC-Sanktionen gegen Tornado Cash keine Überschreitung der Befugnisse der Behörde und keinen Verstoß gegen die Grundrechte der Kläger wie die Vereinigungsfreiheit darstellten (vgl. U.S. District Court Northern District of Florida Pensacola Division, 12–22). Beide Entscheide wurden angefochten.

alle Smart Contracts des Protokolls, welche letztlich die Logik des Protokolls implementiert haben.²⁶⁹³ Ein dritter Softwareentwickler im Zusammenhang mit Tornado Cash wurde in den Niederlanden wegen möglicher Geldwäsche-rei angeklagt.²⁶⁹⁴

2.5 Fazit

Der Erlass eines Technologieverbots wäre mit anderen Worten aus grundrechtlichen Überlegungen kaum je rechtfertig- und durchsetzbar. Zudem hätte ein Verbot entsprechende negative, da abschreckende Auswirkungen auf die Innovationskraft einer Gesellschaft.²⁶⁹⁵

²⁶⁹³ Siehe U.S. District Court Southern District of New York, USA vs. Storm and Semenov, 6–20; kritisch Gruenstein/Norris/Barabander, Secret Notes And Anonymous Coins, 9–16; Van Valkenburgh, Tornado Cash indictments, *passim*.

²⁶⁹⁴ Siehe Schickler, Developers of Tornado Cash, CoinDesk, *passim*.

²⁶⁹⁵ Vgl. etwa Hoffmann-Riem, AöR 2006, 271–272; ferner zu überschüssenden Tendenzen im Risikorecht Camenisch, Innovationsoffenheit als Verfassungsgrundsatz, 105–106

3. Anleger- und Funktionsschutz

3.1 Anlegerschutz

Der finanzmarktrechtliche Anlegerschutz befasst sich nach verbreiteter Auffassung mit dem Schutz des Anlegers vor dem missbräuchlichem Verhalten eines Finanzintermediärs.²⁶⁹⁶ Anleger sollen mit anderen Worten in ihrer Rolle als Kunden in ihrem berechtigten Vertrauen in die Vertragspartei geschützt werden. Darüber hinaus, so etwa im Prospektrecht, sollen Anleger in ihrer Rolle als Investoren vor vergleichbaren Verhaltensweisen des Emittenten von Effekten und Finanzinstrumenten und weiteren Personen, die an der Emission oder Platzierung beteiligt sind, geschützt werden.

Trotz der Anknüpfung an das Verhältnis zwischen Kunde und Finanzintermediär bzw. Investor und Emittent werden mit dem Finanzmarktaufsichtsrecht in erster Linie nicht die (Vermögens-)Interessen des *einzelnen* Anlegers geschützt. Dieser ist für individuelle Streitigkeiten auf den Zivil- oder Schiedsprozess verwiesen. In Bezug auf Retrozessionen ist dies eindrücklich Realität geworden.²⁶⁹⁷ Auch aus Ressourcenüberlegungen ist effektiver Anlegerschutz Kollektivanlegerschutz.²⁶⁹⁸ Konsequenterweise sieht sich die FINMA selbst nicht als Individualanlegerschutzbehörde.²⁶⁹⁹ Der einzelne Anleger ist in diesem Sinne – ähnlich wie im Funktionsschutz (siehe sogleich unten) – bloss Funktionsträger des Finanzmarktrechts.²⁷⁰⁰ Dies soll indessen nicht ausschliessen, dass einzelne Normen nach ihrem Zweck, namentlich im Bereich des FIDLEG, individuelle Rechtsgüter schützende Normen darstellen können.²⁷⁰¹

Als Begründung für Anlegerschutzbestimmungen werden einerseits das allgemein bestehende Informationsgefälle zwischen Kapitalgeber und -nehmer bzw. Intermediär und andererseits der Kontrollverlust, das Machtgefälle sowie die Interessenkonflikte, die mit der Kapitaleinbringung in den Kapitalmarkt

²⁶⁹⁶ Siehe statt vieler Zobl/Kramer, Kapitalmarktrecht, Rz. 26; SK FIDLEG-Winkler, Art. 1 N 25.

²⁶⁹⁷ Siehe Bärtschi, SZW 2014, 464, der für diesen Fall das Potenzial des «privatrechtlichen Regulierungsrechts» betont; ausführlich zu diesem Begriff Bärtschi, in: Abegg/Bärtschi/Dietrich, § 6 Rz. 532–539.

²⁶⁹⁸ Siehe Abegglen/Andreotti, GesKR 2020, 43 m.w.H.

²⁶⁹⁹ Siehe FINMA, Ziele, *passim*.

²⁷⁰⁰ A.M. wohl Zobl/Kramer, Kapitalmarktrecht, Rz. 25, 31.

²⁷⁰¹ Vgl. hierzu etwa Abegglen/Luterbacher, ZSR 2020 I, 246–251 m.w.N.

verbunden sind, angeführt.²⁷⁰² Dabei handelt es sich um Themen, die ihren Ursprung überwiegend im Prinzipal-Agent-Verhältnis der beteiligten Personen haben.

Anleger sollen demgegenüber nicht vor Verlusten aus ihrer Anlagentätigkeit am Kapitalmarkt bewahrt werden. Das gewöhnliche Investitions- bzw. Anlagerisiko ist systematischer Natur und letztlich nicht vom Finanzintermediär zu verantworten.²⁷⁰³ Dies gilt nach vorliegender Ansicht selbst dann, wenn die eingesetzten Anlageinstrumente und -techniken neuartiger und teils unerprobter Natur sind. Den Nutzern dezentraler Systeme sollen mit anderen Worten nicht generell Anlageopportunitäten aufgrund neuer Technologien vorenthalten werden.²⁷⁰⁴ Generell wird die *Chancengleichheit* der Anleger als Teilaspekt des Funktionsschutzes betrachtet.²⁷⁰⁵ Gute Anlegerschutzregeln sollten unter diesem Gesichtspunkt in erster Linie auf die Herstellung informierter Anlageentscheide ausgerichtet sein.²⁷⁰⁶ Gut informierte, sachkundige Anleger sind denn auch ein zentraler Teilaspekt einer auf wirksamem Wettbewerb fussenden Industrie.²⁷⁰⁷ Andere Ansätze, wie etwa ein Verbot oder eine Einschränkung der Erwerbs auf qualifizierte Anleger, scheinen unter Gesichtspunkten der Wettbewerbsneutralität der Regulierung generell ein fragwürdiger Ansatz und angesichts des Fehlens traditioneller Finanzintermediationsrisiken vorliegend weniger dringlich zu sein.²⁷⁰⁸ Der Bundesrat scheint diese Sichtweise im Grundsatz zu bejahen, wenn er im DLT-Bericht die Rolle des Marktes und die Präferenzen der Gesellschaft hervorhebt.²⁷⁰⁹

²⁷⁰² Ausführlich hierzu Werlen, Konzeptionelle Grundlagen, 33–34, 35–36; ferner Sethe, AcP 2012, 83; Watter, AJP 1997, 272; Köndgen, in: Fleischer/Zimmer, Effizienzorientierung, 109, 114–115, 128–130, 134–138.; Möllers, AcP 2008, 8–9; Baisch/Weber, in: Sethe et al., Transparenz, 173–174; Meier-Schatz, Unternehmenspublizität, 100–101.

²⁷⁰³ Siehe BGE 119 II 333, E. 7a m.w.H.; BGer 4C.205/2006, E. 3.4.1 («[...] le spéculateur doit savoir qu'il ne peut se fier sûrement à un conseil relatif à un événement futur et incertain; en principe, il doit assumer lui-même les risques, s'il suit le conseil de la banque [...]»); ferner Zobl/Kramer, Kapitalmarktrecht, Rz. 26; SK FIDLEG-Winkler, Art. 1 N 28; zur Frage eines paternalistischen Anlegerschutzes Sethe, AcP 2012, 91–92. Die ökonomischen Grundlagen finden sich in der Analyse von systematischen bzw. Portfoliorisiken in Markowitz, The Journal of Finance 1951, 79, 89–90.

²⁷⁰⁴ Vgl. etwa Peirce, Remarks at Meeting of Investor Advisory Committee, *passim*, wonach nicht nur Anlegerschutz, sondern gerade auch «investor opportunity» wesentlich sei.

²⁷⁰⁵ Siehe etwa Hofstetter, SZW 1996, 226 («faire Zuteilung von Chancen und Risiken»); Zobl/Kramer, Kapitalmarktrecht, Rz. 62; BSK KAG-Winzeler, Art. 1 N 16.

²⁷⁰⁶ Siehe zur Einführung von Marktlösungen unten, [VI.4.3](#).

²⁷⁰⁷ Siehe hierzu unten, [VI.4.2b](#).

²⁷⁰⁸ Vgl. Nayak, Picking Crypto Winners and Losers, Bloomberg, *passim*.

²⁷⁰⁹ Siehe Bundesrat, DLT-Bericht 2018, 13.

3.2 Funktions- und Systemschutz

Der finanzmarktrechtliche Funktionsschutz befasst sich mit dem Finanzmarkt als Institution von gesamtwirtschaftlicher Bedeutung. Ziel des Funktionsschutzes ist die Gewährleistung der allokativen, informationellen, operationellen und institutionellen Effizienz des Finanzmarktes.²⁷¹⁰ Die konkreten Zusammenhänge zwischen den unterschiedlichen Effizienztypen sind allerdings komplex.²⁷¹¹ Im Zentrum des Funktionsschutzes stehen auf jeden Fall die ökonomischen Funktionen des Marktes, allen voran die Sicherstellung der Marktliquidität. Entsprechend weist der Funktionsschutz eine grosse Nähe zum allgemeinen Vertrauensschutz auf.²⁷¹²

Als Begründung für den Funktionsschutz werden primär informationelle Marktungleichgewichte, d.h. eine asymmetrische Situation im Informationsstand zwischen Kapitalgebern und -nehmern bzw. Intermediären geltend gemacht.²⁷¹³ Ziel der Kapitalmarktregulierung ist es darum, allokationseffiziente Anlageentscheidungen durch den Abbau von Informationsasymmetrien zu ermöglichen. Ähnlich dem Anlegerschutz erfolgt auch der Funktionsschutz zu einem grossen Teil mittels Transparenzvorschriften, die jedoch anders als beim Anlegerschutz auf die Markttransparenz, d.h. auf die *Bedürfnisse des Marktes* ausgerichtet sind.²⁷¹⁴ Auch in dieser Hinsicht wird die Gesamtheit der Anleger, nicht hingegen der einzelne Investor geschützt.²⁷¹⁵ Der Anleger ist wiederum bloss Funktionsträger der funktionsschützenden Bestimmungen des Finanzmarktrechts.²⁷¹⁶

²⁷¹⁰ Siehe Zobl/Kramer, Kapitalmarktrecht, Rz. 28; Werlen, Konzeptionelle Grundlagen, 45–48; vgl. dazu auch BSK BankG-Bahar/Stupp, Art. 1 N 1; BSK BEHG/FINMAG-Watter, Art. 1 N 11, 14.

²⁷¹¹ Illustrativ Dietrich/Bienert, in: Abegg/Bärtschi/Dietrich, § 1 Rz. 10.

²⁷¹² Siehe Köndgen, in: Fleischer/Zimmer, Effizienzorientierung, 110; Abegg/Bärtschi, in: Abegg/Bärtschi/Dietrich, § 2 Rz. 167; ähnlich auch Zobl/Kramer, Kapitalmarktrecht, Rz. 29; ferner SK FinfraG-Sethe, Art. 1 N 11, 22, 25, der zwischen Vertrauensindividual- und Vertrauenskollektivschutz unterscheidet; ebenso BSK FinfraG-Watter, Art. 1 N 15–16.

²⁷¹³ Siehe Watter, AJP 1997, 272; Ruffner, Ökonomische Grundlagen, 419–420.

²⁷¹⁴ Siehe BSK BEHG/FINMAG-Watter, Art. 1 N 11, 14; Möllers/Kernchen, ZGR 2011, 3 m.w.N.; Klöhn, ZHR 2013, 358, 375–376; BSK FinfraG-Watter, Art. 1 N 19–20; vgl. ferner zu den unterschiedlichen Kategorien von Informationspflichten Andreotti, Produktverbote, 19–23; sodann aus Sicht der Spekulation Klöhn, Spekulation, 154–156.

²⁷¹⁵ Vgl. Zobl/Kramer, Kapitalmarktrecht, Rz. 29; in Bezug auf das Wertpapierhandelsrecht Klöhn, ZHR 2013, 358.

²⁷¹⁶ So Werlen, Konzeptionelle Grundlagen, 49; Zobl/Kramer, Kapitalmarktrecht, Rz. 29.

Der Funktionsschutz soll schliesslich auch den Zusammenbruch des gesamten Finanzmarktes verhindern und die *Systemrisiken*, die von einzelnen Marktteilnehmern ausgehen, minimieren (sog. Systemschutz).²⁷¹⁷

3.3 Implikationen für den Anleger- und Funktionsschutz

a. Netzwerkbasierte Intermediation

In dezentralen Systemen kommt traditionellen Intermediären keine oder nur noch eine sehr geringe Bedeutung zu. Im ersten Kapitel dieser Arbeit wurde diese Erkenntnis als netzwerkbasierte Intermediation bezeichnet.

Die Funktionsweise eines dezentralen Systems ist letztlich das Produkt einer Vielzahl beteiligter Personen. Streng genommen könnte man aus der Tatsache, dass eine Vielzahl an Intermediären an einem Netzwerk beteiligt sind, darauf schliessen, dass das konventionelle Intermediationsrisiko für Nutzer solcher Netzwerke und Applikationen ebenfalls ein Vielfaches darstellen muss. Das Gegenteil ist aber der Fall: Der einzelne an einem dezentralen Netzwerk oder an einer dezentralen Applikation Beteiligte hat einen derart geringen Einfluss auf die Funktionsweise des Systems bzw. ist für diese von derart geringer Bedeutung, dass ein allfälliges Intermediationsrisiko für die Nutzer praktisch bedeutungslos ist. Denn je geringer die Zahl der vertrauenswürdigen Parteien ist, desto geringer ist auch die Zahl der Parteien, die für die Nutzer ein Risiko darstellen können. Ein System ohne Intermediäre ist ein System ohne Intermediationsrisiko und bedarf daher grundsätzlich keiner Regulierung zum Schutz gegen die von Intermediären ausgehenden Risiken.²⁷¹⁸ Nichts anderes ergibt sich aus dem in der Finanzmarktaufsicht verbreiteten funktionalen Regulierungsansatz, der jedoch um die Risikokomponente zu korrigieren ist.²⁷¹⁹

²⁷¹⁷ Siehe Zobl/Kramer, Kapitalmarktrecht, Rz. 30.

²⁷¹⁸ So auch Van Valkenburgh, Differences between Bitcoin and Libra, *passim*; ferner Omlor, ZHR 2019, 343, der darauf hinweist, dass es in dezentralen Systemen an der im Zahlungsverkehr charakteristischen Interessensubordination fehlt; Jutzi/Abbühl, Fintech und DLT, Rz. 1343.

²⁷¹⁹ Siehe insb. FINMA, Ergänzung Wegleitung ICOs, 2 («Der Fokus liegt auf der wirtschaftlichen Funktion und dem Zweck [‘substance over form’] entlang den bewährten Wertungsentscheiden [‘same risks, same rules’] und unter Berücksichtigung der Besonderheiten des Einzelfalls.»); bestätigt in FINMA, Jahresbericht 2020, 29; ferner Bundesrat, DLT-Bericht 2018, 14; sodann auch Bundesrat, Finanzmarktpolitik 2020, 13. Siehe hinsichtlich der Notwendigkeit

Am besten wird dies an der ausschliesslichen Kontrolle der Nutzer über ihre Kryptovermögenswerte erkennbar. In dezentralen Systemen bestehen keine Drittverwahrungs- und somit keine Gegenparteirisiken für einen Nutzer.²⁷²⁰ Anleger in ihrer Rolle als Nutzer finden sich in einer Situation wieder, in welcher sie nicht nur die Entscheidungsmacht über die Ausführung eines Handelsgeschäfts behalten, sondern auch dessen Parameter selbständig bestimmen.²⁷²¹ Gleichsam bieten sich keine aus dem traditionellen Prinzipal-Agent-Verhältnis herrührende Informationsasymmetrien als Regulierungsanlass. Darüber hinaus besteht auch nicht das Risiko, dass ein Anleger aus Gründen der einseitigen Verhandlungsmacht übervorteilt wird.

Die Dezentralität, welche ihrerseits freilich eigene Kosten und Risiken mit sich bringt, indem Nutzer etwa Vertrauen in die Technologie aufzubringen haben,²⁷²² ersetzt die Agency-Kosten traditioneller Finanzintermediation. Aus der Dezentralität solcher Systeme ergeben sich im Ergebnis Disintermediationseffekte, welche die Bedeutung von Anleger- und Funktionsschutz im bisherigen Sinne zu einem wesentlichen Teil in den Hintergrund treten lassen.²⁷²³

Mit Blick auf dezentrale Handelsplattformen sollte aber trotz – oder gerade wegen des – Fehlens traditioneller Prinzipal-Agent-Beziehungen die Einführung eines freiwilligen marktorientierten Offenlegungsregimes auf der Grundlage von Verhaltenskodizes in Betracht gezogen werden.²⁷²⁴

eines funktionalen Regulierungsansatzes bezüglich der Intermediation in einem finanzinnovativen Umfeld Möslin, in: Möslin, Finanzinnovation und Rechtsordnung, 28–29.

²⁷²⁰ Siehe Brito/Van Valkenburgh, Ideal regulatory environment for Bitcoin, *passim*; ferner mit Bezug zu einem internen Hack Voorhees, Story of Sabotage at ShapeShift, Bitcoin.com, *passim* («[...] no customers lost money throughout multiple hacks orchestrated even by an insider. Through decentralization, through code, through innovation, through structure... consumer protection by design is one of this industry's most important contributions to society – something that a century of legacy banking has failed to achieve, as noted by Satoshi's infamous line in the Genesis Block.»).

²⁷²¹ Vgl. ferner hinsichtlich Konsumentenschutz etwa Fairfield, Washington and Lee Law Review Online 2014, 49; Hug, in: Carron/Müller, Protection du consommateur, 166–167.

²⁷²² Siehe hierzu oben, [II.5.3c.i](#).

²⁷²³ Vgl. aber Jutzi/Abbühl, Fintech und DLT, Rz. 1343–1348, die zu Recht auf den Systemschutz in Form der Finanzstabilität hinweisen.

²⁷²⁴ Siehe hierzu ausführlich unten, [VI.4.3c.iv](#).

b. Traditionelle Finanzintermediäre

Dies bedeutet allerdings nicht, dass das DeFi-Ökosystem vollständig der Rechtsordnung entzogen ist. Die Steuerungsfähigkeit wesentlicher mit DeFi interagierender Bereiche ist ohne Weiteres erfüllt.

Einerseits sind traditionelle Finanzintermediäre, die an der Peripherie dezentraler Systeme operieren, grundsätzlich dem Finanzmarktrecht unterstellt. Solche Finanzintermediäre dienen regelmässig als «Fiat-Schnittstelle» zwischen dem traditionellen Finanzsystem und DeFi. Zentrale Handelsplattformen haben etwa die auf Anlegerschutz ausgerichteten Verhaltenspflichten des FIDLEG einzuhalten, wenn sie für ihre Kunden Finanzdienstleistungen im Sinne des Gesetzes erbringen. Zentrale Kryptohandelsplattformen haben sodann aufgrund ihrer Verfügungsmacht über fremde Vermögenswerte die Vorgaben des GwG einzuhalten und können je nach Handelstätigkeit als Wertpapierhaus oder sogar als DLT-Handelssystem reguliert und beaufsichtigt sein. Wo es sich bei den gehandelten Token um Effekten handelt, würden zudem die Marktverhaltensregeln zur Anwendung gelangen. Angesichts des Verdachts, dass Frontrunning und Wash Trading mit gewisser Häufigkeit auf zentralen Plattformen betrieben werden,²⁷²⁵ ist die Verhinderung solcher Handelspraktiken für die Integrität und Funktionsweise der Märkte von vertrauensbildender Bedeutung.

c. Transparenz mit Vor- und Nachteilen

Die verbesserte Informationstransparenz in dezentralen Systemen stellt allerdings auch Herausforderungen dar: So können Marktteilnehmer mit hohen Rechenkapazitäten oder aufgrund ihrer Stellung im Netzwerk diese zu ihren Gunsten ausnutzen (z.B. «Frontrunning» im untechnischen Sinne). Zudem sind die Datenmengen, die für informierte Anlageentscheide und effiziente Markttransparenz erforderlich sind, teilweise so überwältigend, dass Marktteilnehmer regelmässig einem Information Overload ausgesetzt sind. Informationsintermediäre nehmen unter diesen Umständen eine bedeutende Stellung im Markt ein. Gewisse Reintermediationseffekte sind nicht ausgeschlossen. Diesen wird darum im Rahmen des noch zu entwickelnden Dezentralitätstests Rechnung zu tragen sein.²⁷²⁶

²⁷²⁵ Siehe hierzu oben, [IV.5.2d.iii.](#)

²⁷²⁶ Siehe unten, [VII.](#)

Mit Blick auf DeFi ist *de lege lata* offen, inwiefern dezentrale Systeme den Regeln zur Verhinderung von Geldwäscherei und Terrorismusfinanzierung zu unterstellen sind. Selbstredend greift die heutige Regulierung der Finanzintermediation im Geldwäschereibereich bei Eröffnung des Geltungsbereichs.²⁷²⁷ Nach vorliegender Auffassung sind Systeme, die genügend dezentralisiert sind, mangels Verfügungsmacht über fremde Vermögenswerte sowie mangels effektiver Kontrolle über fremde Geldflüsse jedoch nicht dem GwG zu unterstellen. Dabei handelt es sich jedoch vorwiegend um ein technisches Argument. In rechtspolitischer Hinsicht ist darüber hinaus zu fordern, das Kosten-Nutzen-Verhältnis des heutigen Geldwäschereirechts aufgrund von dessen zweifelhafter Effektivität zu hinterfragen.²⁷²⁸ Stattdessen sollte ein grundlegend neues Geldwäschereiregime für DeFi (und wohl auch für das traditionelle Finanzsystem) erarbeitet werden, dessen Funktionsweise die Dezentralität als Rechtsprinzip anerkennt, entsprechende Instrumente entwickelt und die Bedürfnisse der Nutzer nach Schutz ihrer Privatsphäre und Persönlichkeitsrechte ernstnimmt.²⁷²⁹ Das Geldwäschereithema ist allerdings hoch umstritten und wird darum mit grosser Wahrscheinlichkeit auch künftig die politischen und rechtswissenschaftlichen Debatten befeuern.

d. Zivilrechtliche Haftung

Das Zivilrecht regelt die Haftung zwischen Vertragsparteien und bei unerlaubten bzw. deliktischen Handlungen. Dabei setzt es voraus, dass der Schuldner (Art. 97 ff. OR) bzw. der Ersatzpflichtige (Art. 41 ff. OR) dem Geschädigten bekannt sind.

Es ist nicht *a priori* ausgeschlossen, dass Nutzer dezentraler Handelsplattformen – trotz der in der Praxis verwendeten weitgehenden Freizeichnungsklauseln –²⁷³⁰ über zivilrechtliche Ansprüche verfügen. Als Anspruchsgegner kä-

²⁷²⁷ Vgl. etwa Pesch/Böhme, DuD 2017, 97–98, welche die Regulierung von Intermediären der Regulierung von Nutzern, Minern und Entwicklern vorziehen.

²⁷²⁸ Siehe oben, [V.2.12f.](#)

²⁷²⁹ Ausführlich hierzu oben, [V.2.12g.](#)

²⁷³⁰ Siehe etwa Uniswap, Uniswap Labs Terms of Service, 3. März 2023, Ziff. 5.3 («[...], THE PROTOCOL IS PROVIDED 'AS IS', AT YOUR OWN RISK, AND WITHOUT WARRANTIES OF ANY KIND. ALTHOUGH WE CONTRIBUTED TO THE INITIAL CODE FOR THE PROTOCOL, WE DO NOT PROVIDE, OWN, OR CONTROL THE PROTOCOL, WHICH IS RUN AUTONOMOUSLY WITHOUT ANY HEADCOUNT BY SMART CONTRACTS DEPLOYED ON VARIOUS BLOCKCHAINS. UPGRADES AND MODIFICATIONS TO THE PROTOCOL ARE GENERALLY MANAGED IN A COMMUNITY-DRIVEN WAY BY HOLDERS OF THE UNI GOVERNANCE TOKEN. [...]»).

men etwa Softwareentwickler, Betreiber von Smart Contracts²⁷³¹ und andere Personen mit Kontrolle über wesentliche Komponenten einer dezentralen Applikation infrage.²⁷³²

Allerdings muss darauf hingewiesen werden, dass regelmässig keine traditionelle Agency-Beziehung zwischen Entwicklern, Netzwerkteilnehmern und den Nutzern einer Applikation besteht, welche durch latente Informationsasymmetrien oder ein Machtungleichgewicht geprägt ist.²⁷³³ In dezentralen Netzwerken, wie etwa Bitcoin, besitzen Softwareentwickler regelmässig auch gar nicht die Autorität bzw. Macht, Änderungen am Protokoll vorzunehmen.²⁷³⁴ Die Governance solcher Systeme ist oftmals viel komplexer als in der Literatur gemeinhin angenommen wird.²⁷³⁵ Zudem übernimmt der Entwickler in aller Regel nicht die vertragliche Pflicht, ausschliesslich im Interesse eines bestimmten Nutzers oder Nutzerkreises einer Applikation tätig zu werden. Unabhängig davon, wie dieses Interesse zu bestimmen wäre, kommt aus diesem Blickwinkel lediglich ausnahmsweise eine Haftung infrage.²⁷³⁶

In den USA wurde die vertragliche Haftung der Entwickler einer dezentralen Handelsplattform soweit ersichtlich bisher abgelehnt. Die Rolle der Entwickler sei ein Nebenprodukt. Die Geschädigten hätten sich demgegenüber direkt an den betrügerisch vorgegangenen Emittenten eines Tokens schadlos zu halten, wenn diese die wesentlichen Parameter der Liquiditätspools des Uniswap-AMM kontrolliert haben (indem sie etwa die Verkaufsfunktion eines Smart Contracts deaktivierten).²⁷³⁷ Theoretisch denkbar ist allerdings die Anwendbarkeit deliktischer und spezialgesetzlicher Haftungsstatbestände auf die Softwareprodukte eines Entwicklers.²⁷³⁸

²⁷³¹ Siehe etwa die Informationshaftung in Art. 973i OR.

²⁷³² Für eine Übersicht siehe Weber, Jusletter vom 4. Dezember 2017, *passim*; Hess/Lienhard, in: Emmenegger, Unautorisierte Zahlungen, 171–172.

²⁷³³ Vgl. Ribstein, Boston University Law Review 2010, 901–902.

²⁷³⁴ Siehe Nabilou, Stanford Journal of Blockchain Law & Policy 2021, 32–33.

²⁷³⁵ Vgl. hierzu ausführlich oben, [IV.5.2e.iv](#).

²⁷³⁶ Vgl. auch Zetzsche/Buckley/Arner, University of Illinois Law Review 2018, 1406, welche davon ausgehen, dass das Haftungsrisiko in dezentralen Netzwerken zwar nicht null ist und stark vom Einzelfall abhängt, aber dennoch viel kleiner als in «permissioned ledgers» ist.

²⁷³⁷ Siehe U.S. District Court Southern District of New York, Risley et al. vs. Universal Navigation et al., 29–38.

²⁷³⁸ Vgl. hierzu Weber, SJZ 2021, 684–685; auf die Schwierigkeiten hinweisend Bundesrat, Digital Finance, 8.

4. Marktorientierung in der Finanzmarktregulierung

4.1 Einleitung

Unbeschadet allfälliger marktorientierter Lösungen für den Anleger- und Funktionsschutz bietet sich selbstredend der bereits eingeschlagene Weg an, traditionelle Finanzintermediäre und neue FinTech-Unternehmen, die an der Peripherie von DeFi operieren, den bestehenden Finanzmarktgesetzen zu unterstellen. Darüber hinaus ist es offensichtlich angezeigt, gegen betrügerisches und missbräuchliches Verhalten im Markt vorzugehen, und dies selbst wenn solche Aktivitäten dem Umfeld eines dezentralen Systems entstammen. Umgehungen bestehender Regulierung unter dem Vorwand der Dezentralität sind bereits aus technologieneutralen Gründen und Risikoüberlegungen denselben Regeln zu unterwerfen.²⁷³⁹ Vergleichbare Aktivitäten mit vergleichbarem Risikoprofil sind gleich zu behandeln.²⁷⁴⁰

Bei Vorliegen echter Dezentralität handelt es sich dagegen gerade nicht um ein finanzinnovatives Ausweichmanöver der involvierten Personen, die etwa vergleichbar mit verpönte²⁷⁴¹ regulatorischer Arbitrage ist. Bei Dezentralität handelt es sich demgegenüber um eine genuin neuartige Markterscheinung, welche nach vorliegender Ansicht rechtlich *anders* zu behandeln ist.²⁷⁴² Entsprechend muss der Ordnungsrahmen allenfalls angepasst werden, um dem eingetretenen soziotechnischen Wandel aufs Neue Rechnung zu tragen.²⁷⁴³

²⁷³⁹ So etwa Bieri/Uhlmann, Die Volkswirtschaft 5/2019, 9; ferner Hanke/Sekerke, Crypto's Legal White Space, National Review, *passim*, wobei die Autoren nicht zwischen zentralen und dezentralen Produkten und Dienstleistungen zu unterscheiden scheinen.

²⁷⁴⁰ Siehe etwa Bundesrat, DLT-Bericht 2018, 14.

²⁷⁴¹ Hierzu etwa Kuhn, SZW 2014, 376–377, der von einer «geschäftsmässig nicht zu rechtfertigende[n] Anknüpfung zum Recht eines Staates [...], der über keine äquivalente [Regulierung] verfügt» spricht; in makroprudenzieller Hinsicht sodann Nouy, Regulatory arbitrage, *passim* («[S]tructuring [...] activities in a way that reduces the impact of regulation without a corresponding reduction in the underlying risk.»).

²⁷⁴² Siehe zur Dezentralität als Rechtskonzept unten, [VII](#).

²⁷⁴³ So auch Jacquemart, Offene Blockchainsysteme, Rz. 601–603; vgl. ferner Möslin, in: Möslin, Finanzinnovation und Rechtsordnung, 27; sodann auch Bärtschi/Hirschi, SZW 2017, 790, welche aber im technologieneutralen Ansatz der Regulierung ein potenzielles Hindernis erkennen.

Nachfolgend sollen potenzielle marktbasierte Lösungen untersucht werden, welche im Interesse der Anleger und der Marktintegrität künftig integraler Bestandteil der Finanzmarktregulierung bilden könnten. Der Fokus liegt dabei auf dezentralen Handelsplattformen. Vorab soll aber summarisch der Frage nachgegangen werden, ob Wettbewerb und Innovation als nützliche Instrumente des Aufsichtsregimes bereits heute grössere Beachtung erhalten sollen.

4.2 Wettbewerb und Innovation

a. Wettbewerb als «Regulator»

Ein Ansatz, der in der juristischen Literatur nahezu in Vergessenheit geraten zu sein scheint, ist die «Regulierung» von Produkten und Dienstleistungen durch den Wettbewerb, worunter primär der Wettbewerb der Anbieter bzw. Finanzdienstleister gemeint ist.²⁷⁴⁴ Der Wettbewerb kann als eine dritte Ebene der Marktkontrolle bezeichnet werden, welche neben die Selbstregulierung und staatliche Regulierung tritt.²⁷⁴⁵

Die Vernachlässigung des Wettbewerbs als Regulierungskonzept ist gemäss PETER NOBEL wenig überraschend, seien doch die Verfassungsvorgaben für den Finanzsektor «nicht sehr aussagekräftig» und werde doch allzu rasch und ohne vertiefte Auseinandersetzung vom Vorliegen eines öffentlichen (Regulierungs-)Interesse ausgegangen.²⁷⁴⁶ Die grundsätzlich anerkannte subsidiäre Rolle staatlicher Regeln wird in diesem Zusammenhang oftmals ignoriert.²⁷⁴⁷ Weil aber bestehende Regulierungskonzepte bei dezentralen Systemen an ihre Grenzen stossen, stellt sich die Frage, ob den Wettbewerbskräften mitunter durch innovationsoffene Regulierung nicht mehr Raum eingeräumt werden sollte.

²⁷⁴⁴ Vgl. Stigler, The Journal of Business 1964, 124 («So far as the efficiency and growth of the American economy are concerned, efficient capital markets are even more important than the protection of investors – in fact efficient capital markets are the major protection of investors.»).

²⁷⁴⁵ Siehe etwa Fey, Banken, 19–22.

²⁷⁴⁶ Siehe Nobel, SZW 2014, 592–593 m.w.H.

²⁷⁴⁷ Siehe Fey, Banken, 25–26.

b. Anlegerwohlfahrt

Kaum ein Ordnungsprinzip²⁷⁴⁸ scheint in der Finanzmarktaufsicht so sehr vernachlässigt zu werden wie der *Anbieterwettbewerb* im Finanzdienstleistungsmarkt. Die oft zu vernehmende Aussage, dass Wettbewerb und Regulierung als Antagonisten zu betrachten seien, bringt dies gut zum Ausdruck.²⁷⁴⁹ Allgemein wird die Auffassung vertreten, dass der dem Marktmodell inhärente Anleger- bzw. Konsumentenschutz ungenügend sei.²⁷⁵⁰ Dass diese Ansicht zu kurz greift, ist etwa daran ersichtlich, dass Wettbewerb die Effektivität von Regulierung, insb. wenn diese auf erhöhte Transparenz ausgerichtet ist,²⁷⁵¹ verbessern kann.²⁷⁵²

Der Wettbewerb wird vorliegend als Koordinations- und Steuerungssystem wirtschaftlicher Aktivitäten verstanden. Er beruht im Wesentlichen auf dem Preismechanismus als dezentrales System der Wissens- und Handlungskoordination.²⁷⁵³ Er ist gegensätzlich zum zentralen Plan einer staatlichen Behörde oder zur Gruppen- bzw. Kartellvereinbarung zwischen Marktteilnehmern.²⁷⁵⁴ In Bezug auf die Förderung der Anlegerwohlfahrt können in erster Linie zwei Aspekte des Wettbewerbs unterschieden werden: Innovation und Konsumentensouveränität bzw. Wahlfreiheit.²⁷⁵⁵ Daneben tritt der Aspekt der Faktorallokation.²⁷⁵⁶

²⁷⁴⁸ Zum Konzept unten, [VII.2.2.](#)

²⁷⁴⁹ Anschaulich für diese Haltung etwa König, in: Körber, Wettbewerb als Ordnungsprinzip auf den Finanzmärkten, *passim*;

²⁷⁵⁰ Stellvertretend für diese Ansicht bspw. Werlen, Konzeptionelle Grundlagen, 41 m.w.N.

²⁷⁵¹ Siehe etwa zu den wirtschaftswissenschaftlichen Begründungen von zwingenden Transparenzregimen Bainbridge, University of Cincinnati Law Review 2000, 1031–1032.

²⁷⁵² Siehe Dietrich/Bienert, in: Abegg/Bärtschi/Dietrich, § 1 Rz. 128; ferner wohl auch SK FinfraG-Sethe, Art. 1 N 23, der funktionierende Marktmechanismen und u.a. umfassende Information in Verbindung zueinander setzt.

²⁷⁵³ So insb. von Hayek, American Economic Review 1945, 521 («*Competition, on the other hand, means decentralized planning by many separate persons.*»), 524–525, 526–527; ferner von Hayek, in: von Hayek, Meaning of Competition, 106 («*Competition is essentially a process of the formation of opinion[.]*»).

²⁷⁵⁴ Siehe Schluep, in: Jagmetti/Schluep, Wirtschaftsrecht, 74–75.

²⁷⁵⁵ Siehe Kieninger, Wettbewerb der Privatrechtsordnungen, 24.

²⁷⁵⁶ Siehe statt vieler von Hayek, in: von Hayek, Meaning of Competition, 104–105, der allerdings alles andere als eine simplistische Sichtweise der Allokationseffizienz einnimmt («*[...] we should worry much less about whether competition in a given case is perfect and worry much more whether there is competition at all.*»).

Innovation ist eng mit dem Wettbewerb verknüpft: Richterweise sind wettbewerblich verfasste Finanzmärkte ohne Finanzinnovation «schlechterdings undenkbar».²⁷⁵⁷ VON HAYEK spricht sodann vom «Wettbewerb als Entdeckungsverfahren».²⁷⁵⁸ Der konkrete Zusammenhang zwischen unternehmerischer Schöpfungskraft und Wettbewerber in empirischer Hinsicht ist ohne Zweifel komplex.²⁷⁵⁹ Dazu passt, dass die zentrale Rolle von Unternehmen als Innovatoren in den vorherrschenden ökonomischen Modellen weitgehend vernachlässigt wird.²⁷⁶⁰ Es ist angesichts der empirischen Evidenz allerdings unbestritten, dass Innovation überkommene Marktstrukturen aufbrechen und nachhaltig umgestalten kann. Innovation schafft individuelle und kollektive Chancen, die durch den Wettbewerb der Innovatoren potenziert und gesellschaftlich verteilt werden.²⁷⁶¹ Bestehende Marktführer werden sodann in ihren Monopol- bzw. Oligopolrenten herausgefordert, was für Konsumenten i.d.R. tiefere Preise und bessere Konditionen bedeutet.²⁷⁶²

Wirksamer Wettbewerb zwischen den Teilnehmern des Finanzmarktes schafft im Prinzip günstige ökonomische Ergebnisse für Gläubiger, Anleger und Versicherte sowie auch für weitere im Finanzmarkt tätige Personen.²⁷⁶³ Es verschafft ihnen im Verlauf dieses Prozesses grössere Wahlfreiheit und damit letztlich die Chance auf *Konsumentensouveränität*. Kurzum: Der Wettbewerb der Marktteilnehmer ist nach einem liberalen Staatsverständnis im Interesse des Gemeinwohls.²⁷⁶⁴

²⁷⁵⁷ So etwa Möslein, in: Möslein, Finanzinnovation und Rechtsordnung, 8.

²⁷⁵⁸ Siehe hierzu von Hayek, in: Streit, Wettbewerb als Entdeckungsverfahren, *passim*; ähnlich wohl auch Nobel/Zimmermann, in: Möslein, Finanzinnovationen, 83.

²⁷⁵⁹ Vgl. etwa Aghion et al., *The Quarterly Journal of Economics* 2005, *passim*; ferner WEF, *Rethinking Financial Innovation*, 14–15.

²⁷⁶⁰ Für einen Überblick siehe Foss/Klein, *Organizing Entrepreneurial Judgment*, 8–20; ferner Kirzner, in: Boettke/Sautet, *Competition and Entrepreneurship*, 71–74.

²⁷⁶¹ So auch WEF, *Rethinking Financial Innovation*, 11; vgl. etwa auch Kirzner, in: Boettke/Sautet, *Competition and Entrepreneurship*, 76, wonach Unternehmertum und Wettbewerb nicht auseinander gedacht werden können; Prosi, in: Radnitzky/Bouillon, *Europäische Integration*, 119–120; ferner Hettich, *Kooperative Risikoversorge*, Rz. 22, 31.

²⁷⁶² Ausführlich etwa Mankiw, *Microeconomics*, 134–138, 142–146, 300–303, 347–348, 354, was mikroökonomisch auch als «Konsumentenrente» bezeichnet wird.

²⁷⁶³ Gl.M. Heinemann, in: Heiss/Loacker, *Konsumentenschutz*, N 9.93 («Wirksamer und unverfälschter Wettbewerb ist das mächtigste Instrument zum Schutz der Konsumenten [...]»); Inderst, *EBOR* 2009, 457, 461–464 («*Competition is the most powerful ally of consumers.*»); ferner McCall, *SEC regulation*, *passim*; im Allgemeinen sodann Vallender, in: *SGK BV*, Art. 94 N 35; vgl. ferner die Ausführungen bei Hettich, *Wirksamer Wettbewerb*, N 687–688.

²⁷⁶⁴ So etwa bereits BGE 45 I 347, E. 1 («allgemein[e] Volkswohlfahrt»).

Wettbewerb und Innovation haben gerade im Bereich der Digitalisierung eine überragende historische Rolle gespielt.²⁷⁶⁵ Die inzwischen eingetretene Machtkonzentration durch Internet-Intermediäre, wie namentlich Amazon, Apple, Google und Facebook, widerspricht nicht grundsätzlich dieser Entwicklung. Dezentrale Systeme können denn auch als eine Gegenbewegung zur Konzentration von Marktmacht aufgefasst werden.²⁷⁶⁶

c. Wettbewerb im FINMAG

Gemäss Art. 4 FINMAG bezweckt die Finanzmarktaufsicht nach Massgabe der Finanzmarktgesetze den Schutz der Gläubiger, der Anleger, der Versicherten sowie den Schutz der Funktionsfähigkeit der Finanzmärkte. Bei diesen Aufsichtszielen handelt es sich aus juristischer Sicht um die Grundfunktionen der Finanzmarktregulierung. Aus ihnen lässt sich grundsätzlich jede Form von Eingriff in den Markt ableiten.²⁷⁶⁷ Die Finanzmarktaufsicht soll durch Verfolgung der Aufsichtsziele, auch dies ist in Art. 4 FINMAG erwähnt, zur Stärkung des Ansehens, *der Wettbewerbsfähigkeit und der Zukunftsfähigkeit des Finanzplatzes Schweiz* beitragen.

Wie in allen marktwirtschaftlich organisierten Industrien spielt Wettbewerb auch in Finanzmärkten eine bedeutende Rolle. Der hohe Regulierungsdruck wird aber gemeinhin als negativ für den Eintritt neuer Marktteilnehmer und somit für den potenziellen Wettbewerb angesehen. Dies wirkt sich sodann tendenziell negativ auf die Innovationskraft der betroffenen Industrie aus. Die Vorteile einer Wettbewerbsordnung werden in den Materialien der Finanzmarktregulierung kaum je hervorgehoben.²⁷⁶⁸ Bezeichnenderweise wird Regulierung fast immer als Voraussetzung für einen funktionierenden Wettbewerb betrachtet.²⁷⁶⁹ Soweit ersichtlich, hat auch die FINMA zum Wettbewerb als

²⁷⁶⁵ Siehe etwa Thierer, *Permissionless Innovation*, 47–51; sodann Savary, *Regulierung dominanter Internetplattformen*, 64–65.

²⁷⁶⁶ Siehe hierzu ausführlich Barabas/Narula/Zuckerman, *Defending Internet Freedom through Decentralization*, *passim*.

²⁷⁶⁷ Vgl. Bühler, SJZ 2010, 471; ferner Nobel, SZW 2014, 592, der u.a. die fehlende Verfassungsgerichtsbarkeit in der Schweiz bedauert (vgl. Art. 190 BV).

²⁷⁶⁸ Vgl. immerhin, aber doch nicht richtig überzeugt Botschaft FINMAG 2006, 2860 (*«Der Schutz von Gläubigerinnen und Gläubigern, Anlegerinnen und Anlegern sowie der Versicherten vor Insolvenzrisiken wird am wirksamsten gewährleistet, wenn die Finanzintermediärinnen und -intermediäre wettbewerbsfähig sind.»*).

²⁷⁶⁹ Siehe etwa Botschaft FIDLEG/FINIG 2015, 8912 (*«ausreichende Transparenz»*), 8930, 8941, 9090 (*«gleiche Wettbewerbsbedingungen geschaffen»*); ferner Bundesrat, Bericht Kostenfolgen FINMA-Rundschreiben, 6–7.

mögliches Instrument des Anleger- oder Funktionsschutzes bisher nicht ausdrücklich Stellung genommen.

Die in Art. 4 FINMAG enthaltene Stärkung der Wettbewerbsfähigkeit des schweizerischen Finanzplatzes ist demgegenüber als wirtschaftspolitisch motiviertes Ziel für den gesamten Schweizer Finanzplatz zu verstehen.²⁷⁷⁰ Es geht mit anderen Worten um Themen wie Marktzugang, insb. zu EU-Mitgliedsstaaten.²⁷⁷¹ Ferner ist damit die Wettbewerbsfähigkeit der Schweizer Volkswirtschaft im Vergleich zu ausländischen Märkten gemeint.²⁷⁷² Ein derartiges Wettbewerbsverständnis ist rein relativer Natur, ohne es inhaltlich an qualitativen oder quantitativen Kriterien zu messen. Als Aufsichtsziel weist die Stärkung der Wettbewerbsfähigkeit mit anderen Worten keinen unmittelbaren Bezug zur mikroökonomischen Wettbewerbsstruktur des Finanzmarktes und von dessen Teilnehmern auf.²⁷⁷³

In der Botschaft zum FINMAG wurde die Aufsichtsbehörde dazu aufgefordert, insb. die Kosten, die den Beaufsichtigten entstehen, die Auswirkungen auf den Wettbewerb, die Innovationsfähigkeit und die internationale Wettbewerbsfähigkeit des Finanzplatzes zu berücksichtigen.²⁷⁷⁴ Die FINMA hat diese *Regulierungsgrundsätze* im Rahmen des Erlasses von Verordnungen und Rundschreiben und nach vorliegender Ansicht grundsätzlich auch darüber hinaus (z.B. bei Veröffentlichung von Aufsichtsmitteilungen) zu beachten. Namentlich hält Art. 7 Abs. 2 lit. b FINMAG die FINMA dazu an, u.a. die Auswirkungen ihrer Regulierung auf den Wettbewerb und die Innovationsfähigkeit zu berücksichtigen. Nach dem neuen Art. 6 Abs. 3 der Verordnung zum Finanzmarktaufsichtsgesetz (FINMAV) hat die FINMA Regulierungen wettbewerbs- und technologieneutral auszugestalten. Abweichungen von diesem Grundsatz sind zu begründen. Dabei hat sie die Auswirkungen auf das Wettbewerbsumfeld und die Marktstrukturen möglichst klein zu halten.²⁷⁷⁵ Art. 6 Abs. 3 FINMAV nimmt somit auch die mikroökonomische Dimension des Wettbewerbs

²⁷⁷⁰ So wohl auch BSK FINMAG/FinfraG-Winzler, Art. 5 FINMAG N 14.

²⁷⁷¹ Siehe Sethe, in: Notter et al., Wettbewerb als Regelungsziel, 376; ferner zur Äquivalenzfrage schweizerischen Rechts unter MiFID und MiFIR Sethe, in: Gericke, Drittstaatenzugang, *passim*. Vgl. allerdings zur *ernüchternden* Situation im Bereich des Marktzugangs mit EU-Ländern Jutzi, Jusletter vom 29. November 2021, Rz. 120–123.

²⁷⁷² Beispielhaft etwa Bundesrat, DLT-Bericht 2018, 12.

²⁷⁷³ Vgl. immerhin Sethe, in: Notter et al., Wettbewerb als Regelungsziel, 385, der festhält, dass auch der Wettbewerb «innerhalb» der Märkte mitgemeint sei.

²⁷⁷⁴ Siehe Botschaft FINMAG 2006, 2843; vgl. ferner FINMA, Leitlinien Finanzmarktregulierung, 3, 4.

²⁷⁷⁵ Siehe EFD, Erläuterungen FINMAV 2019, 17.

als Regulierungsanliegen auf.²⁷⁷⁶ Allerdings ist damit offensichtlich nicht das generelle Wettbewerbsniveau des Finanzmarktes gemeint, welches in der Praxis wie bereits erwähnt regelmässig eher schwach ausgeprägt ist. Demgegenüber hat die FINMA lediglich die Auswirkungen einer Regulierung auf das bestehende Wettbewerbsniveau der Marktteilnehmer zu berücksichtigen.

Trotz der erwähnten Bestimmungen, welche die FINMA im Rahmen ihrer Regelsetzungsbefugnisse zur Beachtung allfälliger wettbewerbsbeeinflussender Effekte anhält, ist zu konstatieren, dass dem Wettbewerb als *eigenständiger* Faktor im Zusammenhang mit dem aufsichtsrechtlichen Anleger- und Funktionsschutz kaum Bedeutung zuzukommen scheint. Auch wenn polizeilich motivierte Eingriffe, etwa zum Schutz der Gläubiger einer insolventen Bank oder zum Schutz der Stabilität des Finanzmarktes, gerechtfertigt erscheinen,²⁷⁷⁷ so sollte die Finanzmarktaufsicht nach vorliegender Ansicht insb. den auf Innovation gerichteten Wettbewerb zwischen den Anbietern von Produkten und Dienstleistungen im Interesse der Anleger als eigenständiges Aufsichtsziel vermehrt Rechnung tragen.²⁷⁷⁸ Darüber hinaus ist zu erwarten, dass infolge Aufbrechens bestehender Marktkonzentrationen die Systemrisiken verringert und die Stabilität des Gesamtsystems verbessert werden könnten.²⁷⁷⁹

Die Berücksichtigung von Marktkräften ist angesichts des Umstandes, dass es sich bei dezentralen Systemen um schwer regulierbare Aktivitäten handelt,²⁷⁸⁰ besonders *dringlich*. In diesem Zusammenhang sei abschliessend auf Art. 170 BV hingewiesen, wonach die Bundesversammlung dafür zu sorgen hat, dass die Massnahmen des Bundes (regelmässig) auf ihre Wirksamkeit hin überprüft werden. Unwirksame Regulierungsregime sind demgegenüber anzupassen und allenfalls sogar aufzuheben.²⁷⁸¹

²⁷⁷⁶ Vgl. auch Botschaft FINMAG 2006, 2861 («Wettbewerb zwischen den einzelnen Beaufsichtigten»); BSK FINMAG/FinfraG-Winzeler, Art. 7 FINMAG N 82, der zwischen «Wettbewerb nach innen (zwischen den Finanzintermediären) und aussen (mit den anderen Finanzplätzen)» unterscheidet.

²⁷⁷⁷ So das Bundesgericht etwa in BGE 111 Ib 126 E. 2a («rechts- und sittenwidrige Geschäfte»); 137 II 431, E. 4.1 («ökonomische Stabilität und der Schutz des Finanzmarkts»); ferner hierzu Hettich, in: SGK BV, Art. 98 N 2–3, 5; BSK BV-Kaufmann/Utz, Art. 98 N 2, 35.

²⁷⁷⁸ So auch Brummer/Yadav, *The Georgetown Law Journal* 2019, 246–247; ausführlich Van Loo, *UCLA Law Review* 2018, 251–253.

²⁷⁷⁹ Siehe Van Loo, *UCLA Law Review* 2018, 249–251.

²⁷⁸⁰ Siehe hierzu einleitend unten, [VI.4.3a](#).

²⁷⁸¹ Siehe Hettich, *Kooperative Risikovorsorge*, Rz. 743.

4.3 Marktorientierter Regulierungsansatz

a. Begründung

Der Fokus auf marktorientierte Regulierung gründet in der Erkenntnis, dass die Rechtsordnung die unterschiedlichen Dimensionen der Steuerung gesellschaftlicher Risiken zu beachten hat.²⁷⁸² Dabei können Steuerungsfähigkeit, Steuerungswirkung und Steuerungsbedürfnis unterschieden werden.

Das Auseinanderfallen einzelner Dimensionen ist besonders im Falle dezentraler Systeme relevant, welche, wie anfangs dargelegt, nur unter erschwerten Bedingungen regulierbar sind. Dezentrale Systeme stehen offensichtlich nicht ausserhalb der Rechtsordnung. Es handelt sich bei ihnen nicht etwa um Naturkräfte oder dergleichen. Sie sind theoretisch durchaus *steuerungsfähig*. Es wird vorliegend auch nicht behauptet, dass dezentrale Systeme von der *Steuerungswirkung* des Rechts völlig unbeeinflusst sind. Ein formelles Verbot solcher Systeme würde ohne Weiteres das Verhalten vieler Marktteilnehmer beeinflussen. Im Resultat würde ein Verbot wohl die praktische Bedeutung von DeFi marginalisieren.²⁷⁸³ Die Steuerungswirkung des Rechts scheint aufgrund der Eigenschaften dezentraler Systeme indessen stark eingeschränkt. Für den Gesetzgeber stellen sich allerdings nicht nur Fragen nach der Steuerungsfähigkeit und -wirkung, sondern insb. auch, ob und inwieweit quelloffener Computercode das *Steuerungsbedürfnis* des Rechts verringert. Dabei scheint die Tatsache, dass dezentrale Systeme aufgrund ihrer vielgestaltigen Dynamik einen hohen soziotechnischen Komplexitätsgrad erreichen können, einfache Steuerungsinstrumente nahezulegen.²⁷⁸⁴ An dieser Stelle kommen darum marktorientierte Regulierungsansätze ins Spiel.

b. Inhalt und Umfang

Marktorientierte bzw. marktbasierende Regulierungsansätze beruhen in erster Linie auf einer Änderung der *wirtschaftlichen* Anreizstruktur und der Informa-

²⁷⁸² Die Rechtsordnung selbst ist ein System des Risikomanagements; siehe diesbezüglich Nobel, SZW 2016, 555–556.

²⁷⁸³ Vgl. aber zur Problematik eines Verbots aus grundrechtlichen Überlegungen oben, [VI.2](#).

²⁷⁸⁴ Vgl. Haldane/Madouros, in: Federal Reserve Bank of Kansas, *The Dog and the Frisbee*, 115; ferner Epstein, *Simple Rules for a Complex World*, 21; Gigerenzer, *Bauchentscheidungen*, 209–210.

tionslage der Marktteilnehmer.²⁷⁸⁵ Es handelt sich dabei nicht um reine Marktregulierung bzw. -steuerung im Sinne reiner Konsumentensouveränität, wobei aber deren Implikationen gerade ausgenutzt werden sollen.²⁷⁸⁶ *Im Ergebnis wird mit marktorientierter Regulierung beabsichtigt, die Grundlagen für gute Nachfrageentscheidungen im Markt herzustellen.*

Im Zentrum der vorliegenden Ansätze steht insb. die Verringerung von Informationsasymmetrien, welche ihren Ursprung in den Agency-Beziehungen der Marktteilnehmer haben.

Marktorientierte Ansätze können einerseits in einer innovationsoffenen und andererseits in einer wettbewerbsfördernden Form realisiert werden.²⁷⁸⁷ Es wird mit solchen Instrumenten in erster Linie ein Verhaltens- und Schutzniveau angestrebt, das nicht direkt von den individuellen Beiträgen der einzelnen Marktteilnehmer abhängig ist, sondern durch das Kollektiv aller Akteure, d.h. Anbieter und Nachfrager, erfüllt wird.²⁷⁸⁸ Schliesslich sollte unter einem marktbasierten Ansatz auch der Einbezug von Marktteilnehmern in den Regulierungsprozess verstanden werden, was gleichermassen eine positive Anreizwirkung auf die Einhaltung von Regeln in der Praxis ausüben kann.²⁷⁸⁹

c. Vorschläge in Bezug auf dezentrale Handelsplattformen

i. Übersicht der Regulierungsansätze

Nachfolgend werden fünf mögliche marktorientierte Regulierungsansätze vorgestellt, welche sich weder gegenseitig ausschliessen noch zwingend miteinander kombiniert werden müssen. Das Kernstück bildet allerdings das Offenlegungsregime.

Bei den vorgeschlagenen Regulierungsansätzen handelt es sich namentlich um:

²⁷⁸⁵ Vgl. etwa May, in: Salomon, Social Regulation, 157, 173–174 («marketlike incentives»).

²⁷⁸⁶ Vgl. zur Marktsteuerung Spindler/Thorun, MMR-Beilage 2016, 9.

²⁷⁸⁷ Vgl. zu dieser Unterscheidung Zetzsche et al., University of Pennsylvania Journal of Business Law 2020, 325–330.

²⁷⁸⁸ Siehe Hettich, Kooperative Risikoversorge, Rz. 294; ferner Möslin, in: Möslin, Finanzinnovation und Rechtsordnung, 15.

²⁷⁸⁹ Siehe hierzu Senn, Journal of Corporate Law Studies 2005, 442, 451, 463.

- Anerkennung dezentraler Systeme als öffentlicher Koordinationsmechanismus für (finanz-)wirtschaftliche Aktivitäten;
- Setzen von Anreizen zur frühzeitigen Kooperation mit den Behörden;
- Erlass von Verhaltenskodizes in polyzentrischer ko-regulierender Weise²⁷⁹⁰ mit dem Ziel, Informationen für die Marktteilnehmer zu standardisieren;
- Investor Education mithilfe entsprechender Materialien von Behörden und Privaten, um die besonderen Risiken von DeFi hervorzuheben;
- Öffnung dezentraler Systeme für die traditionelle Finanzintermediation.

ii. Anerkennung dezentraler Systeme als öffentlicher Koordinationsmechanismus

Dezentrale Systeme sind, wie im zweiten Kapitel ausgeführt, neuartige institutionelle Koordinationsmechanismen mit überwiegend öffentlichem Charakter. Sie sind wirtschaftlich betrachtet weder rein private noch rein öffentliche Güter, sondern sie kombinieren Elemente von Märkten, Hierarchien und Netzwerken in einer neuartigen Weise. Es handelt sich mit anderen Worten nicht bloss um ein herkömmliches Produkt oder eine herkömmliche Dienstleistung von Akteuren des Finanzsektors, sondern um eine eigenständige Form der Koordination wirtschaftlicher und sozialer Aktivitäten.²⁷⁹¹ Wohingegen Produkte und Dienstleistungen in einer Weise angeboten werden, welche die vollständige Privatisierung der Gewinne bei einer Person oder einer Gruppe von miteinander verbundenen Personen zulässt, sollte das Finanzmarktrecht diese Produkte und Dienstleistungen den gleichen Regeln unterstellen wie traditionelle Finanzmarktgüter.

Die Finanzmarktordnung könnte darum in einem ersten Schritt dezentrale Systeme als neuartige Koordinationsmechanismen für (finanz-)wirtschaftliche Aktivitäten ausdrücklich anerkennen.²⁷⁹² Wohl verstanden ist damit nicht bloss

²⁷⁹⁰ Vgl. zum Konzept Finck, Digital Regulation, LSE Law, Society and Economy Working Papers 15/2017, 23–25.

²⁷⁹¹ Siehe hierzu oben, [II.5.2a](#).

²⁷⁹² Ähnlich Allen et al., Research Policy 2020, 2 («In a context of innovation of institutional technologies, crypto-friendly policy is innovation policy. Governments should adopt crypto-friendliness as a generalisable principle for policy, enabling the process of institutional evolution and competition to take place.»); sodann Shcherbak, European Journal of Legal Studies 2014, 79, der vorschlägt, dass Aufsichtsbehörden offiziell Bitcoin als «unregulated technology» anerkennen sollten; ferner Rettig/Mosier/Gilman, Genuine DeFi, 36–38, die dafür plädieren, DeFi-Systeme als «critical infrastructure» (überwiegend) ausserhalb des

die Anerkennung von Selbstregulierung als Mindeststandard und somit als nützliche Form der Regulierung durch die Marktteilnehmer gemeint.²⁷⁹³ Dagegen geht es darum, dass die Finanzmarktordnung sich, soweit erforderlich und sinnvoll, auf dezentrale Systeme als Koordinationsmechanismen ausrichtet. Dabei ist konkret zu fordern, dass dezentrale Systeme in erster Linie der dezentralen Governance der Teilnehmer und Nutzer überlassen werden.²⁷⁹⁴

In diesem Rahmen sollte die Rechtsordnung ausserdem *Dezentralität als Rechtsprinzip* explizit oder implizit anerkennen.²⁷⁹⁵ Zu einem gewissen Grad, wie weiter unten noch aufzuzeigen sein wird, haben die schweizerischen Behörden Dezentralität als soziotechnische Realität der Finanzmarktordnung bereits anerkannt. Namentlich wird aus den behördlichen Ausführungen ersichtlich, dass Dezentralität als eigenständiges Ordnungsprinzip im Spannungsverhältnis zwischen einerseits einer reinen *Laisser-faire*-Haltung und andererseits der rechtlichen Unterstellung von dezentralen Systemen unter die bestehenden Regeln Bedeutung erlangt hat.²⁷⁹⁶ Die Schaffung von Registerwertrechten zeigt, dass Rechtsinnovationen zur vorhergegangenen Finanzinnovation hinzutreten können.²⁷⁹⁷

Im Rahmen der regulatorischen Anerkennung dezentraler Systeme wäre es ferner wünschenswert, dass ungerechtfertigte regulatorische Wettbewerbshindernisse für die an der Peripherie dezentraler Systeme handelnden Personen abgebaut oder zumindest einheitliche Wettbewerbsbedingungen mit dem traditionellen Finanzintermediationssystem hergestellt würden. Gerade im Geldwäschereibereich scheint letzteres heute nicht der Fall zu sein.²⁷⁹⁸

Schliesslich sollte sich der schweizerische Finanzmarkt gegenüber ausländischen Märkten öffnen, und zwar auch *unilateral*. Ein solcher Schritt erhöht tendenziell den lokalen Wettbewerb und somit die Innovationskraft des Finanz-

Finanzmarktrechts zu regulieren. Eine Weiterentwicklung dieses Regulierungsansatzes wäre die Etablierung von *Public-Private Ownerships*; vgl. hierzu Zellweger-Gutknecht/Weber, EuZ 06/2022, G 22.

²⁷⁹³ Vgl. Art. 7 Abs. 3 FINMAG.

²⁷⁹⁴ Vgl. in diesem Zusammenhang Schlegel/Schuppli, ex ante 2/2019, 11, welche drei Szenarien hinsichtlich der Auswirkungen innovationsgetriebener Transaktionskostenveränderungen auf die Regulierung formulieren: (1) Rückzug des Staates, (2) Ausdehnung der Regulierung, (3) Zugriff des Staates auf die Sphäre des Einzelnen. Vorliegend wird der Fall des Rückzuges des Staates stipuliert.

²⁷⁹⁵ Vgl. zur Dezentralität als Rechtskonzept, VII.

²⁷⁹⁶ Siehe hierzu unten, VII.2.

²⁷⁹⁷ Vgl. Möslein, in: Möslein, Finanzinnovation und Rechtsordnung, 15–17.

²⁷⁹⁸ Siehe hierzu bspw. oben, V.2.7e.

platzes, was letztlich den Kunden und Anlegern zugutekommt.²⁷⁹⁹ Das Ziel einer solchen Öffnung besteht darin, dass Inländern die Nutzung von und Teilnahme an Protokollen, die im Wesentlichen im Ausland entwickelt und unterhalten werden, offensteht und dass Ausländern die Nutzung von und Teilnahme an Protokollen offensteht, die u.a. in der Schweiz entwickelt und unterhalten werden. Es besteht in diesem Punkt allerdings nicht allzu viel Hoffnung, haben doch erst kürzlich umgesetzte Gesetzesvorhaben, wie namentlich MiFID II und MiFIR sowie FIDLEG, zu einer Verschärfung der grenzüberschreitenden Regulierungsregime in Europa geführt.²⁸⁰⁰

iii. Anreize zur Kooperation

Angesichts der rechtlich schwer fassbaren Aktivitäten in DeFi empfiehlt es sich, dass die Finanzmarktaufsicht den Marktteilnehmern frühzeitig Anreize zur Kooperation setzt.

Hierzu gehören etwa Sandbox-Regime, Safe-Harbor-Regeln, No-Action-Letters und spezialisierte DeFi- bzw. FinTech-Desks.²⁸⁰¹ Entwicklerteams können dadurch vor dem Start eines Netzwerks oder einer Applikation mit den Behörden ihre Pläne diskutieren und allenfalls Protokolle im Rahmen eines Spezialregimes entwickeln. Eine kooperative Herangehensweise erhöht nicht nur die Rechtssicherheit für Projekte, sondern verbessert v.a. auch die Informationslage der Aufsichtsbehörde.²⁸⁰² Der Ansatz trägt insofern zur Lösung des Wissensproblems der Finanzmarktaufsicht bei, welche mit der Entwicklungsdynamik von Finanzinnovationen konfrontiert ist.²⁸⁰³

²⁷⁹⁹ GL.M. im Grundsatz in Bezug auf die Öffnung der EU-Märkte gegenüber Drittstaaten Sethe, in: Notter et al., Wettbewerb als Regelungsziel, 380; ferner Sethe, in: Gericke, Drittstaatenzugang, 139.

²⁸⁰⁰ In diesem Sinne ernüchternd Bundesrat, Zugang zum Finanzmarkt, *passim*; ferner Bahar/Nedwed, SZW 2019, 638, welche vom Ende eines liberalen Zeitalters im grenzüberschreitenden Verkehr sprechen; *differenzierend* im Vergleich zu den Regelungen in EU-Staaten Jutzi, Jusletter vom 29. November 2021, Rz. 115–116.

²⁸⁰¹ So auch WEF, Decentralized Finance, 24.

²⁸⁰² Siehe etwa Finck, German Law Journal 2018, 685; Brummer/Yadav, The Georgetown Law Journal 2019, 304–305; Zetzsche et al., University of Pennsylvania Journal of Business Law 2020, 326–327; ausführlich zu der als *Bottom-up*-Ansatz bezeichneten Kooperation zwischen Privaten und Behörden Hess, Penn State Law Review 2024, 43–47.

²⁸⁰³ Siehe Möslin, in: Möslin, Finanzinnovation und Rechtsordnung, 31–32 m.w.N.

Ferner können Reden von Behördenvertretern sowie die Veröffentlichung von Aufsichtsmitteilungen über eine entsprechende Signalwirkung die Marktteilnehmer zur Kooperation mit der Finanzmarktaufsicht veranlassen.²⁸⁰⁴

In diesem Rahmen könnte sodann bewusst ein innovationsoffener Ansatz zur «Förderung» von Dezentralität implementiert werden: Denkbar und prüfungswert ist die Einführung einer *Safe-Harbor*-Regelung, die Entwicklerteams einen zeitgebundenen Innovationsraum für die Entwicklung dezentraler Systeme einräumt.²⁸⁰⁵ In diesem Fall würden während einer bestimmten Phase alle oder einzelne Finanzmarktgesetze nicht zur Anwendung gelangen, wenn das Entwicklerteam unter Offenlegung bestimmter Informationen beabsichtigt und effektiv daran arbeitet, das Protokoll eines Netzwerks oder einer Applikation zu dezentralisieren. Im Vordergrund steht mit anderen Worten die regulatorische «Starthilfe» für ein neues Projekt, das innert angemessener Frist zu einem dezentralen System ausgebildet werden muss.²⁸⁰⁶

Das SEC-Kommissionsmitglied PEIRCE hat einen solchen Vorschlag erarbeitet und aufgrund von Rückmeldungen aus der DeFi-Community verfeinert. Darin ist vorgesehen, dass ein Protokoll nach Ablauf der Frist entweder genügend dezentralisiert oder aber dass ein Netzwerk vollständig funktional sein muss, um weiterhin von den entsprechenden Registrierungspflichten des US-amerikanischen Wertpapierrechts ausgenommen zu sein.²⁸⁰⁷ Der Vorschlag wurde SEC-intern als ungenügend kritisiert, wobei insb. der Fokus auf den Anleger-schutz gelegt wurde.²⁸⁰⁸ Ein Ansatz, der gleichzeitig innovationsoffen ist und

²⁸⁰⁴ Siehe Brummer/Yadav, *The Georgetown Law Journal* 2019, 283.

²⁸⁰⁵ Ablehnend gegenüber einer Sandbox und einem generellen Carve-out im Finanzmarktinfrakturenrecht hingegen Bundesrat, DLT-Bericht 2018, 113–114.

²⁸⁰⁶ Skeptisch hinsichtlich praktischer Umsetzbarkeit des Vorschlags Palley, *Safe Harbors for Token Sales*, *passim*.

²⁸⁰⁷ Siehe für den Vorschlag einer *Safe-Harbor*-Regel im US-amerikanischen Wertpapierrecht Peirce, *Proposal to Fill the Gap Between Regulation and Decentralization*, *passim*; siehe zum genauen Wortlaut des Vorschlags Peirce, *SafeHarbor 2.0*, GitHub, *passim* («*The application of the federal securities laws to the primary distribution of Tokens and secondary transactions frustrates the network's ability to achieve maturity and prevents Tokens sold as a security from functioning as non-securities on the network. Accordingly, this safe harbor is intended to provide Initial Development Teams with a three-year time period within which they can facilitate participation in, and the continued development of, a functional or decentralized network, exempt from the registration provisions of the federal securities laws so long as certain conditions are met. The safe harbor is designed to protect Token purchasers by requiring disclosures tailored to the needs of the purchasers and preserving the application of the anti-fraud provisions of the federal securities laws to Token distributions by an Initial Development Team relying on the safe harbor.*»).

²⁸⁰⁸ Siehe Crenshaw, *Bridge to Better Outcomes*, *passim*.

Rechtssicherheit gewährleistet, kann auch als *Do No Harm*-Regulierungsmodell bezeichnet werden.²⁸⁰⁹ In den 1990er Jahren hat sich die Anwendung dieses Ansatzes als wegweisend für das Internet erwiesen.²⁸¹⁰ Der Bundesrat hat sich im DLT-Bericht von 2018 grundsätzlich für einen solchen Ansatz ausgesprochen.²⁸¹¹

Ein solches Regime würden nicht nur den beteiligten Parteien die Möglichkeit geben, mit neuen Ideen zu experimentieren,²⁸¹² sondern auch dem Regulator die erforderliche Zeit gewähren, um neue, allenfalls vielversprechende Geschäftsmodelle aus der Warte des Aufsichtsrechts zu «testen». Erst dadurch wird es für letzteren überhaupt möglich, die Kosten und den Nutzen bestehender Finanzmarktregulierung zu quantifizieren und qualifizieren.

iv. Offenlegungsregime auf der Grundlage von Verhaltenskodizes

Als weiterer Schritt sollte darauf hingewirkt werden, die Transparenz innerhalb des DeFi-Marktes zu erhöhen.²⁸¹³ Es handelt sich dabei um das Kernstück der vorliegenden marktbasierten Regulierungsvorschläge. Eine Verbesserung des Transparenzniveaus führt zum Abbau von Informationsasymmetrien zwischen den unterschiedlichen Marktteilnehmern, was sich insgesamt positiv auf den Abbau von den in dezentralen Systemen vorhandenen Informationsrisiken auswirken dürfte.²⁸¹⁴

Erste brancheneigene Ansätze existieren bereits: So publizierte etwa *DeFi Watch* regelmässig Informationen zur Sicherheit und Governance unterschiedlicher DeFi-Projekte.²⁸¹⁵ Allerdings handelt es sich dabei um ein Vorhaben, welches breitere Kreise der Community bislang nicht erfolgreich miteinbeziehen konnte.

²⁸⁰⁹ Siehe hierzu Giancarlo, Blockchain: A Regulatory Use Case, *passim*; ferner WEF, Rethinking Financial Innovation, 57.

²⁸¹⁰ Siehe die Ausführungen zur Regulierung des Internets in Giancarlo, Policy Challenges of a Decentralized Revolution, *passim*.

²⁸¹¹ Siehe zu den Grundsätzen des schweizerischen Regulierungsansatzes für Blockchain und DLT Bundesrat, DLT-Bericht 2018, 13–15.

²⁸¹² GLM. Finck, German Law Journal 2018, 688 («[...] the encouragement of experimentation and innovation is probably the most important step regulators can take.»).

²⁸¹³ So auch Crenshaw, The International Journal of Blockchain Law 2021, 8–9, welche allerdings aus Sicht der SEC spricht; ferner Auer et al., BIS Working Papers Nr. 1013, Mai 2022, 3–4; bereits OECD, Why Decentralised Finance Matters, 60.

²⁸¹⁴ Siehe betreffend den unterschiedlichen Ausprägungen von Informationsrisiken oben, [IV.5.2d](#).

²⁸¹⁵ Siehe DeFi Watch, About, *passim*.

Die für die Herausgabe von Registerwertrechten vorgesehenen gesetzlichen Publizitätsanforderungen können ebenfalls als eine solche Form der Regelsetzung betrachtet werden, die jedoch ausschliesslich an den Emittenten der Registerwertrechte anknüpft.²⁸¹⁶ Dezentrale Handelsplattformen sind demgegenüber in aller Regel nicht davon erfasst.²⁸¹⁷

PHILIPP PAECH hat im Zusammenhang mit der Regulierung von Blockchains das Abstellen auf anreizorientierte Mechanismen vorgeschlagen, welchen im internationalen Kontext wohl am ehesten gewisse Steuerungswirkung zukommen könne.²⁸¹⁸ Solche Mechanismen sollten nach vorliegender Ansicht zu einem marktorientierten Offenlegungsregime weiterentwickelt werden:

Regelungsgegenstand eines solchen Regimes sollten die spezifischen Nutzungsrisiken im Zusammenhang mit dezentralen Systemen sein.²⁸¹⁹ Die Grundlage würden Verhaltensregeln in Form eines *Verhaltenskodex* bilden. Solche Verhaltensregeln würden rechtlich unverbindliche, aber inhaltlich überzeugende Leitlinien für die Marktteilnehmer aufstellen,²⁸²⁰ wie sie bereits im Zusammenhang mit der Selbstregulierung von Internetplattformen, wie etwa Online-Suchmaschinen, oder börsenkotierten Gesellschaften bekannt sind.²⁸²¹ Das Ziel bestünde einerseits darin, auf Basis von sachlichen und neutralen Informationen Personen zu befähigen, informierte Entscheide hinsichtlich der Teilnahme an oder der Nutzung von dezentralen Systemen zu treffen. Die Basis solcher Entscheidungen setzen einen sinnvollen Grad an Standardisierung der Informationen voraus, was sodann auch die Vergleichbarkeit verschiedener Projekte ermöglicht. Andererseits würden die Informationen auch Aufsichtsbehörden eine qualifizierte Aufsichtstätigkeit ermöglichen.²⁸²²

²⁸¹⁶ Vgl. Art. 973d Abs. 2 Ziff. 3 und 4 OR.

²⁸¹⁷ Siehe hierzu oben, [V.3.6](#).

²⁸¹⁸ Vgl. Paech, *The Modern Law Review* 2017, 1103.

²⁸¹⁹ Ähnlich WEF, *Decentralized Finance*, 22.

²⁸²⁰ Ähnlich betreffend «voluntary compliance» EC, Roukny Report, 39–41; a.A. IOSCO, *Final Report DeFi 2023*, 37–38, die einen verpflichtenden Offenlegungsstandard fordert.

²⁸²¹ Vgl. Savary, *Regulierung dominanter Internetplattformen*, 102–103; Bühler, *Corporate Governance*, Rz. 89.

²⁸²² So etwa IMF, *Crypto Ecosystem*, 54, wonach die Überwindung von Datenlücken zentral für informierte Policy-Entscheidungen sei.

Der Verhaltenskodex sollte in umfassender Weise entscheidungsrelevante Informationen, soweit diese im Einzelfall einschlägig sind, abdecken.²⁸²³ Hierzu gehören mit Blick auf dezentrale Handelsplattformen namentlich folgende Angaben:

Angaben	Wesentliche Punkte
Überblick	
Allgemeines	Überblick über die dezentrale Handelsplattform: – Name; – historischer Abriss über das Projekt (Gründung, Entwicklungsphasen etc.); – derzeitiger Entwicklungsstand bzw. Fortschritt des Projekts (Release-Version, Bestehen eines Guarded Launch²⁸²⁴ usw.).
Funktionsweise	
Funktionsweise dezentrale Applikation	Ausführliche Darstellung der Funktionsweise der Handelsplattform mit Blick auf die nachfolgenden Funktionen: – Verwahrung bzw. Kontrolle über Vermögenswerte, insb. zur Frage, wie non-custodial die Plattform ist; – Orderbuch, AMM usw.; – Ausführung von Aufträgen inkl. Matching; – Abwicklung (Layer 1, Layer 2 etc.).
Funktionsweise dezentrales Netzwerk	Darstellung der Funktionsweise des zugrundeliegenden dezentralen Netzwerks anhand der Hauptmerkmale, insb. Angaben zu: – Netzwerk (Layer, Sidechain, separates Netzwerk usw.), welches die Basis für die dezentrale Handelsplattform bildet; – Konsensalgorithmus (PoW, PoS usw.).

²⁸²³ Einen vergleichbaren Informationskatalog allerdings in Bezug auf Nutzungs-Token, die i.d.R. im Rahmen eines ICOs herausgegeben werden, findet sich bei Liebau/Krapels, Cryptoeconomic Systems 2021, *passim*. Dieses Regime passt vorliegend nur bedingt, steht hinter einem ICO ja typischerweise eine zentrale Herausgeberin eines Tokens.

²⁸²⁴ Im Rahmen eines *Guarded Launch* wird mit konservativen Funktionseinstellungen gearbeitet. Das bedeutet für DeFi-Protokolle, dass Nutzer etwa nur kleine Beträge in Smart Contracts einsetzen können. Wenn sich das Protokoll als sicher erweist, können solche Betragsobergrenzen kontinuierlich angehoben werden; vgl. hierzu Deeter, DeRisking DeFi, Medium, *passim*.

Software	
Software / Smart Contracts	Ausführungen zum verwendeten Code, namentlich zu: – Nutzungsbedingungen im urheberrechtlichen Sinne inkl. Einschränkungen in der Nutzung;²⁸²⁵ – Adressen aller relevanten Smart Contracts der Plattform, jeweils unter Hinweis auf ihre konkreten Funktionen (Exchange Contract etc.).
Quellcode	– Ort der Veröffentlichung des Quellcodes, der mit dem zur Ausführung gelangenden Bytecode²⁸²⁶ übereinstimmt (GitHub, GitLab usw.); – Ort der Dokumentation des Quellcodes.
Code Audit	– Anzahl Audits; – Datum der Audits; – Name des Codeauditors; – Ort der Veröffentlichung der Code Audits.
Entwicklerteam	Übersicht über: – Entwicklerteam (Anzahl Entwickler, berufliche Erfahrung usw.); – involvierte Unternehmen (Firma, Geschäftssitz); – Webseite und Kommunikationskanäle; – Markenrechte.
Drittbeteiligung im Rahmen der Softwareentwicklung	Durchführung von Bug Bounties, Programmen für unabhängige Entwickler (Grants), Einbeziehung von Community-Feedback usw.
Historie der Hackerangriffe	Angaben zu: – vergangenen Hacks; – Sicherheitslücken, die rechtzeitig behoben werden konnten, ohne dass es zu einem Hackerangriff kam.

²⁸²⁵ Auf auffällige Besonderheiten in den Nutzungsbedingungen sollte im Sinne von Art. 8 UWG (AGB-Inhaltskontrolle) deutlich hingewiesen werden.

²⁸²⁶ Während Quellcode in einer Programmiersprache (in Ethereum insb. Solidity) verfasst wird und somit menschenlesbar ist, ist Bytecode der in der virtuellen Maschine einer Blockchain zur Ausführung gelangende Quellcode. Bytecode ist «Zwischencode» zwischen Quellcode und binärem Maschinencode (teils auch als Objektcode bezeichnet), der direkt auf Hardware abläuft; siehe zum Unterschied zwischen Quell- und Bytecode Antonopoulos/Wood, Mastering Ethereum, xxvi, 7.

Versicherung	– Bestehen einer Versicherung; – Umfang der Versicherungsdeckung bei Smart Contract-Risiken (inkl. Orakel-Risiken).
Governance	
Governance / DAO	Funktionsweise der Governance des Protokolls, insb. Angaben zu: – Existenz und Funktionsweise der DAO; – Ausgabe und Funktionsweise von Governance Token; – Quoren für Anträge und Abstimmungen in der DAO; – Verteilungsschlüssel betreffend Governance Token, Bezeichnung der Wallet-Adressen der grössten Tokenbesitzer (> 10%) und Existenz allfälliger Stimmabsprachen; – Token-Voting-Mechanismen, wie insb. Delegation von Token an Dritte unter Offenlegung der Delegationskriterien; – Verwaltung der sich im Treasury befindlichen Token; – Mechanismus betreffend Minting neuer Token.
Admin Keys	Ausführliche Angaben zu: – Existenz von Admin Keys; – Art und Umfang der damit verbundenen Eingriffsrechte (z.B. Möglichkeit allgemeiner <i>Upgradeability</i>²⁸²⁷ der Smart Contracts oder lediglich beschränkte Eingriffsmöglichkeiten); – Bestehen von Timelocks und deren Bedingungen zum Schutz der Nutzer; – Anzahl der unterschiedlichen Admin Key-Inhaber und Quorum, welches für die Ausübung der Eingriffsrechte vorausgesetzt wird (z.B. 5-of-7-Multisig); – Adresse des für die Multisig verwendeten Smart Contracts (z.B. Gnosis).
Orakel	Bezeichnung der verwendeten Orakel sowie Beschreibung derer Funktionsweise

²⁸²⁷ *Upgradeability* bedeutet üblicherweise, dass *alle* Funktionen des Smart Contracts nachträglich durch die Inhaber von Admin Keys abgeändert werden können. Vgl. ferner zu Admin Key-Risiken oben, [IV.5.2d.ii.](#)

Allgemeine Risiken	
Risiken im Allgemeinen	Ausführliche Darstellung der allgemeinen Risiken der Nutzung einer dezentralen Handelsplattform: – Smart Contract-Risiken, wie etwa Programmierfehler;²⁸²⁸ – wesentliche Plattformrisiken; – Slippage, Impermanent Loss etc.; – Darstellung der Funktionalitäten der Admin Keys anhand eines Worst-Case-Szenarios aus Sicht der Nutzer; – Governance-Risiken; – Orakel-Risiken; – Verlust des Private Keys.
Weitere Informationen	
Kontakt	Kontakt bzw. Anlaufstelle für weitergehende Informationen, wie etwa Webseite, E-Mail, Forum, Medium, Discord, Twitter, Telegram etc.
Notfall	Informationskanal bei Notfällen (z.B. Hackerangriff)

Die in der Tabelle aufgeführten Informationen sind in geeigneter Weise offenzulegen. In Frage kämen etwa die gemeinschaftliche Einrichtung und Verwaltung einer *Webseite* durch in der Community akzeptierte Vertreter der DeFi-Community.

In Anlegerschutzsicht sollte durch das Abfragen dieser Punkte erreicht werden, dass Nutzer einer dezentralen Handelsplattform um die potenziellen Risiken für ihre Vermögenswerte und übrigen Interessen wissen können, wenn sie die Plattform nutzen. Die Ausführungen sollten in leicht verständlicher Sprache beschreiben, wie der Code funktioniert und welche Funktionen er aufweist (vgl. Art. 61 Abs. 1 FIDLEG).²⁸²⁹ Dies ist bedeutsam, denn nur wenige Personen sind normalerweise imstande, den Softwarecode zu lesen und dessen Inhalt zu prüfen.²⁸³⁰ Dabei ist ein Schwerpunkt auf allfällige Verwahrungsrissen, die bei dezentralen Handelsplattformen *per definitionem* grundsätzlich ausgeschlossen sind, und auf Admin Key-Risiken zu legen. Ferner ist für Nutzer wesentlich, Bescheid darüber zu erhalten, wie Entscheidungen über

²⁸²⁸ Eine relativ verständliche Beschreibung der Risiken findet sich etwa bei Yearn Finance, Disclaimer, *passim*.

²⁸²⁹ Siehe Cohen/Angelovska-Wilson/Strong, Decentralized Finance, *passim*.

²⁸³⁰ So auch Crenshaw, The International Journal of Blockchain Law 2021, 9 («It is not reasonable to build a financial system that demands investors also be sophisticated interpreters of complex code.»).

die Weiterentwicklung eines Protokolls getroffen werden, insb. in welchem Rahmen sie selbst an der Willensbildung teilnehmen können und wie gross ihr prozentualer Anteil am Einfluss auf Entscheidungen ist (Governance-Risiken). Die Ausführungen sollten schliesslich bei wesentlichen Veränderungen im Code eines Protokolls zeitnah *aktualisiert* werden.

In der Praxis wären Softwareentwickler in aller Regel technisch und operationell am ehesten imstande, die Leitlinien umzusetzen. Dabei ist zu beachten, dass Entwickler kaum einen Anreiz zur Veröffentlichung von Informationen haben, wenn sie in der Folge höheren Haftungsrisiken ausgesetzt sind. Der freiwilligen Offenlegung von Informationen wäre in einem allfälligen Zivil-, Straf- oder Aufsichtsverfahren entsprechend Rechnung zu tragen.²⁸³¹ Andernfalls bildet sich ein schwer lösbares Spannungsverhältnis zwischen den Zielen eines Verhaltenskodex und den von ihm tatsächlich ausgelöstem Verhalten der Marktteilnehmer.²⁸³² Zusätzlich kann ein kryptografischer Fingerabdruck (Hash) der betreffenden Informationen hinzugefügt werden, sodass Nutzer überprüfen können, dass die an der entsprechenden Stelle gemachten Angaben die richtigen sind und nicht nachträglich verändert wurden.

PHILIPP HACKERS Vorschlag eines *Blockchain Governance Code*, welcher nach dem in der Corporate-Governance-Forschung entwickelten *Comply-or-Explain*-Ansatz funktioniert, geht in die hier vorgeschlagene Richtung. Allerdings scheint der Autor davon überzeugt zu sein, dass es langfristig zwingender staatlicher Vorgaben braucht.²⁸³³ In seinen Ausführungen wird allerdings nicht ersichtlich, welche Person innerhalb einer globalen, verteilten Gemeinschaft rechtlich zu verpflichten wäre, die gesetzlich erforderlichen Informationen zu veröffentlichen. Generell vernachlässigen seine Ausführungen die in der Praxis feststellbaren Möglichkeiten und Grenzen der Governance in dezentralen Systemen. CHRIS BRUMMER geht einen Schritt weiter, indem er einen Konsumentenschutzansatz mit neuartigen Offenlegungsmodellen kombiniert, wie etwa «Disclosure NFTs», welche den Endabnehmern relevante Informationen über ein Protokoll in verständlicher Form präsentieren.²⁸³⁴

²⁸³¹ Vgl. in diesem Zusammenhang die *Haftungserleichterung* in Art. 69 Abs. 3 FIDLEG, wonach für falsche oder irreführende Angaben über wesentliche Perspektiven nur gehaftet wird, wenn die Angaben wider besseres Wissen oder ohne Hinweis auf die Ungewissheit zukünftiger Entwicklungen gemacht oder verbreitet wurden; siehe hierzu etwa unter US-amerikanischem Prospektrecht de R. Barondes, *The Journal of Corporation Law* 1994, 277–278.

²⁸³² Ähnlich Shapiro, Paradox, Twitter, *passim*.

²⁸³³ Siehe Hacker, in: Hacker et al., *Corporate Governance*, 155–160, 160–161.

²⁸³⁴ Siehe Brummer, *Stanford Journal of Blockchain Law & Policy* 2022, 149–172.

Falls die Entwicklungsgemeinde oder andere beteiligte Personen darauf verzichten, Angaben zu ihrer Plattform oder über sich selbst zu veröffentlichen, liegt es primär an den Marktteilnehmern, sich selbst ein Urteil über die Plattform zu bilden. Unter dem vorgeschlagenen freiwilligen Offenlegungsregime ist es den Marktteilnehmern überlassen, ob sie Transparenz von den Protokollentwicklern «einfordern» oder ob sie unter Berücksichtigung der Risiken bereit sind, darauf zu verzichten. Und es ist den letzteren überlassen, ob sie den Informationsbedürfnissen des Marktes einen Stellenwert einräumen. Unter der Annahme, dass ökonomische Anreize auf beiden Seiten vorhanden sind, kann davon ausgegangen werden, dass die notwendigen Informationen produziert werden.²⁸³⁵ Erfahrungswerte in historischen und modernen Kapitalmärkten untermauern diese Ansicht.²⁸³⁶ Dasselbe gilt in empirischer Hinsicht für ICO-Märkte zwischen 2014 und 2018, wonach Projekte mit höherem Informationsniveau erfolgreicher in der Kapitalaufnahme als opakere Projekte waren.²⁸³⁷ Aufgrund der Möglichkeit, die veröffentlichten Informationen mit dem quelloffenen Computercode abzugleichen, verfügen Marktteilnehmer zudem über einen gewissen Kontrollmechanismus. Den Aussagen zu einer dezentralen Handelsplattform muss in diesem Sinne nicht einfach blind vertraut werden.²⁸³⁸ Dies ist ein wesentlicher Unterschied zu den Aussagen eines Bankmanagers zur Bonität seines Instituts.

Die Dezentralität solcher Systeme lässt keine Herangehensweise zu, welche die betroffenen Personen ausschließen würde.²⁸³⁹ Angesichts der Transnationalität des Themas wäre es aber empfehlenswert, dass staatliche und supranationale Akteure zusammen mit internationalen Branchenverbänden den Erlass von Verhaltenskodizes koordinieren.²⁸⁴⁰ Die Entwicklung eines Verhal-

²⁸³⁵ GL.M. Hacker, in: Hacker et al., *Corporate Governance*, 153–155, welcher in der Umsetzung des Blockchain Governance Codes einen Wettbewerbsvorteil des jeweiligen Protokolls sieht; ferner Liebau/Krapels, *Cryptoeconomic Systems* 2021, 5 m.w.N.

²⁸³⁶ Siehe etwa Stringham, *Private Governance*, 98–99; ferner Easterbrook/Fischel, *Corporate Law*, 4–7; ausführlich Romano, *Theoretical Inquiries in Law* 2001, 485–491; Bainbridge, *University of Cincinnati Law Review* 2000, 1033; kritischer hingegen Latimer/Maume, *Promoting Information*, 26–28, wonach schlechte Nachrichten tendenziell zu spät oder unzureichend veröffentlicht würden.

²⁸³⁷ Siehe Bourveau et al., *Journal of Accounting Research* 2021, 6, 25; vgl. ferner Chod/Lyandres, *Management Science* 2021, 5981.

²⁸³⁸ Optimistisch in dieser Hinsicht Peirce, *Lawless in Austin*, *passim*.

²⁸³⁹ Vgl. Black, *Current Legal Problems* 2001, 104 («self-regulation [...] as an inescapable fact of life»).

²⁸⁴⁰ Vgl. hinsichtlich ähnlicher Empfehlungen für die wettbewerbsrechtliche Erfassung digitaler Plattformen Bundesrat, *Rahmenbedingungen digitale Wirtschaft*, 171–172; ferner auch Gasser/Schulz, *Governance of Online Intermediaries*, 18.

tenskodex sollte durch einen Bottom-up- bzw. partizipatorischen Ansatz erfolgen, wie er insb. im Bereich der Internet-Governance²⁸⁴¹ vertreten wird. Dieser Ansatz wird in der einschlägigen Literatur auch als verteilte oder dezentrale Governance bezeichnet.²⁸⁴² In Anlehnung an das Werk von Ostrom²⁸⁴³ wird die Governance dezentraler Systeme vorliegend als Gemeingut betrachtet, welche die Kommodifizierung wirtschaftlich knapper Güter in Form von digitalen Daten erlaubt (*Digital Value Commons*). Die Güter werden von einer Vielzahl von Personen verwaltet und entsprechend sind deren Interessen im Rahmen einer allfälligen regulatorischen Standardisierung zu berücksichtigen. Ein Top-down-Ansatz würde demgegenüber der Komplexität der Regulierung dezentraler Systeme zu wenig Rechnung tragen.²⁸⁴⁴ Ziel muss es also sein, den unterschiedlichen Bedürfnissen der involvierten Stakeholder-Gruppen Rechnung zu tragen.²⁸⁴⁵ Eine bedeutende Gruppe bilden freilich gerade die Nutzergemeinschaft von DeFi-Anwendungen.²⁸⁴⁶

Dabei wäre es wohl kaum wünschenswert (und realistisch), über lediglich einen global gültigen Verhaltenskodex zu verfügen. Denn auch im regulatorischen Bereich kann Wettbewerb innovations- und vertrauensfördernd wir-

²⁸⁴¹ Siehe insb. Weber, *Shaping Internet Governance*, 88–103 m.w.H.; ferner Weber, SRIEL 2016, 204, der eine Verschiebung zu sog. *Mesh Regulation* feststellt («*The move towards mesh regulation is considered to be founded on two major transformations in the legal and political landscape, namely (i) the weakened position of the statutes as the primary instrument of legal control and (ii) the increased use of the notion of governance instead of government. The first transformation leads from a centralized sovereign authority to a flexible, decentralized, adaptive, and often negotiated regulation. The second transformation causes a process allowing to co-ordinate the efforts of actors and social groups in fragmented and uncertain environments.*»); sodann Kaufmann, SRIEL 2016, 218–220, welche auf das theoretische Fundament des Multistakeholder-Ansatzes u.a. im Werk von Elinor Ostrom (und ihres Ehemannes) zur polyzentrischen Governance hinweist; vgl. ferner in Bezug auf das internationale Standardsetting durch IOSCO im Bereich der Wertpapierregulierung Raymond/DeNardis, *International Theory* 2015, 599–600, deren Multistakeholder-Ansatz allerdings wenig inklusiv ist; hinsichtlich der Bedeutung technischer Standards siehe wiederum Weber, *Point of No Return*, 8–12.

²⁸⁴² Siehe Weber, ZSR 2016 I, 249 m.w.N.

²⁸⁴³ Siehe hierzu oben, [II.5.2b](#) und [IV.5.2g.i](#).

²⁸⁴⁴ Siehe Ostrom, *Governing the Commons*, 10, 22 («*Many policy prescriptions [...] advocate oversimplified, idealized institutions – paradoxically, almost ‘institution-free’ institutions*»); ferner Lai, in: Cappelletto/Carullo, *Law and Governance*, insb. 300.

²⁸⁴⁵ GLM. Takanashi et al., *Stanford Journal of Blockchain Law & Policy* 2020, 127, 134–137, 142, ähnlich, jedoch in Bezug auf technologiegestützte Regulierung Reyes, *Villanova Law Review* 2016, 227–231. Vgl. auch Weber, SJZ 2016, 301.

²⁸⁴⁶ Vgl. Brescia, *Nebraska Law Review* 2016, 134.

ken.²⁸⁴⁷ Dies scheint zudem auch notwendig, weil dezentrale Systeme keine monolithischen Protokolle darstellen, sondern wesentliche Unterschiede zwischen den einzelnen Systemen existieren, die entsprechend unterschiedliche Implikationen für den Anleger- und Funktionsschutz aufweisen.

Die Umsetzung von Informationsstandards hängt neben Marktkräften im Wesentlichen von der *Akzeptanz der Marktteilnehmer* ab. Die Standards haben aus sich heraus zu überzeugen. Dieses Phänomen ist allerdings kaum neu für den Finanzmarkt.²⁸⁴⁸ Umso bedeutender ist die Teilnahme aller Stakeholder an der Ausarbeitung von Verhaltenskodizes. Der IMF möchte demgegenüber auch hinsichtlich der Regulierung von Krypto-Ökosystemen auf den in der heutigen internationalen Finanzmarktordnung verbreiteten Top-down-Ansatz setzen.²⁸⁴⁹

Ein freiwilliges Offenlegungsregime auf Basis eines Verhaltenskodex beruht letztlich auf der Überzeugungskraft sozialer Normen.²⁸⁵⁰ Vorausgesetzt, dass sie genügend breit abgestützt sind, können soziale Normen einen wesentlichen Einfluss auf die Verhaltensweisen und Erwartungshaltungen der Nutzer und Teilnehmer dezentraler System ausüben. Die Schwierigkeiten liegen in der Globalität und Heterogenität der Netzwerke. Zudem können Aufsichtsbehörden soziale Normen in aller Regel nur indirekt beeinflussen.²⁸⁵¹ Dennoch ist es realistisch, dass die Umsetzung von Verhaltenskodizes in Form der Offenlegung standardisierter Informationen, anfänglich nur durch einige wenige Projekte, langfristig tiefgreifende Auswirkungen auf den Gesamtmarkt haben könnte. Verhaltenskodizes würden zu einem Gütesiegel für seriöse Projekte avancieren.

v. Investor Education

Ausgehend davon, dass dezentrale Systeme ein unaufhaltbares Phänomen in einer global vernetzten, digitalisierten Welt sind,²⁸⁵² sollten Gesetzgeber und Finanzmarktaufsichtsbehörde ihre Bemühungen im Bereich der *Investor Edu-*

²⁸⁴⁷ Siehe etwa Weber, SZW 2015, 580; Tietje/Lehmann, in: Cottier/Jackson/Lastra, International Law, 148, 150; ferner grundlegend Romano, Theoretical Inquiries in Law 2001, *passim*; teilweise relativierend für den EU-Binnenmarktkontext Kieninger, Wettbewerb der Privatrechtsordnungen, 24–44.

²⁸⁴⁸ Siehe etwa Weber, Journal of International Economic Law 2010, 698–699.

²⁸⁴⁹ Siehe IMF, Crypto Ecosystem, 54.

²⁸⁵⁰ Siehe hierzu oben, [II.5.3c](#).

²⁸⁵¹ Vgl. De Filippi/Wright, Blockchain and the Law, 187–189.

²⁸⁵² Vgl. bereits IOSCO, Role of Investor Education, 3, wo darauf hingewiesen wird, dass das Internet die Bedeutung von Investor Education erhöht hat.

cation verstärken. Es muss das Ziel sein, dass Nutzer dezentraler Systeme unter Berücksichtigung von Chancen und Risiken angemessene Entscheide treffen können.²⁸⁵³ So sieht das US-amerikanische WHITE HOUSE im vielbeachteten Factsheet zu Digital Assets von 2022 vor, dass der Individualschutz auch gerade über den öffentlichen Diskurs zu erfolgen hat.²⁸⁵⁴ Zu Recht hat ANDREAS HEINEMANN darauf hingewiesen, dass gut informierte und kritische Konsumenten den Wettbewerb komplementieren, indem sie dafür sorgen, dass dieser seine Funktionen erfüllt.²⁸⁵⁵

Ein Mittel, dieses Ziel zu erreichen, besteht darin, dass die Finanzmarktaufsicht in einem proaktiven Dialog mit der Öffentlichkeit steht. Darunter fällt ansatzweise die heutige Praxis, Warnungen betreffend spezifische Anbieter, welche nach Meinung der Finanzmarktaufsichtsbehörde «möglicherweise» ohne Bewilligung tätig sind, zu veröffentlichen.²⁸⁵⁶ Klar ist, dass es sich bei diesen Anbietern eher um Extremfälle handelt, und deren *Name and Shame* nicht generell zu einer aufgeklärten Öffentlichkeit führt. Ferner publiziert die FINMA unter der Rubrik «Public» ihrer Webseite Informationen für Privatanleger, etwa in Form von «Fragen & Antworten», Faktenblättern, Angaben, wie Anleger sich vor Betrugereien schützen können, und Finanzwissen, das allerdings von Drittanbietern zur Verfügung gestellt wird. Vorliegend von Interesse ist schliesslich die (inzwischen ein wenig in die Jahre gekommene) Broschüre der FINMA mit praktischen Tipps, wie sich Anleger vor illegal tätigen Anbietern schützen können.²⁸⁵⁷ Darin finden sich etwa Informationen zu virtuellen Währungen, ICOs, Crowdfunding und binärem Optionshandel.

Die IOSCO hat im Bereich der Investor Education eine wichtige Vorreiterrolle insb. mit Blick auf digitale und Vermögenswerte und ICOs eingenommen. Die Organisation empfiehlt vier Bereiche, welche von nationalen Aufsichtsbehörden verfolgt werden können: (1) Entwicklung von Bildungsinhalten über Krypto-Assets, (2) Information der Öffentlichkeit über nicht lizenzierte oder betrügerische Unternehmen, (3) Nutzung einer Vielzahl von Kommunikationskanälen zur Information der Anleger, und (4) Bildung von Partnerschaften zur Entwicklung und Verbreitung von Informationsmaterial.²⁸⁵⁸ Informationsmaterial und Warnhinweise für Anleger können dazu beitragen, dass Klein-

²⁸⁵³ So bereits Jacquemart, Offene Blockchainsysteme, Rz. 600.

²⁸⁵⁴ Siehe White House, Fact Sheet Digital Assets, *passim*.

²⁸⁵⁵ Siehe Heinemann, in: Heiss/Loacker, Konsumentenschutz, N 9.95. Zu den Funktionen des Wettbewerbs, siehe oben, [VI.4.2b](#).

²⁸⁵⁶ Siehe betreffend diese Warnliste FINMA, Warnung, *passim*.

²⁸⁵⁷ Siehe FINMA, Wie sich schützen können, *passim*.

²⁸⁵⁸ Ausführlich hierzu IOSCO, Investor Education on Crypto-Assets, 12–22.

anleger das Wesen von Kryptovermögenswerte und die damit verbundenen Risiken verstehen. Die Aufklärung kann Kleinanlegern auch helfen, nicht zugelassene oder betrügerische Unternehmen zu erkennen. Aufklärungsmaterial und Warnhinweise zu Produkten und Aktivitäten können die regulatorischen Anforderungen ergänzen, die für Kryptovermögenswerte gelten, die von Finanzintermediären Kleinanlegern vermarktet, angeboten oder verkauft werden.²⁸⁵⁹ Auf den experimentellen Charakter vieler Protokolle sollte sodann explizit hingewiesen werden.

Soweit die Öffentlichkeit von einer staatlichen Behörde informiert wird, besteht die Schwierigkeit des vorgeschlagenen Ansatzes darin, ausgewogen und wettbewerbsneutral zu informieren. Zudem wäre es illusorisch, dass eine derartige Information angesichts des globalen und rasch voranschreitenden Innovationsumfelds jemals vollständig ausfallen könnte.²⁸⁶⁰ Im Ergebnis ist darum ein Ansatz vorzuziehen, der auf die allgemeine Aus- und Weiterbildung von Marktteilnehmern betreffend Chancen und Risiken der Finanzanlage im Allgemeinen und innovativer Produkte und Dienstleistungen im Besonderen abzielt.²⁸⁶¹ Eine zweckmässige Aufsichtspraxis betreffend dezentrale Systeme könnte darum aus Investor Education bestehen.²⁸⁶²

Investor Education ist als Kompetenzförderung im Umgang mit dezentralen Systemen im Allgemeinen und dezentralen Handelsplattformen im Besonderen zu verstehen. Kompetenzförderung schafft einen Ausgleich zwischen den Risiken einer uneingeschränkten und, wie erwähnt, kaum regulierbaren Nutzung von Angeboten über das Internet und der eigenverantwortlichen Gestaltungsfreiheit der persönlichen Lebensumstände.²⁸⁶³ Dass es sich dabei um einen pädagogischen Balanceakt handeln dürfte, wird etwa am Beispiel kryptografischer Zugangsverfahren ersichtlich: Diese dienen als ein Instrument zur eigenständigen Kontrolle digitaler Daten, wie etwa Kryptovermögenswerte oder von digitalen Identitäten. Allerdings ist ein Verlust oder Diebstahl der Zugangsmittel ohne entsprechende Sicherungsvorkehrungen mit dem unwi-

²⁸⁵⁹ So ausdrücklich IOSCO, *Investor Education on Crypto-Assets*, 4.

²⁸⁶⁰ Ebenfalls kritisch IOSCO, *Role of Investor Education*, 8.

²⁸⁶¹ Zu diesem Zweck könnten bestehende Investor Education Frameworks weiterentwickelt werden; vgl. bspw. IOSCO/OECD, *Financial Literacy for Investors*, *passim*.

²⁸⁶² Vgl. in diesem Zusammenhang Kaissar, *Investors Need More Than Regulators*, Bloomberg, *passim*; genereller diese Ansicht vertretend Sethe, SZW 2018, 614–615.

²⁸⁶³ Vgl. zum eigenverantwortlichen Umgang mit neuen Medien Müller, in: Gschwend et al., *Eigenverantwortung*, 567–569.

derrufflichen Verlust der Verfügungsmacht über die Daten verbunden.²⁸⁶⁴ Angesichts unzähliger Entwicklungen in diesem Bereich kann allerdings davon ausgegangen werden, dass die Mittel zur selbständigen Kontrolle von Private Keys künftig einfacher und sicherer werden.²⁸⁶⁵ Eine ähnliche Herausforderung stellt sich für Privatanleger im Bereich des Schutzes ihrer Privatsphäre. Die weitgehende transaktionale Transparenz von verteilten Registern kann bei unsachgemässer Nutzung dezentraler Systeme sensible Informationen über den Nutzer offenbaren. Im Rahmen der Investor Education sind die Nutzer auf die fragilen Eigenschaften der Privatsphäre in dezentralen Systemen ausdrücklich hinzuweisen. In diesem Sinne ist Teil der Investor Education auch die Förderung der Digital Literacy.²⁸⁶⁶

vi. Öffnung dezentraler Systeme für traditionelle Finanzintermediäre

Schliesslich wäre wünschenswert, dass die FINMA durch eine entsprechende liberale Aufsichtspraxis den beaufsichtigten Finanzintermediären freistellt, in den DeFi-Markt einzusteigen.²⁸⁶⁷ Ziel der Finanzmarktaufsicht muss es sein, sozusagen in indirekt marktstruktureller Weise die Bifurkation des Finanzsystems in zwei miteinander unvereinbare Teilsysteme zu vermeiden. Ein wichtiger Schritt in diese Richtung ist die eingangs erwähnte Anerkennung dezentraler Systeme als Teil der Finanzwirtschaft.²⁸⁶⁸ Traditionelle Finanzintermediäre könnten in der Folge etwa auf eigene Rechnung oder auf Rechnung ihrer Kunden als Liquiditätsbereitsteller über eine dezentrale Handelsplattform auftreten. Bereits heute bieten Schweizer Finanzintermediäre ihren Kunden bspw. Staking-Dienstleistungen für Proof-of-Stake-Konsensprotokolle an.²⁸⁶⁹ Denkbar ist auch, dass Finanzintermediäre in einem ersten Schritt lediglich über *Permissioned* Protokolle,

²⁸⁶⁴ Ebenfalls auf diesen Aspekt hinweisend Jacquemart/Meyer, in: Krauskopf/Babey, Globalisierte Digitalisierung, 12–13; sodann Hess/Lienhard, in: Emmenegger, Unautorisierte Zahlungen, 173; ferner Narayanan/Clark, *acmqueue* 2017, 22, die von einem «endpoint-security risk» sprechen, das in Blockchains deutlich ausgeprägter als im traditionellen Finanzsystem sei; ebenso Gervais, *digma* 2017, 130, der vom schwächsten Glied in der Kette spricht.

²⁸⁶⁵ Siehe etwa Buterin, *Social recovery wallets*, *passim*.

²⁸⁶⁶ Vgl. Weber, *Jusletter IT* vom 30. September 2021, Rz. 41.

²⁸⁶⁷ Ähnlich Lipton/Cohen, *International Financial Law Review* 2021, *passim*, die jedoch zu weit gehen, indem sie von den Aufsichtsbehörden die aktive Förderung der Nutzung durch traditionelle Akteure fordern; dies ebenfalls fordernd Casey, *IMF Finance & Development* September 2022, 24, 26.

²⁸⁶⁸ Siehe oben, [VI.4.3c.ii](#).

²⁸⁶⁹ Vgl. für eine Übersicht der grössten Staker in Ethereum 2.0, wozu u.a. die *Bitcoin Suisse* AG gehört, Nansen, *Eth2 Deposit Contract*, *passim*.

welche etwa als Teil des Code des Smart Contracts bzw. eines Tokenstandards umgesetzt werden, an dezentralen Systemen teilhaben.²⁸⁷⁰ Ein Modell, in welchem bestehende Finanzinstitute in dezentralen Umgebungen in gesetzestkonformer Weise ihre Aktivitäten anbieten können, kann als «hybrid finance (services)» bezeichnet werden.²⁸⁷¹

Die Erwartungen der FINMA an regulierte Institute sind allerdings sehr hoch, wahrscheinlich zu hoch, um in der Praxis einen sinnvollen Umgang mit offenen Protokollen zu erlauben.²⁸⁷² Namentlich hat eine Bank u.a. den prudenziellen Status des DeFi-Projekts und der involvierten natürlichen und juristischen Personen vertieft abzuklären. Hieran wird es in den meisten Fällen mangels internationaler und nationaler Standards, aber auch aufgrund des Umstands, dass DeFi-Anwendungen gerade in verteilter Weise erbracht werden, scheitern.

Durch einen solchen Ansatz erhält die Aufsichtsbehörde über das traditionelle Finanzintermediationssystem mittelbar und einigermaßen ressourcenschonend Zugang zu Informationen, welche sie sodann für ihre Aufsichtstätigkeit verwerten kann. Zudem könnte dieser Ansatz sicherstellen, dass über die Zeit allenfalls ein bedeutender Teil aller DeFi-Aktivitäten unter dem bestehenden Regelwerk ausgeübt würde. Dies würde dazu führen, dass *Gatekeeping*-Funktionen bestehender Intermediäre, soweit diese noch sinnvoll sind, in DeFi zum Einsatz kommen können.²⁸⁷³ Marktteilnehmer, welche sich dagegen ausserhalb der Pistenmarkierung bewegen wollen, könnten dies weiterhin tun.²⁸⁷⁴

Demgegenüber verfolgt der Basler Ausschuss mit den Empfehlungen im Bereich der Eigenmittelanforderungen für Banken und kontoführende Wertpapierhäuser eine Strategie der «Isolierung» der Risiken im Zusammenhang mit Kryptowährungen und DeFi.²⁸⁷⁵ Der Auslöser für die verschärfte Sichtweise auf

²⁸⁷⁰ Siehe hierzu übersichtshalber Warren Compliant peer-to-peer trading, *passim*.

²⁸⁷¹ Siehe Hess, Penn State Law Review 2024, 4–5, 50.

²⁸⁷² Siehe FINMA, Jahresbericht 2022, 21–22.

²⁸⁷³ Vgl. Crenshaw, The International Journal of Blockchain Law 2021, 9; ähnlich Nabilou, International Journal of Law and Information Technology 2019, 279, 281–283 («surrogate regulators»); ferner auch Jutzi/Abbühl, Rz. 1355.

²⁸⁷⁴ Dies noch *anerkennt* in seiner berühmt gewordenen Skipisten-Metapher Zuberbühler, in: Héritier Lachat/Hirsch, Finanzmarktregulierung, 294, der in diesem Zusammenhang vom «Mut zur Lücke» in der Finanzmarktaufsicht spricht.

²⁸⁷⁵ Siehe BIS/BCBS, Prudential treatment of cryptoasset exposures, 4 («[The Group 2 exposure thresholds] aim to safeguard the banking sector against the potentially significant risks posed by Group 2 cryptoassets.»); in *konzeptioneller* Hinsicht Aquilina/Frost/Schrimpf, BIS Bulletin Nr. 66, 12. Januar 2023, 4, wo die regulatorischen Optionen als «ban», «contain» und «regulate» bezeichnet werden; ferner Nabilou, International Journal

die Kryptoindustrie ist u.a. im Kollaps des (experimentellen) TerraLuna-Ökosystems und dem Konkurs der Kryptohandelsplattform FTX im Jahr 2022 zu sehen.²⁸⁷⁶ Infolge dieser beiden Ereignisse erlebten die Kryptomärkte mehrere grössere Insolvenzen, wie etwa von Three Arrows Capital, Voyager Digital, Celsius, BlockFi und Genesis, in deren Rahmen die gegenseitigen Verstrickungen und Schulden der Unternehmen an das Tageslicht gebracht wurden.²⁸⁷⁷ Es ist wichtig anzumerken, dass diese Ausfälle in erster Linie traditionelle Intermediäre betrafen und nicht etwa DeFi-Protokolle.²⁸⁷⁸

An den Anforderungen des Basler Ausschusses besteht inzwischen auch begründete Kritik.²⁸⁷⁹ Selbst bei Verfolgung eines ausschliesslich die Risiken reduzierenden Ansatzes im Bankenbereich sind die vorgeschlagenen Risikogewichte und Grenzwerte zu strikt, ja prohibitiv; zudem wird die Nutzung von öffentlichen Blockchains in einer Weise diskriminiert, die kaum mehr mit prudenziellen Argumenten gerechtfertigt werden kann.

Es ist schliesslich auch damit zu rechnen, dass sich noch stärker als heute spezialisierte Marktteilnehmer herausbilden, welche ähnlich wie Kreditratings für Schuldverschreibungen Analysen und Bewertungen von DeFi-Protokollen veröffentlichen.²⁸⁸⁰

4.4 Fazit

Dank des ausgeprägten Wettbewerbs im DeFi-Bereich hat sich eine Vielzahl dezentraler Handelsplattformen herausgebildet, welche ganz unterschiedliche Bedürfnisse der Nutzergemeinschaft befriedigen. Die Handlungsoptionen der Nutzer sind entsprechend gross. Allerdings mangelt es oft an objektiven Informationen über die einzelnen Projekte. Mithilfe eines partizipativen Ansatzes der involvierten Stakeholder in DeFi könnte auf relativ effiziente Weise höhere Transparenz hinsichtlich der vorhandenen Angebote erreicht werden. Dies

of Law and Information Technology 2019, 285–287, der insb. die Liquiditäts- und Kapitalrisiken von Kryptowährungen für regulierte Marktteilnehmer beschreibt.

²⁸⁷⁶ Vgl. betreffend Kollaps des TerraUSD Stablecoins BIS, Crypto Ecosystem, 8.

²⁸⁷⁷ Vgl. für eine Übersicht Reuters, *Crypto's string of bankruptcies*, 20. Januar 2023, <https://www.reuters.com/business/finance/cryptos-string-bankruptcies-2023-01-20/>.

²⁸⁷⁸ Vgl. Honegger/Mordrelle, Lehman-Moment, NZZ, *passim*.

²⁸⁷⁹ Ausführlich Kuhn/Weber, Jusletter IT vom 15. Februar 2024, Rz. 59–82.

²⁸⁸⁰ Siehe Cohen/Angelovska-Wilson/Strong, *Decentralized Finance*, *passim*; ferner Cohnen et al., *Columbia Law Review* 2019, 659–660; zu den positiven Effekten dieser Informationsintermediäre im ICO-Markt Bourveau et al., *Journal of Accounting Research* 2021, 32.

würde die Entscheidungssituation der Nutzer massgeblich verbessern, was sich wiederum positiv auf die Qualität und Quantität des Wettbewerbs auswirken dürfte.²⁸⁸¹

Zwar mag die Situation im Einzelfall finanzmarktrechtlich alles andere als perfekt erscheinen, doch angesichts der Schwierigkeiten bei der Anwendbarkeit und Durchsetzbarkeit nationalstaatlicher und internationaler Regeln im Bereich dezentraler Handelsplattform dürfte sie besser sein als gemeinhin angenommen wird. Die in der Theorie scheinbar *perfekte* Lösung, deren Existenz nach vorliegender Auffassung auch gerne einmal hinterfragt werden kann, darf – frei nach Voltaires Diktum –²⁸⁸² nicht zum Feind eines *guten* praktikablen Regulierungs- und Aufsichtsansatzes werden.

Gesetzgeber und FINMA tun in einer globalen, offenen Finanzmarktordnung gut daran, Wettbewerb und Innovation vermehrt als Mittel des Anleger- und Funktionsschutzes zu betrachten. Der Regulator und traditionelle Finanzintermediäre können dabei eine wichtige Signalfunktion für Marktteilnehmer im Allgemeinen und ihre Kunden im Besonderen übernehmen.

²⁸⁸¹ Vgl. Sethe, in: Heiss/Loacker, Konsumentenschutz, N 8.11, wo der Autor die Konsumenten bzw. der Konsumentenschutz als *Garanten* eines funktionstüchtigen Wettbewerbs bezeichnet.

²⁸⁸² Vgl. Voltaire, La Bégueule, *passim*.

5. Zusammenfassung Kapitel VI

Im ersten Abschnitt dieses Kapitels beschäftigt sich die vorliegende Arbeit mit den Herausforderungen dezentraler Systeme für Aufsicht und Regulierung. Der Regulierbarkeit solcher Systeme ist in mehrfacher Hinsicht eingeschränkt. Im Extremfall setzt eine dezentrale Handelsplattform bloss entsprechenden Computercode voraus, der von jedermann mit Internetzugang und einem internetfähigen Gerät verwendet werden kann. Die Arbeit kommt darum zum Schluss, dass eine teilweise Abkehr vom Finanzintermediationsmodell unumgänglich für das Finanzmarktrecht ist.

Der zweite Abschnitt untersucht im Sinne eines Exkurs die Gründe, weshalb dezentrale Systeme nicht einfach zu verbieten sind. Bei diesen handelt es sich letztlich um Technologien, die für eine Vielzahl von Anwendungen eingesetzt werden können, wovon dezentrale Handelsplattformen nur eine bilden. Grundrechtliche Überlegungen, insb. in den Bereichen der Meinungsäusserungs- und Informationsfreiheit sowie der Wirtschaftsfreiheit, schliessen nach vorliegender Ansicht ein Verbot *a priori* aus.

Im dritten Abschnitt werden die Konzepte des Anleger- und Funktionsschutzes kurz erläutert. Dabei zeichnet sich eine Angleichung zwischen Kollektiv-anlegerschutz und Vertrauensschutz ab. Damit scheinen letztlich alle Schutzziele des Aufsichtsrechts auf das Anlegerkollektiv ausgerichtet zu sein.²⁸⁸³ In einem zweiten Schritt werden sodann die Implikationen dezentraler Handelsplattformen für den Anleger- und Funktionsschutz bewertet: Es zeigt sich, dass einige der Beweggründe für Anlegerschutzbestimmungen nicht mehr gegeben sind. Der Funktionsschutz wird demgegenüber am effizientesten über das traditionelle Finanzintermediationssystem adressiert. Namentlich kann auf die «Fiat-Schnittstelle» zwischen Finanzintermediären und DeFi abgestellt werden. *De lege lata* ist sodann offen, inwiefern dezentrale Systeme den Regeln zur Verhinderung von Geldwäscherei und Terrorismusfinanzierung zu unterstellen sind. Allerdings sollte nach vorliegender Auffassung unbedingt den Schwachstellen des heutigen Geldwäschereiregimes Rechnung getragen werden. Schliesslich können ausnahmsweise auch zivilrechtliche Haftungsnormen als Grundlage des privatrechtlichen Regulierungsrechts zur Anwendung gelangen.

²⁸⁸³ Vgl. bereits Werlen, Konzeptionelle Grundlagen, 50–51.

Der *vierte* und letzte Abschnitt des Kapitels widmet sich möglichen Regulierungsalternativen. Bei dezentralen Systemen handelt es sich um eine genuin neuartige Markterscheinung, welche darum rechtlich eigenständig zu erfassen ist. Vorab geht die Arbeit allerdings auf die Faktoren des Wettbewerbs und der Innovation als potenzielle Mittel des Anleger- und Funktionsschutzes ein. Dabei zeigt sich, dass das heutige Aufsichtsrecht dem Wettbewerb nur am Rande eine eigenständige regulatorische Rolle einräumt. Sodann formuliert die Arbeit mögliche Regulierungsansätze: Den im ersten Abschnitt wiedergegebenen Herausforderungen kann nach vorliegender Ansicht am besten mit marktorientierten Regulierungsansätzen gerecht werden. Im Vordergrund stehen Regeln, welche die Anreizstruktur und das Transparenzniveau im DeFi-Markt verbessern. Zudem können marktorientierte Regeln innovationsoffen und wettbewerbsfördernd ausgestaltet werden. Entsprechend wird insb. der Erlass eines Offenlegungsregimes auf Basis freiwilliger Verhaltenskodizes vorgeschlagen. Zu diesem Zweck erarbeitet die Arbeit einen Informationskatalog, welche die im Umfeld einer dezentralen Handelsplattform involvierten Personen befolgen können. Weitere marktorientierte Regulierungsansätze sind die rechtliche Anerkennung dezentraler Systeme als wichtige Koordinationsmechanismen in der Finanzwirtschaft, das Setzen von Anreizen zur frühzeitigen Kooperation mit der Finanzmarktaufsicht, Investor Education sowie die Öffnung dezentraler Systeme für traditionelle Anbieter.

VII. Dezentralität als neues Rechtsprinzip

*Most people have a tendency to see centralized systems in everything.
When they see a flock of birds, they think that the front bird is the boss
and that the other birds are following it,
when actually it's a decentralized system,
where simple rules produce complex behaviors,
just like fish in a school or cars on a highway.*

– Daniel Cohen²⁸⁸⁴

1. Dezentralität als soziotechnisches Phänomen

1.1 Einleitung

In Kapitel III wurden als technische Eigenschaften dezentraler Systeme die verteilte, gemeinschaftliche Verwaltung, die Verwendung offener, interoperabler Protokolle und der Einsatz kryptografisch abgesicherter Vermögenswerte bestimmt.²⁸⁸⁵ In der Verbindung von Technologie mit menschlicher Interaktion liegt die soziotechnische Komponente dezentraler Systeme.²⁸⁸⁶ In der Folge wurde am Ende von Kapitel IV auch ein Definitionsversuch hinsichtlich dezentraler Handelsplattformen unternommen.²⁸⁸⁷

Dezentralität als *Rechtsprinzip* muss an diese technischen Vorarbeiten anschliessen, hat jedoch, um rechtlich operabel zu sein, weitere Konkretisierungen vorzunehmen. Dabei wird zwar konzeptionell zwischen Netzwerken und Applikationen unterschieden, doch soll dem Rechtsprinzip der Dezentralität hinsichtlich beider Systeme normative Bedeutung zukommen.²⁸⁸⁸

²⁸⁸⁴ Cohen, Modern Times, 1.

²⁸⁸⁵ Siehe oben, [III.2](#).

²⁸⁸⁶ Siehe hierzu oben, [II.5.3](#).

²⁸⁸⁷ Siehe oben, [IV.6](#).

²⁸⁸⁸ Diese Frage bloss aufwerfend Cambridge Centre for Alternative Finance, Regulatory Landscape Study, 51.

Schwergewichtig geht es um die Frage, *ab welchem Grad oder aufgrund welcher Umstände* Netzwerke und Applikationen, und hier besonders dezentrale Handelsplattformen, als genügend dezentralisiert gelten. Oder als Frage mit Bezug zum heutigen Finanzintermediationssystem formuliert: Kann und soll Dezentralität – in Form eines Rechtsprinzips – eigenständige Bedeutung erlangen und für diesen Bereich punktuell oder generell das regulatorische Finanzintermediationsmodell ersetzen? Das nachfolgende Kapitel widmet sich dieser Frage.

1.2 Mittel zum Zweck

Über die Chancen und Risiken dezentraler Systeme ist viel geschrieben und diskutiert worden. Die vorliegende Arbeit hat sie am Beispiel dezentraler Handelsplattform vertieft.²⁸⁸⁹ Dabei gehen die Meinungen in der Literatur weit auseinander: von praktischer Irrelevanz oder sogar Schädlichkeit der Dezentralität für Anwendungen bis zur Dezentralität als Selbstzweck. Dabei scheinen die beiden Extreme gemeinsam zu haben, dass sie im Wesentlichen ideologisch motiviert sind.

Nach vorliegender Ansicht ist Dezentralität lediglich, aber immerhin ein *Mittel zum Zweck*.²⁸⁹⁰ Der Zweck besteht nach vorliegender Ansicht in der Offenheit der Systeme. Damit verbunden ist ein Nutzen, der gegenüber dem heutigen Finanzintermediationsmodell heraussticht (siehe sogleich unten).

Klar ist demgegenüber aber auch, dass Blockchain-basierte Systeme ohne Dezentralität angesichts der Skalierungsnachteile der Technologie praktisch obsolet wären. Insoweit ist Dezentralität tatsächlich die *raison d'être* von Blockchains bzw. DLT. Private und permissioned Blockchains fristen entsprechend bis heute, wenn überhaupt, ein Nischendasein. Selbst als Infrastruktur für CB-DCs scheint wenig überraschend kein Bedarf für geschlossene Blockchainsysteme zu existieren. Ein rechtlicher Eingriff in die Dezentralität offener Netzwerke und Applikationen wäre darum mit der faktischen Abschaffung der Technologie vergleichbar.

²⁸⁸⁹ Siehe hierzu oben, [IV.5](#).

²⁸⁹⁰ So auch Qureshi, Decentralization not as important, *passim* («It's the properties decentralization gives us that we care about, not decentralization itself.»); ferner Blair, Enemy of Decentralization, *passim*.

Entsprechend kritisch sollte die Einführung von Permissioned Tokens und Pools in DeFi-Anwendungen betrachtet werden.²⁸⁹¹ Das Risiko besteht namentlich darin, dass dadurch der konkrete Nutzen von Dezentralität wieder verloren geht.

1.3 Nutzen von Dezentralität

Dezentralität ist nach vorliegender Ansicht *nützlich*, weil sie nutzungs-, teilnahme- und entwicklungsoffene Systeme möglich macht.²⁸⁹²

Der Hauptnutzen von Dezentralität besteht darin, inklusive bzw. integrative und neutrale Systeme zu schaffen, die analog zum Internet möglichst vielen Menschen offenstehen und ihnen die Teilnahme u.a. an einem globalen Finanzwesen ermöglichen (permissionless). Dabei ist es technisch gerade ausgeschlossen, aufgrund der Herkunft, der Rasse, des Geschlechts, des Alters, der Sprache, der sozialen Stellung, der Lebensform, der religiösen, weltanschaulichen oder politischen Überzeugung oder wegen einer körperlichen Behinderung oder aus anderen unsachlichen Gründen zu differenzieren (vgl. Art. 8 Abs. 2 BV).²⁸⁹³ Zugleich spielen im Grundsatz auch keine betrieblichen Risikoüberlegungen in die Offenheit des Systems hinein. Im traditionellen Finanzintermediationssystem ist *De-Risking* hingegen ein wichtiger Faktor in der Marginalisierung von Kunden.²⁸⁹⁴ Schätzungen gehen davon aus, dass rund die Hälfte aller Menschen keinen oder lediglich einen sehr eingeschränkten Zugang zu Finanzprodukten und -dienstleistungen haben. Das heutige Finanzsystem bezieht insb. Menschen aus Entwicklungs- und Schwellenländern nicht oder nur sehr schlecht in die globale Wirtschaft mit ein.²⁸⁹⁵

²⁸⁹¹ Siehe etwa zu solchen Einschränkungen aus geldwäschereirechtlichen Gründen oben, [V.2.12g](#).

²⁸⁹² Ähnlich auch Schär, IMF Finance & Development, 34–35, der zudem die erhöhte Transparenz und die Verhinderung von Vertrauensmissbrauch durch zentralisierte Anbieter erwähnt.

²⁸⁹³ So offenbar auch Harvey/Ramachandran/Santoro, DeFi, 150.

²⁸⁹⁴ Siehe hierzu FATF, Unintended Consequences, 2, wonach *De-Risking*-Verhalten von Finanzintermediären u.a. auf deren hohen Compliance-Kosten zurückzuführen ist; vgl. ferner hinsichtlich der negativen Auswirkungen des *De-Risking* auf internationale Korrespondenzbankenbeziehungen Bundesrat, Einfluss der Finanzmarktregulierung auf Afrika, 12–13.

²⁸⁹⁵ Vgl. für die Zahlen World Bank, Global Financial Development Report 2019/2020, 112; ferner Harvey/Ramachandran/Santoro, DeFi, 3–4.

Demgegenüber sind die Nutzung einer dezentralen Applikation oder die Teilnahme an einem dezentralen Netzwerk nicht von der Vorlage eines Identitätsnachweises, der Prüfung gewisser betrieblicher oder rechtlicher Kriterien oder der Erlaubnis einer Drittperson abhängig.²⁸⁹⁶ Für dezentrale Handelsplattformen bedeutet dies in starkem Kontrast zu traditionellen Handelssystemen, dass jedermann diese nutzen und darüber hinaus grundsätzlich auch als Market Maker bzw. Liquiditätsbereitsteller agieren kann. Von der gewöhnlichen, in aller Regel nichtgewerbsmässigen Nutzung dezentraler Applikationen ist die gewerbsmässige Nutzung abzugrenzen, welche unter Umständen finanzmarktrechtlich erfasst sein kann.²⁸⁹⁷

Dezentralität ist deshalb als Mittel zu betrachten, um die bestehenden Walled Gardens der Finanzwelt und darüber hinaus aufzubrechen. Dezentralität kann, indem die Manipulationsresistenz von Daten erhöht wird, die Zensurmöglichkeiten autoritärer Staaten und der dabei als Erfüllungsgehilfen agierenden Technologieunternehmen verringern. Dezentralität kann schliesslich als Koordinationsmechanismus gegen Machtungleichgewichte, intransparente Prozesse und Strukturen sowie Korruption bzw. Rent Seeking in Gesellschaft und Politik betrachtet werden.²⁸⁹⁸

Darüber hinaus ermöglicht Dezentralität die Teilnahme an der technischen Entwicklung von Protokollen und Anwendungen durch eine Vielzahl von Personen. Ausserhalb von zentralen Entschädigungsmodellen kann die Entwicklungsarbeit durch kryptoökonomische Anreize gefördert werden. Damit verbunden ist eine Innovationsoffenheit, welche mit entsprechenden positiven sozioökonomischen Effekten für die globale Gemeinschaft verbunden sein kann.²⁸⁹⁹

Schliesslich ist Dezentralität eng verbunden mit Datenintegrität und -souveränität. Die verteilten Register dezentraler Netzwerke stellen Datenbanken dar, über welche keine spezifische Person privilegierte Rechte besitzt. Dem-

²⁸⁹⁶ Siehe etwa Harvey/Ramachandran/Santoro, DeFi, 60–61; Ammori, Decentralized Finance, *passim*.

²⁸⁹⁷ Siehe ausführlich hierzu oben, [V](#).

²⁸⁹⁸ Siehe etwa Buterin, Meaning of Decentralization, Medium, *passim*, der auch die einschlägigen Vorbehalte erwähnt; kritisch Anker-Sørensen/Zetzsche, Fake-DeFi, 14–16, wonach Rent Seeking gerade eine Antwort auf die Tragik der Allmende von echtem DeFi ist (vgl. hierzu oben, [IV.5.2g](#)).

²⁸⁹⁹ Siehe etwa Dixon, Why Decentralization Matters, *passim*.

gegenüber sind Nutzer an den sie betreffenden oder ihnen zugedachten Daten technisch unmittelbar selbst berechtigt.²⁹⁰⁰

Dezentralität bietet nach dem Gesagten Vorteile, die sich potenziell weit über das heutige Finanzsystem erstrecken können. Eine innovationsoffene Rechtsordnung sollte sich nach vorliegender Auffassung die Vorteile zunutze machen, indem sie Dezentralität als Rechtsprinzip anerkennt.

²⁹⁰⁰ Siehe Srinivasan, You May Need a Blockchain, Coindesk, *passim*, wobei der Autor die Nutzung von öffentlich zugänglichen Datenbanken basierend auf dem Modell dezentraler Systeme für das gesamte Internet weiterdenkt.

2. Anerkennung von Dezentralität als Ordnungsprinzip

2.1 Vorbemerkung

Vorab ist festzustellen, ob und inwieweit die bisherige Praxis und Literatur Dezentralität als eigenständiges Phänomen überhaupt anerkennen. Falls dies der Fall ist, kann Dezentralität allenfalls als Ordnungsprinzip aufgefasst und in einem zweiten Schritt sodann zu einem Rechtsprinzip weiterentwickelt werden.

2.2 Parallele zum Wettbewerb als Ordnungsprinzip

Die Marktwirtschaft kann als ein dezentraler Wissens- und Preismechanismus verstanden werden, der durch den Wettbewerb *koordiniert* wird.²⁹⁰¹ Der Wettbewerb gilt nach Auffassung von Vertretern der Freiburger Schule der Nationalökonomie, die auch als Ordoliberalismus bezeichnet wird, als Ordnungsprinzip. Konkret wird darunter eine wettbewerbsorientierte Wirtschaftsordnung verstanden.²⁹⁰² Der Wettbewerb als Koordinationsmechanismus der Volkswirtschaft steht im Gegensatz zur zentralplanerisch geleiteten Wirtschaftsordnung.²⁹⁰³

Der Wettbewerb soll demnach eine lenkende Funktion im Wirtschaftsleben wahrnehmen. Er fungiert insb. als primärer Mechanismus für die Allokation knapper Ressourcen. Staatliche Verteilungsregeln stehen mit anderen Worten hinter den Wettbewerb als Ordnungsprinzip zurück, soweit dieser für verteilungsgerechte Ergebnisse sorgt.²⁹⁰⁴ Sodann verringert Wettbewerb die Macht des Staates sowie der Marktteilnehmer untereinander und gegenüber Konsumenten.²⁹⁰⁵ Staatliche Regeln, wozu insb. das Kartell- und Wettbewerbsrecht gehören, stecken demgegenüber den Rahmen ab, in welchem sich die Wett-

²⁹⁰¹ So bereits von Hayek, *American Economic Review* 1945, *passim*.

²⁹⁰² Vgl. etwa Eucken, *Nationalökonomie*, 53; Böhm, *Wettbewerb und Monopolkampf*, 105, 175; Böhm, *Ordnung der Wirtschaft*, XX, 5.

²⁹⁰³ Siehe Kolev, *Rolle des Staates*, 21; kritisch zu dieser Zweiteilung Ötsch/Pühringer/Hirte, *Netzwerke des Marktes*, 93–94.

²⁹⁰⁴ Siehe Eucken, in: Eucken/Hensel, *Grundsätze der Wirtschaftspolitik*, 250, 336, 370; eine gute Übersicht findet sich bei Wörsdörfer, *Grundlagen des Ordoliberalismus*, 179–180.

²⁹⁰⁵ So bereits Stigler, in: Sills, *Competition* 181 (*«The essence of perfect competition, therefore, is not strong rivalry but rather the utter dispersion of power to influence market behavior.»*).

bewerbskräfte abzuspielen haben.²⁹⁰⁶ Die Verteilung staatlicher und privater Macht kann als eines der Hauptparadigmen der Freiburger Schule bezeichnet werden.²⁹⁰⁷

2.3 Dezentralität im Verfassungsrecht

a. Einleitung

Der Wettbewerb als Ordnungsprinzip hat sodann Eingang in das schweizerische Verfassungsrecht gefunden, und zwar im doppelten Sinne: Einerseits ist die Wettbewerbsordnung zentraler Grundpfeiler für die *wirtschaftliche Organisation und Koordination* der Marktteilnehmer; andererseits kommt dem Gedanken des Wettbewerbs im Rahmen der *politischen Staatsordnung* ebenfalls weitreichende Bedeutung zu.

b. Wirtschaftsordnung

Das schweizerische Verfassungsrecht basiert auf marktwirtschaftlichen Prinzipien. Dies ist einerseits an den individualrechtlichen Art. 26 BV (Eigentumsgarantie) und Art. 27 BV (Wirtschaftsfreiheit) sowie andererseits am ordnungspolitischen Entscheid in Art. 94 BV gut erkennbar. Damit bringt der Verfassungsgeber zum Ausdruck, dass die Wirtschaftsfreiheit als Ordnungsprinzip gelten soll.²⁹⁰⁸

Ferner sieht auch das Bundesgericht im Grundsatzentscheid von Art. 94 BV ein «*grundlegendes Ordnungsprinzip einer auf marktwirtschaftlichen Prinzipien beruhenden Wirtschaftsordnung*».²⁹⁰⁹ Die Koordination der Wirtschaftstätigkeit hat demzufolge grundsätzlich *dezentral* aufgrund der Entscheidungen und Handlungen der Gesamtheit der Marktteilnehmer zu erfolgen.²⁹¹⁰ Ge-

²⁹⁰⁶ Vgl. Art. 96 Abs. 1 BV.

²⁹⁰⁷ Siehe insb. zu Euckens Ordnungstheorie Kolev, Rolle des Staates, 19, 90; vgl. ferner auch Müller, ZSR 1981 II, 78.

²⁹⁰⁸ Siehe Botschaft BV 1996, 175–176; ferner Vallender, in: SGK BV, Art. 94 N 4; Vallender, in: SGK BV, Art. 27 N 91–99, wo auch von einem «ordnungspolitischen Grundentscheid» gesprochen wird.

²⁹⁰⁹ Siehe BGE 138 I 378, E. 6.1.

²⁹¹⁰ So *explizit* Vallender, in: SGK BV, Art. 94 N 16; Vallender, in: SGK BV, Art. 27 N 98. Mit Blick auf die *Eigentumsgarantie* als Ordnungsprinzip sodann Vallender/Hettich, in: SGK BV, Art. 26 N 79–88, welche auf die Dezentralität des Eigentums in einer marktwirtschaftlich

schützt wird damit in erster Linie die Wettbewerbswirtschaft.²⁹¹¹ Abweichungen davon sind qualifiziert begründungspflichtig.²⁹¹²

Dieser verfassungsrechtliche Grundsatzentscheid hat Bedeutung für die gesamte schweizerische Rechtsordnung inkl. das Finanzmarktrecht. Insb. ist dieses Ordnungsprinzip als Leitbild bei der Auslegung von Bestimmungen der übrigen Rechtsordnung zu berücksichtigen.²⁹¹³

c. Politische Ordnung

Der schweizerische Bundesstaat beruht u.a. auf den Prinzipien des Föderalismus und der Subsidiarität.²⁹¹⁴

Art. 3 BV hält fest, dass die Kantone souverän sind, soweit ihre Souveränität nicht durch die Bundesverfassung beschränkt ist. Sie üben zudem alle Rechte aus, die nicht dem Bund übertragen sind. Art. 5a BV enthält sodann den *Grundsatz der Subsidiarität* in allgemeiner Weise fest. Namentlich ist bei der Zuweisung und Erfüllung staatlicher Aufgaben die Subsidiarität zu beachten. Demnach sind staatliche Aufgaben auf derjenigen Ebene – Bund, Kanton, Gemeinde – anzugehen, welche die besten Voraussetzungen für eine zweckmässige Aufgabenerfüllung bietet.²⁹¹⁵ Schliesslich widmet sich das erste Kapitel im dritten Titel der Bundesverfassung in mehreren Bestimmungen dem Verhältnis zwischen Bund, den Kantonen und Gemeinden. Gemäss Art. 43a Abs. 1 BV übernimmt der Bund nur die Aufgaben, welche die Kraft der Kantone übersteigen oder einer einheitlichen Regelung durch den Bund bedürfen. Ferner ist insb. auch das Bekenntnis zur Gemeindeautonomie in Art. 50 BV zu erwähnen.

In diesem Kontext ist Dezentralisierung als die Verschiebung von Macht, Ressourcen und Kompetenzen vom Bund hin zu den Kantonen und Gemeinden zu

organisierten Wirtschaftsordnung hinweisen; ferner Müller, ZSR 1981 II, 77–79, der zudem von der «Dezentralisierungsfunktion des Eigentums» spricht.

²⁹¹¹ Siehe BGE 138 I 378, E. 6.3; ferner BSK BV-Uhlmann, Art. 94 N 5–6.

²⁹¹² Siehe Schott, in: Belser/Waldmann, Wettbewerb der Systeme, *passim*; ferner in Bezug auf Innovation Camenisch, Innovationsoffenheit, 100–101, 311–312.

²⁹¹³ Siehe Vallender, in: SGK BV, Art. 94 N 37; BSK BV-Uhlmann, Art. 94 N 4.

²⁹¹⁴ Vgl. in theoretischer Hinsicht zum Thema der politischen Dezentralisierung Treisman, Political Decentralization, 23–25.

²⁹¹⁵ So ausdrücklich Botschaft BV 1996, 16, ferner 209; ferner hinsichtlich der (De-)Zentralisierung der Aufgabenzuordnung zwischen den Staatsebenen Botschaft NFA 2001, 2305–2307; sodann Schweizer/Müller, in: SGK BV, Art. 5a N 12; ausführlich zur Subsidiarität im Kontext der EU.

verstehen.²⁹¹⁶ Politische Dezentralität entspricht der Dezentralität einer Wirtschaftsordnung insoweit, als wettbewerbliche und innovative Elemente für den Aufbau und die Funktionsweise des Staates relevant sind.²⁹¹⁷ Dezentrale Strukturen sind mit anderen Worten fester Bestandteil der schweizerischen Bundesstaatsordnung und als institutioneller Ausdruck einer skeptischen Haltung gegenüber der politischen Zentralisierung von Macht und Kontrolle zu verstehen.²⁹¹⁸

Das Prinzip kann sodann auch auf private Akteure ausgedehnt werden, wie etwa die Familie und zivilgesellschaftliche Organisationen.²⁹¹⁹

2.4 Dezentralität im Zivilrecht

a. Privatautonomie

Das *Vertragsrecht* ist als Prototyp einer dezentralen (Wirtschafts-)Ordnung zu betrachten.²⁹²⁰ Die soeben erwähnten verfassungsmässigen Vorgaben finden etwa Ausdruck in den Grundsätzen der Privatautonomie und der Vertragsfreiheit der Parteien (vgl. insb. Art. 11 Abs. 1 und 19 Abs. 1 OR).²⁹²¹ Bereits früh hat der Bundesrat anerkannt – was verfassungsmässig und gesetzlich²⁹²² ohnehin gilt und darum freilich keiner formellen Anerkennung oder Erlaubnis einer Behörde bedarf –, dass es den Marktteilnehmern freisteht, virtuelle Währung als

²⁹¹⁶ Vgl. Schneider, *Studies in Comparative International Development* 2003, 33–35.

²⁹¹⁷ Siehe Furubotn/Richter, *New Institutional Economics*, 26; ferner mit Bezug zur EU Giersch, in: Gerken, *Vertikale Kompetenzverteilung*, 35.

²⁹¹⁸ Siehe etwa Schweizer/Müller, in: SGK BV, Art. 5a N 10 m.w.N.; Botschaft NFA 2001, 2303–2304, 2306–2307 («vertikale[n] Machthemmung»); ebenso Botschaft NFA 2005, 6053; ferner Nef, *Non-Zentralismus*, 19, der aber den Begriff der *Non-Zentralität* demjenigen der Dezentralität vorzieht; vgl. ferner Schweizer/Müller, in: SGK BV, Art. 43a N 9; Kägi-Diener, in: SGK BV, Art. 50 N 9; BSK BV-Biaggini, Art. 5a N 9; BSK BV-Meyer, Art. 50 N 5, 26; ferner aus Sicht des Privateigentums auch Müller, ZSR 1981 II, 78.

²⁹¹⁹ Siehe Kley, in: Biaggini/Gächter/Kiener, *Staatsrecht*, § 10 N 17; prägend für diese Sichtweise de Tocqueville, *De la démocratie en Amérique*, 461–465.

²⁹²⁰ So auch Furubotn/Richter, *New Institutional Economics*, 16.

²⁹²¹ Vgl. ausführlich zur Vertragsfreiheit als zentraler Institution des Privat- und Eigentumsrechts Kramer, in: BK OR, Art. 19–20 N 17–20, 35–41; ferner zum *institutionalisierenden Wirtschaftsfolgerecht* Schlupe, in: Walder/Jaag/Zobl, *Funktionalität im Wirtschaftsrecht*, 169–170.

²⁹²² Vgl. zur Erfüllung von Geldschulden aufgrund einer von der gesetzlichen Ordnung abweichenden Parteivereinbarung Weber, in: BK OR, Art. 84 N 8, 156, 312.

Zahlungs- oder Tauschmittel zu verwenden und dass dieser Vorgang grundsätzlich nicht den Regeln des Finanzmarktrechts unterstellt ist.²⁹²³

Diese Anerkennung kann ordnungspolitisch als das *Primat der P2P-Transaktionen* betrachtet werden. Ein solches Primat hat in zweifacher Hinsicht Implikationen: Wenn Menschen aus freien Stücken einig sind, Kryptovermögenswerte zu verwenden, sei es im Rahmen eines Kaufes oder einer Austauschhandlung (z.B. über eine dezentrale Handelsplattform), soll die Rechtsordnung diesen Vorgang einerseits nicht behindern und andererseits darüber hinaus mit entsprechenden Rechtswirkungen versehen.

b. Konzernrecht

Ähnlich verhält es sich etwa im Gesellschaftsrecht und dort insb. im *Konzernrecht*: Ein eigentliches Konzernrecht existiert zwar in der Schweiz nicht, doch bestehen Regeln und Praxis zu punktuellen Sachverhalten.²⁹²⁴ Namentlich ist im Börsenrecht die Rede vom «regulatorischen Durchgriff», weshalb der Konzern als einheitliches Gebilde betrachtet wird.²⁹²⁵ Beim Konzern handelt es sich um ein wirtschaftliches Phänomen bestehend aus einer herrschenden Mutter- bzw. Obergesellschaft und einer oder mehreren direkt oder indirekt beherrschten Tochter- bzw. Untergesellschaften.²⁹²⁶ Die Konzernvielfalt umfasst je nach Blickwinkel Unterordnungs-, Gleichordnungs- sowie Vertrags- und faktische Konzerne.²⁹²⁷

Eine Gruppe von wirtschaftlich zusammengehörigen Unternehmen kann so dann als eine Organisation zur Wissensbeschaffung verstanden werden, deren Herausforderung darin besteht, «zwischen Zentralität und Dezentralität zu oszillieren».²⁹²⁸ Konzerne können entsprechend als Einheiten zweiter Ordnung betrachtet werden, die sich aus dem verbundmässigen Zusammenwirken von (dezentral tätigen) Einheiten erster Ordnung bilden.²⁹²⁹ Dies bedeutet, dass trotz der Hierarchisierung der Einheiten erster Ordnung Handlungsspielraum für unterschiedliche Führungsstile besteht und die einzelnen Einhei-

²⁹²³ Siehe Bundesrat, Bericht zu virtuellen Währungen, 10, 13, 15.

²⁹²⁴ Siehe statt vieler Meier-Hayoz/Forstmoser, Schweizerisches Gesellschaftsrecht, § 5 N 7, § 24 N 33–41.

²⁹²⁵ Ausführlich zum Konzept des «regulatorischen Durchgriffs» im Börsenrecht Schenker, in: Kunz/Arter/Jörg, Konzerne im Börsenrecht, 165, 173–197.

²⁹²⁶ Siehe Meier-Hayoz/Forstmoser, Schweizerisches Gesellschaftsrecht, § 24 N 42.

²⁹²⁷ Siehe Forstmoser/Meier-Hayoz/Nobel, Schweizerisches Aktienrecht, § 60 N 10.

²⁹²⁸ Siehe Amstutz, SZW 2016, 5.

²⁹²⁹ Siehe Amstutz, SZW 2016, 9.

ten im Einzelfall über einen hohen Grad an Autonomie verfügen können.²⁹³⁰ GUNTHER TEUBNER spricht letztlich vom «Netzwerk-Konzern», der gleichzeitig dezentrale Autonomie und hohe Systemintegration zu steigern sucht.²⁹³¹ Es handelt sich gemäss dem Autor um eine Organisationsform, in welcher die strategische Handlungseinheit aber trotz aller Dezentralisierung nicht verloren geht.²⁹³²

Auch bei Betrachtung des Konzern(recht)s setzt sich am Ende die Erkenntnis durch, dass Dezentralität eng mit Kontroll- und Machtverteilung verbunden ist.²⁹³³

2.5 Dezentralität im Wertpapier- und Finanzmarktrecht

a. Einleitung

Es wurde oben aufgezeigt, dass Dezentralität als Ordnungsprinzip verfassungs- und zivilrechtlich von Bedeutung ist. Mehr noch: Dezentralität scheint einen zentralen Platz in den Rechtswissenschaften einzunehmen. Die Rechtsordnung scheint damit in keiner Weise gegenüber Dezentralität als Rechtsprinzip feindlich oder überrascht eingestellt zu sein. Nachfolgend soll untersucht werden, welche konkreten wertpapier- und finanzmarktrechtlichen Bezüge zwischen *dezentralen Systemen* und dem Ordnungsprinzip der Dezentralität bestehen.

b. Gründe für eine Anerkennung

Dass der Dezentralität in rechtlicher Hinsicht überhaupt Bedeutung zukommen soll, ist nicht offensichtlich. Immerhin scheint das gesamte Finanzmarktrecht um das Intermediationsparadigma zu rotieren.²⁹³⁴ Es wäre durchaus denkbar, dass die Rechtsordnung der Dezentralität von Aktivitäten keine Be-

²⁹³⁰ Ähnlich Meier-Hayoz/Forstmoser, Schweizerisches Gesellschaftsrecht, § 24 N 59; Böckli, Schweizer Aktienrecht, 4. Aufl., § 11 Rz. 359–360; Häusermann, SZW 2023, 560–562 m.w.N., 566 («effiziente Selbstorganisation»).

²⁹³¹ Siehe Teubner, ZGR 1991, 191.

²⁹³² Siehe Teubner, ZGR 1991, 203–204.

²⁹³³ Siehe Teubner, ZGR 1991, 202–203. Vgl. auch das in Art. 963 Abs. 2 OR vorgesehene Kontrollprinzip.

²⁹³⁴ Vgl. zum finanzmarktrechtlichen Konzept des Finanzintermediärs oben, [V1.3](#).

deutung zuschreibt oder eine solche unverblümt verbietet. Letzteres ist in einigen Ländern tatsächlich auch geschehen.²⁹³⁵ Allerdings ist die Durchsetzung von Verboten oder Einschränkungen von Kryptowährungen und Blockchain-Technologie – vergleichbar mit technischen Blockaden von Webseiten im World Wide Web – in der Praxis nur sehr bedingt wirksam.²⁹³⁶

Auf den ersten Blick scheinen einzig die Praktikabilität der Anwendbarkeit und Durchsetzbarkeit von Rechtsnormen und allenfalls ein gewisser rechtspolitischer Pragmatismus der Dezentralität rechtspolitische Akzeptanz zu verleihen.²⁹³⁷ Neben praktischen und rechtspolitischen Erwägungen sprechen allerdings *auch* unmittelbar Gründe des Anleger- und Funktionsschutzes für die Anerkennung von Dezentralität als Ordnungsprinzip im Finanzmarktrecht. Dezentralität ermöglicht namentlich inklusive und neutrale Systeme, in welchen Informationsasymmetrien und Machtungleichgewichte zwischen Marktteilnehmern beseitigt oder zumindest abgeschwächt, die individuelle Kontrolle über Vermögenswerte (Self-Custody) gestärkt und die Transparenz der Funktionsweise des Systems verbessert werden können.²⁹³⁸

Davon zu unterscheiden ist die Frage, die in der Literatur lediglich selten ausdrücklich gestellt wird, ob das *heutige* Finanzmarktrecht überhaupt überzeugende Antworten auf dezentrale Prozesse und Strukturen bereithält.²⁹³⁹ In diesem Zusammenhang ist zu fordern, dass die bisherige Regulierung nicht einfach unbesehen auf dezentrale Systeme übernommen werden kann. Den Besonderheiten solcher Systeme, etwa der selbstverwaltenden, verteilten Natur, ist angemessen Rechnung zu tragen.²⁹⁴⁰

²⁹³⁵ Vgl. Noone, Case against bitcoin, *passim*.

²⁹³⁶ Vgl. Price, Bitcoin Ban, *passim*.

²⁹³⁷ Siehe die einschlägigen Veröffentlichungen zur Finanzmarktpolitik in Bundesrat, Finanzmarktpolitik 2016, 12–13 («Chancen der Digitalisierung»), 18; ferner Bundesrat, Finanzmarktpolitik 2020, 8 («Standortwettbewerb»); sodann zur bewussten Positionierung der Schweiz im Blockchain- und FinTech-Bereich statt vieler Werlen/Weber, CapLaw-2023-39, *passim*, die von «Safe Haven» sprechen.

²⁹³⁸ Siehe zum Nutzen der Dezentralität oben, VII.1.3.

²⁹³⁹ Siehe Bundesrat, DLT-Bericht 2018, 113, wo bloss von «spezifischen Herausforderungen» im Finanzmarktinfrastrukturrecht für Blockchain- bzw. DLT-basierte Geschäftsmodelle die Rede ist; ferner dieses Thema ebenfalls andeutend Molo/Drzalic, AJP 2019, 41.

²⁹⁴⁰ So bereits Furrer/Glarner/Linder/Müller, Jusletter vom 26. November 2018, Rz. 12; dies ebenfalls anerkennend Bundesrat, DLT-Bericht 2018, 14 («Ausnahmebereiche»).

c. Anerkennung dezentraler Netzwerke

i. Wertpapierrecht

Dezentralität als Ordnungsprinzip wurde im Rahmen der DLT-Mantelrevision – zumindest stillschweigend – anerkannt:

Im Vorentwurf zu Art. 973d OR war noch ausdrücklich vom «verteilten elektronischen Register» bzw. von Distributed Ledger Technology (DLT) die Rede.²⁹⁴¹ Diese Formulierung wurde zu Recht zugunsten einer technologieneutralen Begriffsverwendung aufgegeben.²⁹⁴² Nunmehr wird in technologieunspezifischer Weise von «Wertrechtregistern» gesprochen. Solche Register werden in Bezug auf ihre Rechtswirkungen technisch auf dieselbe Ebene wie die physische Urkunde eines Wertpapiers öffentlichen Glaubens gestellt.²⁹⁴³ Vor diesem Hintergrund sind Registerwertrechte in ein Wertrechtregister einzutragen, das den Mindestanforderungen in Art. 973d Abs. 2 OR genügt. Ausserdem sind sie zudem über dieses Register geltend zu machen und auf andere zu übertragen.

Nach Auffassung des Bundesrates erfüllen insb. dezentrale Netzwerke, wie etwa Bitcoin und Ethereum, die in Abs. 2 statuierten Anforderungen. Dies gilt grundsätzlich unabhängig vom verwendeten Konsensmechanismus.²⁹⁴⁴ Als eindeutiger Hinweis auf die Dezentralität eines Netzwerks ist insb. Art. 973d Abs. 2 Ziff. 2 OR zu betrachten: Die Integrität des Wertrechtregisters ist danach durch angemessene technische und organisatorische Massnahmen, wie die gemeinsame Verwaltung durch mehrere voneinander unabhängige Beteiligte, gegen unbefugte Veränderungen zu schützen. Das Element der *gemeinsamen Verwaltung durch mehrere voneinander unabhängige Beteiligte* nimmt ausdrücklich Bezug auf die Verteiltheit elektronischer Datenkopien in dezentralen Netzwerken.²⁹⁴⁵ Die Integrität der Daten und Operationen eines Regis-

²⁹⁴¹ Art. 973d Abs. 1 VE-OR; siehe hierzu der Erläuternde Bericht zur Vernehmlassungsvorlage EFD, Erläuternder Bericht DLT-Vernehmlassungsvorlage 2019, 28–29.

²⁹⁴² Siehe Botschaft DLT 2019, 259–260, 279–280.

²⁹⁴³ Siehe Botschaft DLT 2019, 259, 276.

²⁹⁴⁴ Siehe Botschaft DLT 2019, 281–282.

²⁹⁴⁵ Vgl. bereits EFD, Erläuternder Bericht DLT-Vernehmlassungsvorlage 2019, 8–9, 31, wo von «zahlreiche[n] Teilnehmer[n]» und einer «Vielzahl von Beteiligten» die Rede ist. Ganz grundsätzlich schien der Erläuternde Bericht zur Vernehmlassungsvorlage noch stärker von den Konzepten der Verteiltheit und der Dezentralität durchdrungen zu sein.

ters kann mit anderen Worten durch eine gemeinschaftliche Verwaltung der Netzwerkteilnehmer erreicht werden. In dieser Hinsicht wird die Botschaft sogar sehr deutlich:

*«Wenn die Parteien die Registrierung ihres Rechts mittels einer solchen bekannten dezentralen Lösung vereinbaren, wird jedoch als Mindestanforderung zu verlangen sein, dass diese zu jedem Zeitpunkt tatsächlich ein Mindestmass an Dezentralisierung und damit Resilienz bereitstellt. Dafür muss das System über mehrere Teilnehmende verfügen, die ihrerseits am verwendeten Konsensmechanismus tatsächlich teilnehmen und voneinander unabhängig sind.»*²⁹⁴⁶

Zwar handelt es sich bei der gemeinsamen Verwaltung durch mehrere voneinander unabhängige Beteiligte lediglich um eine beispielhafte Aufzählung, was durch den Einschub der Konjunktion «wie» in Art. 973d Abs. 2 Ziff. 2 OR klargestellt wird, doch verlangt die Botschaft mindestens denselben Sicherheitsgrad von allfälligen anderen Lösungen.²⁹⁴⁷ In diesem Licht ist auch die Erwähnung von permissioned bzw. private Blockchains als Grundlage für Wertrechtereigister zu sehen. Diese haben ebenfalls die vom Gesetz geforderte Integrität des Registers sicherzustellen.²⁹⁴⁸ An die Integrität des Registers sind nach vorliegender Auffassung bei Netzwerken mit bloss wenigen Teilnehmern, die sich zudem kennen und ohne Weiteres miteinander kollidieren könnten, höhere Anforderungen als bei permissionless bzw. public Blockchains zu stellen.²⁹⁴⁹ In der Vernehmlassung zum Vorentwurf wurde sodann teilweise auch mehr Rechtssicherheit hinsichtlich der Frage, ab wann genügende Dezentralität vorliegt, gefordert.²⁹⁵⁰

Die wertpapierrechtliche Rezeption von über Blockchains oder DLT herausgegebenen Rechte als Registerwertrechte kann somit als *erstmalige Anerkennung* der Dezentralität als Ordnungsprinzip durch den Gesetzgeber betrachtet wer-

²⁹⁴⁶ Botschaft DLT 2019, 281.

²⁹⁴⁷ Siehe Botschaft DLT 2019, 280.

²⁹⁴⁸ Siehe Botschaft DLT 2019, 282

²⁹⁴⁹ Ähnlich Kuhn et al., Jusletter IT vom 23. Mai 2019, Rz. 21 (unter dem Gesichtspunkt der Manipulationsresistenz); vgl. demgegenüber Kramer/Oser/Meier, Jusletter vom 6. Mai 2019, Rz. 17 FN 35; SBF, Circular 2021/01, 8, dessen Autoren unter Bezugnahme auf den Paxos-Konsensalgorithmus ausnahmsweise auch bei bloss zwei Beteiligten, die voneinander unabhängig sind, davon ausgehen, dass die Integrität sichergestellt sein kann; wohl auch Kuhn, in: Weber/Kuhn, Digitale Aktiven im schweizerischen Privatrecht, Rz 61; Stengel, in: Reutter/Werlen, Blockchain/Distributed Ledger Technology, 148–149, wonach es auf den Grad der Dezentralität des Wertrechtereigisters für die zivilrechtliche Qualifikation nicht ankommen könne (abgehandelt unter dem Aspekt der Verfügungsmacht); zurückhaltender demgegenüber von der Crone/Derungs, SZW 2019, 9–10.

²⁹⁵⁰ Vgl. EFD, Ergebnisbericht Vernehmlassung DLT 2019, 7.

den. Die Bedeutung dieses Schritts durch den Schweizer Gesetzgeber ist nicht zu unterschätzen. Er hat nach vorliegender Ansicht namentlich weitgehende Konsequenzen für das Finanzmarktrecht.

ii. Finanzmarktrecht

In der DLT-Botschaft macht der Bundesrat deutlich, dass die Anforderungen an ein Wertrechteregister *im Finanzmarktrecht* höher sein können als im Wertpapierrecht, da ersteres auch dem Anleger- und Funktionsschutz Rechnung zu tragen hat.²⁹⁵¹ Dies zeigt sich namentlich darin, dass der Gesetzgeber in Art. 73d Abs. 3 lit. a FinfraG dem Bundesrat die Kompetenz einräumt, *Mindestanforderungen* an DLT-Effekten namentlich hinsichtlich deren Integrität und Publizität vorzusehen, die an einem DLT-Handelssystem zugelassen werden. Diese Anforderungen wirken sich letztlich auf die Wahl des zugrundeliegenden Wertrechteregisters und somit auf das dezentrale Netzwerk aus. Der Delegationsnorm im Gesetz nachkommend, statuiert der Bundesrat in Art. 58g Abs. 1 FinfraV, dass DLT-Effekten zugelassen werden können, wenn das «verteilte elektronische Register» mindestens die Anforderungen nach Art. 973d Abs. 2 OR erfüllt.

Damit schliesst der Bundesrat vorerst den Kreis der akzeptablen Register: In zivil- und finanzmarktrechtlicher Hinsicht bieten dezentrale Netzwerke, wie sie vorliegend verstanden werden, eine geeignete Grundlage für die Ausgabe von Registerwertrechten gemäss OR bzw. DLT-Effekten sowie weiterer Vermögenswerte gemäss FinfraG. Im Ergebnis können sich DLT-Handelssysteme für ihre Handelsschritte (z.B. die Verwahrung und Abwicklung) ohne Weiteres etwa auf die dezentralen Netzwerke etwa von Bitcoin oder Ethereum verlassen.

Der Bundesrat greift in der Botschaft ausserdem mehrfach auf die Abgrenzung von Wertrechteregistern gegenüber «zentral geführten Registern» zurück.²⁹⁵² Dies ist zwar anders als der Bundesrat nicht primär eine Frage der Verfügungsmacht des Gläubigers (Art. 973d Abs. 2 Ziff. 1 OR), denn diese kann grundsätzlich auch in einem zentral geführten System sichergestellt werden.

²⁹⁵¹ Siehe Botschaft DLT 2019, 260–261.

²⁹⁵² Siehe Botschaft DLT 2019, 278, 279 bzw. 281, an welchen Stellen von einer «vertrauenswürdigen zentralen Instanz, welche das Register alleine verwaltet», und von einer «zentralen, vertrauenswürdigen Instanz», welche die Authentifizierung von Transaktionen vornimmt, die Rede ist.

Demgegenüber handelt es sich auch hier in erster Linie um eine Frage der Integrität der in einem Register abgespeicherten Daten.²⁹⁵³

Dezentrale Netzwerke sind somit auch im Finanzmarktrecht ausdrücklich vom Gesetzgeber anerkannt worden. Die FINMA kam ihrerseits unter dem Untertitel «Keine eigentliche Kryptowährung» bereits im Dezember 2017 in einem Enforcementverfahren zum Schluss, dass die hinter «E-Coins» stehenden Personen «[i]m Gegensatz zu dezentral gespeicherten und auf Blockchain-Technologie beruhenden Kryptowährungen» die Währungseinheiten ausschliesslich kontrolliert und auf deren eigenen Servern gespeichert und somit gegen das Bankengesetz verstossen haben.²⁹⁵⁴

d. Anerkennung dezentraler Applikationen und insb. dezentraler Handelsplattformen

Ein Wertrechtereister muss die Anforderungen in Art. 973d Abs. 2 OR erfüllen. Jedoch erwartet der Gesetzgeber nicht, dass Wertrechtereister denselben Grad an Dezentralität wie dezentrale Netzwerke aufweisen. Wertrechtereister haben demgegenüber vielmehr die Zuordnung der Verfügungsmacht über die Rechte zu vermitteln. Namentlich muss das Register mittels technischer Verfahren ausschliesslich dem Gläubiger eines Rechts, nicht aber dem Schuldner, die *Verfügungsmacht* über das Registerwertrecht vermitteln (Art. 973d Abs. 2 Ziff. 1 OR).

Allerdings kommt dem Schuldner gemäss Art. 973d Abs. 3 OR die Organisationsverantwortung für das Wertrechtereister zu. Es wird somit implizit vorausgesetzt, dass der Schuldner gewisse Funktionen des Registers ausüben kann bzw. diese ihm vorbehalten sind. Naheliegend sind die Schaffung und Emission von Registerwertrechten. Diese Aktivitäten sind auch bei traditioneller wertpapierrechtlicher Verurkundung in aller Regel dem Aufgaben- und Kontrollbereich des Emittenten zuzuordnen.

Damit das Erfordernis der Verfügungsmacht des Gläubigers erfüllt ist, darf der Schuldner indessen lediglich in einem begrenztem Umfang auf das Wertrechtereister Einfluss nehmen können. Die Lehre spricht davon, dass der Schuld-

²⁹⁵³ GLM. wohl SBF, Circular 2021/01, 6, 7–8; Kuhn, in: Weber/Kuhn, Digitale Aktiven im schweizerischen Privatrecht, Rz. 59.

²⁹⁵⁴ Siehe FINMA, Scheinkryptowährungen, 2; ferner auch Branson, Technologie und die Finanzbranche, 1 («Wir anerkennen das grosse Potenzial, das Fintech und die Blockchain-Technologie dem Finanzplatz bieten. Wir sehen uns als Aufsichtsbehörde hier auch in einer Rolle: Wir wollen Innovation ermöglichen.»).

ner nach der Registrierung des Rechts und dessen Begebung nicht mehr in der Lage sein darf, den Registereintrag unilateral zu verändern.²⁹⁵⁵ Vor diesem Hintergrund können in der Praxis gewisse Smart Contract-Funktionen, wie etwa das Whitelisting bzw. Blacklisting oder das Freezing von Wallet-Adressen oder das einseitige Pausieren oder Updaten von Smart Contracts, problematisch sein. Da einige dieser Funktionen allerdings auch einen gewissen Nutzen für die Gläubiger aufweisen können (z.B. das Recovery verloren gegangener Token) oder im öffentlichen Interesse sind (z.B. das Freezing einer Wallet-Adresse im Zusammenhang mit einer Strafverfolgung), ist ihr kompletter technischer Ausschluss nicht immer erwünscht. In der Literatur wird darum gefordert, dass den Einflussmöglichkeiten des Schuldners mittels geeigneter Governance entgegenzusteuern ist.²⁹⁵⁶ Das Ziel solcher Governance muss die Verhinderung *missbräuchlicher* Einflussnahme auf das Wertrechteregister durch den Schuldner sein.

Dezentrale Applikationen, darunter dezentrale Handelsplattformen, beruhen technisch auf dezentralen Netzwerken.²⁹⁵⁷ Dezentrale Applikationen können auf ein Wertrechteregister zurückgreifen oder ausnahmsweise selbst ein solches darstellen. Letzteres ist etwa der Fall, wenn ein Smart Contract die Emission von Token bezweckt, welche als Registerwertrechte qualifizieren, und dieser Smart Contract von jedermann angerufen werden kann (z.B. ein Faucet für Anlage-Token)²⁹⁵⁸. Demgegenüber können dezentrale Handelsplattformen etwa den Handel mit Anlage-Token ermöglichen, die ihrerseits in einem Wertrechteregister eingetragen sind und nur über dieses geltend gemacht und auf andere übertragen werden können. Die Smart Contracts, welche die dezentrale Handelsplattform ausmachen, stellen demgegenüber *nicht* das Wertrechteregister dar.²⁹⁵⁹

Die vorliegende Arbeit weicht, wie bereits erwähnt, in Bezug auf dezentrale Handelsplattformen terminologisch vom Bericht des Bundesrates ab.²⁹⁶⁰ Der Bericht nimmt eine Abgrenzung zwischen «dezentralen Handelsplattformen» und «verteilten Peer-to-Peer-Plattformen» vor, wobei die Unterscheidungs-

²⁹⁵⁵ Siehe Kuhn, in: Weber/Kuhn, Digitale Aktiven im schweizerischen Privatrecht, Rz. 57.

²⁹⁵⁶ So etwa SBF, Circular 2021/01, 6–7; bereits SBF, Circular 2019/01, 7; Stengel, in: Reutter/Werlen, Blockchain/Distributed Ledger Technology, 149–150; Kuhn, in: Weber/Kuhn, Digitale Aktiven im schweizerischen Privatrecht, Rz. 58 («sauber festzulegen und in der Registrierungsvereinbarung offen zu legen»).

²⁹⁵⁷ Siehe hierzu oben, [III.4.1](#).

²⁹⁵⁸ Siehe zur Faucet-Funktion Antonopoulos/Wood, Mastering Ethereum, 27.

²⁹⁵⁹ Siehe diesbezüglich oben, [V.3.6c](#).

²⁹⁶⁰ Siehe oben, [IV.1.2](#).

merkmale nicht weiter vertieft werden. Die Abgrenzung ist folgenreich, denn «dezentrale Handelsplattformen» können nach Auffassung des Bundesrates im Einzelfall dem FinfraG und dem GwG unterstellt sein.²⁹⁶¹ Demgegenüber befinden sich «verteilte Peer-to-Peer-Plattformen» ausserhalb des Geltungsbereichs dieser Gesetze.²⁹⁶² Zur Begründung wird angeführt, dass es in letzteren Fällen an einem unmittelbaren und klar identifizierbaren Betreiber fehlt bzw. lediglich eine Vermittlungstätigkeit ohne Einbezug in die Zahlungsflüsse vorliegt.²⁹⁶³

Das Element der Dezentralität einer Handelsplattform spielt mit anderen Worten auch in diesem Bereich eine zentrale Rolle. Die Tatsache, dass der Bundesrat die Dezentralität als Begründung für die Nichtunterstellung dezentraler Handelsplattformen, wie sie in der vorliegenden Arbeit definiert werden, anführt, bedeutet, dass er Dezentralität als Ordnungsprinzip grundsätzlich anerkennt. *Wie bereits für dezentrale Netzwerke gilt das Ordnungsprinzip somit auch für die Applikationsebene.*

2.6 Steuerrecht

Auch in steuerrechtlicher Hinsicht wurde die Dezentralität als reale Erscheinung anerkannt: Das Bundesverwaltungsgericht hat in einem vielbeachteten mehrwertsteuerrechtlichen Entscheid festgehalten, dass die konkreten Steuernerfolgen für Staker davon abhängen, ob die Staking Rewards vom Protokoll neu geschöpft oder aber von den Nutzern der Blockchain (konkret Polkadot und Kusama) geleistet werden. Das Bundesverwaltungsgericht setzt *in puncto* Dezentralität der Blockchain voraus, dass das Netzwerk keine zentrale «Protokollgesellschaft» aufweise, welche die «alleinige Verfügungsmacht» (wohl im Sinne von «Steuerungs- und Leitungsfunktionen») über das Netzwerk innehat.²⁹⁶⁴ Demgegenüber bleibt offen, wie ein Staker, der die Validierungsleistungen erbringt, konkret der Mehrwertsteuerpflicht nachkommen kann, wenn er *in casu* nicht genau weiss, in welchem Land der Nutzer der Blockchain als Empfänger der Validierungsleistungen domiziliert ist.²⁹⁶⁵

²⁹⁶¹ Siehe Bundesrat, DLT-Bericht 2018, 105–106, 146–147.

²⁹⁶² Siehe Bundesrat, DLT-Bericht 2018, 105–106, 146–147.

²⁹⁶³ Siehe Bundesrat, DLT-Bericht 2018, 115, 147; Botschaft DLT 2019, 270–271, 273.

²⁹⁶⁴ Siehe BVerfG A-5638/2022 vom 29. August 2023, E. 3.4.2.3–3.4.2.4.

²⁹⁶⁵ Siehe hierzu SBF, Zirkular 2023/01, Fassung vom April 2024, *passim*.

2.7 Politischer und regulatorischer Kurswechsel?

Die wertpapier- und finanzmarktrechtliche Bedeutung von Dezentralität als Ordnungsprinzip kann nach dem Gesagten als erstellt betrachtet werden. Der Bundesrat selbst hat die Entwicklung von zentralen zu dezentralen Strukturen in der Vergangenheit mehrfach als «Paradigmenwechsel» bezeichnet,²⁹⁶⁶ dem ähnlich wie dem vorherrschenden Intermediationsmodell rechtlich Beachtung zu schenken ist.

Allerdings könnte dem Prinzip aus *finanzmarktrechtlichen* Überlegungen, die angeblich im Anleger- und Funktionsschutz begründet zu sein scheinen,²⁹⁶⁷ bereits wieder ein regulatorischer Kurswechsel drohen: Bereits im DLT-Bericht von 2018 kündigte der Bundesrat an, «einen konkreten Regulierungsvorschlag für dezentrale Finanzmarktinfrastrukturen zu gegebener Zeit» präsentieren zu wollen, um dem ausgelösten Paradigmenwechsel Rechnung zu tragen.²⁹⁶⁸ Anstelle der heutigen Anknüpfung am Betreiber einer Finanzmarktinfrastuktur (*entity-based approach*) soll der sachlich-persönliche Geltungsbereich des FinfraG vermehrt durch die Ausübung bestimmter Aktivitäten (*activity-based approach*) ausgelöst werden, was nach Auffassung des Bundesrates «sowohl zentralen als auch dezentralen Finanzmarktinfrastrukturen gerecht» würde.²⁹⁶⁹ Dabei gilt es allerdings zu beachten, dass der aktivitätsbasierte Regulierungsansatz bereits heute im Finanzmarktrecht gebräuchlich ist.²⁹⁷⁰ Das völlige Ausblenden der Person des Leistungserbringers würde nach vorliegender Auffassung demgegenüber Regeln produzieren, die gerade im Bereich von DeFi nur schwer einzuhalten und durchzusetzen wären.

Sodann kommt hinzu, dass das Staatssekretariat für Finanzfragen SIF bereits im November 2019 einen Untersuchungsauftrag zwecks Evaluation des FinfraG ausgeschrieben hat. Das Augenmerk liegt allerdings auf den Marktverhaltenspflichten im Derivatebereich.²⁹⁷¹

²⁹⁶⁶ Siehe Bundesrat, DLT-Bericht 2018, 115–116.

²⁹⁶⁷ Siehe hierzu oben, [VL3](#).

²⁹⁶⁸ Siehe Bundesrat, DLT-Bericht 2018, 115–116.

²⁹⁶⁹ Siehe Bundesrat, DLT-Bericht 2018, 115; ebenso FSB, *Decentralised financial technologies*, 23 a.E.; ebenfalls anregend EUBOF, *Decentralised Finance*, 39–40. Vgl. zur Abgrenzung der beiden Regulierungsansätze Borio/Claessens/Tarashev, BIS FSI Occasional Paper Nr. 19, August 2022, 4, 9.

²⁹⁷⁰ Vgl. etwa Bundesrat, DLT-Bericht 2018, 46.

²⁹⁷¹ Siehe SIF, Evaluation FinfraG, *passim*.

Die FINMA hat ihrerseits im Jahresbericht 2020 festgestellt, dass die zunehmende Dezentralisierung von Geschäftsmodellen die aufsichtsrechtliche Arbeit vor neue Herausforderungen stelle. Namentlich liege die Herausforderung darin, dass «die technologische Entwicklung zunehmend Betriebsmodelle ermöglicht, bei denen die Tätigkeit in zahlreiche Bestandteile aufgeteilt ist, was die Zuordnung der gesamthaft betrachteten bewilligungspflichtigen Dienstleistungen erschwert».²⁹⁷² Hierzu gehören nach Aussage der FINMA neben der Verwahrung von Token deren Wechsel und Handel.²⁹⁷³ Die FINMA erachtet den funktionalen Ansatz weiterhin als gerechtfertigt, wonach in erster Linie auf die wirtschaftlichen Funktionen der zu beurteilenden Projekte abzustellen sei. Dabei orientiere sich die FINMA jedoch auch an den «bewährten und vom Gesetzgeber vorgegebenen Wertungsentscheidungen (same business, same risks, same rules)».²⁹⁷⁴ Gerade die Dezentralität kann nach vorliegender Auffassung als eine solche Wertungsentscheidung des Gesetzgebers betrachtet werden. Sodann führte auch die Evaluation des FinfraG im September 2022 nicht zu einer Abkehr vom bisherigen Kurs; dezentrale Handelsplattformen ohne bestimmbare Betreiberin bilden weiterhin keinen Regulierungsgegenstand.²⁹⁷⁵

Ähnlich klingt es von den beiden US-amerikanischen Aufsichtsbehörden auf nationaler Ebene: Der Vorsitzende der SEC ruft den Gesetzgeber dazu auf, bestehende Lücken in der Regulierung zu schliessen und sich dabei insb. auf DeFi-Applikationen zu fokussieren.²⁹⁷⁶ Für die CFTC gleicht das Fehlen von Finanzintermediären in dezentralen Finanzsystemen sogar einem *Hobbes'schen Marktplatz*.²⁹⁷⁷ Entsprechend ist in den letzten Jahren eine Zunahme an Enforcement-Bemühungen gegen DEX bzw. Personen, die eine DEX mutmasslich betreiben, festzustellen,²⁹⁷⁸ die im Falle der Ooki DAO gerichtlich bestätigt wurde.²⁹⁷⁹ Die Rede ist von «regulation by enforcement», welche im Ergebnis

²⁹⁷² FINMA, Jahresbericht 2020, 29.

²⁹⁷³ Siehe FINMA, Jahresbericht 2020, 29.

²⁹⁷⁴ Siehe FINMA, Jahresbericht 2020, 29; FINMA, Jahresbericht 2021, 20.

²⁹⁷⁵ Vgl. EFD/SIF, Evaluation FinfraG, *passim*.

²⁹⁷⁶ Siehe Gensler, Aspen Security Forum, *passim*.

²⁹⁷⁷ Siehe Berkovitz, Decentralized Finance, *passim* («In a pure 'peer-to-peer' DeFi system, none of these benefits or protections exist. There is no intermediary to monitor markets for fraud and manipulation, prevent money laundering, safeguard deposited funds, ensure counterparty performance, or make customers whole when processes fail. A system without intermediaries is a Hobbesian marketplace with each person looking out for themselves. Caveat emptor – 'let the buyer beware.'»).

²⁹⁷⁸ Siehe U.S. District Court Northern District of California, CFTC vs. Ooki DAO, Complaint, *passim*; ferner CFTC vs. ZeroEx, Inc., Order, *passim*.

²⁹⁷⁹ Siehe U.S. District Court Northern District of California, CFTC vs. Ooki DAO, Order, 7–13.

wenig effizient und wirksam ist und deren Motive oft primär prestigegetrieben sind.²⁹⁸⁰

Ebenfalls in diese Richtung stösst das U.S. DEPARTMENT OF THE TREASURY. Gemäss Ausführungen der Behörde in ihrem vielbeachteten Bericht zu den Risiken der Finanzkriminalität sind Formen der Disintermediation mangels Zugriffs auf allenfalls relevante Finanzdaten nicht wünschenswert.²⁹⁸¹ Unter US-Sanktionsrecht liegen sodann inzwischen zwei Entscheidungen erstinstanzlicher Gerichte vor, die im Falle von *Tornado Cash* trotz Vorliegen autonomer Smart Contracts mit einer weiten Auslegung des bestehenden Rechts «klare Verantwortliche» ausgemacht haben wollen; beide Entscheide wurden angefochten.²⁹⁸² Mit Blick auf Geldwäscherei- und Terrorismusfinanzierungsrisiken hat schliesslich die FATF spezifisch die *dezentrale* Natur von DLT-basierten Technologien hervorgehoben.²⁹⁸³ Immerhin anerkennt die FATF, dass es dezentrale Systeme gibt, welche mangels Involvierung unterstellter Personen oder aufgrund der ausgeübten Aktivitäten der betreffenden Personen gänzlich ohne VASPs auskommen.²⁹⁸⁴

Gleichzeitig existieren auch Regulierungsbestrebungen, die u.U. weitgehende Auswirkungen auf dezentrale Handelsplattformen haben: In den USA etwa soll der *Exchange*-Begriff im Securities Exchange Act von 1934 erweitert werden. Neu sollen auch *Communication Protocol Systems* eine Exchange i.S.d. Gesetzes darstellen.²⁹⁸⁵ Angesichts der breiten Kritik am Entwurf spricht die SEC nunmehr einschränkend von *Negotiation Protocols*.²⁹⁸⁶ Dennoch könnte dies Auswirkungen auf die Unterstellung von DEX bzw. von daran anschliessenden grafischen Benutzeroberflächen haben. Offen ist weiterhin, wie allfällige Betreiber solcher Komponenten die auf intermediäre Strukturen ausgelegten Wertpapierregeln, namentlich Registrierungs- und Offenlegungspflichten, überhaupt einhalten könnten.²⁹⁸⁷ Parallel dazu stellen sich ähnliche Fragen

²⁹⁸⁰ Für eine aktuelle Übersicht der aktuellen Aufsichtspraxis und Rechtsprechung siehe Hess, Penn State Law Review 2024, 23–27; ferner zum andauernden Revierkampf zwischen SEC und CFTC Goforth, Chapman Law Review 2023, *passim*.

²⁹⁸¹ U.S. Department of the Treasury, Illicit Finance Risk, 28–29.

²⁹⁸² Vgl. hierzu oben, FN 2692.

²⁹⁸³ Siehe FATF, New Technologies for AML/CFT, 26.

²⁹⁸⁴ Siehe FATF, VASP Guidance 2021, 31 («very few»).

²⁹⁸⁵ Siehe SEC, Exchange 2022, 8–9.

²⁹⁸⁶ Siehe SEC, Exchange 2023, 42–46 m.w.H.

²⁹⁸⁷ Siehe für einen Überblick der Kritikpunkte SEC, Exchange 2023, 6–8 m.w.H.; ferner Peirce, Dissenting Statement, *passim*; in verfassungsrechtlicher Hinsicht Coin Center, Comments Exchange, 2–5.

auch für Liquiditätsbereitsteller auf dezentralen Handelsplattformen.²⁹⁸⁸ Die EU hat sich demgegenüber gegen die Unterstellung von dezentralen Handelsplattformen und anderen «in ausschliesslich dezentralisierter Weise» ausgeführten Applikationen unter MiCAR entschieden,²⁹⁸⁹ wobei allerdings die konkrete Bedeutung dieses Entscheids in der Praxis im Einzelnen umstritten ist.

Bei den erwähnten Beispielen handelt es sich nur um einen kleinen Ausschnitt aus einer Vielzahl ähnlich gelagerter Ansichten, Bemerkungen, Regulierungsbestrebungen und Urteile seitens von Aufsichtsbehörden, internationalen Organisationen und Gerichten zum Thema Dezentralität. Dezentralität wird demnach zunehmend als *regulatorisches und rechtliches Risiko* aufgefasst, dem durch rechtliche Vorgaben oder eine entsprechende Aufsichtspraxis Rechnung getragen werden müsse.

Am ausgeprägtesten ist die *ablehnende* Haltung gegenüber Dezentralität in den Aussagen des FSB²⁹⁹⁰, der BIS und der IOSCO zu spüren: Es wird etwa die Frage aufgeworfen, ob die weniger einschneidenden Eigenmittelvorgaben auf das Halten tokenisierter traditioneller Vermögenswerte und Stablecoins durch eine Bank zur Anwendung gelangen sollen, wenn die Token in einem dezentralen System ausgegeben werden.²⁹⁹¹ Ferner wird in Abrede gestellt, dass es «true DeFi» geben kann, was wenig überrascht angesichts der Bereitschaft, praktisch in jedem Anwendungsfall eine verantwortliche Person identifizieren zu wollen, und zwar ungeachtet dessen, ob die fragliche Person überhaupt eine finanznahe Tätigkeit ausübt.²⁹⁹² In Ergebnis würde dadurch für DeFi zu einem «activity-based approach» gewechselt werden, der dem Dezentralitätsgrad im Einzelfall keine oder nur wenig Beachtung schenken würde.²⁹⁹³

Tatsächlich kann im Bereich der Verhinderung von Geldwäscherei und Terrorismusfinanzierung *im Ansatz* bereits ein regulatorischer Paradigmenwechsel erkannt werden: Mit Art. 4 Abs. 1 lit. b GwV wird im Rahmen von Dienstleistungen im Zahlungsverkehr erstmals nicht mehr an den Umstand angeknüpft, dass ein Finanzintermediär die ausschliessliche und unmittelbare Verfügungsmacht über fremde Vermögenswerte innehaben muss. Dies könnte als erster

²⁹⁸⁸ Siehe SEC, Dealer, 44, 78–79.

²⁹⁸⁹ Siehe Verordnung (EU) 2023/1114, Erwägungsgrund 22.

²⁹⁹⁰ Illustrativ für die Haltung FSB, Financial Stability Risks 2023, *passim*.

²⁹⁹¹ Siehe BIS/BCBS, Prudential treatment of cryptoasset exposures, 4, 30; nunmehr *ablehnend* BIS/BCBS, Cryptoasset standard amendments, 1; ferner Aquilina/Frost/Schrimpf, Bulletin Nr. 66, 12. Januar 2023, *passim*.

²⁹⁹² Siehe IOSCO, Final Report DeFi 2023, 21–25 («seek to identify any Responsible Persons»).

²⁹⁹³ Vgl. die Ausführungen in IOSCO, Final Report DeFi 2023, 51.

Einschnitt der Dezentralität als Ordnungsprinzip angesehen werden. Allerdings lässt sich durch die in der vorliegenden Arbeit vertretenen einschränkende Auslegung der Bestimmung, wonach es weiterhin auf die Kontrolle über fremde Vermögenswerte ankommt,²⁹⁹⁴ durchaus auch ein Ergebnis erzielen, dass mit dem Ordnungsprinzip in Einklang gebracht werden kann. Die Empfehlungen der FATF rund um den VASP-Begriff deuten nichtsdestotrotz darauf hin, dass Dezentralität vermehrt hinter das heute vorherrschende Intermediationsmodell im Geldwäschereirecht zurückzutreten hat.²⁹⁹⁵

Demgegenüber scheinbar aufsichtsrechtlich unangetastet bleiben mit grosser Wahrscheinlichkeit dezentrale Netzwerke. Für Netzwerkteilnehmer ist nicht damit zu rechnen, dass diese den schweizerischen Finanzmarktgesetzen unterstellt werden. Belastbare Rechtssicherheit existiert demgegenüber auch hier nicht.²⁹⁹⁶

²⁹⁹⁴ Siehe etwa oben, [V.2.6c](#).

²⁹⁹⁵ Siehe hierzu ausführlich oben, [V.2.3d](#).

²⁹⁹⁶ Siehe etwa zu den potenziellen steuerpolitischen Auswirkungen des US-amerikanischen Infrastrukturgesetzes auf die Kryptoindustrie Editorial Board, Bipartisan Cryptocurrency Crackup, WSJ, *passim*.

3. Konkretisierung von Dezentralität in Form eines Rechtsprinzips

3.1 Rechtsprinzip

a. Begriff und Normativität

Der Begriff des Rechtsprinzips wird in der Literatur oft nicht erklärt. Alternativ ist auch die Rede von Rechtsgrundsätzen oder Rechtskonzepten. In der Folge bleiben die Begriffe trotz zentraler Stellung regelmässig undefiniert.²⁹⁹⁷

Zu den allgemein anerkannten Rechtsprinzipien zählen etwa das Vertrauensprinzip, das Prinzip der Vertragsfreiheit, die Kausalität und das Verschulden im Privatrecht sowie das Legalitäts- und Verhältnismässigkeitsprinzip und das Gebot von Treu und Glauben im öffentlichen Recht.²⁹⁹⁸

Der *normative Gehalt* von Rechtsprinzipien ist nicht immer eindeutig.²⁹⁹⁹ Die Flexibilität in der Verwirklichung von Rechtsprinzipien unterscheidet sie von Rechtsnormen, welche angewendet werden wollen.³⁰⁰⁰ Aus gewissen Verfassungsprinzipien müssen die staatlichen Organen einerseits grundlegende Verhaltensanweisungen ableiten (z.B. Art. 5 BV).³⁰⁰¹ Andererseits kommen verfassungsmässigen (Struktur-)Prinzipien nach allgemeiner Auffassung keine oder nur eine begrenzte Rechtswirkung zu (z.B. das Subsidiaritätsprinzip in Art. 5a BV).³⁰⁰² In der EU stellt das Subsidiaritätsprinzip gemäss Art. 5 Abs. 3 EUV demgegenüber ein genügend konkretisiertes Rechtsprinzip dar, das mit rechtlichen Mitteln durchgesetzt werden kann.³⁰⁰³ Auch die Diskussionen um die Einführung eines allgemeinen Anlegerschutzprinzips ins Schweizer Finanz-

²⁹⁹⁷ Vgl. etwa Kübler, Effizienz als Rechtsprinzip, *passim*; Gleeson, Legal Concept of Money, *passim*.

²⁹⁹⁸ Siehe Tschentscher, Grundprinzipien des Rechts, 18.

²⁹⁹⁹ Vgl. zur Menschenwürde Kley, in: Schwinges, Menschenwürde als Rechtsprinzip, 278; ferner zum programmatischen, jedoch auch teilweise justiziablen Charakter des umweltrechtlichen Vorsorgeprinzips Griffel, 28–30.

³⁰⁰⁰ Siehe Emmenegger/Tschentscher, in: BK ZGB, 2012, Art. 1 N 508–513.

³⁰⁰¹ Siehe Biaggini, in: Biaggini/Gächter/Kiener, § 7 N 18.

³⁰⁰² Siehe Biaggini, in: Biaggini/Gächter/Kiener, § 8 N 36, 38–39.

³⁰⁰³ Siehe Kley, in: Biaggini/Gächter/Kiener, § 10 N 20.

marktrecht kreisen um die Frage der Normativität eines solchen Prinzips.³⁰⁰⁴ Was den Rechtsprinzipien allerdings gemein ist, ist ihr «systembildende[r] Charakter».³⁰⁰⁵

Der Dezentralität als noch zu entwickelndes Rechtsprinzip soll nach vorliegender Auffassung im Grundsatz normativer Gehalt zukommen. Die Normativität des Prinzips stützt sich auf die zahlreichen Konkretisierungen des Ordnungsprinzips der Dezentralität im positiven Recht: Einerseits anerkennt das schweizerische Verfassungsrecht die Dezentralität als Ordnungsprinzip in der Wirtschafts- und politischen Ordnung. Andererseits finden sich auch Ausprägungen der Dezentralität im Zivilrecht und nunmehr besonders im Wertpapierrecht, wobei sich, wie gesehen, letztere Erscheinungsformen direkt auf das Finanzmarktrecht auswirken.³⁰⁰⁶ Zumindest in Bezug auf das Wertpapier- und Finanzmarktrecht scheint sich darum eine normative Dimension des Rechtsprinzips zu rechtfertigen.

b. Konsequenzen eines solchen Rechtsprinzips

Die Anerkennung der Normativität des Rechtsprinzips der Dezentralität führt zu einer Situation, in welcher der Schleier der dezentralen Entität nicht durchstoßen und in der Folge nicht auf die dahinterstehenden Einzelteile durchgegriffen wird (*pars pro toto*), sondern die Rechtsordnung die Eigenständigkeit der Entität von der sie ausmachenden Personen anerkennt und akzeptiert (*totum pro parte*).³⁰⁰⁷ Damit ist die Feststellung verbunden, dass die Teilnehmer eines dezentralen Systems nicht die alleinige Verantwortung für die «Handlungen» des Systems tragen können.

Dies heisst indessen nicht, dass einer dezentralen Entität Rechtspersönlichkeit oder der Charakter einer Rechtsgemeinschaft zukommen muss oder dass staatliche Behörden oder private Kläger nicht ausnahmsweise auf die System-

³⁰⁰⁴ Siehe Sethe, Anlegerschutz, 114–115, der zwischen Anlegerschutz entweder als Rechtsprinzip oder lediglich als einen Systembegriff differenziert; ferner Zobl/Kramer, Kapitalmarktrecht, Rz. 32 m.Verw. auf Hopt, Kapitalanlegerschutz, *passim*; ferner Zobl, in: Forstmoser/Tercier/Zäch, Vermögensverwaltungsauftrag der Banken, 329.

³⁰⁰⁵ So Emmenegger/Tschentscher, in: BK ZGB, 2012, Art. 1 N 97, die an dortiger Stelle von Rechtsgrundsätzen sprechen; vgl. in rechtstheoretischer Hinsicht auch Mahlmann, Rechtsphilosophie und Rechtstheorie, § 13 N 17–18.

³⁰⁰⁶ Siehe oben, [VII.2](#).

³⁰⁰⁷ Ähnlich Buckley/Arner/Zetzsche, FinTech, 126–127, welche die «node perspective» (Teilnehmer) von der «ledger perspective» (Netzwerk bzw. System) unterscheiden; demgegenüber kritisch Schwinger, New York Law Journal 2023, *passim*.

teilnehmer direkt zurückgreifen können. Dies ist etwa bei offensichtlichem Missbrauch der Berufung auf die Dezentralität eines Systems der Fall, wenn die Teilnehmer derselben wirtschaftlichen Gruppe angehören, d.h. von Anfang an keine Dezentralität oder Verteiltheit vorliegt.

Dezentrale Systeme sollen angesichts ihrer globalen Natur das interpersonale Vertrauen auf das notwendige Minimum reduzieren – darin liegt der sozioökonomische (Mehr-)Wert von Blockchains und ihrer Governance.³⁰⁰⁸ Dennoch ist es unerlässlich, dass die fundamentalen Regeln des gesellschaftlichen Zusammenlebens auch von dezentralen Entitäten beachtet werden.³⁰⁰⁹

Es heisst aber umgekehrt, dass Teilnehmer eines dezentralen Systems sich in guten Treuen in *justiziable* Weise auf die Realität solcher Systeme berufen können. Ein «Durchgriff» für systematische Aktivitäten scheitert mit anderen Worten am Rechtsprinzip der Dezentralität.

c. Feststellung der Konkretisierungsbedürftigkeit

In der Literatur lassen sich keine konkreten Angaben zur Frage finden, ab welchem Grad an Dezentralität ein Netzwerk und besonders eine Handelsplattform als genügend dezentral gelten. Illustrativ ist etwa der Vorwurf, dass Dezentralität in technischer Hinsicht lediglich antonymisch, d.h. indirekt über den gegenteiligen Begriff der Zentralität bestimmt werden könne.³⁰¹⁰

Der Grad der Dezentralität ist auch in rechtlicher Hinsicht *konkretisierungsbedürftig*. Dies wurde auch in der Vernehmlassung zur DLT-Mantelrevision und zwar u.a. von der FINMA bemerkt.³⁰¹¹ Die Konkretisierung ist bedeutsam, um Dezentralität als Rechtsprinzip operabel zu machen. In der Literatur werden insb. unter der Bezeichnung eines Dezentralitätstests unterschiedliche Kriterien angeführt, die nachfolgend vertieft untersucht werden sollen.

³⁰⁰⁸ Siehe Shapiro, In defense of Szabo's Law, *passim*.

³⁰⁰⁹ Ähnlich etwa auch Zamfir, Against Szabo's Law, *passim*; ferner bereits Wood, *Allegality, passim*, der von «illegal entities» spricht, die sich zwar nicht um rechtliche Vorgaben «kümmern» müssen (und können), aber nicht losgelöst von sozialen Konventionen operieren können.

³⁰¹⁰ So Sheng, Let's ditch decentralized, *passim*.

³⁰¹¹ Vgl. EFD, Ergebnisbericht Vernehmlassung DLT 2019, 7; ferner SFTA, Vernehmlassung DLT-Gesetz, 3, deren Vertreter die Konkretisierung des Begriffs «distributed» in einer Verordnung oder einem Rundschreiben der FINMA forderten.

3.2 Dezentralitätstest

a. Vorschlag eines «Dezentralitätstests» in Lehre und Praxis

Die ausländische Lehre und Praxis haben verschiedentlich den Versuch unternommen, einen «Dezentralitätstest» zu entwickeln, welche unterstellte von nichtunterstellten Netzwerken oder Applikationen abgrenzen. Als Grundlage werden je nach Ansatz qualitative, quantitative oder eine Kombination solcher Kriterien verwendet.³⁰¹²

Dass die meisten dieser Tests mit Blick auf das US-amerikanische Wertpapierrecht entwickelt worden sind, liegt primär daran, dass die Abgrenzung zwischen zentralen und dezentralen Systemen nach aktueller SEC-Praxis massgeblich für die Unterstellung unter das Wertpapierrecht ist. Aussagen von Vertretern der SEC – und auch der CFTC –³⁰¹³ lassen vermuten, dass die Aufsichtsbehörde der Dezentralität als Rechtsprinzip einen massgeblichen Stellenwert einräumt:

«If the network on which the token or coin is to function is sufficiently decentralized – where purchasers would no longer reasonably expect a person or group to carry out essential managerial or entrepreneurial efforts – the assets may not represent an investment contract. [...] And, as with Bitcoin, applying the disclosure regime of the federal securities laws to current transactions in Ether would

³⁰¹² Siehe für primär quantitative Analysen Srinivasan, Quantifying Decentralization, *passim*; Helmy, Measuring Bitcoin's Decentralization, *passim*; Muzzy/Anderson, Measuring Blockchain Decentralization, *passim*; demgegenüber für primär qualitative Untersuchungen Garcia/Leung, Ketsal Open Standards, insb. 5–8, 24, die zwischen «computational centralization», «economic centralization» und «political centralization» unterscheiden; Rettig, Decentralization, *passim*; sodann insb. in Bezug auf Eigenschaften der Gewährleistung von Privatsphäre Troncoso et al., Proceedings on Privacy Enhancing Technologies 2017, 309–313, 320, 323–324; ferner in regulatorischer Hinsicht Henderson/Raskin, Columbia Business Law Review 2019, insb. 459–469, 489–490, welche den Howey-Test u.a. zum «Bahamas Test» weiterentwickeln, der auf die Existenz von zentralen Kontrollstrukturen abstellt; sodann Peirce, Proposal to Fill the Gap Between Regulation and Decentralization, *passim*, welche eine Safe-Harbor-Regel vorschlägt, welche unter Einhaltung gewisser regulatorischer Bedingungen den Entwicklerteams die Möglichkeit gibt, während einer Frist von drei Jahren ein dezentrales Netzwerk zu entwickeln («network maturity»); schliesslich basierend auf einem Modell der relativen Stimmkraft in der Governance einer DAO Brukham, Blockchain voters, *passim*.

³⁰¹³ So zitiert in De, CFTC Chairman Heath Tarbert, Coindesk, *passim* («The more decentralized it becomes over time and the more that it effectively runs itself, the more likely it is it's going to fall within the commodity category and not the securities [group].»).

*seem to add little value. Over time, there may be other sufficiently decentralized networks and systems where regulating the tokens or coins that function on them as securities may not be required. And of course there will continue to be systems that rely on central actors whose efforts are a key to the success of the enterprise. In those cases, application of the securities laws protects the investors who purchase the tokens or coins.»*³⁰¹⁴

In Präzisierung der langjährigen Howey-Praxis des Obersten Gerichtshofs der Vereinigten Staaten³⁰¹⁵ soll demnach ein allfälliger Dezentralitätstest möglichst eindeutige Prognosen zur Rechtsnatur von Kryptovermögenswerten als «Investment Contracts» bzw. «Securities» erlauben.³⁰¹⁶ Dabei steht insb. die Frage im Zentrum, ob der Erwerber eines Token sich ausschliesslich oder hauptsächlich auf die unternehmerischen Leistungen Dritter, namentlich insb. des Veräusserers des Tokens, verlässt.³⁰¹⁷ Dadurch wird eine Annäherung des Dezentralitätsbegriffs an eine Bedingung der Howey-Analyse erreicht («profits to come solely from the efforts of others»).

Über die konkreten Anforderungen des Dezentralitätstests besteht aber bis heute wenig Einigkeit. Die US-amerikanischen Aufsichtsbehörden haben bisher auch keinen eigentlichen Test formuliert. Die heute in der Literatur und Industrie wohl überwiegend vertretene Auffassung ist, dass bitcoin und ether keine Securities sind und deshalb einem allfälligen Dezentralitätstest der SEC standhalten würden. Angesichts der Offenheit des Howey-Tests war dies aber anfänglich noch sehr umstritten.³⁰¹⁸ Ob weitere Protokolle rechtlich wie Bitcoin und Ethereum zu behandeln sind, ist offen und teils, wie im Falle von

³⁰¹⁴ Hinman, When Howey Met Gary, *passim*; ebenso Peirce, Proposal to Fill the Gap Between Regulation and Decentralization, *passim*.

³⁰¹⁵ Siehe U.S. Supreme Court, SEC vs. W.J. Howey Co. et al., 301 («The test is whether the scheme involves an investment of money in a common enterprise with profits to come solely from the efforts of others.»).

³⁰¹⁶ Eine Nichtunterstellung unter das Wertpapierrecht ist selbst dann angezeigt, wenn die Token eines genügend dezentralisierten Netzwerks grundsätzlich regulierte Securities oder Investment Contracts darstellen (würden); vgl. hierzu Shapiro, Open letter to SEC Commissioner Peirce, *passim*; zurückhaltender hingegen Guseva, The Journal of Corporation Law 2021, 686 («decentralization is merely one of the variables»).

³⁰¹⁷ Vgl. SEC, Framework Digital Assets, 2–3. Auch für den Schweizer Effektenbegriff wird in der Literatur argumentiert, dass ab einem gewissen Grad an Dezentralität keine Effekte mehr vorliegen könne; vgl. Mauchle, GesKR 2022, 192–193; Abbühl, iusNet BR-KR 23.12.2021, *passim*.

³⁰¹⁸ Vgl. etwa stanfordlawschool, Professor Grundfest on Bitcoin, Youtube, *passim*.

Ripple, Gegenstand von Klageverfahren.³⁰¹⁹ Die SEC sieht dies nun allerdings anders.³⁰²⁰

Ein sinnvoller Ansatz zur Messung von Dezentralität ist nach vorliegender Ansicht der Beizug quantitativer Metriken, die in einem zweiten Schritt anhand qualitativer Kriterien «bereinigt» werden.³⁰²¹ Konkret: Testrelevant ist damit, dass nicht etwa nur die Anzahl Full Nodes eines dezentralen Netzwerks von Relevanz ist, sondern auch die Tatsache, dass diese tatsächlich unabhängig voneinander betrieben werden.

Die Formulierung eines Dezentralitätstests bedarf gewisser *Orientierungspunkte*. Im Folgenden werden die beiden Konzepte der (i) Vertrauensminimierung und (ii) Entmachtung bzw. Kontrollverteilung (siehe weiter unten) als solche vorgestellt.

b. Vertrauensminimierung

Eine mögliche Herangehensweise an Dezentralität ist das Abstellen auf die in einem dezentralen System bestehenden Vertrauensbeziehungen.³⁰²² Im Zentrum der Betrachtung stehen Systeme, die kein Vertrauen (trustless) oder lediglich ein sehr verringertes Vertrauen (trust-minimized) voraussetzen. Damit gemeint ist interpersonales Vertrauen zwischen den an einem System beteiligten Personen. An die Stelle zwischenmenschlichen Vertrauens tritt Technologievertrauen. Subordination und Kooperation werden durch Koordination abgelöst. Als Basis dafür dienen kryptoökonomische Anreizsysteme, die mikroökonomisch aufgeladen werden.³⁰²³

TONY SHENG und BEN SPARANGO bilden zwecks Beschreibung von Dezentralität unterschiedliche Vertrauensmodelle. Danach ist die Dezentralität eines Protokolls tendenziell hoch, wenn die Teilnahme oder Nutzung des Protokolls kein

³⁰¹⁹ Siehe in Bezug auf der SEC-Klage gegen Ripple Chapparo, *Ripple lawsuit*, The Block, *passim*, wonach XRP und ETH rechtlich gleich zu behandeln sind; ferner Deaton, *Ethereum Free Pass*, *passim*.

³⁰²⁰ Das zu diesem Thema bedeutendste Verfahren ist Ende Februar 2024 vor erstinstanzlichem Gericht anhängig; vgl. U.S. District Court Southern District of New York, *SEC vs. Coinbase, Inc. et al.*, *passim*.

³⁰²¹ Gl.M. Walch, in: Brummer, *Deconstructing Decentralization*, 48, 59–60, die zu Recht davor warnt, dass rein quantitative Metriken ein falsches Bild erzeugen könnten; *umfassend* zum Stand der Literatur Anfang 2021 Sai et al., *Information Processing and Management* 2021, *passim*.

³⁰²² Siehe insb. Sheng/Sparango, *Trust Spectrum*, *passim*.

³⁰²³ Zum Ganzen oben, [II.5.3b.ii](#).

oder nur ein geringfügiges Vertrauen in eine andere involvierte Person (z.B. einen Entwickler oder Betreiber einer Plattform) voraussetzt.

Als relevante Vertrauensbereiche werden definiert:

Vertrauensbereich	Beschreibung
Verwahrung von Vermögenswerten	Diesem Vertrauensbereich ist Genüge getan, wenn Nutzer für die Aufbewahrung ihrer Vermögenswerte keiner Drittperson zu vertrauen haben. Dies umfasst auch die vorübergehende Aufbewahrung in einem Smart Contract bspw. zwecks Abwicklung eines Handelsgeschäfts. In diesem Fall dürfen die Entwickler eines Protokolls nicht einseitig auf die Vermögenswerte zugreifen können.
Manipulationsresistenz	Mit Manipulationsresistenz ist das Problem gemeint, dass sich Protokolländerungen negativ auf die übrigen Vertrauensbereiche auswirken können. Diesem Vertrauensbereich ist nur dann Genüge getan, wenn entweder keine relevanten Änderungen am Code vorgenommen werden können (z.B. Uniswap) oder aber Änderungen am Code über eine DAO mit genügend verteiltem Tokenbesitz erfolgen.
Nachweisbarkeit von Sicherheit	Im Wesentlichen ist die Vertrauenswürdigkeit eines Protokolls gewährleistet, wenn die Entwickler für die Entwicklung des Codes nachweisbar den Stand der Technik einhalten und insb. Code Audits durchführen. Der Softwarecode muss zudem öffentlich einsehbar sein.
Rechtliche und regulatorische Absicherung	Die Vertrauenswürdigkeit eines Protokolls ist höher, wenn Nutzer bei Verlusten und Hackerangriffen Rückgriff auf die Rechtsordnung nehmen können.
Versicherung	Das interpersonale Vertrauen kann schliesslich reduziert werden, wenn verloren gegangene oder gestohlene Vermögenswerte aufgrund eines Versicherungsmechanismus erstattet werden.

Im Wesentlichen stellen die Autoren darauf ab, wie viel Vertrauen Nutzer aufbringen müssen, dass ihre Vermögenswerte sicher sind und nicht verloren gehen, und, falls diese doch verloren bzw. gestohlen gehen, ob und wie die Vermögenswerte wiedererlangt werden können. Als Relativierungen des Vertrauens werden bspw. der Diebstahl der Vermögenswerte durch den Betreiber oder einen Hacker, die Blockierung von Vermögenswerten durch den Betreiber, etwa aufgrund einer rechtlichen Anordnung oder eines Softwarefehlers, die Aneignung von Kontrolle über Vermögenswerte aufgrund von Änderungen des Protokolls sowie das Fehlen einer Versicherung der Vermögenswerte im

Falle des Verlusts erwähnt.³⁰²⁴ Gerade im letzten Punkt besteht eine wichtige Differenz zum nachfolgend dargestellten «Entmachtungstest».

Bei den von den beiden Autoren entwickelten Dezentralitätstest handelt es sich in erster Linie um eine qualitative Analyse.

c. Entmachtung bzw. Kontrollverteilung

i. Einleitung

Sodann kann Dezentralisierung auch als Entmachtung verstanden werden. Dabei ist zu erwähnen, dass in der Neoklassischen Ökonomik Macht kein eigenständiges Konzept darstellt.³⁰²⁵ Sodann wird Macht als verteilt wahrgenommen, wenn ein Markt wettbewerblich organisiert ist. Macht kommt demnach ökonomisch nur eine Bedeutung zu, wenn sie ungleich verteilt ist, wie etwa im Falle monopolistischer oder oligopolistischer Marktstrukturen.³⁰²⁶

Allerdings findet Macht im Prinzipal-Agenten-Modell der Neuen Institutionenökonomik Niederschlag. So kann etwa opportunistisches Verhalten einer Vertragspartei Ausdruck von Macht sein.³⁰²⁷ In rechtswissenschaftlicher Hinsicht bietet es sich sodann an, anstelle der Verwendung des Machtbegriffs von Kontrolle zu sprechen.³⁰²⁸ Kontrollbegriffe sind bereits in verschiedenen Rechtsgebieten gebräuchlich, namentlich im Konzern- und Börsengesellschaftsrecht.³⁰²⁹ Inhaltlich sollen die beiden Orientierungshilfen vorliegend allerdings gleichgesetzt werden.

ii. Machtbereiche

Vorliegend von besonderem Interesse ist der von GABRIEL SHAPIRO entwickelte Dezentralitätstest.³⁰³⁰ Der Autor formuliert beruhend auf einem Machtbegriff

³⁰²⁴ Siehe Sheng/Sparango, *Trust Spectrum*, *passim*.

³⁰²⁵ Kritisch darum Granovetter, *American Journal of Sociology* 1985, 501–502.

³⁰²⁶ Siehe hierzu kritisch Furubotn/Richter, *New Institutional Economics*, 15–17.

³⁰²⁷ Siehe Furubotn/Richter, *New Institutional Economics*, 186–187 m.w.H.

³⁰²⁸ So etwa Cohen/Angelovska-Wilson/Strong, *Decentralized Finance*, *passim*; SBF, Circular 2020/01, 9.

³⁰²⁹ Vgl. etwa Art. 963 Abs. 2 OR und Art. 120 Abs. 1 FinfraG i.V.m. Art. 10 Abs. 1 FinfraV-FINMA.

³⁰³⁰ Siehe Shapiro, *Defining Decentralization*, *passim*; ähnlich Vergne, *Envisioning Decentralization Strategically*, *passim*, der unter Dezentralisierung die Möglichkeit versteht, auf Informationen zuzugreifen und zum Entscheidungsprozess beizutragen («authority dispersion»).

(Power) einen rechtlich relevanten Test für dezentrale Netzwerke.³⁰³¹

SHAPIRO unterscheidet taxonomisch zwischen den folgenden fünf Machtbereichen.³⁰³²

Machtbereich	Beschreibung
Validation Power	Dieser Machtbereich genügt dem Dezentralitätstest, wenn es Netzwerkteilnehmern möglich ist, einerseits autonom Transaktionen zu validieren und andererseits den Softwarecode einzusehen. Während der zweite Punkt der Quelloffenheit bei Open-Source-Protokollen grundsätzlich erfüllt ist, sind nicht alle verteilte Register gleichermaßen technisch einfach validierbar. Gewisse Blockchains bedürfen in der Praxis sehr grosser Rechenkapazitäten (z.B. Solana),³⁰³³ weshalb sie in diesem Machtbereich grundsätzlich als weniger dezentral zu betrachten sind.³⁰³⁴
Consensus Power	Die Consensus Power ist ausreichend dezentralisiert, wenn Konsensfindung durch eine Vielzahl von Personen erfolgt, die nicht miteinander verbunden sind. Dies setzt zudem voraus, dass der Eintritt in das Netzwerk nicht von formalen Kriterien abhängig ist (z.B. regulatorischer Bewilligungsstatus) und keiner Bewilligung durch eine Drittperson (i.d.R. eine zentrale Autorität) bedarf.³⁰³⁵ Grundsätzlich gehen alle Konsensmodelle von der Annahme aus, dass eine Mehrheit der Netzwerkteilnehmer, welche diese Funktion ausüben, ehrlich agieren muss, damit das Protokoll stabil ist. Technisch wird dies durch kryptoökonomische Anreize sichergestellt. Historisch haben Proof-of-Work-Protokolle (z.B. Bitcoin und Ethereum) trotz der vielgeübten Kritik an gewissen Zentralisierungstendenzen³⁰³⁶ einen relativ hohen Grad an Dezentralität in diesem Bereich erreicht. Eine gewisse Zentralisierung ist wohl in der Praxis kaum vermeidbar, weisen doch Spezialisierungs- und Netzwerkeffekte bedeutende Vorteile gegenüber vollständiger Dezentralisierung des Netzwerks auf.

³⁰³¹ Ähnlich Cambridge Centre for Alternative Finance, Distributed Ledger Technology, 45 («power dynamics»); Sheng, Let's ditch decentralized, *passim*; Lewis, Authority, Twitter, *passim* («In its simplest definition, decentralization is the degree to which an entity within the system can resist coercion and still function as part of the system.»); ferner wohl auch Bodó/Brekke/Hoepman, Internet Policy Review 2021, 8–9; kritisch demgegenüber Omarova, Journal of Financial Regulation 2020, 91–92.

³⁰³² Siehe Shapiro, Defining Decentralization, *passim*.

³⁰³³ Siehe etwa die Analyse von Jameson Lopp, 2021 Altcoin Node Sync Tests, 1. August 2021, <https://blog.lopp.net/2021-altcoin-node-sync-tests/>.

³⁰³⁴ So etwa auch Garcia/Leung, Ketsal Open Standards, 9, 11, 19–20.

³⁰³⁵ Siehe Henderson/Raskin, Columbia Business Law Review 2019, 466.

³⁰³⁶ Dies als kritischen Punkt betrachtend Garcia/Leung, Ketsal Open Standards, 16; ferner Muzzy/Anderson, Measuring Blockchain Decentralization, *passim*.

	Massgeblich ist hier letztlich die wirtschaftliche und rechtliche Unabhängigkeit der Netzwerkteilnehmer, welche die Konsensfunktion ausüben. Vorfälle, wie sie etwa bei EOS' Delegated Proof-of-Stake aufgetreten sind,³⁰³⁷ stellen in rechtlicher Hinsicht die Dezentralität der Konsensfindung infrage.
Protocol/ Client Power	Dieses Kriterium genügt dem Dezentralitätstest, wenn die Entwicklung des Protokolls sowie der Client-Implementierungen durch eine Mehrzahl von Personen erfolgt, die nicht miteinander verbunden sind.³⁰³⁸ Im Idealfall bestehen mehrere Client-Implementierungen desselben Protokolls, wodurch der Einfluss der jeweiligen Entwicklergruppe auf den ausgeführten Netzwerkcode abnimmt.³⁰³⁹ Im Rahmen der SEC-Klage gegen Ripple Labs, der Entwicklerin des Ripple Netzwerks, wurde das Argument der konzentrierten Protocol Power ausdrücklich angerufen.³⁰⁴⁰ Wiederum steht hier die wirtschaftliche und rechtliche Unabhängigkeit der Entwickler eines Protokolls oder Software Clients im Fokus. Protokolle, die praktisch ausschliesslich von Entwicklern programmiert werden, die bei bestimmten Rechtsträgern (z.B. einer Stiftung oder einem Unternehmen) angestellt sind, weisen tendenziell eine höhere Protocol/Client Power auf. Anders verhält es sich typischerweise bei Protokollen, die von einer Vielzahl von Personen aus einer offenen Entwicklungsgemeinschaft entwickelt und deren Arbeiten aus unterschiedlichen Quellen finanziert werden, wie dies etwa bei Bitcoin der Fall ist. Die Protocol/Client Power kann abhängig von den konkreten Umständen sehr unterschiedlich ausfallen. Zu denken ist insb. an Upgrades, die aufgrund eines Softwarebugs innert kürzester Frist durchgeführt werden müssen, um das System vor einem grösseren Schaden zu bewahren.³⁰⁴¹ In diesen Fällen, in denen ein Informationsungleichgewicht zugunsten der Entwicklergemeinde bestehen kann, wird die Dezentralität vorübergehend relativiert.³⁰⁴²

³⁰³⁷ Siehe hierzu oben, [IV.3.10a](#).

³⁰³⁸ Zurückhaltender BA, The Hinman Token Standard, Medium, *passim* («[...] having some level of centralized leadership will not condemn a token to being classified as a security on that basis alone.»).

³⁰³⁹ Vgl. in diesem Zusammenhang der mehrstündige Ausfall der Solana Blockchain, welche durch ein Softwareupdate des Entwicklerteams hinter der derzeit einzigen Client Implementierung behoben wurde, was dem Team u.U. gerade in einer Notsituation einen enormen Einfluss auf den Code des Netzwerks geben kann; ausführlich hierzu Shin, Solana's Outage, Unchained Podcast, *passim*.

³⁰⁴⁰ Siehe SEC, Complaint against Ripple Labs, Inc. et al., 44–45 («[...] not only are Ripple [Labs]'s touted efforts with respect to XRP significant, they are essential to the success or failure of the enterprise.»).

³⁰⁴¹ Siehe Walch, New York University Journal of Law & Business 2021, 702–703.

³⁰⁴² In einem solchen Fall kann der Howey-Test, dessen Motivation die Informationseffizienz der Kapitalmärkte ist, bedeutsam werden, vgl. Brummer, Stanford Journal of Blockchain Law & Policy 2022, 145.

	Ferner kommt dem Umstand, dass Satoshi Nakamoto als Begründer von Bitcoin anonym geblieben ist, erhöhte Bedeutung für die Dezentralität des Netzwerks zu. Dies verhinderte, dass die hinter dem Pseudonym stehende Person eine Führungsrolle für die Governance des Netzwerks entwickeln konnte.³⁰⁴³ Das «Satoshi-Modell» kann als ideal für den Start eines Protokolls eines dezentrales Systems betrachtet werden. Eher unwahrscheinlich, aber nicht ausgeschlossen ist, dass die Entwicklungstätigkeit rechtlich einklagbare Ansprüche gegen einzelne Entwickler oder deren Arbeit- und Auftraggeber begründen kann.³⁰⁴⁴ Dies würde mutmasslich dazu führen, dass die Protocol/Client Power kleiner, aber nicht zwingend dezentraler würde,³⁰⁴⁵ wobei der konkrete Effekt wohl letztlich von der Ausgestaltung der Haftung abhinge.³⁰⁴⁶ Zudem können Reputationsmechanismen eine bedeutende Rolle spielen, wobei diese allerdings in rechtlicher Hinsicht nur schwer fassbar sind. On-Chain-Governance von Protollupdates (z.B. Tezos) kann schliesslich u.U. die Protocol/Client Power von Entwicklern verringern. Allerdings kann in diesem Fall der Machtbereich der Economic Power (siehe sogleich) problematischer sein.
Economic Power	Die Economic Power ist ausreichend dezentralisiert, wenn einzelne Nutzer oder Entwickler nicht imstande sind, aufgrund ihres Tokenbesitzes oder Zugriffs auf Finanzmittel, die etwa aus einem ICO stammen, wesentlichen Einfluss auf den Preis eines Token oder die Weiterentwicklung des Protokolls oder sonstiger relevanter Software auszuüben. Die Economic Power ist ausserhalb der Tokenbesitzverhältnisse ein relativ schwer bestimmbarer Faktor. Wo Entscheidungsmacht allerdings an den Tokenbesitz anknüpft, wie etwa in Proof-of-Stake-Protokollen, bei On-Chain-Governance oder DAO-basierter Governance von dezentralen Applikationen, kommt der Economic Power eine erhöhte Bedeutung zu.³⁰⁴⁷ Auch der Besitz von Immaterialgüterrechten sollten unter diesem Gesichtspunkt Beachtung geschenkt werden. So kontrollieren etwa die Zcash Foundation und

³⁰⁴³ Vgl. zur Frage der Legitimität und von Führungspersonen als Schellingpunkte Andreotti, in: Kessler, Dezentrale Governance, 133–134.

³⁰⁴⁴ So etwa Walch, in: Hacker et al., Software Developers as Fiduciaries, 71–76; ferner auch oben, VI.3.3d.

³⁰⁴⁵ Siehe Haque et al., Stanford Journal of Blockchain Law & Policy 2019, 185 («Imputing fiduciary obligations to protocol developers may cause the protocol developers to take more authority over the network and subvert the purpose of public blockchains.»), 188, wo die Autoren davor warnen, die Haftung allzu weit auszudehnen, weil dadurch eine «corporate capture» des Protokolls erfolgen könnte.

³⁰⁴⁶ Vgl. auch Garcia/Leung, Ketsal Open Standards, 26.

³⁰⁴⁷ So auch Shapiro, Defining Decentralization, *passim* («[...] in any legal test for determining decentralization, economic power should be assessed the most stringently of any of the forms of power over a blockchain system.»).

	Electronic Coin Company zusammen die Markenrechte an der gleichnamigen Kryptowährung.³⁰⁴⁸ Die Gefahr einer Hard Fork mag unter diesen Umständen nur bedingt disziplinierende Wirkung auf Parteien mit grösserer Economic Power haben. Economic Power ist stark mit dem wirtschaftlichen Phänomen von Rent Seeking verbunden. Dabei steht weniger die Vernetzung der Beteiligten im Vordergrund als die Möglichkeit, durch entsprechendes Stimmverhalten die Entwicklung des Protokolls im eigenen Interesse voranzutreiben oder sich vorhandene Geldmittel im eigenen Interesse anzueignen.³⁰⁴⁹
User Power	Schliesslich ist für den Dezentralitätstest auch die User Power zu berücksichtigen. Dabei handelt es sich um die Fähigkeit von Nutzern, sich gegen die vorhin erwähnten Machtbereiche effektiv zur Wehr setzen zu können. User Power ist in den heutigen dezentralen Systemen eher ein «Korrektiv» der übrigen Machtbereiche. Die User Power manifestiert sich etwa darin, dass Netzwerkteilnehmer Protokollupdates autonom auszuführen haben und entsprechend selbst über die Teilnahme an einer Fork entscheiden können. Beispielhaft sind hier die Aktivierung von SegWit und die Hard Fork von Bitcoin Cash zu erwähnen sowie die The DAO Hard Fork von Ethereum. In diesem Fällen übte die Nutzergemeinschaft mithilfe der Entwickler (Protocol/Client Power) einen wesentlichen Einfluss auf die Evolution des Netzwerks aus, und zwar auch gegenüber der Machtbereiche von Consensus Power und Economic Power. Die oft anzutreffende Schwierigkeit der effektiven Ausübung von User Power ist in der Koordination kollektiver Handlungen begründet. Das Aufkommen von DeFi hat die User Power allerdings nachhaltig verändert: Da die Wertschöpfung offener und interoperabler Protokolle und Smart Contracts zu einem wesentlichen Grad voneinander abhängig ist, ist zu erwarten, dass der Wille zur autonomen Ausübung von User Power nur noch sehr zurückhaltend vorhanden ist.³⁰⁵⁰

d. Fazit

Eine theoretisch problematische Machtballung in einem der erwähnten Bereiche stellt in der Praxis nicht zwingend die rechtlich relevante Dezentralität des Netzwerks infrage. Dasselbe gilt grundsätzlich auch für die Perspektive der Vertrauensminimierung.

³⁰⁴⁸ Siehe Wilcox, Final text of ZIP 1014, *passim*.

³⁰⁴⁹ Siehe etwa für das kontroverse Beispiel des DeFi Education Funds, der durch einen Governance-Entscheid der Community mit Mitteln aus der Uniswap Treasury ausgestattet wurde, HarvardLawBFI, Governance Proposal DeFi Education Fund, *passim*.

³⁰⁵⁰ Siehe Qureshi/Lee, Ethereum is now unforkable, *passim*.

Konkret weisen die meisten Blockchain-Protokolle eine relativ ausgeprägte Konsolidierung im Consensus Power-Bereich auf, was in der Praxis aber etwa in Bitcoin aufgrund der kryptoökonomischen Anreize von Minern und der Möglichkeit der übrigen Netzwerkteilnehmer, ein abweichendes Protokoll zu verwenden, kaum ins Gewicht fällt.³⁰⁵¹ Andererseits ist zu ergänzen, dass die unterschiedlichen Machtbereiche in einer Gruppe von Personen, die miteinander verbunden sind, zusammenlaufen können. So könnten Miner in einem Proof-of-Work-Protokoll nicht nur über die Mehrheit der Consensus Power verfügen, sondern durch entsprechende Entwicklungsprogramme (Grants etc.) auch wesentlich die Entwicklung des Protokolls beeinflussen (Protocol/Client Power) oder aber die bedeutendsten Handelsplattformen betreiben (Economic Power und User Power).

Gewisse Elemente, wie noch auszuführen sein wird, können allerdings auch auf dezentrale Handelsplattformen übernommen werden.³⁰⁵² So kann insb. der Machtbereich der Protocol/Client Power auf Smart Contracts und dort insb. auf Admin Keys und ähnliche Mechanismen ausgedehnt werden. Smart Contracts, die für relevante Funktionen einer dezentralen Handelsplattform verantwortlich sind und letztlich von einem Entwicklerteam kontrolliert werden, können im Lichte des Dezentralitätstests problematisch sein. Dies ist insb. dann der Fall, wenn die miteinander verbundenen Inhaber von Admin Keys auf Kryptovermögenswerte der Nutzer zugreifen oder Updates der Smart Contracts durchführen können, welche deren Vermögenswerte gefährden würden.³⁰⁵³ Auf diese Punkte ist im Rahmen der Formulierung eines Dezentralitätstests für Handelsplattformen zurückzukommen.³⁰⁵⁴

Rechtlich relevant ist letztlich eine *Gesamtbetrachtung* der Machtbereiche des zu untersuchenden dezentralen Systems.³⁰⁵⁵ Im Rahmen dieser Gesamtbetrachtung sind schliesslich auch die gegenseitigen Abhängigkeiten dezentraler Applikationen zu berücksichtigen, wie etwa einer dezentralen Handelsplattform von einem (zentralisierten) Orakel. In der Literatur wurde dafür der Begriff der «centralization inheritance» eingeführt.³⁰⁵⁶

³⁰⁵¹ Siehe hierzu oben, [IV.5.2c.iii](#).

³⁰⁵² *Zustimmend* Shapiro, Open letter to SEC Commissioner Peirce, *passim*, der fordert, dass dezentrale Handelsplattformen bei genügender Dezentralisierung sich nicht als Security Exchange bzw. Alternative Trading System zu registrieren haben. Siehe ferner unten, [VII.4](#).

³⁰⁵³ Ähnlich Shapiro, Defining Decentralization, *passim*.

³⁰⁵⁴ Siehe hierzu unten, [VII.4.2](#).

³⁰⁵⁵ So auch Garcia/Leung, Ketsal Open Standards, 8; ferner Finck, Blockchain Regulation, 205–206.

³⁰⁵⁶ Siehe Schuler/Cloots/Schär, DeFi and On-Chain CeFi, 9.

3.3 Konkretisierung der Dezentralität am Beispiel eines dezentralen Netzwerks

a. Vorbemerkung

Der vorhergehende Abschnitt ist u.a. auf die beiden Orientierungspunkte der Vertrauensminimierung und Entmachtung bzw. Kontrollverteilung näher eingegangen. Dabei hat sich herausgestellt, dass ein auf dem Kontrollbegriff fussender Dezentralitätstest besser geeignet ist, zur Konkretisierung des Rechtsprinzips Dezentralität beizutragen. Nachfolgend werden die unterschiedlichen Komponenten der Dezentralität eines (dezentralen) Netzwerks anhand des Kontrollbegriffs genauer untersucht.

b. Vielzahl von Netzwerkteilnehmern

Ein dezentrales Netzwerk muss von einer *Vielzahl von Personen* gemeinschaftlich verwaltet werden. Unklar ist, ab welcher Grössenordnung von einer Vielzahl von Personen gesprochen werden kann. Die Botschaft zur DLT-Revision verwendet ebenfalls keine konkreten Zahlen, sondern spricht von einem «Mindestmass an Dezentralisierung».³⁰⁵⁷ Klar ist, dass es sich nicht zwingend um hunderte oder sogar tausende Netzwerkteilnehmer handeln muss. Materiell wichtiger ist, dass die Teilnehmer voneinander unabhängig sind (siehe hierzu sogleich).

Allerdings muss auch hervorgehoben werden, dass Netzwerke, wie etwa Bitcoin und Ethereum, heute von mehreren tausenden Teilnehmern gemeinschaftlich unterhalten werden. Bitcoin bspw. weist eine Netzwerkgrösse von mehr als zehntausend Full Nodes auf, d.h. von Computern, welche eine vollständige Kopie des verteilten Registers führen und die Protokollregeln autonom durchsetzen. Die *geografische* Verteilung der Full Nodes ist dabei global, was ebenfalls einen positiven Effekt auf die Dezentralität eines Netzwerks hat.³⁰⁵⁸ Eine geografische Zentralisierung kann etwa drohen, wenn ein Grossteil der Teilnehmer eines Netzwerks für die Ausführung der Software auf dasselbe Rechenzentrum oder sogar denselben Anbieter solcher Dienstleistungen (z.B. Amazon Web Services) zurückgreift.³⁰⁵⁹

³⁰⁵⁷ Siehe oben, [VII.2.5c](#).

³⁰⁵⁸ Siehe für aktuelle Statistiken zum Bitcoin Netzwerk <https://bitnodes.io/>; zum Ethereum Netzwerk <https://www.ethernodes.org/>.

³⁰⁵⁹ Vgl. etwa Malwa, Centralized Services, Decrypt, *passim*.

Der Massstab sollte nach vorliegender Ansicht nicht allzu tief angesetzt werden. Insb. haben Netzwerke mit Konsensmechanismen, wie etwa Delegated Proof-of-Stake (DPoS), je nach Ausgestaltungsweise eine nicht zu vernachlässigende Wahrscheinlichkeit der Kollusion der beteiligten Netzwerkteilnehmer über die Zeit. Ein praktisches Beispiel mit mehreren solchen Vorfällen ist etwa die Blockchain EOS mit ihren 21 an der Konsensbildung beteiligten Delegierten.³⁰⁶⁰

Die konkrete Anzahl an Teilnehmern sollte sich folglich daran messen, dass diese nur unter sehr erschwerten Bedingungen sich koordinieren und somit gegen die Interessen der übrigen Teilnehmer und der Nutzer kolludieren können.³⁰⁶¹ Die anonyme Teilnahme kann mit anderen Worten die Dezentralität eines Netzwerks verbessern. Allerdings erschwert sie auch sinnvolle und damit «gute» Koordination, wie z.B. die Durchführung eines Protokollupgrades nach Entdeckung einer Schwachstelle in der verwendeten Software.

c. Unabhängigkeit der Netzwerkteilnehmer

Die Feststellung, dass eine Vielzahl von Computern an einem Netzwerk beteiligt sind, kann lediglich den Anfang einer Analyse bilden. Das Verhalten dieser Vielzahl von Computern kann u.U. von ein und derselben Gruppe von Personen gesteuert werden. In einem zweiten Schritt ist darum zu fordern, dass die beteiligten Entitäten auch *effektiv von unterschiedlichen Personen kontrolliert werden*.³⁰⁶² Hieran wird deutlich, dass Dezentralität in erster Linie als eine Frage der verteilten Kontrolle bzw. dezentralen Entscheidungsautonomie zu verstehen ist.

Die Botschaft zur DLT-Mantelrevision führt aus, dass die einzelnen Netzwerkteilnehmer *voneinander unabhängig* sein müssen.³⁰⁶³ Dieser Auffassung folgt im Wesentlichen auch die Literatur.³⁰⁶⁴ Die Unabhängigkeit ist auch nach vor-

³⁰⁶⁰ Siehe hierzu die weiterführenden Hinweise oben, [IV.3.10a](#).

³⁰⁶¹ So auch Buterin, *Meaning of Decentralization*, Medium, *passim*.

³⁰⁶² So explizit SBF, Circular 2021/01, 8; ferner im Verfahren gegen E-Coins scheinbar auch FINMA, *Scheinkryptowährungen*, 2 («[...] wurden die 'E-Coins' ausschliesslich vom Anbieter kontrolliert und auf dessen lokalen Servern gespeichert.»); ferner Stampfli, Anforderungen an eine Blockchain, 37.

³⁰⁶³ Siehe oben, [VII.2.5c](#).

³⁰⁶⁴ Siehe u.a. SBF, Circular 2021/01, 8 («participants are mutually independent»); ebenso Kuhn, in: Weber/Kuhn, *Digitale Aktiven im schweizerischen Privatrecht*, Rz. 61; Kuhn et al., *Jusletter IT* vom 23. Mai 2019, Rz. 21 («abhängig von der Zahl und Art der Validatoren [...] sowie von allfälligen Abhängigkeiten zwischen diesen [...]»); Stengel, in: Reutter/Wer-

liegender Auffassung das zentrale Kriterium für die Dezentralität eines Netzwerks oder einer Applikation und darum wohl in den meisten Fällen die Knacknuss in regulatorischer Hinsicht. BUTERIN spricht angesichts der nicht immer einfach feststellbaren Unabhängigkeit der beteiligten Personen vom Prinzip der glaubwürdigen Neutralität solcher Systeme.³⁰⁶⁵

Vorab zu klären ist, was in diesem Zusammenhang unter *Netzwerkteilnehmern* verstanden wird. Wohl unbestrittenermassen sind diejenigen Netzwerkteilnehmer gemeint, welche an der Konsensbildung beteiligt sind, namentlich Miner und Staker.³⁰⁶⁶ Die Konzentration von Rechenkapazitäten bzw. Kapital in Form von Mining Pools bzw. Staking Pools ist ein Anhaltspunkt für zunehmende Zentralisierung innerhalb eines dezentralen Systems. Allerdings ist auch dem Umstand Rechnung zu tragen, dass individuelle Netzwerkteilnehmer (d.h. Miners und Stakers) typischerweise jederzeit den Pool wechseln können, weshalb die scheinbar bestehenden Abhängigkeiten zwischen den Netzwerkteilnehmern nicht zwingend die Dezentralität des Netzwerks infrage stellen müssen. Darüber hinaus sind nach vorliegender Ansicht auch Betreiber von Full Nodes, d.h. Netzwerkknoten, welche durch Ausführung des Protokolls die Konsensregeln selbständig überprüfen können, zu dieser Gruppe zu zählen. Ein Netzwerk, das hinsichtlich dieser beiden Funktionen von Personen betrieben würde, die voneinander abhängig sind, wäre offensichtlich ungenügend dezentralisiert.³⁰⁶⁷

Der Begriff der Unabhängigkeit weist zwei Elemente auf.³⁰⁶⁸ Netzwerkteilnehmer haben einerseits *rechtlich* voneinander unabhängig zu sein. D.h., es be-

len, Blockchain/Distributed Ledger Technology, 149, welche demgegenüber auf die Unabhängigkeit der Betreiber von den Parteien, d.h. Schuldner und Gläubiger, abstellt.

³⁰⁶⁵ Siehe Buterin, *Credible Neutrality*, *passim* («Mechanisms such as blockchains, political systems and social media are designed to facilitate cooperation across large, and diverse, groups of people. In order for a mechanism to actually be able to serve as this kind of common substrate, everyone participating must be able to see that the mechanism is fair, and everyone participating must be able to see that everyone else is able to see that the mechanism is fair, because everyone participating wants to be sure that everyone else will not abandon the mechanism the next day.»).

³⁰⁶⁶ So auch Botschaft DLT 2019, 281.

³⁰⁶⁷ Vgl. etwa ferner die Ausführungen des Bundesverwaltungsgerichts im Verfahren gegen E-Coins BVGer B-5769/2017 vom 21. Januar 2019, E. 3; ferner das Parallelverfahren BVGer B-6413/2017 vom 21. Januar 2019, E. 4.

³⁰⁶⁸ Vgl. auch Stampfli, *Anforderungen an eine Blockchain*, 22–23, der für den Unabhängigkeitsbegriff auf Art. 728 Abs. 1 OR zurückgreift. Nach vorliegender Auffassung ist dieser Analogieschluss jedoch abzulehnen, da Revisionsstellen und Netzwerkteilnehmer grundlegend verschiedene Funktionen ausüben und eine Unabhängigkeit dem Anschein nach für öffentliche Blockchains nicht massgeblich sein kann.

stehen keine vertraglichen oder sonstigen Rechtsbeziehungen, welche darauf ausgerichtet sind, die Entscheidungsautonomie der beteiligten Personen einzuschränken oder sogar zu verbieten. Problematisch könnte etwa das Eingehen gegenseitiger rechtlicher Verpflichtungen sein, in deren Rahmen sich Netzwerkteilnehmer ein bestimmtes Verhalten, etwa im Rahmen von Governance-Entscheidungen, zusichern. In diese Richtung geht etwa das «EOS User Agreement» zwischen den Blockproduzenten, das von der Community der EOS Blockchain angenommen wurde.³⁰⁶⁹ Allerdings sind darin keine klaren vertraglichen Pflichten zu einer Abstimmung des Verhaltens zu erkennen. Weitergehend ist sodann das «Network Operating Agreement» zwischen den Nutzern und Teilnehmern der Telos Blockchain. Diese Vereinbarung sieht vor, dass alle Streitigkeiten zwischen Nutzern und Teilnehmern des Netzwerks nach den Regeln eines zu wählenden Schiedsgerichts beizulegen und die Urteile von den Blockproduzenten zu vollstrecken sind.³⁰⁷⁰ Auch hierin werden, soweit ersichtlich, keine expliziten Abhängigkeiten zwischen den Teilnehmern statuiert. Es handelt sich in beiden Fällen wohl eher um unschädliche Koordination der Teilnehmer.

Darüber hinaus ist der Begriff der Unabhängigkeit auch in *wirtschaftlicher* Hinsicht zu verstehen. Es darf namentlich keine wesentlichen wirtschaftlichen Faktoren geben, aufgrund derer die Entscheidungsautonomie der beteiligten Personen infrage gestellt ist. Dabei kann es sich einerseits um blockchain-interne Faktoren handeln. Zu denken ist etwa an den Fall, dass eine einflussreiche Gruppe von Netzwerkteilnehmern Druck auf andere Netzwerkteilnehmer ausübt, indem sie ihnen androhen, deren Transaktionen oder die Transaktionen von bestimmten Nutzern vorübergehend oder permanent zu ignorieren. Falls die bedrängten Netzwerkteilnehmer ihr Verhalten in der Folge an dasjenige der Gruppe anpassen, spricht dies dafür, dass eine relevante wirtschaftliche Abhängigkeit besteht. Ein blockchain-externer Faktor könnte andererseits vorliegen, wenn Netzwerkteilnehmer für die Ausführung des Protokolls von einem Hardwareproduzenten abhängig sind, was diesem erlaubt, das Verhalten der Netzwerkteilnehmer mittelbar zu beeinflussen.

³⁰⁶⁹ Siehe eosnewyork, EOS User Agreement, *passim*; vgl. hierzu Stokes, EOS User Agreement, *passim*.

³⁰⁷⁰ Siehe Telos Blockchain Network Operating Agreement (TBNOA), *passim*; vgl. hierzu die Erläuterungen in Telos Foundation, Telos Governance Explained, *passim*.

d. Manipulationsresistenz von Daten

Die Manipulationsresistenz der Daten in einem verteilten Register ist eine zentrale Eigenschaft dezentraler Systeme. Das Gesetz spricht von der «Integrität des Wertrechtereigenschafts».³⁰⁷¹ Mit Integrität ist die Korrektheit oder Unversehrtheit der im verteilten Register abgelegten Daten gemeint, wobei darunter die vollständige und unveränderte Datenlage gemäss der Datenspeicherung der hierzu autorisierten Person verstanden wird.³⁰⁷² In der Literatur wird teilweise die Meinung vertreten, dass ein System in technischer Hinsicht bereits Manipulationsresistenz gewährleistet, solange wenigstens ein Full Node über eine «richtige» Kopie der Datenstrukturen verfügt, weshalb das gesamte Netzwerk nach einem Ausfall aufgrund dieser Kopie neustarten könnte.³⁰⁷³ Dies scheint aber eine kaum haltbare Auffassung mit Blick auf die Dezentralität als Rechtsprinzip zu sein.

Die Manipulationsresistenz eines verteilten Registers hat in der Praxis zwei Erscheinungsformen:

- *Vorgängige* Manipulationsresistenz bedeutet, dass Netzwerkteilnehmer die Eintragung etwa von Transaktionen in die Blockchain nicht oder wenigstens nicht über eine längere Zeit verhindern können. Vorliegend wird diese Form der Manipulationsresistenz auch als die Zensurreistenz des Systems bezeichnet. In technischer Hinsicht ist teilweise die Rede von der sog. *Liveness*.³⁰⁷⁴
- *Nachträgliche* Manipulationsresistenz bedeutet demgegenüber, dass Netzwerkteilnehmer Transaktionen, die bereits in einen Block aufgenommen worden sind, nicht nachträglich abändern können. Diese Form der Manipulationsresistenz wird vorliegend als die Unveränderlichkeit des verteilten Registers bezeichnet.

Manipulationsresistenz wird mittels zweier Komponenten erreicht:³⁰⁷⁵ In technischer Hinsicht wird die Integrität des verteilten Registers durch den Einsatz kryptografischer Verfahren sichergestellt, wie insb. durch die Methoden der

³⁰⁷¹ Art. 973d Abs. 2 Ziff. 2 OR.

³⁰⁷² Siehe Botschaft DLT 2019, 280 m.w.N.

³⁰⁷³ Siehe Crain, Solana, epicenter Podcast, *passim*.

³⁰⁷⁴ Siehe Amler et al., DeFi-ning DeFi, 2.

³⁰⁷⁵ Vgl. ferner Kuhn et al., Jusletter IT vom 23. Mai 2019, Rz. 20, welche neben technischen und organisatorischen auch rechtliche Massnahmen zulassen. In Falle rechtlicher Massnahmen, wie insb. einer vertraglichen Interessenwahrungspflicht des Netzwerksbetreibers, wird es sich jedoch in aller Regel nicht um ein dezentrales Netzwerk nach vorliegender Auffassung handeln.

Public Key-Kryptografie.³⁰⁷⁶ Namentlich kann einzig der Inhaber des Private Keys über den dazugehörigen Kryptovermögenswert verfügen (vgl. Art. 973d Abs. 2 Ziff. 1 OR). Gerade nicht der Fall war dies bei E-Coins, einer zentralisierten digitalen Währung, für deren Übertragung die Inhaber in jedem Fall auf die Mitwirkung der Emittenten angewiesen waren.³⁰⁷⁷ In organisatorischer Hinsicht wird ein manipulationsresistentes Register sodann durch den Umstand gewährleistet, dass eine Vielzahl von Personen am Netzwerk beteiligt ist (siehe hierzu oben). Allerdings ist festzuhalten, dass es sich bei der Eigenschaft der organisatorisch-bedingten Manipulationsresistenz vielmehr um die Folge der Existenz einer Vielzahl von Netzwerkteilnehmern, die voneinander unabhängig sind, als um eine eigentliche Vorbedingung der Dezentralität handelt.

Eine sinnvolle Abgrenzung der vorliegend relevanten Kontrolle kann über die Frage erfolgen, ob eine Person oder eine Gruppe von Personen, die miteinander verbunden sind, *unilateral* Transaktionen blockieren und/oder Änderungen an den verteilt abgespeicherten Daten vornehmen kann.³⁰⁷⁸ Eine solche Änderung könnte mittels direkter Manipulation der Daten in einem Smart Contract oder auf dem Weg der Rückabwicklung der Transaktionshistorie erfolgen. Eine unilaterale Kontrolle liegt demgegenüber noch nicht vor, wenn zufällige Forks auftreten, die in der Folge zur Reorganisationen von Transaktionen führen können. Solche systembedingten Phänomene³⁰⁷⁹ sind klar zu unterscheiden von kontrollrelevanten Ereignissen. Demgegenüber besteht eine problematische Kontrollsituation, wenn mehrere miteinander verbundene Netzwerkteilnehmer aufgrund ihrer Rechenkapazitäten uneingeschränkt Daten abändern und dabei insb. Transaktionen und somit Tokenbesitzstände rückgängig machen oder auf andere Weise verändern können.³⁰⁸⁰ In einem

³⁰⁷⁶ Siehe Botschaft DLT 2019, 281–282.

³⁰⁷⁷ Siehe BVGer B-5769/2017 vom 21. Januar 2019, E. 3.2; ferner BVGer B-6413/2017 vom 21. Januar 2019, E. 5.1.

³⁰⁷⁸ Siehe Sheng, Let's ditch decentralized, *passim*; vgl. auch Botschaft DLT 2019, 279.

³⁰⁷⁹ Ausführlich hierzu Jacquemart/Meyer, GesKR 2017, 471–472 («natürliche Folge der verwendeten Mechanismen offener Blockchainsysteme»).

³⁰⁸⁰ Vgl. BVGer B-5769/2017 vom 21. Januar 2019, E. 3.2 («[...] die Systemadministratoren sowohl den Algorithmus als auch die Nutzer-Guthaben jederzeit beeinflussen könnten. Mit der von [E-Coins] verwendeten Technologie könne somit weder eine genügende Individualisierung der EC erreicht, noch könnten die von der EC-Gruppe intern zugewiesenen EC von den Nutzern unabhängig beherrscht werden.»); ebenso BVGer B-6413/2017 vom 21. Januar 2019, E. 5.1.

solchen Fall ist die Manipulationsresistenz und somit die Integrität des Registers nicht gewährleistet, weshalb das betroffene Netzwerk nicht (mehr) als genügend dezentral gilt.³⁰⁸¹

e. Publizität von Code und Daten

Sodann ist die Publizität eine weitere zentrale Eigenschaft dezentraler Systeme. Diesbezüglich können zwei Formen der Publizität unterschieden werden, namentlich hinsichtlich des verwendeten Codes und der im verteilten Register abgelegten Daten.

Codepublizität bezieht sich auf den Umstand, dass der Computercode eines dezentralen Netzwerks oder einer dezentralen Applikation frei zugänglich ist (z.B. auf GitHub oder GitLab). Solche Publikationsplattformen erlauben Dritten, die nicht direkt an der Programmierung des Systems beteiligt sind, die Funktionsweise bspw. einer dezentralen Handelsplattform anhand des Softwarecodes nachzuvollziehen bzw. von einer Person mit der nötigen Expertise nachvollziehen zu lassen.

Ferner ist *Datenpublizität* eine zentrale Voraussetzung für die Teilnahme an einem dezentralen Netzwerk. Ohne Publizität wäre es den beteiligten Personen nicht möglich, Transaktionen und somit ihren Tokenbesitz autonom zu verifizieren. Sie wären auf die Informationsdienste Dritter (z.B. des Emittenten eines Token) angewiesen, was als Intermediationsrisiko zu betrachten wäre und somit die Dezentralität des Systems infrage stellen würde.³⁰⁸² In der Praxis ist der Grossteil der Nutzer dezentraler Systeme, wenn sie nicht unmittelbar selbst am Netzwerk teilnehmen, tatsächlich auf die Dienstleistungen Dritter (z.B. eines Wallet-Anbieters oder eines Block Explorers) angewiesen. Die Vielzahl der dabei verfügbaren öffentlichen Datenquellen relativiert allerdings die Bedeutung dieser Form der Informationsintermediation.

Zwar existieren dezentrale Netzwerke, wie etwa Zcash und Monero, deren verteilte Register aus Gründen des Privatsphärenschutzes nicht über dieselbe Publizitätswirkungen verfügen. Dasselbe gilt für dezentrale Applikationen, welche die Transaktionsnachverfolgung bewusst verunmöglichen (z.B. Tor-

³⁰⁸¹ Vgl. die Hinweise zur Manipulationsresistenz in Botschaft DLT 2019, 259, 276, 283; ausführlich Kuhn et al., Jusletter IT vom 23. Mai 2019, Rz. 18–19, 21.

³⁰⁸² Vgl. BVGer B-5769/2017 vom 21. Januar 2019, E. 3.2 («Die Nutzer könnten nicht jederzeit ohne Mitwirkung von [der Betreiber von E-Coins] über ihr EC-Guthaben verfügen [...]»); ebenso BVGer B-6413/2017 vom 21. Januar 2019, E. 5.1.

nado Cash). Doch selbst in diesen Fällen ist es den betroffenen Beteiligten möglich, zumindest die sie betreffenden Transaktionen und ihren eigenen Tokenbesitz autonom zu verifizieren.³⁰⁸³

Wie bereits im Zusammenhang mit der Manipulationsresistenz von Daten erwähnt, ist auch in Bezug auf die Publizitätsanforderungen dezentraler Systeme zu fordern, dass sie *kontrollrelevante* Auswirkungen für das System aufweisen. Dies ist insb. dann der Fall, wenn die beteiligten Personen autonom die Funktionsweise des Systems sowie der gemeinsamen verteilten Datenverwaltung überprüfen können.

f. Belastbarkeit der kryptoökonomischen Anreize

Dezentrale Netzwerke müssen schliesslich *kryptoökonomische Anreizbedingungen* vorsehen, welche die Stabilität des Systems langfristig sicherstellen können. Dies ist bei Permissionless Blockchains unbestreitbar nur dann möglich, wenn Personen in erster Linie aus Gründen des Eigeninteresses teilnehmen. Dezentrale Netzwerke sind aufgrund des Fehlens zentraler Autoritäten *per definitionem* kontradiktorische Systeme, deren Stabilitätserwartungen von der Annahme der Existenz innerer und äusserer Feinde abhängigen.³⁰⁸⁴ Das Zusammentreffen von verteilten Netzwerken mit tausenden Teilnehmern auf kryptoökonomische Anreizmechanismen ist zentral für die Stabilität und Integrität in der Praxis; gleichzeitig bildet dieser Bereich auch die mit Abstand komplexeste Komponente solcher Systeme.³⁰⁸⁵

Im Zentrum stehen spieltheoretische Erwägungen, welche dysfunktionales, feindliches Eigeninteresse in funktionales, stabilitätsförderndes Eigeninteresse umwandeln soll. In der Praxis kommen zu diesem Zweck v.a., aber nicht ausschliesslich positive und negative finanzielle Anreize zur Anwendung.³⁰⁸⁶ Denkbar ist auch, dass Reputation- und Reziprozitätsmechanismen stabilitäts-

³⁰⁸³ Vgl. Botschaft DLT 2019, 283; ferner Kuhn et al., Jusletter IT vom 23. Mai 2019, Rz. 25.

³⁰⁸⁴ Siehe in allgemeiner Hinsicht Troncoso et al., Proceedings on Privacy Enhancing Technologies 2017, 308.

³⁰⁸⁵ Bezeichnend darum die Aussage in Azouvi/Hicks, Cryptoeconomic Systems 2020, 8 («[...] decentralization relates to the participants and their behavior rather than solely to the protocol. Any decentralized protocol can always run in a centralized manner, so it is not enough to design a system that can be used in a decentralized manner. Rather, the requirement is to design a system that is advantageous to use in decentralized manner.»).

³⁰⁸⁶ Vgl. Mockchain.io, Mockchain, *passim*, wonach erstens ein Reward existieren muss und zweitens die Datenverarbeitung mit Kosten verbunden sein muss.

fördernd wirken. Die Belastbarkeit letzterer Anreize ist typischerweise schwerer quantifizierbar als im Falle reiner monetärer Vergütungen und Sanktionen und eignet sich darum nur bedingt für die Formulierung eines Protokolls.³⁰⁸⁷

g. Fazit

Dezentrale Systeme stellen Alternativen zu den bisherigen, überwiegend zentralen Koordinationsmodellen menschlicher Interaktion dar. Die dabei erreichte Dezentralität ist nicht gleichzusetzen mit vollständiger Disintermediation, an deren Ende die betreffenden Parteien ausschliesslich direkt miteinander interagieren. Entsprechend wurde im zweiten Kapitel der Begriff der netzwerkasierten Intermediation eingeführt.³⁰⁸⁸

Wie zentralisierte Prozesse und Strukturen unterliegt auch dezentrale Koordination menschlicher Interaktion impliziten oder expliziten Mechanismen der Willensbildung und Entscheidung (Governance). Hier stellt sich allerdings eine Neuerung ein, die in soziotechnischer Hinsicht erstmalig zu sein scheint und sozioökonomisch als Paradoxon zu bezeichnen ist: In der Dezentralität liegt die Herbeiführung der Einigung. Entscheidungsautonomie wird protokollgestützt zu einem Konsens zusammengeführt. BUTERIN spricht darum von der «logischen Zentralisierung» in Blockchain-Systemen, welche sozusagen der netzwerkartigen und ökonomischen bzw. politischen Dezentralisierung der Systeme entgegenläuft.³⁰⁸⁹

Entgegen der Begriffsverwendung im wirtschaftlichen und politischen Kontext sind dezentrale Netzwerke und Applikationen systembedingt auf Konsensbildung angewiesen. Letztlich haben alle Netzwerkteilnehmer in technischer Hinsicht dieselbe Realität abzubilden, andernfalls das Risiko besteht, dass zwei Netzwerke mitsamt ihren Applikationen und somit zwei Systeme entstehen können. Dies führt zum Schluss, dass Dezentralität auch (oder gerade) ein Phänomen des *verteilten Konsens* ist. Wo es hingegen an diesem verteilten Konsens fehlt, entsteht eine Fork des Netzwerks, welche letztlich den Anspruch auf logische Zentralisierung relativieren würde.

³⁰⁸⁷ Siehe hierzu insb. oben, [II.5.3b.ii](#) und [II.5.3c.ii](#).

³⁰⁸⁸ Siehe hierzu oben, [II.5](#).

³⁰⁸⁹ Siehe Buterin, *Meaning of Decentralization*, Medium, *passim*.

4. Dezentralitätstest für Handelsplattformen

4.1 Vorbemerkungen

Vorab ist zu bemerken, dass der nachfolgend auf dezentrale Handelsplattformen anwendbare Dezentralitätstest von *genereller* Natur ist. Je nach Sachverhalt und rechtlicher Fragestellung ist er gegebenenfalls mit bestimmten Schwerpunkten anzuwenden. Der Test berücksichtigt die oben gemachten Erwägungen zum Anleger- und Funktionsschutz.³⁰⁹⁰ Namentlich wird darauf abgestellt, ob potenzielle Informationsasymmetrien, Machtungleichgewichte, das Risiko des Vermögensverlusts, Intransparenz und Interessenkonflikte systembedingt ausgeschlossen oder zumindest technisch minimiert werden können.

In diesem Sinne ist der hier vorgeschlagene Dezentralitätstest durch das für andere neue Technologien entwickelte Modell der *Risikovorsorge* motiviert.³⁰⁹¹ Unter Risikovorsorge wird dabei insb. das Ergreifen von präventiven Massnahmen zum Schutz klassischer Polizeigüter aufgrund einer noch relativ unspezifischen Gefährdungslage verstanden.³⁰⁹² Vorliegend wichtig ist darum etwa die Frage, ob ein allfälliger Betreiber potenziell auf die Vermögenswerte der Nutzer einer Handelsplattform zugreifen und diese entwenden kann oder ob eine Drittperson potenziell Schwachstellen eines Governance-Systems entgegen den berechtigten Erwartungen der beteiligten Personen zu ihren Gunsten ausnutzen und in diesem Rahmen eine Gefährdungslage für die übrigen Beteiligten erzeugen kann. In dezentralen Systemen ist allerdings eine Verschiebung der rechtlichen Risikovorsorge zu einer *technischen Risikovorsorge* zu beobachten. Falls die Risikovorsorge in technischer Hinsicht gewährleistet ist, erübrigt sich ein Eingreifen des Finanzmarktrisikorechts³⁰⁹³.

Davon zu unterscheiden ist die Frage, ob im Finanzmarktrecht insb. mit Blick auf Finanzinnovationen das Vorsorgeprinzip gelten solle.³⁰⁹⁴ Die vorliegende

³⁰⁹⁰ Vgl. oben, [VL3](#).

³⁰⁹¹ Vgl. etwa für den Bereich der *Gentechnik* Züst, Genomeditierte Nutzpflanzen, *passim*.

³⁰⁹² Siehe Hettich, Kooperative Risikovorsorge, Rz. 72–80.

³⁰⁹³ Zum Begriff des Risikorechts Hettich, Kooperative Risikovorsorge, Rz. 72; ausführlich Rhinow et al., Öffentliches Wirtschaftsrecht, § 40 N 9–18.

³⁰⁹⁴ Vgl. hierzu Möslin, in: Möslin, Finanzinnovation und Rechtsordnung, 40–41.

Arbeit vertritt die Auffassung, dass das Vorsorgeprinzip in Bezug auf dezentrale Systeme grundsätzlich zurückzustehen hat.³⁰⁹⁵

4.2 Funktionaler Dezentralitätstest

a. Hauptfunktionen

i. Einleitung

Vorliegend handelt es sich um einen Test, welcher die Dezentralität von Handelsplattformen aufgrund ihrer relevanten Funktionen untersucht. Eine funktionale Betrachtungsweise bietet sich an, weil sie der Realität von Handelsplattformen Rechnung trägt, welche aus *mehreren Komponenten* mit je unterschiedlichen Funktionen bestehen. Zu diesen Komponenten sind neben den eigentlichen Handelsfunktionen auch das dezentrale System, auf welcher die Plattform aufbaut, sowie die Governance der Plattform zu zählen.³⁰⁹⁶ Die Anwendung einer *funktionalen* Betrachtung bedeutet demgegenüber nicht, dass Software alleine aufgrund der Tatsache, dass sie den Austausch von Vermögenswerten, wie etwa eine regulierte Börse, ermöglicht, aufsichtsrechtlich gleich wie diese zu behandeln ist.³⁰⁹⁷ Die Funktionalität eines Phänomens soll mit anderen Worten nicht dessen regulatorische Beurteilung indizieren. Entsprechend wird vorliegend gefordert, dass die funktionale Betrachtungsweise einer dezentralen Handelsplattform mittels wertender Risikoerwägungen korrigiert wird.³⁰⁹⁸

Als relevante Funktionen können (i) Systemfunktionen, (ii) technische Handelsfunktionen und (iii) politökonomische Funktionen unterschieden werden:

³⁰⁹⁵ Siehe zum Regulierungsansatz der *Anerkennung* dezentraler Systeme oben, [VI.4.3c.ii](#).

³⁰⁹⁶ Vgl. in diesem Zusammenhang FSB, *Decentralised financial technologies*, 3–4, welches *funktionell* zwischen dezentraler Entscheidungsfindung, dezentraler Risikotragung und dezentraler Datenverwaltung unterscheidet.

³⁰⁹⁷ So aber scheinbar die Auffassung der SEC im Fall «EtherDelta»; vgl. del Castillo, *Cryptocurrency Exchange On Notice*, Forbes, *passim*.

³⁰⁹⁸ Vgl. auch oben, [VI.3.3a](#) und [VI.4.1](#).

ii. **Systemfunktionen**

Als Systemfunktionen gelten die Anforderungen an das Netzwerk, das der Handelsplattform technisch zugrunde liegt. Wie bereits gesehen, handelt es sich dabei im Wesentlichen um die folgenden fünf Elemente³⁰⁹⁹

Systemfunktionen	
Funktion	Beschreibung
Vielzahl von Netzwerkteilnehmern	Das der dezentralen Handelsplattform zugrundeliegende Netzwerk wird von einer Vielzahl von Personen gemeinschaftlich verwaltet.
Unabhängigkeit der Netzwerkteilnehmer	Die Teilnehmer des Netzwerks sind voneinander in rechtlicher und wirtschaftlicher Hinsicht unabhängig.
Manipulationsresistenz der Daten	Die im verteilten Register abzuspeichernden und abgespeicherten Daten sind im Wesentlichen gegen vorgängige und nachträgliche Änderungen durch Drittpersonen manipulationsresistent.
Publizität von Code und Daten	Der verwendete Code des Netzwerkprotokolls ist öffentlich zugänglich und kann von Drittpersonen ohne Einschränkungen überprüft werden. Die Daten des verteilten Registers sind grundsätzlich öffentlich, oder aber zumindest von der Person, welche davon betroffen ist, einsehbar, sodass eine selbständige Verifizierung der Informationen möglich ist.
Belastbarkeit der kryptoökonomischen Anreizmechanismen	Die Stabilität des Netzwerks wird langfristig durch geeignete kryptoökonomische Anreizmechanismen sichergestellt.

Falls bereits das Netzwerk ungenügend dezentralisiert ist, erübrigt sich eine Prüfung der übrigen Funktionen der Handelsplattform.³¹⁰⁰ Im Rahmen der Analyse dezentraler Handelsplattformen sollten darum auch die oben gemachten Überlegungen zu den Machtbereichen in dezentralen Netzwerken mitberücksichtigt werden.

³⁰⁹⁹ Siehe hierzu oben, [VII.3.3](#).

³¹⁰⁰ Siehe Glaser, in: Bui/Sprague, *Pervasive Decentralisation*, 1547. Dies wäre fraglich etwa im Falle des *Ripple* Netzwerks, vgl. die Untersuchung von Amores-Sesar/Cachin/Mićić, in: Bramas/Oshman/Romano, *Ripple Consensus*, 10:3 («[The Ripple consensus protocol] relies heavily on synchronized clocks, timely message delivery, the presence of a fault-free network, and an a-priori agreement on common trusted nodes.»).

iii. Technische Handelsfunktionen

Als technische Handelsfunktionen dezentraler Handelsplattformen gelten typischerweise die folgenden:

Technische Handelsfunktionen	
Funktion	Beschreibung
Aufbewahrung von Kryptovermögenswerten	Die Nutzer der Handelsplattform verfügen bis zur Ausführung des Auftrages jederzeit über die ausschliessliche Kontrolle über ihre eigenen Kryptovermögenswerte. Dies schliesst nicht aus, dass die Nutzer die Vermögenswerte vorübergehend in einem Smart Contract hinterlegen. Massgeblich ist, dass keine Drittperson auf die Vermögenswerte zugreifen kann.
Führung des Orderbuchs	Die konkrete technische Ausgestaltung des Orderbuchs ist grundsätzlich nicht relevant (s. AMM-Modell). Soweit jedoch ein Orderbuch existiert, hat dieses von einer Gruppe von Personen, die die in rechtlicher und wirtschaftlicher Hinsicht voneinander unabhängig sind, unterhalten zu werden. Darunter fallen typischerweise Orderbücher, die unmittelbar von den Teilnehmern eines dezentralen Netzwerks, d.h. <i>on-chain</i> , geführt werden. Ferner kann es sich auch um ein oder mehrere Orderbücher handeln, die innerhalb eines <i>separaten</i> verteilten Netzwerks <i>off-chain</i> geführt werden, wobei ausgeschlossen sein muss, dass die Teilnehmer eines solchen Netzwerks die von Nutzern eingestellten Orders einseitig ändern können. ³¹⁰¹
Handelsausführung (inkl. Matching)	Die konkrete technische Ausgestaltung des Matching-Mechanismus ist ebenfalls grundsätzlich nicht relevant. So können Orders automatisch oder manuell zusammengeführt werden, sofern letzteres durch die an einem Austauschgeschäft beteiligten Personen selbst geschieht. Massgeblich ist, dass keine Drittperson auf die Ausführung und insb. das Matching von Orders Einfluss nehmen kann. ³¹⁰²
Handelsabwicklung	Die Handelsabwicklung von zusammengeführten Aufträgen erfolgt durch den Konsensmechanismus über das verteilte Register des dezentralen Netzwerks. Der Austausch der Kryptovermögenswerte erfolgt mit anderen Worten unmittelbar und atomistisch zwischen den Nutzern der Handelsplattform, lediglich mediatisiert durch das dezentrale Netzwerk (netzwerkbasierte Intermediation).

³¹⁰¹ So wohl auch Lin, Stanford Journal of Blockchain Law & Policy 2019, 67.

³¹⁰² Ebenso Lin, Stanford Journal of Blockchain Law & Policy 2019, 63.

	Dies schliesst grundsätzlich nicht aus, dass die Handelsabwicklung über ein Layer-2-Netzwerk erfolgt, falls die daran beteiligten Netzwerkteilnehmer voneinander rechtlich und wirtschaftlich unabhängig sind und die Nutzer innert nützlicher Frist ihre Kryptovermögenswerte im verteilten Register des dezentralen Netzwerks (Layer 1) abbilden können.

Im Kern handelt es sich bei der Analyse technischer Handelsfunktionen um eine *Erweiterung des Kriteriums der Manipulationsresistenz* dezentraler Netzwerk hinsichtlich der in einem verteilten Register abgespeicherten Daten (siehe oben). Dieses Kriterium kann auch auf dezentrale Applikationen und insb. dezentrale Handelsplattformen angewendet werden. Demnach ist die Dezentralität einer Handelsplattform gegeben, wenn die beteiligten Parteien autonom alle wesentlichen Parameter des Austauschgeschäfts festlegen und zur Ausführung bringen können. Demgegenüber ist eine Handelsplattform nicht dezentral, wenn eine Drittperson oder eine Gruppe von miteinander verbundenen Personen etwa aufgrund von Admin Keys Transaktionen permanent verhindern kann oder deren Freigabe für den Austausch der Kryptovermögenswerte erforderlich ist.

iv. Politökonomische Funktionen

Als politökonomische Funktionen dezentraler Handelsplattformen gelten Governance-bezogene Aspekte. Diese werden primär durch Anreize ökonomischer Natur bestimmt, welche je nach Ausgestaltung einen grösseren oder kleineren Effekt auf die Dezentralität haben können.³¹⁰³ Zu den politökonomischen Funktionen gehören insb. die folgenden:

Politökonomische Funktionen	
Funktion	Beschreibung
Quelloffenheit der Software	Der für die wesentlichen technischen Handelsfunktionen verwendete Code ist öffentlich zugänglich sein und kann von Drittpersonen ohne Einschränkung überprüft werden.

³¹⁰³ Vgl. Lin, Stanford Journal of Blockchain Law & Policy 2019, 60.

Handelszulassung von Kryptovermögenswerten	Grundsätzlich können Nutzer Kryptovermögenswerte eigenständig zum Handel zulassen (z.B. durch entsprechende Ausführung eines Smart Contracts). Es existiert keine Drittperson, welche über die Zulassung zu entscheiden hat, die Zulassung entziehen oder den Handel eines bestimmten Vermögenswerts vorübergehend oder permanent sistieren kann. Falls die Nutzer über die Zulassung nicht selbst bestimmen können, ist es erforderlich, dass stattdessen eine Gruppe von Personen, die voneinander rechtlich und wirtschaftlich unabhängig sind, darüber entscheiden (z.B. eine DAO).
Governance technischer Handelsfunktionen	Es besteht grundsätzlich keine Governance hinsichtlich der <i>technischen</i> Handelsfunktionen (siehe zum Begriff oben).³¹⁰⁴ Es bestehen bspw. keine Admin Keys hinsichtlich solcher für die Operationen der Plattform zentralen Funktionen. Im Besonderen kann keine Drittperson in den Handelsablauf eingreifen (z.B. durch Blockierung von Vermögenswerten). Änderungen von technischen Handelsfunktionen bedürfen grundsätzlich der Programmierung und Ausführung eines neuen Smart Contracts. Falls Governance-Mechanismen hinsichtlich Funktionen bestehen, welche für die technischen Handelsfunktionen massgeblich sind, ist es erforderlich, dass diese durch eine Gruppe von Personen, die voneinander rechtlich und wirtschaftlich unabhängig sind, ausgeübt werden (z.B. eine DAO oder eine Multisig mit hohen Anforderungen an das Signing Quorum [z.B. 12 von 15 Personen]). Ferner ist es in diesem Fall grundsätzlich notwendig, dass die Implementierung von Änderungen durch weitere Sicherheitsmassnahmen, wie insb. Timelocks, abgesichert wird. Die Existenz von Admin Keys, welche es etwa einer DAO erlaubt, gewisse Parameter eines Protokolls anzupassen (z.B. die Handelsgebühren), die für den Handelsablauf nicht zentral sind, sind für den Dezentralitätstest in der Regel unerheblich. Im Allgemeinen ist zu erwarten, dass ein Protokoll die Governance-Kompetenzen einer DAO oder ähnlichen Struktur über die Zeit zunehmend zu minimieren versucht.³¹⁰⁵

³¹⁰⁴ Vgl. etwa Carter/Jeng, in: Coen/Maurice, DeFi Protocol Risks, 25.

³¹⁰⁵ Vgl. Buterin, Beyond coin voting governance, *passim*; ähnlich Messari, Methodology Token, *passim*; ferner für ein Bsp. in der Praxis GEB Docs, Governance Minimization Guide, *passim*.

Verteilung von Governance Token	Keine Person oder Gruppe von Personen, die voneinander rechtlich und wirtschaftlich unabhängig sind, besitzt grundsätzlich mehr als 20-30% aller Governance Token. Der übrige Besitz von 70-80% ist innerhalb der Community breit gestreut. Nur bei genügender Verteilung des Tokenbesitzes kann davon gesprochen werden, dass die einzelnen Entscheidungsträger keinen rechtlich relevanten Einfluss auf die Entwicklung des Protokolls und weitere Entscheidungen in diesem Zusammenhang ausüben können.
Ausübung der Governance	Die Anforderungen an die Ausübung der Governance ist derart ausgestaltet (z.B. Quoren für Anträge und Abstimmungen), dass die Community <i>effektiv</i> an der Fortentwicklung eines Projekts partizipieren kann.³¹⁰⁶ Angesichts der heute eher starken Konzentration von Governance Token bei einzelnen Personen³¹⁰⁷ ist von einem erhöhten regulatorischen Risiko für dezentrale Handelsplattformen auszugehen.

b. Nebenfunktionen

i. Einleitung

Darüber hinaus weisen dezentrale Handelsplattformen weitere Funktionen auf, die aus Sicht des Dezentralitätstests regelmässig von geringer oder keiner Bedeutung sind. Dabei handelt es sich insb. um die nachfolgenden Funktionen:

ii. Softwareentwicklung

Im Gegensatz zu dezentralen Netzwerken ist die Grösse und Zusammensetzung des Entwicklerteams von Protokollen dezentraler Handelsplattformen nach vorliegender Ansicht nicht gleich bedeutsam. Projekte können bspw. nach betriebswirtschaftlichen Grundsätzen organisiert sein.

Das Hauptentwicklerteam hinter Uniswap ist etwa bei Uniswap Labs bzw. Universal Navigation Inc. mit Sitz in Delaware angestellt. Der «Postauto-Test», wonach gefragt wird, ob das Projekt weiterleben würde, wenn die fragliche Person unter das Postauto käme, ist hier nur mit Zurückhaltung anzuwenden.

³¹⁰⁶ Siehe Garcia/Leung, Ketsal Open Standards, 12–13; vgl. ferner etwa für die Anforderungen im Fall von Uniswap Sinclair, Uniswap's First Governance Vote, Coindesk, *passim*.

³¹⁰⁷ Siehe hierzu oben, [IV.5.2d.ii](#).

Für sich alleine ist dieses Kriterium nur von geringer Bedeutung. In diesem Zusammenhang ist auch nicht allein massgeblich, ob aus einer rechtlichen Struktur heraus am Projekt gearbeitet wird. Hinter einem wesentlichen Teil der Entwicklung des Lending-Protokolls Aave sowie dem Betrieb des Frontends <https://aave.com/> stand vor dem Wechsel zu einem IPFS-gehosteten Interface etwa die Aave GmbH mit Sitz in Chiasso.³¹⁰⁸ Demgegenüber bestehen freilich Projekte, deren Entwickler überwiegend anonym agieren und die lediglich eine lose Organisationsstruktur aufweisen, wie etwa THORChain. Freilich haben auch solche Projekte zentrale Anlaufstellen, wie namentlich einen Twitter- und Discord-Kanal.

Entscheidend ist demgegenüber, dass der in einem Protokoll verwendete Code öffentlich zugänglich ist, sodass Drittpersonen ihn selbständig uneingeschränkt verifizieren können. Im Vordergrund steht sodann die «Angreifbarkeit» der dezentralen Applikation.³¹⁰⁹ Wenn unbeteiligte Dritte ohne Weiteres den Source Code einer dezentralen Applikation für eigene Anwendungen verwenden können, ist dem Dezentralitätstest in diesem Punkt in der Regel Genüge getan.³¹¹⁰ Wenn die Smart Contracts oder dergleichen schliesslich ohne oder nur mit eingeschränkten Admin Keys des Entwicklerteams oder einer DAO zur Ausführung gelangen, befindet sich die dezentrale Applikation nicht mehr unter der Kontrolle der erwähnten Personen oder Entitäten, sondern sie bildet Teil des öffentlich zugänglichen Bereichs dezentraler Systeme.³¹¹¹

DeFi-Projekte, die von einem einzigen Team entwickelt werden, bewegen sich allerdings in einem regulatorischen Graubereich, wenn das Entwicklerteam aufgrund der einseitigen Verteilung des Governance Token einen massgeblichen Einfluss auf die Governance des Protokolls ausüben kann.³¹¹² Projekte mit einem *Fair Launch* des Token können demgegenüber die Dezentralität eines Protokolls erhöhen, indem sie die Nutzergemeinschaft von Beginn weg einzubinden versuchen.³¹¹³

³¹⁰⁸ Siehe Aave, Terms of Use, 7. Juni 2023, <https://aave.com/term-of-use>, *passim*.

³¹⁰⁹ BUTERIN spricht von der *Fork-Freundlichkeit* der Software; vgl. Buterin, Beyond coin voting governance, *passim*.

³¹¹⁰ Siehe in diesem Zusammenhang auch Van Valkenburgh, Decentralization in the context of the law, *passim*.

³¹¹¹ Vgl. Glaser, in: Bui/Sprague, Pervasive Decentralisation, 1548.

³¹¹² Vgl. Michaels/Kiernan, Crypto's 'DeFi' Projects Aren't Immune to Regulation, Wallstreet Journal, *passim*; ferner Walden, Progressive Decentralization, *passim*.

³¹¹³ Im Rahmen eines *Fair Launch* können die Governance Token etwa Personen bzw. Wallet-Adressen zugeteilt werden, welche eine Applikation in der Vergangenheit bereits benutzt haben. Zudem besteht ein möglicher Ansatz darin, Early Adopters mit einem prozentual höheren Tokenanteil als spätere Nutzer zu «belohnen». Sodann kann ein *Fair Launch* auch

iii. Benutzeroberfläche

Von geringer Bedeutung ist sodann der Umstand, dass eine Benutzeroberfläche (Frontend, GUI etc.), welche Nutzern als Zugang zur dezentralen Handelsplattform dient, zentral gehostet wird und somit von einer bestimmten Person beherrscht wird.

Zwar können webbasierte Frontends von Plattformen, wie mehrere Vorfälle im Zusammenhang mit EtherDelta in der Vergangenheit gezeigt haben, durchaus Opfer von Hacks sein.³¹¹⁴ Zudem mag ein Serverfehler vorübergehend die Erreichbarkeit der Webseite und somit der Plattform, sozusagen dem «Backend» einer Anwendung, einschränken bzw. erschweren. Die Erreichbarkeit der Plattform ist jedoch im Gegensatz zu Code, der ausschliesslich auf zentralen Servern läuft,³¹¹⁵ nicht generell ausgeschlossen.

Aufsichtsbehörden, wie etwa die SEC,³¹¹⁶ aber auch die OECD³¹¹⁷ scheinen sodann der Benutzeroberfläche bzw. der verwendeten Webseite besonderes Gewicht einzuräumen.³¹¹⁸ Dies scheint wohl einer allzu funktionalen Betrachtungsweise im Aufsichtsrecht geschuldet zu sein.³¹¹⁹ Dabei wird vergessen, dass eine bestimmte Benutzeroberfläche nur *eine* von vielen Schnittstellen zu dezentralen Applikationen darstellt, sie selbst aber nicht unmittelbar eine technische Handelsfunktion ausübt.

Der der Betrieb eines Frontends vereinfacht die *Kommunikation* zwischen den an einem Austauschgeschäft beteiligten Parteien. Dies alleine stellt jedoch nach vorliegender Auffassung noch keine unmittelbare und somit relevante

vorsehen, dass das Publikum Token über einen längeren Zeitraum zu einem relativ gleichbleibenden Preis erwerben kann; vgl. hierzu Balaji/Hasu, *Mythical Fair Launch*, Medium, *passim*.

³¹¹⁴ Siehe hierzu oben, [IV.5.2d.iv](#).

³¹¹⁵ Siehe Barrett, Facebook, Wired, *passim*.

³¹¹⁶ Siehe SEC, Order Coburn, 2, 3, 4 FN 8, 9, welche der Webseite von EtherDelta bzw. deren Funktionalitäten ein hohes Gewicht beizumessen scheint («Users who are nodes [or connected to nodes] on the Ethereum Blockchain can interact directly with the EtherDelta smart contract, which is publicly-available on github.com. Alternatively, during the Relevant Period, Users could interact with the EtherDelta smart contract through a user-friendly interface created by Coburn, called The EtherDelta Graphic User Interface [...]. EtherDelta's website, allowed Users to interact with the EtherDelta smart contract without having to be a node on the Ethereum Blockchain and without having to understand the details of blockchain technology.»).

³¹¹⁷ Siehe OECD, *Tokenisation and Implications for Financial Markets*, 30.

³¹¹⁸ So aber auch Meirich, *Decentralized Finance*, Rz. 899.

³¹¹⁹ Vgl. auch Glarner/Lindgren, *EtherDelta*, 2, 7.

Kontrolle über die dezentrale Handelsplattform dar. Sodann kann die vorliegende Auffassung damit begründet werden, dass die Funktionalitäten von Frontends zu dezentralen Applikationen – zumindest, wenn der Schnittstellencode Open Source ist – bei Bedarf von Dritten relativ einfach über andere Domains repliziert werden können.³¹²⁰ Dafür können sie etwa APIs verwenden, die sie auf ihrem eigenen Server hosten. Idealerweise entscheiden sich Entwicklerteams von Beginn weg für ein dezentrales Hosting des Frontends bspw. über IPFS oder ein anderes Protokoll, das eine dezentrale Datenablage und -verwaltung ermöglicht.³¹²¹ Aus diesen Gründen kann nicht von einer zentral beherrschten Webseitendomain oder einer zentral gehosteten Benutzeroberfläche auf die Zentralisierung der Handelsplattform geschlossen werden.³¹²²

Ein *praktische Beispiel* mag an dieser Stelle weiterführend sein: Die Smart Contracts der dezentralen Handelsplattform Uniswap können heute über die vom US-amerikanischen Softwareunternehmen Uniswap Labs bzw. Universal Navigation Inc. betriebene «offizielle» Domain (<https://app.uniswap.org/>) bzw. dessen webbasiertes Frontend benutzt werden. Darüber hinaus können sie allerdings auch über andere Benutzeroberflächen und Schnittstellen angesteuert werden. Hierzu gehören etwa andere Webseiten, welche eine grafische Schnittstelle implementieren, wie namentlich Etherscan (<https://etherscan.io/>), dezentrale Applikationen, wie Aggregatoren, und Anwendungen, welche die quelloffene API von Uniswap nutzen (z.B. Wallets und Trading Bots). Schliesslich können die Smart Contracts auch direkt über die Kommandozeile eines Ethereum Clients angesteuert werden.

Auf der Webseite von Uniswap hiess es in einer früheren Version der Nutzungsbedingungen hierzu:

«[...] just as you can access email email protocols such as SMTP through multiple email clients, you can access the Uniswap protocol through dozens of web or mobile interfaces.»³¹²³

³¹²⁰ GL.M. mit Verweis auf das Stellar Netzwerk Lin, Stanford Journal of Blockchain Law & Policy 2019, 63.

³¹²¹ Vgl. etwa das Protokoll Skynet, über welches die Applikation Homescreeen die Entwicklung von dezentral abgespeicherten Frontends erlaubt; für mehr hierzu siehe Vorick, Decentralized Frontends for Web3, *passim*.

³¹²² GL.M. SBF, Circular 2020/01, 16; MME, Stellungnahme, 27.

³¹²³ Uniswap, Uniswap Protocol Disclaimer, undatiert, <https://uniswap.org/disclaimer/>, *passim* (30.11.2021).

Mit anderen Worten: Selbst wenn das Frontend über die «offizielle» Domain nicht erreichbar sein sollte, wäre die dezentrale Handelsplattform Uniswap aufgrund der unmittelbaren Ausführung der Smart Contracts auf der Ethereum Blockchain weiterhin nutzbar, wenn auch allenfalls auf eine Art und Weise, die für den durchschnittlichen Nutzer umständlicher ist. Programmierer könnten schliesslich, weil der Schnittstellencode von Uniswap quelloffen ist, relativ schnell von Grund auf ein neues Frontend zu den Uniswap-Smart Contracts programmieren.

Genau dies geschah, als Uniswap Labs sich am 23. Juli 2021 – vermutlich auf regulatorischen Druck der SEC hin –³¹²⁴ dazu entschieden hat, gewisse synthetische Produkte, die Ähnlichkeiten mit Contracts for Difference und Swaps aufweisen und somit allenfalls als Securities unter US-amerikanischem Wertpapierrecht qualifizieren könnten, auf der von ihr betriebenen Webseite nicht mehr aufzuführen.³¹²⁵ Über andere Frontends bzw. GUIs zu den Uniswap-Smart Contracts, die etwa von Aggregatoren oder Wallet-Anbietern betrieben werden, konnten (und können) Nutzer die betroffenen Tokens allerdings weiter frei handeln.³¹²⁶ Ferner war der Handel solcher synthetischer Token über Domains, die auf IPFS-gehostete Daten von Uniswap zielen, oder aber direkt über einen lokalen Client von IPFS weiterhin möglich.³¹²⁷ Eine ähnliche Situation ereignete sich bereits im Dezember 2019, der Zugang zu uniswap.exchange für Personen aus bestimmten Ländern blockiert wurde, die mutmasslich mit den Sanktionsprogrammen des US-amerikanischen Office of Foreign Assets Control (OFAC) übereinstimmen.³¹²⁸

An diesen Beispielen wird gut ersichtlich, dass die dezentrale Handelsplattform Uniswap genügend dezentralisiert ist und dass es auf das Frontend grundsätzlich nicht ankommen kann, solange alternative Schnittstellen existieren. Das einzelfallweise auftretende Geoblocking von IP-Adressen von Nutzern aus bestimmten Ländern oder Regionen durch den Webseitenbetrei-

³¹²⁴ Vgl. die kurz davor ergangenen Ausführungen des SEC-Vorsitzenden Gensler, Remarks Before the American Bar Association Derivatives and Futures Law Committee, *passim* («It doesn't matter whether it's a stock token, a stable value token backed by securities, or any other virtual product that provides synthetic exposure to underlying securities. These platforms – whether in the decentralized or centralized finance space – are implicated by the securities laws and must work within our securities regime.»).

³¹²⁵ Vgl. den Blog-Eintrag bei Uniswap, Token access, *passim*.

³¹²⁶ Vgl. Hayden, Twitter, *passim*.

³¹²⁷ So z.B. über die ENS-Domain <https://uniswap.eth.link/> oder <https://app-uniswap-org.ipns.dweb.link/>; ferner Uniswap, Interface, GitHub, *passim*.

³¹²⁸ Siehe The Defiant, Uniswap Website Geo-Ban Can't Stop DeFi, *passim*.

ber,³¹²⁹ welche eine GUI zu dezentralen Handelsplattformen anbieten, ist ein weiterer Beleg für diese Tatsache.³¹³⁰

iv. Immaterialgüterrechte

Als Immaterialgüterrechte im Bereich der Softwareentwicklung kommen v.a. Urheberrechte und allenfalls – so etwa im Bereich von Algorithmen zur Erstellung digitaler Signaturen –³¹³¹ Patentrechte infrage.³¹³² In Bezug auf dezentrale Handelsplattformen interessieren aber weniger Patentrechte, sondern in erster Linie Urheber- und sodann auch Markenrechte.

Computerprogramme und der ihnen zugrundeliegende Computercode können als Werk *urheberrechtlich* geschützt sein,³¹³³ woraus den Entwicklern als den Urhebern das geistige Eigentum an der Software mitsamt exklusiven Nutzungs- und Verwertungsrechten entsteht. Bei Computercode, der unter einer Open-Source-Lizenz veröffentlicht wird, räumt der Entwickler demgegenüber Dritten weitgehende Nutzungsbefugnisse an der von ihm entwickelten Softwarecode ein.³¹³⁴ Ausnahmsweise verzichtet er sogar gänzlich auf die Urheberrechte, wodurch die Software in die Public Domain gerät.³¹³⁵ Der Nutzer von Open-Source-Software erhält umgekehrt im Rahmen der anwendbaren Lizenz Nutzungsbefugnisse bzw. bei vollständiger Freigabe des Codes die uneingeschränkte Verfügungsmöglichkeit über das Computerprogramm.

Das *Markenrecht* kann sich sodann etwa auf die Bezeichnung einer Softwareapplikation beziehen (z.B. das Zeichen «Uniswap»). Selbstredend weisen Markenrechte gewisse zentralisierende Effekte auf, denn die Existenz einer Marke schafft eine Verbindung zwischen der an ihr berechtigten Person (i.d.R. ein Softwareunternehmen) und dem Protokoll einer Applikation. Eine Marke

³¹²⁹ Vgl. zu der technischen Ausgestaltung von Geoblocking Federrath, ZUM 2015, *passim*.

³¹³⁰ Siehe etwa Bancor, Service Restrictions, *passim* («We would like to clarify that this functionality will be blocked to users accessing the website *bancor.network*, which offers an interface to blockchain activity. As the Bancor Liquidity Network is a collection of smart contracts on the blockchain, we cannot restrict users from accessing the blockchain itself. This cannot be blocked.»).

³¹³¹ So waren *Schnorr-Signaturen*, die nunmehr mit Taproot in Bitcoin Anwendung finden, bis Februar 2008 aufgrund eines Patents von der freien Nutzung ausgeschlossen; vgl. hierzu Maxwell et al., Designs, Codes and Cryptography 2019, 2143.

³¹³² Vgl. für eine Übersicht Leins-Zurmuehle, Software Engineering, 89–90, 102.

³¹³³ Vgl. Art. 2 Abs. 3 URG.

³¹³⁴ Siehe Fröhlich-Bleuler, in: Jörg/Arter, Open Source Software, 196–200.

³¹³⁵ Siehe Fröhlich-Bleuler, in: Jörg/Arter, Open Source Software, 184; ferner Straub, Softwareschutz, Rz. 640.

schaftt zudem Vertrauen in ein Produkt bei den Marktteilnehmern und somit auch in die an ihr berechtigten Person.³¹³⁶

Dennoch ist die Existenz von Urheberrechten an Open-Source-Code oder einer Marke an einer Plattform in aller Regel nur von geringer Bedeutung für den vorliegenden Dezentralitätstest.³¹³⁷ Die erfolgreiche Fork des Codes von Uniswap Version 2 hat aufgezeigt, dass die Existenz der Marke Uniswap, welche vom dahinterstehenden Unternehmen Uniswap Labs (genauer: Universal Navigation Inc. mit Sitz in Delaware) eingetragen wurde, Dritte nicht daran hindern konnte, die Funktionalitäten der dezentralen Handelsplattform unter der neuen Bezeichnung «SushiSwap» zu replizieren. Die Existenz einer Marke an einer dezentralen Applikation ist darum für den Dezentralitätstest nicht massgeblich, solange der Softwarecode derselben Applikation ohne Einschränkungen eingesehen, kopiert, verbreitet und geändert werden kann.

Aus ähnlichen Grund haben laufende Markenrechtsstreitigkeiten betreffend Bitcoin und andere Protokolle dezentraler Netzwerke Teilnehmer und Nutzer bisher nicht daran hindern können, die zugrundeliegende Software auszuführen.³¹³⁸ Die Stiftung Ethereum mit Sitz in Zug verfügt bspw. über die Marke ETHEREUM.³¹³⁹ Zumindest für Bitcoin könnte argumentiert werden, dass es sich beim Zeichen um ein markenschutzrechtliches *Gemeingut* handelt, weshalb die Schutzfähigkeit ausgeschlossen sein sollte.³¹⁴⁰ Eine solche Einstufung unter dem MSchG verhindert zwar den rechtlichen Zeichenschutz, ermöglicht dafür u.a. im Rahmen der Vorgaben des Lauterkeitsrechts den freien, uneingeschränkten Zeichengebrauch durch die Öffentlichkeit.³¹⁴¹ Der Mangel an zentraler Emission oder Steuerung von bitcoins würde nach vorliegender Ansicht diese Sichtweise rechtfertigen.

Eine Alternative zur Zentralisierung einer Marke innerhalb eines traditionellen Rechtsrahmens könnte die Eintragung einer Marke durch eine DAO oder die Übertragung der Marke an eine solche sein. Der derzeit ungeklärte Rechtsstatus einer DAO in der Schweiz stellt jedoch ein praktisches Hindernis für derartige Vorgänge dar.³¹⁴² Zweifelsohne würde die «Verrechtlichung» einer DAO

³¹³⁶ Vgl. auch Leins-Zurmuehle, Software Engineering, 94.

³¹³⁷ Ebenso in Bezug auf die Unterstellung unter das FinfraG SBF, Circular 2020/01, 9.

³¹³⁸ Siehe für eine Übersicht etwa McLeod, CITMA Review März/April 2019, *passim*.

³¹³⁹ Vgl. die entsprechenden Einträge auf Swissreg (<https://www.swissreg.ch>) und bei der Weltorganisation für geistiges Eigentum (<https://www.wipo.int>).

³¹⁴⁰ Vgl. Art. 2 lit. a MSchG.

³¹⁴¹ Siehe hierzu SHK MSchG-Aschmann, Art. 2 lit. a N 4.

³¹⁴² Vgl. hierzu die Ausführungen im DLT-Bericht zur Gesellschaftsform bei kollektiven Kapitalanlagen Bundesrat, DLT-Bericht 2018, 136–137 *in fine*, 137–138; sodann ausführlich Bärts-

in einer Körperschaft oder Rechtsgemeinschaft, deren Aktivitäten einem bestimmten nationalen Recht unterstehen, zentralisierende Effekte für eine dezentrale Handelsplattform, welche durch die genannte DAO verwaltet wird, mit sich bringen. Im Falle von The DAO hätte sodann die DAO.LINK GmbH mit Sitz in Neuenburg im Aussenverhältnis gegenüber den Kapitalnehmern treuhänderisch für die DAO bzw. deren Tokeninhabern auftreten sollen, wozu es jedoch aufgrund des Hackerangriffs nie kommen sollte.³¹⁴³ Zudem ist es oftmals nur bedingt erheblich, ob die Geschäftstätigkeit einer global agierenden DAO unter schweizerischem oder ausländischem Recht erfolgen würde; die transnationale Natur einer DAO löst selbstredend Rechtskonflikte aus.³¹⁴⁴ Entsprechend wird in der Kryptogemeinschaft zu Recht teils gefordert, dass DAOs auch ein ausser- bzw. überrechtlicher Charakter zukomme.³¹⁴⁵

Dies bedeutet freilich nicht, dass das Recht im Einzelfall nicht auf DAOs zur Anwendung gelangen kann.³¹⁴⁶ Nach vorliegender Ansicht kommt es auf die mit der codebasierten Kooperation oder Koordination verfolgten Ziele an. In der Praxis werden darum wohl zwei Hauptformen von DAOs zu unterscheiden sein: DAOs mit einem mitgliedschaftlichen Schwerpunkt (Kooperation) und solche, deren Hauptziel in der Automatisierung von Prozessen liegt und die somit gewisse Ähnlichkeiten mit Anstalten aufweisen (Koordination).³¹⁴⁷ In letzteren Fällen wird es jedoch regelmässig am Bedürfnis nach Verrechtlichung in einer Körperschaft oder Rechtsgemeinschaft fehlen. Bitcoin und Ethereum als Konsenssysteme können etwa hierzu gezählt werden.

v. Gebühren

Gebühren können in zwei Grundtypen aufgeteilt werden: Einerseits können Nutzer einer dezentralen Handelsplattform für Leistungen entschädigt werden. Die Existenz von *Handelsgebühren*, die insb. als Gegenleistung für die Be-

chi, in: Jung/Krauskopf/Cramer, Digitaler Wandel, 11–15 m.w.N.; ferner Müller, Expert Focus 2019, 487–488; für das *deutsche Recht* statt vieler Langenbacher, AcP 2018, 421–425; *demgegenüber* Gyr, Jusletter vom 4. Dezember 2017, Rz. 24–35, 50, welche in Bezug auf «The DAO» vom Vorliegen einer einfachen Gesellschaft nach Art. 530 ff. OR ausgeht; siehe sodann Bull, Wyoming's DAO Law, Coindesk, *passim*.

³¹⁴³ Siehe hierzu Mann, NZG 2017, 1018.

³¹⁴⁴ Vgl. zur Problematik des Widerstands einer Rechtsordnung gegenüber autonom handelnden Systemen Bayern et al., AJP 2017, 203.

³¹⁴⁵ So Shapiro, DAO 2, Twitter, *passim*.

³¹⁴⁶ Siehe Shapiro, DAO 1, Twitter, *passim*; ferner coala, Model Law for DAOs, 5–6; Foxley, Legal DAO, Coindesk, *passim*.

³¹⁴⁷ Vgl. in US-amerikanischer Hinsicht die Gedanken zum Konzept des *Business Trusts* bei Reyes, The George Washington Law Review 2019, 411–418.

reitestellung von Liquidität bezahlt werden, stellt für sich alleine aus Sicht des Dezentralitätstests keine relevante Funktion dar. Falls sodann die Entschädigungsleistung in Form von Governance Token des Protokolls erfolgt, kann dies bei einer Vielzahl von Liquiditätsbereitstellern einen positiven dezentralisierenden Effekt auf ein Protokoll haben.

Andererseits können Entwickler oder andere Personen, die mit dem Entwicklerteam verbunden sind (z.B. Eigenkapitalgeber des dahinterstehenden Softwareunternehmens, sog. *Venture Capitalists*), mit insb. Governance Token entschädigt werden, welche in Form von Nutzungsgebühren von den Nutzern erhoben oder über andere Mechanismen geschaffen werden. Falls auf diesem Weg der Vereinnahmung von Gebühren die breite Streuung des Governance Tokens, welchem zudem kontrollrelevante Funktionen aus Sicht des Protokolls zukommt, zugunsten bestimmter Parteien eingeschränkt wird, kann dies u.U. die Dezentralität des Protokolls infrage stellen.³¹⁴⁸ Die blosse Tatsache allerdings, dass die vereinnahmten Gebühren für die Finanzierung der Protokollentwicklung verwendet werden, führt nach vorliegender Ansicht nicht bereits zum Scheitern des Dezentralitätstests.³¹⁴⁹ Dass Personen, die Zeit und/oder Geld für die Entwicklung eines Protokolls aufwenden und die damit einhergehenden Risiken auf sich nehmen, dafür entschädigt werden, ist nichts als verständlich, weshalb dieser Tatsache Rechnung getragen werden sollte.³¹⁵⁰

4.3 Notwendigkeit einer Gesamtbetrachtung der Funktionen

Die Hauptfunktionen müssen aufgrund einer Gesamtbetrachtung genügend dezentral ausgestaltet sein, um den funktionalen Dezentralitätstest zu bestehen.

³¹⁴⁸ Vgl. auch WEF, *Decentralized Finance*, 10.

³¹⁴⁹ A.M. offenbar Poskriakov, in: Richa/Canapa, *Conservation et négoce de cryptoactifs*, 120; wohl auch Meirich, *Decentralized Finance*, Rz. 898, der die Generierung von Gebühren als «Indiz» für den Einrichtungsbegriff gemäss FinfraG betrachtet; ferner wohl auch Gary Gensler, Vorsitzender der SEC; vgl. hierzu Wieczner, Gary Gensler, New York, *passim* («The 'decentralized' ones – they're not that decentralized, actually. It's not just software. There is somebody there who has designed an incentive system, a business model, earning fees, has a governance token, and is setting up the protocol in the middle.»).

³¹⁵⁰ Vgl. in diesem Zusammenhang The Defiant, *DeFi Transparency*, Youtube, *passim*; ferner Cohen/Angelovska-Wilson/Strong, *Decentralized Finance*, *passim*, die von einem «significant financial benefit» sprechen.

Namentlich verlangt der Test nicht, dass jede Funktion für sich vollständig und in absoluter Weise dezentralisiert ist.³¹⁵¹ Allerdings kann bereits die Zentralisierung einer einzigen Hauptfunktion, so insb. die Aufbewahrung der Kryptovermögenswerte von Nutzern, für das Scheitern des Tests ausreichen. Der Dezentralitätstest sollte darauf ausgerichtet sein, zu untersuchen, ob Macht in gewissen, v.a. relevanten Funktionen konzentriert ist, welche unter Berücksichtigung aller Umstände für die Funktionsweise einer dezentralen Handelsplattform relevant ist. Falls solche konzentrierten Bereiche existieren, ist zu fordern, dass im Sinne von *Checks and Balances* ein massgeblicher Ausgleich durch die übrigen Komponenten des Systems und/oder die beteiligten Personen erfolgt.³¹⁵² Zudem sind auch relevante gegenseitige Abhängigkeiten dezentraler Applikationen in die Gesamtbetrachtung miteinzubeziehen.

Im Ergebnis kommt es auf eine quantitative und qualitative Gesamtbetrachtung aller relevanten Umstände des Einzelfalls an:

*«We need to move beyond naive conceptualizations of decentralization (like the % of nodes owned by an entity), and instead, holistically, understand how trust and power are given, distributed and interact.»*³¹⁵³

Als konzeptionelles Vorbild für eine Prüfung kann der in der Finanzmarktaufsichtspraxis entwickelte Gruppenbegriff betrachtet werden.³¹⁵⁴ Eine solche Herangehensweise an den Dezentralitätstest scheint sich angesichts der grundsätzlichen prinzipienbasierten Ausrichtung des schweizerischen Finanzmarktrechts (Art. 7 Abs. 2 FINMAG) besser zu eignen als die Formulierung konkreter quantitativer Vorgaben an dezentrale Systeme.

³¹⁵¹ So wohl auch Lin, *Stanford Journal of Blockchain Law & Policy* 2019, 60 («A decentralized exchange application may not be fully decentralized in all four components. Note that for many decentralized exchange applications, one or more components may be off-chain/centralized, or otherwise feature economic incentives which would promote a tendency towards centralization.»).

³¹⁵² Siehe Cambridge Centre for Alternative Finance, *Distributed Ledger Technology*, 29; kritisch hingegen, was einen «konstitutionellen Ansatz» anbelangt, da weder Interessenwahrungs- noch (politische) Vertretungspflichten einschlägig seien, Nabilou, *Stanford Journal of Blockchain Law & Policy* 2021, 31.

³¹⁵³ Siehe Lewis, *Holistic concept*, Twitter, *passim*.

³¹⁵⁴ Siehe oben, [V.1.5](#).

4.4 Rechtsfolgen des Dezentralitätstests

a. Vorbemerkungen

Die konkreten Rechtsfolgen für eine *spezifische* Handelsplattform hängen vom Bestehen oder Nichtbestehen des oben etablierten funktionalen Dezentralitätstests ab. Im Wesentlichen steht dabei die aufsichtsrechtliche und zivilrechtliche Verantwortlichkeit der beteiligten Personen im Vordergrund. Nachfolgend wird allerdings nur auf finanzmarktrechtliche Unterstellungsfragen eingegangen.

b. Bei Bestehen des Dezentralitätstests

Das Bestehen des Dezentralitätstests indiziert die Nichtunterstellung einer Handelsplattform unter die Finanzmarktgesetze. Damit ist gemeint, dass eine aufsichtsrechtliche Verantwortlichkeit für Personen ausser Betracht fällt, welche im Zusammenhang mit einer dezentralen Handelsplattform aktiv sind (insb. Softwareentwickler). Die involvierten Personen leisten *für sich allein* in rechtlicher Hinsicht vernachlässigbare Teilbeiträge zum Betrieb der Plattform. Gleichzeitig scheitert die Zurechnung der Aktivitäten zu einer bestimmten Person oder Gruppe von Personen, die miteinander verbunden sind, infolge ungenügender Kontrolle über die Plattform bzw. die Handelsaktivitäten.

Aufgrund der Dezentralität solcher Plattformen erscheint eine Unterstellung dezentraler Handelsplattformen unter die Finanzmarktgesetze als nicht notwendig.³¹⁵⁵ Für solche Handelsplattformen bedeutet dies, dass namentlich die Bestimmungen des GwG, FinfraG, BankG/FINIG oder FIDLEG nicht unmittelbar auf sie zur Anwendung gelangen. Dezentralität wirkt mit anderen Worten wie das bereits bekannte Rechtskonzept der Durchgriffshaftung bei juristischen Personen (*Piercing the Corporate Veil*), wonach nur ausnahmsweise bei Rechtsmissbrauch auf den dahinterstehenden Eigentümer zurückgegriffen werden kann.³¹⁵⁶ Im Falle von EtherDelta etwa hat die SEC den «*Veil of De-*

³¹⁵⁵ GLM. wohl Stephen D. Palley im Podcast Unchained; siehe diesbezüglich Shin, SEC Enforcement Action, Unchained Podcast («*Perhaps, there are parts of our financial world that we don't need regulators to be involved in.*»).

³¹⁵⁶ Ausführlich hierzu Meier-Hayoz/Forstmoser, Schweizerisches Gesellschaftsrecht, § 2 N 63–72 m.w.N.

centralization»³¹⁵⁷ der Handelsplattform durchstochen, was nach vorliegender Auffassung eine vertretbare Entscheidung war.

Die im Einzelfall einschlägigen Rechtsnormen sollten allerdings trotz eines positiven Testurteils, wonach grundsätzlich die Nichtunterstellung einer Handelsplattform indiziert ist, aufgrund der konkreten Umstände auf ihre Anwendbarkeit überprüft werden. Dieser Umstand wird insb. mit Blick auf die neue Regelung in Art. 4 Abs. 1 lit. b GwV evident, welche den bisherigen eindeutigen Begriff der ausschliesslichen und unmittelbaren Verfügungsmacht über fremde Vermögenswerte zugunsten eines weniger rechtssicheren Regimes aufgeben hat.³¹⁵⁸

c. Bei Nichtbestehen des Dezentralitätstests

Im Falle des Nichtbestehens des Dezentralitätstests ist grundsätzlich davon auszugehen, dass die fragliche Handelsplattform in den Geltungsbereich der Finanzmarktgesetze fällt. In diesen Fällen ist die Kontrolle über die Plattform regelmässig ungenügend verteilt, sodass die Aktivitäten der Plattform einer bestimmten Person oder einer Gruppe miteinander verbundener Personen zugerechnet werden können. Die Teilbeiträge der beteiligten Personen sind für die Existenz und den Fortbestand der Plattform entscheidend. Diese Personen sind entsprechend aufsichtsrechtlich und regelmässig auch zivilrechtlich verantwortlich.³¹⁵⁹

Im Einzelfall sollte aber ungeachtet des Ergebnisses des Dezentralitätstests in einem zweiten Schritt die Nichtanwendbarkeit der einschlägigen Bestimmungen geprüft werden. So kann es sein, dass eine semidezentrale bzw. hybride Handelsplattform trotz des negativen Testurteils ausnahmsweise dennoch nicht in den Geltungsbereich eines *bestimmten* Finanzmarktgesetzes fällt oder aber von einer Ausnahme Gebrauch machen kann.

³¹⁵⁷ Zum Begriff Walch, in: Brummer, Deconstructing Decentralization, 62.

³¹⁵⁸ Siehe hierzu oben, [V.2.6](#).

³¹⁵⁹ So auch Rettig/Mosier/Gilman, Genuine DeFi, 30, die von «System Control Person» sprechen. Siehe ferner hinsichtlich *Secondary-Liability* von u.a. Softwareentwicklern unter US-amerikanischem Recht Wright, New York University Journal of Law & Business 2021, 692–693.

d. Abschliessende Bemerkungen

Selbstverständlich schliesst das Bestehen des funktionalen Dezentralitätstest durch eine Handelsplattform nicht aus, dass die erwähnten Rechtserlasse auf Personen zur Anwendung gelangen, welche mit dezentralen Handelsplattformen interagieren oder an deren Peripherie operieren.

So können etwa die Vorgaben des FINIG für Personen einschlägig sein, welche gewerbsmässig für ihre Kunden Asset-Token über dezentrale Handelsplattformen handeln oder auf eigene Rechnung solche Token handeln (z.B. als Liquiditätsgeber bzw. Maker in einem separaten Netzwerk, das mit der dezentralen Handelsplattform interagiert).³¹⁶⁰ In diesem Zusammenhang ist sodann denkbar, dass ein berufsmässig tätiger Liquiditätsgeber, der unter das FINIG fällt, auch dem GwG unterstellt ist.³¹⁶¹ Ferner kann ein Relayer von Orders, der mit Blick auf eine dezentrale Handelsplattform ein eigenes Orderbuch mitsamt Matching-Engine unterhält, unter dem FinfraG als Finanzmarktinfrastuktur (insb. als OHS) qualifizieren. Dies könnte selbst dann der Fall sein, wenn der Relayer die wesentlichen Funktionen in einem von ihm kontrollierten Smart Contract automatisiert.³¹⁶² Schliesslich kann das Prospektrecht des FIDLEG vorbehaltlich einer gesetzlichen Ausnahme auf Emittenten zur Anwendung gelangen, wenn diese ihre eigenen Beteiligungsrechte über eine dezentrale Handelsplattform öffentlich anbieten.³¹⁶³

4.5 Einstufung der unterschiedlichen Plattformkategorien

a. Vorbemerkungen

Wie an vielen Praxisbeispielen in dieser Arbeit zum Ausdruck gebracht, stellt Dezentralität kein binäres Phänomen dar.³¹⁶⁴ Demgegenüber eröffnet sich den Entwicklern eines Protokolls ein *Spektrum* an Gestaltungsmöglichkeiten.

³¹⁶⁰ Siehe oben, [V.5.2.](#)

³¹⁶¹ Siehe oben, [V.2.7d.](#)

³¹⁶² Siehe oben, [V.3.3d.i.](#)

³¹⁶³ Siehe oben, [V.6.3b.](#)

³¹⁶⁴ Siehe statt vieler Cambridge Centre for Alternative Finance, Distributed Ledger Technology, 44–46; ferner IOSCO, Public Report DeFi 2022, 9–10, wo der Fokus auf die *Governance* (Tokens) gelegt wird.

Mit Blick auf Handelsplattformen ist das eine Extrem das zentralisierte Modell der Kryptohandelsplattform, welche alle Handelsschritte off-chain über eine zentrale Serverinfrastruktur ausführt.

Am anderen Ende des Spektrums steht der reine P2P-Austausch von Kryptovermögenswerten. In diesen Fall bestehen mit Ausnahme der netzwerkbauierten Intermediation des dezentralen Netzwerks und allenfalls einer dezentralen Applikation überhaupt keine intermediären Prozesse oder Strukturen. Alle Handelsschritte finden unmittelbar über das verteilte Netzwerk statt (on-chain).³¹⁶⁵ Es handelt sich dabei letztlich um softwarebasierte Austauschvorgänge, in deren Rahmen Drittpersonen keine relevanten Interventionsmöglichkeiten und Kontrollrechte haben bzw. die Gruppe dieser Drittpersonen von solcher Grösse ist, dass keine der ihr zugehörigen Personen für sich alleine einen relevanten Einfluss hat. In diesen Fällen kann die dezentrale Handelsplattform richtigerweise finanzmarktrechtlich auf den *Austauschvorgang* zwischen den beteiligten Parteien reduziert werden.³¹⁶⁶

Nachfolgend werden die unterschiedlichen Plattformkategorien, wie sie im vierten Kapitel gebildet wurden, mithilfe des oben entwickelten funktionalen Dezentralitätstests eingestuft. Dabei wird zur Veranschaulichung soweit sinnvoll jeweils auf Praxisbeispiele der einzelnen Kategorien hingewiesen.

b. Custodial und Custodial OTC-Handelsplattformen

Diese Plattformkategorien gelten nicht als dezentral, weil der Betreiber der Plattform neben den allgemeinen technischen Aspekten der Plattform insb. auch alle technischen Handelsfunktionen und politökonomischen Funktionen kontrolliert. Er hat etwa ausschliessliche Verfügungsmacht über die Vermögenswerte seiner Kunden, die er in einem Hosted Wallet auf seinem Server zentral abspeichert. Darüber hinaus bestimmt er die Funktionsweise des Orderbuchs, die Ausführungslogik inkl. das Matching von Orders sowie die Abwicklung eines Handelsgeschäfts. Alle diese Funktionen werden off-chain ausgeführt.

³¹⁶⁵ Vgl. Cambridge Centre for Alternative Finance, Cryptoasset Benchmarking Study, 23, wo von einer «true DEX» gesprochen wird.

³¹⁶⁶ So etwa Van Valkenburgh, No such thing as a decentralized exchange, The Block, *passim* («But if the trade is actually happening peer-to-peer, then the 'DEX' being 'used' is just software and an internet connection. In that case, there isn't a thing called a DEX. There are no DEXs; there is just decentralized exchange, the action, taking place using software tools, open blockchains, and the internet.»); ähnlich Peirce, Lawless in Austin, *passim*.

Der Betreiber alleine bestimmt ferner die «Governance» der Plattform. Der Betreiber unterhält in diesem Rahmen ein Vertragsverhältnis mit seinen Kunden, welches seine Rechte und Pflichten gegenüber den Kunden festhält. Namentlich haben diese in aller Regel keinen Anspruch auf die Zulassung neuer Kryptovermögenswerte zum Handel auf der Plattform des Betreibers. Solche Entscheidungen stehen im ausschliesslichen Ermessen des Betreibers. Es ist offensichtlich, dass der Dezentralitätstest scheitert.

c. Non-custodial P2O-Handelsplattformen

Im Vergleich zu den vorhin erwähnten zentralen Handelsplattkategorien ist eine Non-custodial P2O-Handelsplattform bereits deutlich dezentraler ausgestaltet. Dies gilt insb. mit Blick auf die Verwahrung der Kryptovermögenswerte. Allerdings ist diese Plattformkategorie in finanzmarktrechtlicher Hinsicht insofern nicht genügend dezentral, als dass sie *ebenfalls* über einen eindeutig identifizierbaren Betreiber verfügt, welcher alle technischen Aspekte der Plattform und insb. deren technischen Handelsfunktionen sowie die politökonomischen Funktionen kontrolliert. Der Betreiber tritt namentlich als Gegenpartei der Handelsgeschäfte seiner Kunden auf. Während der Vertragsabschluss zwischen den Handelsparteien (Matching) noch off-chain innerhalb der Systeme des Betreibers erfolgt, ist erst die Abwicklung des Austauschgeschäfts on-chain. Es ist darum auch hier offensichtlich, dass der Dezentralitätstest scheitern muss.

d. Escrow-basierte P2P-Handelsplattformen

Diese Plattformkategorie ist als genügend dezentral einzustufen, wenn ein allfälliger Betreiber mit Ausnahme der Bekanntmachung von Kauf- und Verkaufsinteressen der Marktteilnehmer auf der Plattform weder in das Matching der Vertragsparteien, d.h., der Vertragsschluss erfolgt auf individueller bzw. manueller Basis, noch in die Abwicklung eines Handelsgeschäfts involviert ist.

Die handelsrelevante Funktion eines allfälligen Betreibers ist in diesem Fall beschränkt auf diejenige des Betreibers eines Bulletin Boards oder dergleichen. Dies bedingt, dass der im Abwicklungsprozess eingesetzte Escrow-Mechanismus rein softwarebasiert ist (d.h. Multisig oder Smart Contract) und somit direkt on-chain erfolgt. Eine Ausnahme mag dort angezeigt sein, wo ein allfälliger Betreiber einen Streitschlichtungsmechanismus betreibt, in dessen Rahmen er Vermögenswerte verbindlich zuweisen kann. Eine Streitschlich-

tungsfunktion ist aus finanzmarktrechtlicher Sicht nicht dem eigentlichen Handelsgeschäft zuzurechnen und somit nach vorliegender Ansicht grundsätzlich nicht unterstellungspflichtig.³¹⁶⁷

Im Falle von Bisq ist selbst das Vorliegen der Betreibereigenschaft fraglich: Die Escrow-basierte P2P-Handelsplattform wird von den Nutzern *direkt* auf deren Computern ausgeführt. Die Nutzer bilden in der Folge ein eigenständiges, *ad hoc* gebildetes Netzwerk. In diesem Fall wird selbst die Bulletin Board-Funktion von den Nutzern bereitgestellt. Der Code der Bisq-Software ist ausserdem Open Source und somit für jedermann verifizierbar.³¹⁶⁸ Eine solche Plattform ist nach vorliegender Ansicht offensichtlich genügend dezentralisiert, weshalb sie den Dezentralitätstest bestehen würde.

e. Atomic Swap-basierte P2P-Handelsplattformen

Atomic Swap-basierte P2P-Handelsplattformen sind grundsätzlich vergleichbar mit der vorgenannten Kategorie. Im Wesentlichen unterscheiden sie sich von ihr im Umstand, dass sie den Austausch von Vermögenswerten unterschiedlicher Blockchains ermöglichen und zu diesem Zweck regelmässig ein separates Off-chain-Netzwerk bestehend aus Liquiditätsgebern unterhalten. Soweit die Abwicklung des Austauschprozesses wiederum ausschliesslich softwarebasiert erfolgt und das Maker-Netzwerk genügend verteilt ist, d.h. von mehreren Personen unterhalten wird, die in wirtschaftlicher oder rechtlicher Hinsicht nicht miteinander verbunden sind, ist auch diese Plattformkategorie genügend dezentralisiert (siehe sogleich unten). Massgeblich unter dem funktionalen Dezentralitätstest ist, dass die technischen Handelsfunktionen nicht aus einer Hand erbracht werden.

Ein Beispiel, das *in puncto* Dezentralität besonders heraussticht, ist DCRDEX. Dabei handelt es sich um eine Handelsplattform für Atomic Swaps, deren Software vom Nutzer direkt auf dessen Computer ausgeführt werden muss. Der Betrieb des Orderbuchs und der Matching-Engine erfolgt durch eine Vielzahl von Teilnehmern eines separaten Netzwerks. Die Software ist zudem quelloffen.³¹⁶⁹

³¹⁶⁷ Siehe weiterführend zu den unterschiedlichen Möglichkeiten der Streitbeilegung bei Nutzung dezentraler Handelsplattformen Weber/Yildiz, Jusletter vom 14. Juni 2021, Rz. 53–59, 66–71; ferner zu den Möglichkeiten und Grenzen eines rein auf Smart Contracts basierten Streiterledigungsverfahrens Specogna, Codebasiertes Regelsystem, Rz. 456–482.

³¹⁶⁸ Siehe Bisq, GitHub, *passim*.

³¹⁶⁹ Siehe Decred, DCRDEX, GitHub, *passim*.

f. Smart Contract-basierte P2P-Handelsplattformen

Smart Contract-basierte P2P-Handelsplattformen verwenden Smart Contracts für die Ausführung und Abwicklung von Austauschgeschäften. Der Austausch erfolgt direkt zwischen den beteiligten Personen. Solche Plattformen sind somit grundsätzlich ähnlich wie die vorgenannten Plattformkategorie einzustufen.

Im Falle von *EtherDelta* war die technische Handelsfunktion des Orderbuchs zentralisiert, d.h., das Orderbuch wurde off-chain auf dem Server des Betreibers bzw. Entwicklers abgespeichert und ausgeführt. Die Matching-Funktion wurde demgegenüber manuell durch die Nutzer ausgeübt und war mangels Interventionsmöglichkeit des Betreibers somit genügend dezentralisiert.³¹⁷⁰ Die Nutzer hatten zudem jederzeit die volle Kontrolle über die Vermögenswerte. Der Betreiber von *EtherDelta* hatte allerdings eine politökonomische Nebenfunktion hinsichtlich der Governance der verwendeten Smart Contracts inne, indem er selbständig die Handelsgebühren anpassen konnte. Die Zentralisierung der Orderbuch-Funktion spricht – in Übereinstimmung mit dem Vergleich zwischen Coburn und der SEC – gegen das Vorliegen einer genügend dezentralisierten Handelsplattform.³¹⁷¹ Es handelt sich bei *EtherDelta* um einen Grenzfall, der bei Gesamtbetrachtung dem vorliegend entwickelten Dezentralitätstest eher nicht genügt.

Dass gewisse Funktionen der Plattform off-chain ausgeführt werden, ist aus Sicht des Dezentralitätstests nicht *per se* problematisch. Als zulässige Relativierung wird bspw. die Verwendung von separaten Netzwerken (Relayers) betrachtet, welche etwa das Orderbuch und/oder die Matching-Engine der Handelsplattform off-chain unterhalten. Weil allerdings auch hier keine traditionellen Gegenparteirisiken bestehen, da die Kryptovermögenswerte in jedem Fall unter Kontrolle der Nutzer verbleiben, und die Nutzer das Matching selbst bewirken, ist nach vorliegender Auffassung im Grundsatz von einer dezentralen Handelsplattform auszugehen.³¹⁷² Hierzu gehören etwa Plattformen

³¹⁷⁰ Der Umstand, dass Orders innerhalb der Smart Contract-Logik zusammengeführt werden, spricht nach vorliegender Ansicht nicht für eine ungebührliche Zentralisierung der Ausführungsfunktion der Plattform.

³¹⁷¹ GLM. Glarner/Lindgren, *EtherDelta*, 5–6, die zudem die Vereinnahmung von Gebühren sowie die Kontrolle der Gebührenstruktur der Plattform durch den Betreiber von *EtherDelta* betonen; ferner wohl auch Cohen/Angelovska-Wilson/Strong, *Decentralized Finance*, *passim*.

³¹⁷² A.M. Calusic, *Decentralized Exchanges*, 47, 49, der etwa konkret 0x als DLT-Handelssystem betrachtet.

wie 0x. Diese Auffassung verdient Unterstützung, da eine reine On-chain-Perspektive dezentalisierende Lösungen ausschliessen würde, wie etwa das Hosting eines Web-Frontends und Orderbuchs über IPFS, wobei allenfalls zusätzlich die verwendeten Domänen über den Ethereum Name Service (ENS)³¹⁷³ registriert sein können. Dem Dezentralitätstest ist nach vorliegender Ansicht Genüge getan, wenn die off-chain ausgeübten Funktionen einer Plattform *ih-rerseits* genügend dezentralisiert bzw. verteilt sind. Wohingegen off-chain-Komponenten, wie namentlich die Orderbuchführung zentral erfolgen, könnte es sich aus Sicht des FinfraG um ein Handelssystem handeln, weshalb der Dezentralitätstest diesbezüglich scheitern würde.

In diesem Sinne existieren Beispiele, wie namentlich OasisDEX, Mesa oder DutchX, welche auch die technischen Handelsfunktionen der Orderbuchführung und des Matching-Mechanismus dezentral ausgestalten. Alle Handelsfunktionen laufen in diesem Fall on-chain ab. Die Benutzeroberflächen einzelner Webseiten, welche die API der Smart Contracts verwenden, gleichen am ehesten einem Bulletin Board, welches den Nutzern lediglich die relevanten Handelsdaten kommuniziert. Ferner weisen diese Plattformen keine politökonomischen Funktionen auf, wie etwa Admin Keys, welche privilegierten Personen eine kontrollrelevante Interventionsmöglichkeit mit Blick auf die Plattform gewähren würden. Der Programmcode der Plattformen ist schliesslich *queltoffen*.³¹⁷⁴ Die Benutzeroberfläche von Mesa ist ausserdem über IPFS erreichbar und somit auch in diesem Punkt dezentral ausgestaltet. Diese Plattformen erfüllen darum aller Voraussicht nach den Dezentralitätstest.

g. Smart Contract-basierte Liquiditätspools

Diese Plattformkategorie verwendet anstelle des Orderbuchmodells Liquiditätspools mitsamt automatisiertem Market Making. Zentralisierte Orderbücher können somit gar nicht erst eine Rolle spielen. Das «Matching» mit den Liquiditätsreserven und somit der Vertragsabschluss zwischen Nutzern und der Vielzahl der Liquiditätsbereitsteller erfolgt vollständig automatisiert on-chain. Die Benutzeroberflächen einzelner Webseiten, welche die API der Smart Contracts verwenden, gleichen ebenfalls am ehesten einem Bulletin Board. Die rechtliche Einstufung der Plattform ist somit ähnlich wie im Falle der vorgenannten Kategorie (insb. OasisDEX, Mesa und DutchX).

³¹⁷³ <https://ens.domains/>.

³¹⁷⁴ Siehe Dai Foundation, Maker-OTC, GitHub, *passim*; dOrgTech, dex-react, GitHub, *passim*; Gnosis, dx-contracts, GitHub, *passim*.

Uniswap gilt als das bekannteste Beispiel für diese Plattformkategorie. Das Protokoll von Uniswap beruht auf Smart Contracts, welche mit Ausnahme einiger weniger Parameter (insb. der Zuweisung der Handelsgebühren) nicht aktualisierbar sind und entsprechend auch keine Admin Keys aufweisen. Diejenigen Funktionen des Smart Contracts, die verändert werden können, sind Gegenstand einer DAO. Die Kontrolle der DAO erfolgt über den Governance Token UNI. Zwar wird die Verteilung der UNI-Token teilweise kritisiert, doch ist die Bedeutung der Governance systembedingt bereits sehr eingeschränkt. Neue Handelspaare kann grundsätzlich jedermann selbständig lancieren. Dieser Entscheid ist etwa nicht von der DAO-basierten Governance abhängig. Das Protokoll von Uniswap kann darum als sehr dezentral betrachtet werden.³¹⁷⁵ Dies gilt umso mehr, als die Plattform auch über IPFS-gehostete Frontends erreichbar ist.

h. Smart Contract-basierte Aggregatoren

Gleiches gilt für Smart Contract-basierte Aggregatoren, soweit das Order-Routing vollständig automatisiert on-chain erfolgt. Die Benutzeroberflächen einzelner Webseiten, welche die API der Smart Contracts verwenden, gleichen wiederum am ehesten einem Bulletin Board.

Rechtlich anders einzustufen sind wohl Aggregatoren, die einen Teil der Order-Routing-Berechnungen off-chain erledigen (so offenbar *1inch*).³¹⁷⁶ Die Frontends gewähren in diesem Fall Zugang zu i.d.R. zentral ausgeführten Funktionalitäten, welche über diejenigen blosser Bulletin Boards hinausgehen können. Die Order-Routing-Komponente könnte allenfalls unter FIDLEG-Gesichtspunkten problematisch sein, weshalb der Dezentralitätstest zumindest in dieser Hinsicht scheitern würde.

i. Layer-2-Handelsplattformen

Layer-2-Handelsplattformen setzen sich typischerweise aus Smart Contracts, welche an den Layer 1 des dezentralen Netzwerks anknüpfen, und einem separaten Netzwerk bestehend aus Relayern zusammen. Je nach Funktion und

³¹⁷⁵ GLM. Qureshi, What explains the rise of AMMs?, Medium, *passim* («[...] Uniswap has a very small regulatory surface. [...] Uniswap is trivially decentralized and requires no off-chain inputs. Compared to order book DEXes that have to tiptoe around the perception of operating an exchange, Uniswap is free to innovate as a pure financial utility.»).

³¹⁷⁶ Vgl. *1inch*, *1inch API*, *passim*; siehe hierzu Rai, Decentralized Exchanges, *passim*.

Plattform können Relayers auch anders bezeichnet werden (z.B. Operator, Validator oder Sequencer). Es gelten im Wesentlichen die bereits gemachten Aussagen zu Smart Contract-basierten P2P-Handelsplattformen. Mit Blick auf den Dezentralitätstest ist wesentlich, dass die am separaten Netzwerk beteiligten Relayers hinsichtlich der technischen Handelsfunktionen nicht über eine relevante Kontrolle verfügen. Falls diese separaten Netzwerke ihrerseits genügend dezentralisiert sind, sodass keine Machtkonzentration besteht, die vergleichbar mit dem Machtbereich der Consensus Power ist, können Layer-2-Handelsplattformen den Dezentralitätstest bestehen. Die Consensus Power kann bspw. auch dadurch relativiert werden, indem der Relay in regelmässigen Zeitabständen wechselt.³¹⁷⁷

Im Falle von zkSync, einer Layer-2-Handelsplattform auf Ethereum, findet etwa erst mit dem Wechsel von Version 1 zu Version 2 eine Dezentralisierung des Validatoren-Netzwerks statt.³¹⁷⁸ Falls Relayern demgegenüber etwa Transaktionen permanent verhindern können, stellt dies die Manipulationsresistenz des Layer-2-Protokolls infrage. In diesem Zusammenhang ist auch wesentlich, dass Nutzer ihre Vermögenswerte jederzeit *einseitig*, unter Beachtung einer allfälligen Wartezeit, im verteilten Register des zugrundeliegenden dezentralen Netzwerks (Layer 1) abbilden können.

Die Handelsplattform *Loopring*, welche für das Layer-2-Protokoll auf ZK-Rollups setzt, kann nach vorliegender Ansicht etwa als genügend dezentralisiert eingestuft werden. Wiederum haben Benutzeroberflächen, welche allenfalls auch zentralisiert betrieben werden, die grösste Ähnlichkeit mit Bulletin Boards. Das finanzmarktrechtlich relevante «Backend», mit welchem diese Schnittstellen verbunden sind, bilden die Smart Contracts und das verteilte Layer-2-Netzwerk.

j. On-chain-Handelsplattformen

Diese Plattformkategorie setzt als Systemfunktion, gleich wie alle anderen Plattformkategorien, ein genügend dezentralisiertes Netzwerk voraus. Diese Funktion ist besonders erwähnenswert, weil On-chain-Handelsplattformen aufgrund ihrer Skalierbarkeit besonders rechenintensive Protokolle benötigen. Dies kann u.U. die Validation Power der Netzwerkteilnehmer negativ beeinflussen.

³¹⁷⁷ Vgl. für diesen und weitere Vorschläge Buterin, *Incomplete Guide to Rollups*, *passim*.

³¹⁷⁸ Siehe zkSync, *Decentralization*, *passim*.

Ein Beispiel einer On-chain-Handelsplattform ist *Serum*, welche über die Solana Blockchain ausgeführt wird. Alle technischen Handelsfunktionen werden on-chain ausgeführt. Die Nutzer interagieren direkt miteinander über ein auf dem dezentralen Netzwerk ausgeführtes Programm. Lediglich für die Funktion, die Matching-Engine regelmässig zu aktualisieren, wird auf ein separates Netzwerk von Teilnehmern zurückgegriffen. Vorausgesetzt ist auch hier, dass dieses separate Netzwerk selbst genügend dezentralisiert ist. Bezüglich politökonomischer Funktionen ist zu erwähnen, dass die der Handelsplattform zugrundeliegenden Programme von unterschiedlichen webbasierten Benutzeroberflächen erreichbar sind und dass der Softwarecode der Plattform öffentlich zugänglich ist.³¹⁷⁹ Einmal mehr ist die Rolle solcher Webseiten am ehesten mit der Kursinformationsfunktion von Bulletin Boards vergleichbar.

k. Hybride Handelsplattformen

Schliesslich ist noch auf hybride Handelsplattformen einzugehen. Dieser Plattformtyp kann die unterschiedlichen Komponenten der vorgenannten Plattformkategorien miteinander verbinden. Entsprechend kommt eine verallgemeinernde Einstufung nicht infrage.

Mit Blick auf IDEX ist jedoch festzuhalten, dass die Zentralisierung des Orderbuchs sowie die Kontrollfunktion des Betreibers hinsichtlich der Abwicklung von Handelsgeschäften bereits genügen, dass der Dezentralitätstest scheitert.

³¹⁷⁹ Siehe Project Serum, GitHub, *passim*.

5. Diskussion

In der kurzen Phase, seit sich der Gesetzgeber und die Behörden mit dezentralen Systemen beschäftigen können, konnte sich Dezentralität als Rechtsprinzip *etablieren*. Das Rechtsprinzip hat namentlich nicht nur in der Gesetzgebung (DLT-Mantelrevision), sondern auch in der Aufsichtspraxis der FINMA und der Rechtsprechung des Bundesverwaltungsgerichts (Fall «E-Coins») Bedeutung erlangt. Der genaue Inhalt und Umfang des Prinzips sind allerdings konkretisierungsbedürftig geblieben.

Der vorliegend entwickelte funktionale Dezentralitätstest als Ausfluss des Rechtsprinzips soll aus diesem Grund primär dem Anliegen dienen, möglichst zuverlässige Aussagen über die Unterstellung von Handelsplattformen unter die schweizerischen Finanzmarktgesetze machen zu können. Handelsplattformen, welche die Anforderungen des funktionalen Dezentralitätstest (ständig) erfüllen, fallen demnach *grundsätzlich nicht* in den Geltungsbereich der Finanzmarktgesetze. Sie sind trotz der Existenz von Softwareentwicklern und weiterer beteiligter Personen als «herrenlose» Computerprogramme zu betrachten, die durch eine Unzahl von Personen gemeinsam betrieben werden.

Dezentralität ist aufgrund der *Komplexität* ein objektiv schwer fassbares Phänomen. Dies liegt einerseits daran, dass Macht und Kontrolle vielschichtige und anspruchsvolle Themen sind, die weder ausschliesslich technologisch noch ausschliesslich ökonomisch oder spieltheoretisch verstanden werden können. Andererseits ist die Komplexität in der verwendeten Technologie begründet: Blockchain-Protokolle unterliegen Trade-offs, namentlich zwischen Dezentralisierung, Sicherheit und Skalierbarkeit.³¹⁸⁰ Ein System, das etwa sehr gut skaliert, muss Abstriche entweder in der Sicherheit oder Dezentralität des Netzwerks machen. Projekte seit Bitcoin und Ethereum sind aufgrund abweichender inhaltlicher Vorstellungen unterschiedliche Kompromisse in dieser Hinsicht eingegangen.³¹⁸¹

Ferner sind dezentrale System aufgrund ihrer Teilnahmeanfälligkeit und kryptoökonomischen Anreizsysteme *in dauerndem Wandel* begriffen.³¹⁸² Bitcoins monetäres Emissionsprogramm etwa halbiert sich alle vier Jahre, währenddessen die Rolle von Transaktionsgebühren als «Sicherheitsbudget» des Netzwerks an

³¹⁸⁰ Vgl. zum DCS-Theorem oben, [III.5.1](#).

³¹⁸¹ Siehe Burke, Pathway to Decentralisation, *passim*.

³¹⁸² So auch Walch, in: Brummer, Deconstructing Decentralization, 50, 60–61.

Bedeutung gewinnt.³¹⁸³ Die Herausbildung perfekter Systeme ist unter dynamischen Umständen eher nicht zu erwarten.³¹⁸⁴ «*Sadly, there is no free lunch in decentralization.*»³¹⁸⁵

Perfektion ist aber auch nicht notwendig, um Dezentralität als Rechtsprinzip formulieren zu können. Dies alles ist ein Zeichen dafür, dass viele dezentrale Systeme noch in einem experimentellen Entwicklungsstadium stecken. Letztlich sind soziotechnische Systeme vergleichbar fehleranfällig wie der demokratische Entscheidungsprozess. Daran zu scheitern, Governance als vollendetes öffentliches Gut schaffen zu können, scheint damit letztlich struktureller Defizite des menschlichen Zusammenlebens geschuldet zu sein.³¹⁸⁶ Entsprechend sind auch zentrale Governance-Modelle oft ein Ort von Versuch und Irrtum.

Der *Dezentralitätstest* zeigt sodann auf, dass grundsätzlich kein einziger Aspekt oder Faktor ausschliesslich für das Vorliegen bzw. Nichtvorliegen von Dezentralität verantwortlich ist. Ferner ist das vorbehaltlose Bestehen des Dezentralitätstests in der Praxis ein wohl kaum erreichbares Ideal (und wird es wohl für die nahe Zukunft auch bleiben).³¹⁸⁷

³¹⁸³ Über die Folgen dieser Entwicklung besteht wenig Einigkeit in der Literatur; vgl. etwa Carlsen et al., *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security* 2016, *passim*; Auer, *BIS Working Papers* Nr. 765, Januar 2019, 18–19; ferner für eine Übersicht mit weiteren Nachweisen Shin, *Can Bitcoin Be Secured Only by Transaction Fees?*, *Unchained Podcast*, *passim*.

³¹⁸⁴ Vgl. etwa Kwon et al., *Proceedings of the 1st ACM Conference on Advances in Financial Technologies* 2019, 115–116, 122, deren «Unmöglichkeitanalyse» auf die Widerstandsfähigkeit eines dezentralen Systems gegen Sybil-Attacken abstellt, weshalb sie primär ein wirtschaftliches Verteilungsproblem zum Gegenstand hat.

³¹⁸⁵ Troncoso et al., *Proceedings on Privacy Enhancing Technologies* 2017, 316.

³¹⁸⁶ Dazu passt, dass sich die ökonomische Literatur nicht einig ist, ob Governance bzw. das Rechtssystem als öffentliches Gut mit (relativ) dauerhaft stabilen Bedingungen definiert werden kann; vgl. zur Debatte Cowen, *Economics and Philosophy* 1992, 265, und Friedman, *Economics and Philosophy* 1994, 320.

³¹⁸⁷ G.L.M. Sheng, *Let's ditch decentralized*, *passim* («*It's not something that can be reached, but a useful thing to reach towards.*»); ferner Shapiro, *Defining Decentralization*, *passim* («*This will typically be a difficult test to meet. And it should be a difficult test to meet. The purpose of finding that a blockchain system is sufficiently decentralized as a matter of law is to declare that since no person controls the system, no person is legally responsible for it and it is not subject to regulations, such as securities laws, that would ordinarily apply in similar circumstances. For this, the blockchain system must essentially be an un-owned, public commons. To qualify as such, it should truly exist for the benefit of and under the control of the public, rather than predominantly serving the interests of any specific person or group.*»).

Die Schwierigkeit, ein Computerprotokoll zu dezentralisieren, ist vorwiegend im Umstand begründet, dass dezentrale Prozesse und Strukturen auf die Zwangsläufigkeit ökonomischer Gesetze prallen. Hierzu gehören insb. der natürliche Hang des Marktes zur Spezialisierung und zur Ausnutzung von Netzwerkeffekten. Beide weisen in der Praxis nicht zu unterschätzende Reintermediationseffekte auf, die selbst in einem anfänglich dezentralen System wieder Single Points of Control (SPoCs) einführen können. Mit anderen Worten scheinen gerade relativ simple Anreizsysteme, die in der Praxis gut funktionieren, sich potenziell re-zentralisierend auszuwirken.³¹⁸⁸ Die konkrete Ausgestaltung der Konsensalgorithmen kann darum bedeutende Implikationen für eine all-fällige Re-zentralisierung eines Protokolls mit sich bringen.³¹⁸⁹ Eine system-theoretische Analyse bestätigt diese Erkenntnis: Komplexe Systeme tendieren dazu, in erster Linie hierarchische Subsysteme herauszubilden mit dem Ziel, die systemimmanente Komplexität zu reduzieren.³¹⁹⁰ In dezentralen Systemen können dies etwa Entwicklergemeinschaften, Mining Pools und einflussreiche DAOs sein.

Wenig überraschend bezeichnen Regulatoren viele der aktuell verwendeten Prozesse und Strukturen als *Decentralized In Name Only* bzw. DINO.³¹⁹¹ Kritische Stimmen sprechen von «Dezentralität als Illusion»³¹⁹², einem «Dezentralitäts-Theater»³¹⁹³ oder aber davon, dass lediglich das relativ simple kryptoökonomische Design von Bitcoin die Dezentralitätshypothese langfristig erfüllen könne³¹⁹⁴. Die Dezentralität vieler Phänomene wird kritisch hinterfragt. In vielen Fällen erfolgt dies durchaus zu Recht. Jedoch gibt es Ausnahmen, welchen nach vorliegender Ansicht angemessen Rechnung zu tragen ist.³¹⁹⁵

³¹⁸⁸ Vgl. etwa zur Debatte rund um die Algorand Blockchain, welche zu Beginn gänzlich auf monetäre Anreize verzichtet hat, Castor, No Incentive, Coindesk, *passim*; ferner hierzu Gauba/Koticha, Need for an Incentive Scheme, *passim*.

³¹⁸⁹ Siehe Lewis, Sybil, Twitter, *passim* («The nature of sybil resistance in blockchains dictates how centralization emerges.»).

³¹⁹⁰ Siehe Simon, Proceedings of the American Philosophical Society 1962, 473.

³¹⁹¹ Vgl. etwa den Verweis auf einen solchen Fall bei Peirce, Twitter, *passim*.

³¹⁹² So etwa Schneider, Journal of Cultural Economy 2019, 280, wobei die Unvollständigkeit der Dezentralisierung aus der angeblich fehlenden Verantwortlichkeit der beteiligten Personen abgeleitet wird (siehe 281); ferner Aramonte/Huang/Schrimpff, BIS Quarterly Review, Dezember 2021, 21, wonach «some form of centralisation» unvermeidlich sei, ferner 27–29.

³¹⁹³ Vgl. Morris, Decentralization Theater, Coindesk, *passim*.

³¹⁹⁴ Siehe Farrington/Big Al, Philosophical, Technical, and Economic Critique, 8–14.

³¹⁹⁵ Siehe zum funktionalen Regulierungsansatz oben, [VII.2.6](#).

Nichtsdestotrotz kommt dem Phänomen der Dezentralität normative Bedeutung als Rechtsprinzip zu. Dies scheint nicht zwingend zu sein, könnte doch die Rechtsordnung völlig gleichgültig gegenüber dezentralen Prozessen und Strukturen sein und diese somit gleich oder ähnlich wie die traditionelle Finanzintermediation erfassen.³¹⁹⁶ Kommt man aber wie die vorliegende Arbeit zum Schluss, dass Dezentralität mit Kontroll- und Machtverteilung zu tun hat, wird einem klar, dass die Rechtsordnung Dezentralität als Rechtsprinzip ernst zu nehmen hat. Während das Recht und somit auch der Staat selbst Inbegriff von Macht sind,³¹⁹⁷ gehört das Aufbrechen von als ungerecht empfundenen Kontroll- und Machtstrukturen in der Gesellschaft – in einem gewissen Sinne paradoxerweise – ebenfalls zu den ureigenen Aufgaben der Rechtsordnung.³¹⁹⁸ Es sprechen mit anderen Worten nicht ausschliesslich rein praktische Erwägungen für die Anerkennung des Rechtsprinzips in den Rechtswissenschaften.³¹⁹⁹

Dezentralität als Rechtsprinzip sollte nach vorliegender Ansicht dort zur Abwendung von traditionellen Regulierungsansätzen führen, wo das einem Netzwerk oder einer Applikation zugrundeliegende Protokoll in gemeinschaftlicher Weise ausgeführt und unterhalten wird. Darunter fallen in erster Linie entwicklungs offene Protokolle, deren Regeln von einer Mehrzahl von Personen validiert werden. Auch die DAO-basierte Governance von Applikationen erfüllt diese Anforderungen, wenn die Governance Token genügend breit und gleichmässig verteilt sind und die Teilnahme an bedeutsamen Entscheidungsprozessen ohne grosse Hürden möglich ist. Unproblematisch sind schliesslich Protokolle und Smart Contracts, welche *by design* die Kontrolle durch Dritte eliminieren. Wesentlich ist schliesslich auch, dass Informationsasymmetrien und Machtungleichgewichte protokollbedingt oder aufgrund der Tokenbesitzverhältnisse ausgeschlossen sind. In diesen Fällen treten der finanzmarktrechtliche Anleger- und Funktionsschutz in den Hintergrund.

Können einzelne Netzwerkteilnehmer direkt und permanent Transaktionen beeinflussen oder sehen Smart Contracts Admin Keys für eine Gruppe von miteinander verbundenen Personen vorsehen, gilt dagegen das Rechtsprinzip der Dezentralität *nicht*. Der Finanzmarktaufsicht soll in diesen Fällen durch das Prinzip keine Hürden in den Weg gelegt werden. Das massgebliche Ab-

³¹⁹⁶ Vgl. auch Shapiro, Defining Decentralization, *passim* m.w.H.

³¹⁹⁷ So etwa Bastiat, La Loi, 346–347; Mill, in: Bromwich/Kateb, On Liberty, 73–85; Kelsen, in: Jestaedt, Reine Rechtslehre, 135; ferner Foucault, History of Sexuality, 135–145; schliesslich Rothbard, Treatise on Economics, 1326–1333.

³¹⁹⁸ Siehe etwa Raz, Authority of Law, 169–171.

³¹⁹⁹ Kritisch demgegenüber Walch, in: Brummer, Deconstructing Decentralization, 58.

grenzungskriterium ist darin zu erblicken, ob Netzwerkteilnehmer oder andere kontrollrelevante Personengruppen als derart miteinander verbunden zu betrachten sind, dass eine Gleichbehandlung mit Personen, die nach bisheriger Aufsichtspraxis als finanzmarktrechtlich relevante Gruppe qualifizieren, gerechtfertigt erscheint.

Dezentralität als Rechtsprinzip zielt auf «regulierte Autonomie»³²⁰⁰ ab. Innerhalb dieses Autonomiebereichs gehorchen dezentrale Systeme den eigengesetzlichen Vorgaben. Der Softwarecode wird zum Programm, dessen Inhalt im Idealfall wiederum ausschliesslich durch die eigene Funktionalität bestimmt wird. Ihr dezentraler Charakter macht sie mit anderen Worten für *einzelne* private und öffentliche Akteure gleichermassen *unbeherrschbar*. Dezentralität als Rechtsprinzip fördert und bewahrt die Eigengesetzlichkeit dieser soziotechnischen Systeme.

³²⁰⁰ Siehe hierzu Teubner/Willke, Zeitschrift für Rechtssoziologie, 1984, 24.

6. Zusammenfassung Kapitel VII

Dieses Kapitel untersucht im Wesentlichen die Fragestellung, ob der Dezentralität als einem soziotechnischen Phänomen eine Bedeutung als Rechtsprinzip zukommt:

Im *ersten* Abschnitt wird an die technischen Eigenschaften dezentraler Systeme erinnert. Dezentralität als Rechtsprinzip muss an diese technischen Vorarbeiten anschliessen, bedarf jedoch, um rechtlich operabel zu sein, weiterer Konkretisierungen (siehe unten). Sodann wird festgehalten, dass Dezentralität keinen Selbstzweck bildet, sondern ein Mittel zum Zweck darstellt. Der Zweck besteht namentlich darin, nutzungs-, teilnahme- und entwicklungsoffene Systeme zu begründen und verfügbar zu machen. Bei diesen Systemen handelt es sich um öffentliche Koordinationsmechanismen, welche grundsätzlich in allen drei Dimensionen (Nutzung, Teilnahme und Entwicklung) frei zugänglich sind und darum einen konkreten gesamtgesellschaftlichen Wert darstellen. Die Vorteile von Dezentralität erstrecken sich potenziell weit über das heutige Finanzsystem hinaus. Eine innovationsoffene Rechtsordnung sollte sich nach vorliegender Auffassung die Vorteile zunutze machen, indem sie Dezentralität als Rechtsprinzip anerkennt.

Im *zweiten* Abschnitt des Kapitels geht die vorliegende Arbeit auf die bestehende Verankerung von Dezentralität als Ordnungsprinzip in der Wirtschafts- und Rechtsordnung ein. Ausgehend von einer Parallele zur wettbewerblich orientierten Wirtschaftsordnung im Ordoliberalismus zeigt die Arbeit auf, dass Dezentralität im heutigen Verfassungsrecht, Zivilrecht, Wertpapier- und Finanzmarktrecht sowie Steuerrecht bereits bedeutende Ableger gefunden hat. Als Beispiele im Verfassungsrecht sind sowohl der wirtschaftsverfassungsrechtliche Grundsatzentscheid in Art. 94 BV als auch die politische Ordnung bestehend aus Föderalismus und Subsidiaritätsprinzip zu erwähnen. Im Zivilrecht können etwa die Privatautonomie und das Konzernrecht als Ausprägungen des Ordnungsprinzips der Dezentralität verstanden werden. Allen diesen Bereichen gemeinsam ist die Frage der angemessenen Macht- und Kontrollverteilung. Schliesslich untersucht die Arbeit, ob Dezentralität als Ordnungsprinzip auch Einzug in das Wertpapier- und Finanzmarktrecht gefunden hat. Es lässt sich aufzeigen, dass beide Rechtsgebiete aufgrund der kürzlich durchgeführten DLT-Mantelrevision nunmehr das Ordnungsprinzip der Dezentralität anerkennen. Dabei findet das Prinzip gleichermassen auf dezentrale Netzwerke und dezentrale Applikationen Anwendung. Dennoch zeigen sich gewissen Tendenzen im Finanzmarktrecht, allen

voran im Geldwäschereibereich, wonach in nicht allzu ferner Zukunft mit gewissen regulatorischen Eingriffen in das Ordnungsprinzip der Dezentralität zu rechnen ist.

Der *dritte* Abschnitt beschäftigt sich mit der zentralen Frage nach der Einführung eines Rechtsprinzips im Bereich dezentraler Systeme. Dabei wird ersichtlich, dass der Dezentralitätsbegriff in rechtlicher Hinsicht stark konkretisierungsbedürftig ist. In der Lehre und Praxis wird aus diesem Grund ein Dezentralitätstest vorgeschlagen. Mit dem Dezentralitätstest sollen normative Wirkungen verbunden sein. So unterstehen nach derzeitiger Praxis der SEC dezentrale Netzwerke nicht dem US-amerikanischem Wertpapierrecht, wenn die Netzwerke genügend dezentralisiert sind. Eine einheitliche Auffassung darüber, an welche Kriterien dieser Test anknüpfen soll, fehlt allerdings. Als mögliche Orientierungspunkte kommen nach vorliegender Ansicht zwei Konzepte infrage: Nach dem Konzept der Vertrauensminimierung sind Systeme dann genügend dezentral, wenn Nutzer keiner einzelnen Person für den Fortbestand des Systems vertrauen müssen. Demgegenüber stellt das Konzept der Entmachtung darauf ab, ob die Kontrolle über bestimmte Machtbereiche genügend verteilt sind. Die Arbeit kommt zum Schluss, dass beide Orientierungspunkte als Grundlage dienen können, wobei dem Entmachtungsansatz aber der Vorzug einzuräumen ist. In der Folge wird das Rechtsprinzip der Dezentralität beispielhalber auf dezentrale Netzwerke angewendet. Dabei sticht heraus, dass es nicht bloss auf die Anzahl beteiligter Netzwerkteilnehmer ankommen kann, sondern dass deren effektive Unabhängigkeit voneinander massgeblich ist. Weitere Elemente, die zur Dezentralität eines Netzwerks beitragen, sind die Manipulationsresistenz der Daten, die Publizität von Code und der im verteilten Register abgespeicherten Daten sowie die Belastbarkeit der kryptoökonomischen Anreizmechanismen. Wenn diese Bedingungen vorliegen, kann grundsätzlich von einem genügend dezentralisierten Netzwerk im Sinne des Rechtsprinzips der Dezentralität gesprochen werden.

Im *vierten* Abschnitt wird schliesslich ein Dezentralitätstest für Handelsplattformen entwickelt. Als Prüfpunkte des Tests dienen die konkreten Funktionen einer Handelsplattform. Unterschieden wird zwischen den Hauptfunktionen, wozu die Systemfunktionen, die technischen Handelsfunktionen und die politökonomischen Funktionen gehören, und den Nebenfunktionen. Die Hauptfunktionen sind zentral für das Bestehen bzw. Nichtbestehen des Dezentralitätstests. Nebenfunktionen weisen demgegenüber lediglich eine geringe oder keine Bedeutung für den Ausgang des Tests auf. Entscheidend ist aber letztlich eine Gesamtbetrachtung der Funktionen. Das Bestehen des Dezentralitätstests indiziert, dass grundsätzlich keine Finanzmarktgesetze zur Anwendung

gelangen. Das Nichtbestehen des Tests indiziert demgegenüber die Unterstellung einer Plattform unter die jeweils einschlägigen Gesetze. «Manuelle» Korrekturen am Testergebnis scheinen in beiden Fällen angezeigt. Abschliessend werden die gewonnenen Erkenntnisse auf die in Kapitel IV gebildeten Plattformkategorien angewendet. Mit Blick auf die jeweilige Plattformkategorie können mithilfe des funktionalen Dezentralitätstests bis zu einem gewissen Grad belastbare Aussagen zur Unterstellung gemacht werden.

Der *letzte* Abschnitt geht im Rahmen einer Diskussion auf mögliche Vorbehalte gegenüber dem Rechtsprinzip der Dezentralität ein. Dabei stellt sich heraus, dass v.a. der noch sehr experimentelle Charakter dezentraler Systeme gegen ein allzu umfassendes Rechtsprinzip sprechen könnte.

VIII. Schlussthesen

*The future is open. It is not fixed in advance.
So no one can predict it – except by chance.
The possibilities lying within the future,
both good and bad, are boundless.*

– Karl Popper³²⁰¹

1. **Dezentrale Systeme sind ein Phänomen, das zwischen Markt und Finanzmarktpolitik eingepfercht zu sein scheint**

Das Internet hat seit seinen Anfängen in den frühen 1960er Jahren eine wechselhafte Entwicklung durchlebt: Aus einer ehemals militärischen und sodann akademischen Einrichtung wurde ein kommerzielles Phänomen, das mit dem WWW in den 1990er Jahren seinen Lauf nahm.³²⁰²

Dabei ist das Internet auch immer wieder mit dem Finanzmarkt in Kontakt gekommen: zuerst als effizientes Kommunikationsmittel der Teilnehmer an Handelsplätzen in den 1970er Jahren, sodann als abermals neuer Absatzkanal für Penny Stocks und schliesslich als Schauplatz der zerplatzten Geschäftsmodelle von Internetfirmen in der Dot-com-Blase in den Nullerjahren. Mit dem Auftreten der einflussreichen Online-Intermediäre aus dem Silicon Valley wurde sodann zunehmend auch der politische Geist geweckt.

Ähnliches gilt seit dem Aufkommen von Bitcoin in den Jahren 2008-09. Es gibt derzeit kaum ein Finanzbereich, der so hohe politische Wellen schlägt, wie die Innovation dezentraler Systeme. Aus einfachen monetären Transaktionen über die Blockchain sind Smart Contracts und Protokolle geworden, welche bisher intermediatisierte Prozesse und Strukturen der Finanzwelt zu ersetzen beabsichtigen. Dezentrale Handelsplattformen bilden einen zentralen Teil dieser Entwicklung.

³²⁰¹ Popper, in: Popper, *The Necessity of Peace*, 143.

³²⁰² Siehe ausführlich hierzu Leiner et al., *Brief History of the Internet*, *passim*.

Die konkreten Auswirkungen dezentraler Systeme für die Gesellschaft sind derzeit noch nicht in vollem Umfang absehbar. Dezentrale Handelsplattformen zeigen jedoch ansatzweise bereits, dass ein effizienter unintermediierter Austausch von Vermögenswerten im Finanzmarkt möglich ist. Das politische Interesse an dezentralen Systemen und somit auch an dezentralen Handelsplattformen wird in den kommenden Jahren *deutlich zunehmen*. Ob dabei ein innovationsfreundlicher oder doch eher ein regulierungsfreudiger Ansatz gewählt wird, ist derzeit offen, wobei in der Tendenz die letztere Entwicklung als derzeit wahrscheinlicher erscheint.³²⁰³

Die Tatsache jedoch, dass technologischer Wandel langwierige gesellschaftliche Verwerfungen auslösen kann, weshalb Veränderungen selbst nach der Realisierung erster Ergebnisse weiterhin mit grossen Unsicherheiten verbunden sind, sollte zu einer zurückhaltenden regulatorischen Erfassung dezentraler Systeme mahnen.³²⁰⁴

³²⁰³ Vgl. etwa oben, [VII.2.6](#).

³²⁰⁴ Vgl. hierzu Rosenberg, in: Landau/Taylor/Wright, Uncertainty and Technological Change, *passim*.

2. Die Wechselhaftigkeit von Intermediation und Disintermediation bestätigt sich auch für dezentrale Systeme

Pendelbewegungen zwischen Intermediation und Disintermediation gleichen einer historischen Konstante.³²⁰⁵ Zwar haben Arbeitsteilung, Spezialisierung und Geldwirtschaft dazu geführt, dass immer weitere Teile des Wirtschaftslebens intermediatisiert worden sind, doch lassen sich gerade für das digitale und informationelle Zeitalter vermehrt Disintermediationseffekte finden.

Intermediation und Disintermediation können aus der Perspektive der Zentralisierung bzw. Dezentralisierung von Entscheidungsgewalt und Kontrolle betrachtet werden.³²⁰⁶ In diesem Fall fällt auf, dass Technologie grundsätzlich indifferent gegenüber der Verteilung von Entscheidungsgewalt und Kontrolle ist. Es können mit anderen Worten keine klaren Aussagen zum Entwicklungszusammenhang zwischen Technologie und Zentralisierung bzw. Dezentralisierung gemacht werden.

Im Gegenteil sind beide Entwicklungen möglich und plausibel: Während dezentrale Systeme klarerweise in die Richtung der Dezentralisierung von Macht und Entscheidungsgewalt gehen, stellt die Herausgabe von CBDCs durch Staaten bzw. deren Zentralbanken den geldpolitischen Extremfall von Zentralisierung und somit von Intermediation dar. Besonders wenn diese Entwicklung mit Sichtguthaben der Bürger bei der Zentralbank gepaart wird, kann finanzwirtschaftlich von vollendeter Intermediation gesprochen werden.³²⁰⁷

Demgegenüber ergibt sich ein *geteiltes Bild* für dezentrale Systeme: Im Wesentlichen bildet sich um ein auf Dezentralisierung von Entscheidungsgewalt und Kontrolle ausgerichtetes Netzwerk eine Vielzahl von Applikationen und ein Ökosystem von Dienstleistern aus, welche in vielen Fällen den Gesetzen der logischen Zentralisierung gehorchen. Dies hat für das dezentrale Netzwerk durchaus auch systemwidrige Reintermediationseffekte zur Folge, wie etwa am Machtbereich der Economic Power gut erkennbar ist.³²⁰⁸ Trotz dieser Ent-

³²⁰⁵ Siehe oben, [II.1.2](#) und [II.1.4](#).

³²⁰⁶ Siehe oben, [II.1.5](#).

³²⁰⁷ Siehe oben, [II.3.2e](#).

³²⁰⁸ Siehe hierzu oben, [VII.3.2c.ii](#).

wicklungen besteht daneben, bis zu einem gewissen Grad verselbständigt sozusagen, das dezentrale System als Ausdruck netzwerkbasierter Intermediation.

Im Ergebnis kann also festgehalten werden, dass dezentrale Systeme Anschauungsmaterial für die *unaufhörliche Wechselhaftigkeit* von Intermediation und Disintermediation sind. Dies ändert allerdings nichts an der Tatsache, dass Dezentralität als soziotechnisches Phänomen existiert, weshalb nach vorliegender Ansicht auf dezentrale Netzwerke und Applikationen das Rechtsprinzip der Dezentralität zur Anwendung gelangen soll.

3. Dezentrale Systeme basieren auf eigenständigen Regelungs- und Handlungsstrukturen, weshalb sie mit der Rechtsordnung bis zu einem gewissen Grad in Konkurrenz stehen

Gemäss der vorliegenden Untersuchung weisen dezentrale Systeme Ähnlichkeiten mit Marktmechanismen, hierarchischen Prozessen, wie sie in Firmen existieren, und Netzwerken auf, deren Mitglieder auf gleicher Augenhöhe miteinander kooperieren. Dezentrale Systeme verbinden Eigenschaften dieser unterschiedlichen Organisationsformen. Sie stellen darum eine neuartige Form der gemeinschaftlichen Organisation wirtschaftlicher Transaktionen dar.³²⁰⁹

Kryptowährungen und Smart Contracts sind in erster Linie lediglich die technischen Bausteine dezentraler Netzwerke und Applikationen. Wird jedoch der Fokus auf die koordinierende Funktion von dezentralen Systemen gelegt, so wird deutlich, dass Kryptowährungen und Smart Contracts die Grundlagen für *eigenständige Handlungs- und Regelungsstrukturen* begründen können. Dementsprechend handelt es sich bei dezentralen Systemen um einen öffentlichen und transparenten Governance-Mechanismus, der idealerweise die Interaktionen unzähliger Menschen koordiniert.

Üblicherweise verbindet die Teilnehmer eines dezentralen Netzwerks nicht der Wille, durch ihre Handlungen rechtlich gebunden zu sein. Es liegt somit gerade kein «Vertragsnetzwerk» vor.³²¹⁰ Nicht primär Kooperation, sondern *algorithmische Koordination* steht im Zentrum. Der Computercode soll insofern verbindlich sein, als dass er zur Stabilität des Netzwerks beiträgt. Kryptoökonomische Anreize überlagern in der Folge die soziale und rechtliche Verhaltenssteuerung. Das alleinige oder vorrangige Abstellen auf staatliche Regulierung erscheint demgegenüber angesichts der Quasi-Autonomie von Blockchain-basierter Software als wenig zielführend.

³²⁰⁹ Siehe oben, [II.5.2a](#).

³²¹⁰ Vgl. Teubner, ZHR 1990, *passim*.

Ein dezentrales System muss innerhalb einer gewissen vertretbaren Bandbreite von der Rechtsordnung losgelöst agieren können. Die Rechtsordnung sollte solchen Systemen deshalb einen angemessenen Entfaltungsraum einräumen. Dies bedeutet aber nicht, dass das Recht in einem dezentralen Kontext nicht mehr gilt. Die *Steuerungswirkung* traditioneller Rechtsinstrumente scheint aber aufgrund der Eigenschaften dezentraler Systeme stark eingeschränkt.

Die Rechtsordnung sollte dagegen die Realität legitimer Strukturen in generell-abstrakter Weise *anerkennen*.³²¹¹ Hierin besteht die hauptsächliche Steuerungswirkung des Rechts in Bezug auf dezentrale Systeme. Machbarkeitswahn, der *Law* zu *Code* machen will, würde demgegenüber fast zwangsläufig die Dezentralität des Systems zunichte machen. In diesem Sinne sollte die Machtverschiebung von intermediären zu netzwerkbasierten Prozessen und Strukturen als volkswirtschaftliche Chance und nicht als Problem betrachtet werden.

Der bisher in der Schweiz verfolgte finanzmarktrechtliche Ansatz ist von einem realistischen und sinnvollen Verständnis dezentraler Systeme geprägt, was letztlich auch in der Herausbildung des Rechtsprinzips der Dezentralität zum Ausdruck kommt.

³²¹¹ Siehe oben, [VI.4.3c.ii.](#)

4. Der von der Finanzmarktaufsicht verfolgte funktionale Ansatz ist grundsätzlich auch für DeFi angemessen, muss aber den anders gearteten Risiken dezentraler Handelsplattformen Rechnung tragen

Der Fokus der heutigen Aufsichtspraxis der FINMA liegt auf der wirtschaftlichen Funktion und dem Zweck einer Aktivität (substance over form) entlang den bewährten Wertungsentscheiden des Gesetzgebers (same business, same risks, same rules) und unter Berücksichtigung der Besonderheiten des Einzelfalles.³²¹²

Die Ausrichtung dieser Praxis ist auch in einer Welt der DeFi-Anwendungen im Grundsatz *weiterhin angemessen*. Allerdings ist gerade in Bezug auf dezentrale Handelsplattformen dem in wesentlichen Punkten abweichenden Risikoprofil Rechnung zu tragen. Dezentrale Handelsplattformen bringen etwa keine Gegenparteirisiken mit sich, wie sie für die Bankenaufsicht typisch sind.³²¹³ Entsprechend machen bankenrechtliche Regulierungsansätze für dezentrale Handelsplattformen nur bedingt Sinn. Ähnliches gilt für das Finanzmarktinfrastrukturrecht, das traditionellerweise die einzelnen Handels- und Handelsschritte getrennt reguliert, was etwa den Realitäten des Atomic Settlement eines Smart Contract-basierten Austauschgeschäfts nicht gerecht wird.³²¹⁴

Demgegenüber weisen dezentrale Handelsplattformen *anders geartete Risiken* für die Nutzer auf, welche ihren Ursprung insb. in der Qualität und Sicherheit des verwendeten Softwarecodes haben. Solchen Elementen sollte die Finanzmarktaufsicht vermehrt Rechnung tragen. Die Funktion und der Zweck einer DeFi-Aktivität sind zwar oft identisch oder zumindest vergleichbar mit intermediär erbrachten Dienstleistungen. Die Risikoprofile der jeweiligen Aktivitä-

³²¹² Siehe etwa oben, [VII.2.6](#).

³²¹³ Siehe oben, [V.4.4](#).

³²¹⁴ Siehe oben, [V.3.7b](#).

ten weichen in aller Regel jedoch deutlich voneinander ab. Dementsprechend ist ein anderer Regulierungsansatz zu wählen (*same business, but different risks and therefore different rules*).³²¹⁵

Bereits aus verfassungsrechtlichen Gründen geht es hingegen nicht an, den oben erwähnten Grundsatz auf «*same business, same risks, same regulatory outcome*» auszudehnen.³²¹⁶ Ein solches Vorgehen würde die Besonderheiten einer neuen technologischen Entwicklung mit dem einzigen Ziel vernachlässigen, auf das bestehende (finanzintermediäre) Regulierungsmodell zurückgreifen zu können.³²¹⁷

Als *marktorientierter Regulierungsansatz*, der insb. den Grenzen herkömmlicher Finanzmarktregulierung Rechnung trägt, wird vorliegend die Entwicklung eines Offenlegungsregimes vorgeschlagen. Das Offenlegungsregime soll die spezifischen Risiken der Nutzung dezentraler Handelsplattformen umfassen.³²¹⁸ Hierzu gehören insb. Verwahrungs- und Admin Key-Risiken, die sich aus dem Code der jeweiligen Protokolle ergeben können. Es entspricht einem zweckmässigen Regulierungsansatz, dass den Marktteilnehmern in erster Linie die Risiken, die mit der Nutzung eines Protokolls zusammenhängen, transparent offengelegt werden. Die Marktteilnehmer sollen sodann auf Basis der offengelegten und überprüfbaren Informationen darüber entscheiden, ob sie eine dezentrale Handelsplattform nutzen wollen.

³²¹⁵ So bereits Andreotti, Teil 2, BR-KR 22.12.2022.

³²¹⁶ So etwa FSB, Final Report Crypto-Asset Activities and Markets, 5–6 («*Regardless of whether crypto-asset activities are conducted in purportedly decentralized structures or other ways that frustrate the identification of a responsible entity or an issuer of the crypto-assets, authorities should adopt or have in place a regulatory approach that aims at adequate protection for all relevant parties, including consumers and investors, and at achieving the same regulatory outcome.*»).

³²¹⁷ Siehe auch Andreotti, in: Zellweger-Gutknecht/Tschudi/MacCabe, Handelsplattformen, *passim* («regulatorische[s] Bett des Prokrustes»).

³²¹⁸ Siehe oben, [VI.4.3c.iv.](#)

5. Die grosse Eigenverantwortung der Nutzer macht den Einsatz von Intermediären in gewissen Situationen sinnvoll

DeFi-Anwendungen haben den Vorteil, dass viele der Risiken traditioneller Intermediationsstrukturen nicht vorhanden sind. Dabei handelt es sich namentlich um Kontroll- und Vertrauensrisiken, die ihren Ursprung in den Agency-Beziehungen mit Finanzintermediären haben.³²¹⁹ Die Nutzung dezentraler Handelsplattformen bringt grundsätzlich keine traditionellen Gegenparteirisiken mit sich.³²²⁰ Vorausgesetzt, die Sicherheit des Softwarecodes ist gegeben, kann niemand die Vermögenswerte gegen den Willen des Nutzers aus einem Smart Contract abziehen.

Allerdings auferlegt die Verwendung von offenen Protokollen dem Nutzer einen Grossteil der Verantwortung. Idealerweise würde dieser vorab den öffentlich gemachten Softwarecode auf Programmierfehler überprüfen. Zudem müsste er grundsätzlich auch bedenken, welche spieltheoretischen Erwägungen für die Funktionsweise eines Protokolls relevant sein könnten. Zwar ist letzterer Punkt für die blosser Nutzung dezentraler Handelsplattformen weniger zentral, ist ein Austauschgeschäft doch nach der Abwicklung der einzelnen Transaktionen final. Dennoch mögen solche Überlegungen eine gewisse Relevanz aufweisen, wenn der Nutzer über einen längeren Zeitraum weitere Funktionen ausüben möchte (z.B. das Market Making).

Mit dem vorgeschlagenen Offenlegungsregime können diese Herausforderungen nach vorliegender Ansicht deutlich entschärft werden.³²²¹ Das Ziel des Verhaltenskodex ist es, den Nutzern möglichst alle nutzungsrelevanten Informationen in verständlicher Weise offenzulegen. Selbst der nichtinformierte Nutzer profitiert von einem solchen Regime, denn er kann sich grundsätzlich darauf verlassen, dass informierte Marktteilnehmer ihre Entscheidungen auf der Grundlage des Offenlegungsregimes getroffen haben. In diesem Sinne kann er mit relativ gutem Gewissen diejenigen Applikationen nutzen, welche

³²¹⁹ Siehe oben, [II.2.4b](#).

³²²⁰ Siehe oben, [IV.5.1c.iv](#).

³²²¹ Siehe oben, [VI.4.3c.iv](#).

das grösste Vertrauen im Markt geniessen, was bei dezentralen Handelsplattformen etwa an den Nutzerzahlen, dem Handelsvolumen und der Liquidität bzw. der Grösse der Spreads zu erkennen ist.

Allerdings hilft dieses Regime dort nicht weiter, wo es um Risiken geht, die über ein Transparenzmodell nicht gelöst werden können. Namentlich ist die Eigenverantwortung der Nutzer im Bereich der Verwahrung der Private Keys sehr gross. In gesamtgesellschaftlicher Hinsicht kann dies im Extremfall etwa zu einer Risikoverschiebung weg vom Finanzintermediationssystem hin zu den einzelnen Inhabern von Vermögenswerten führen.³²²² Dieses Szenario hat zwar den Vorteil, dass Grossschäden aus Hackerangriffen oder Veruntreuungen deutlich gesenkt werden können. Die Sicherheit der Vermögenswerte hängt allerdings im Wesentlichen von den individuell unternommen Sicherheitsvorkehrungen ab. Das Risiko, den Private Key zu verlieren, ist dabei nicht vernachlässigbar gering. Daraus schliesst die Arbeit, dass Investor Education ein weiterer Teil eines marktorientierten Regulierungsansatzes bilden sollte.³²²³

Es könnte sich für Nutzer gerade im Verwahrungsbereich anbieten, auf einen Intermediär zurückzugreifen. Anbieter derartiger Lösungen sind nunmehr bei sammelverwahrten kryptobasierten Vermögenswerten dem Bankengesetz unterstellt, soweit es sich um Kryptovermögenswerte mit Zahlungsmittelfunktion handelt.³²²⁴ Abzuwarten bleibt, ob und in welchem Umfang sich im Bereich individuell verwahrter kryptobasierter Vermögenswerte innovative Angebote etablieren können.

Die Reintermediation von Verwahrungsstrukturen scheint nach dem Gesagten bis zu einem gewissen Grad unumgänglich. Aufgrund ihrer zentralen Stellung im Ökosystem ist es zudem absehbar, dass Anbieter für ihre Kunden eine Reihe weiterer Funktionen ausüben werden, die über die blossе Verwahrung hinausgehen (z.B. Staking-Dienstleistungen). In Bezug auf dezentrale Handelsplattformen könnte es sich bspw. anbieten, die Kundenvermögenswerte als Liquidität über entsprechende Protokolle bereitzustellen, um Handelserträge für den Kunden zu generieren. Damit findet mit einer gewissen Wahrscheinlichkeit eine Risikoverschiebung zurück ins Finanzintermediationssystem statt. Die Öffnung des traditionellen Finanzsektors gegenüber DeFi kommt letztlich auch der Finanzmarktaufsicht zugute.³²²⁵

³²²² Vgl. auch FSB, Decentralised financial technologies, 3.

³²²³ Siehe oben, [VI.4.3c.v](#).

³²²⁴ Siehe oben, [V.4.2b](#).

³²²⁵ Siehe oben, [VI.4.3c.vi](#).

6. Das Rechtsprinzip der Dezentralität kann heute als grundsätzlich anerkannt betrachtet werden; dessen langfristige Beständigkeit ist aber fraglich

Trotz nachvollziehbarer Einwände gegen das Rechtsprinzip der Dezentralität spricht sich die vorliegende Arbeit für ein solches aus.³²²⁶ Begründet wird dies u.a. mit der grundsätzlichen Anerkennung der Dezentralität als Ordnungsprinzip in der Verfassung sowie mit dem kürzlich eingeführten Konzept des Wertrechtereigens im Zivilrecht. Letzterer Punkt wirkt sich auch direkt auf das geltende Finanzmarktrecht aus. Ausserdem haben die FINMA und das Bundesverwaltungsgericht den Grad der Zentralisierung gewisser Komponenten einer digitalen Währung als wesentlich für den Gruppenbegriff im Finanzmarktrecht erachtet.³²²⁷

Es ist angesichts der Komplexität des Sachverhalts und der vielfältigen Erscheinungsformen in der Praxis aber kaum verwunderlich, dass Aufsichtsbehörden gegenüber dezentralen Systemen skeptisch eingestellt sind. Diese Skepsis ist oft begründet, wie insb. bei DINO-Anwendungen.³²²⁸ In diesen Fällen steht das Rechtsprinzip der Dezentralität der Anwendung des geltenden Finanzmarktrechts nicht im Weg.

Allerdings gibt es auch regulatorische Vorstösse zu bedauern, die sich nur bedingt mit den Eigenheiten der Dezentralität auseinandergesetzt zu haben scheinen. Ein solcher Fall ist sicherlich in der jüngsten Guidance etwa der FATF oder der BIS wiederzuerkennen.³²²⁹ Danach sollen wesentliche Teile des bestehenden Finanzintermediationsmodells auf dezentrale Prozesse und Strukturen zur Anwendung gelangen. Dies wäre im Ergebnis mit dem Ende der innovativen Elemente hinter solchen Systemen gleichzusetzen. Auch Aussagen des Bundesrates und der FINMA lassen Zweifel an der Beständigkeit des

³²²⁶ Siehe zu den Einwänden oben, [VII.5](#).

³²²⁷ Siehe oben, [VII.2](#).

³²²⁸ Siehe oben, [VII.2.6](#).

³²²⁹ Siehe oben, [V.2.3d](#).

Rechtsprinzips aufkommen.³²³⁰ Allerdings stehen konkrete Regulierungsvorschläge noch aus, und es bleibt ohnehin abzuwarten, auf welche Art und Weise ein nationaler Gesetzgeber dezentrale Phänomene zu erfassen gedenkt.

³²³⁰ Siehe oben, [VII.2.6](#).

7. Regulierung kann ein wichtiger Treiber der Dezentralisierung von Protokollen sein, was bei zurückhaltenden Eingriffen letztlich im Interesse der Nutzer ist

Regulierung soll nach vorliegender Ansicht auch künftig ausschliesslich an das vorherrschende Finanzintermediationsmodell anknüpfen. Fälle, in denen etwa Funktionen einer Handelsplattform in relevanter Weise von einer Person oder einer Gruppe miteinander verbundener Personen kontrolliert werden, sollen ohne Weiteres unter das bestehende Aufsichtsrecht subsumiert werden. Solche Handelsplattformen sind mit anderen Worten ungenügend dezentralisiert.

An das vorherrschende Finanzintermediationsmodell anzuknüpfen, bedeutet aber auch gerade, dass dieses Regulierungsmodell dezentralen Systemen nicht aufgezwungen werden soll. Interventionen, die direkten oder indirekten Zwang auf Protokolle ausüben, diese z.B. durch Einführung eines zentralen Betreibers zu zentralisieren, sollten vermieden werden.

Die aktualisierte Guidance der FATF vom Oktober 2021 übt in dieser Hinsicht eine interessante Doppelrolle aus: Einerseits möchte die FATF den Anwendungsbereich des VASP-Konzepts deutlich über das bestehende Finanzintermediationsmodell hinaus erweitern.³²³¹ Andererseits würde eine einschränkende Auslegung des Konzepts eine mit Art. 4 Abs. 1 lit. b GwV vergleichbare Anknüpfung an die Kontrolle über eine dezentrale Handelsplattform erlauben: Nur Personen oder eine Gruppe miteinander verbundener Personen, welche die *effektive Zugriffsmöglichkeit* auf die Vermögenswerte der Plattformnutzer innehaben, sollen geldwäschereirechtlich erfasst sein.³²³²

Mit diesem Ansatz ist jedoch weiterhin grosse Rechtsunsicherheit verbunden, weshalb vorsichtige Projekte einen Weg bevorzugen werden, der die Kontrolle über ein Protokoll möglichst verteilt. Im Ergebnis bedeutet dies, dass Regulierung ein *wichtiger* Treiber der Dezentralisierung von Projekten sein kann. Projekte, welche Dezentralität nicht genügend ernstnehmen, könnten früher oder

³²³¹ Siehe oben, [V.2.3d](#).

³²³² Siehe oben, [V.2.6c](#).

später in den Fängen der Finanzmarktaufsicht landen. Ein derart ausgerichtetes Vorgehen der Aufsichtsbehörden kann durchaus sinnvolle Ergebnisse im Markt begünstigen, welche letztlich auch im Interesse der Nutzer sind. Der in der MiCAR verfolgte Ansatz, gänzlich dezentrale Phänomene vom Anwendungsbereich auszunehmen, könnte ebenfalls zu interessanten Marktentwicklungen beitragen.

Gleichzeitig sollte Regulierung nicht blind gegenüber legitimen gesellschaftlichen Veränderungen sein. Im Gegenteil: Die Rechtsordnung sollte den veränderten technologischen Umständen angemessen Rechnung tragen, ohne dabei Innovation zu verunmöglichen oder übermässig zu erschweren.³²³³ Die Einführung einer Safe-Harbor-Regelung etwa, welche Entwicklern die Möglichkeit gibt, ihr Projekt innerhalb einer bestimmten Frist zu dezentralisieren, würde diesem Anliegen Rechnung tragen.³²³⁴

³²³³ Vgl. Perez, *Technological Revolutions*, 145 («An adequate set of institutions is needed to complement, shape and guide the transformations that take place in the economic sphere. Yet, it cannot be a blissful return to what worked in the previous paradigm; it must be the complex design of what will work with the new one.»).

³²³⁴ Siehe diesbezüglich oben, [VI.4.3c.iii](#).

Curriculum Vitae

Fabio Andrea Andreotti, geboren 1988, erwarb die Matura an der Kantonschule am Burggraben St. Gallen. Anschliessend absolvierte er das Studium der Rechtswissenschaft an der Universität Zürich (UZH). Nach Tätigkeit als wissenschaftlicher Assistent am Lehrstuhl für Privat-, Handels- und Wirtschaftsrecht von Prof. Dr. iur. Rolf Sethe LL.M. an der Universität Zürich war Fabio Andreotti u.a. beim Staatssekretariat für internationale Finanzfragen (SIF), bei einer Zürcher Wirtschaftskanzlei und bei der Kantonalen Staatsanwaltschaft des Kantons Aargau angestellt. Er ist seit einigen Jahren beruflich in der Finanz- und Kryptoindustrie tätig.

Gegenstand der Dissertation ist eine umfassende rechtstatsächliche und finanzmarktrechtliche Einordnung des Phänomens der dezentralen Handelsplattformen (Decentralized Exchanges, DEX). Der Autor behandelt die Frage, ob dezentrale Handelsplattformen unter Berücksichtigung der mit ihnen verbundenen Innovationschancen und der von ihnen ausgehenden Risiken einen Regulierungsanlass darstellen und wie darauf reagiert werden kann. Die Arbeit zeigt die praktischen Einordnungsprobleme auf, mit welchen das heutige Finanzmarktrecht konfrontiert ist. Um für diese Probleme mögliche Antworten zu entwickeln, erarbeitet der Autor auf der Grundlage eines Rechtsprinzips der Dezentralität Kriterien, welche die Abgrenzung dezentraler Handelsplattformen von Erscheinungsformen erlauben, die über keine ausreichende Verteilung der Kontroll- und Machtstrukturen verfügen (Dezentralitätstest). Der Autor kommt zum Schluss, dass für dezentrale Phänomene in erster Linie Regulierungsansätze überzeugend sind, die ihre Grundlage in einer selbstverantwortlich und wettbewerblich organisierten Finanzmarktordnung haben.