EuZ
ZEITSCHRIFT FÜR EUROPARECHT

AUSGABE:
07| 2025

LEITARTIKEL:

Fabio Andreotti /Joshua R. Taucher Marktmissbrauch im Kryptomarkt: Eine Einordnung nach MiCAR und Schweizer Finanzmarktrecht

Marktmissbrauch im Kryptomarkt

Eine Einordnung nach MiCAR und Schweizer Finanzmarktrecht

Fabio Andreotti/Joshua R. Taucher*

Inhalt

* Dr. iur. Fabio Andreotti, Deputy General Counsel, Bitcoin Suisse AG, und Dr. iur. Joshua R. Taucher, Rechtsanwalt, LL.M., Senior Legal Counsel, Sygnum Bank AG. Der vorliegende Beitrag gibt die persönliche Ansicht der Autoren wieder.

A. Einleitung

I. Ausgangslage und Herausforderung

Der Kryptomarkt[1] zeichnet sich durch eine Reihe besonderer Eigenschaften aus, die sich teilweise deutlich vom traditionellen Finanzmarkt unterscheiden. Namentlich sind klassische Markteffekte wie Preisbildung aufgrund von Fundamentaldaten oder etablierte Marktmechanismen oft nur eingeschränkt vorhanden. Stattdessen sind spekulative Dynamiken, der Einsatz sozialer Medien, eine hohe Beteiligung von Retail-Investoren, rascher technologischer Wandel und – ausserhalb der Blockchain[2] – ein grösseres Mass an Intransparenz bedeutende Faktoren.[3] Der bestehende Regulierungsrahmen – etwa jener für Handelsplätze und Wertpapierhäuser sowie traditionelle Finanzinstrumente und Effekten – ist zudem auf Kryptowerte[4] häufig

---

1 Unter *Kryptomarkt* wird vorliegend die Gesamtheit der Plattformen für den Austausch von Kryptowerten verstanden. Grundsätzlich sind somit sowohl *zentral* verwaltete (CEX) als auch *dezentrale* Handelsplattformen (DEX) erfasst, unabhängig davon, ob sie selbst in den Geltungsbereich der Finanzmarkterlasse fallen; vgl. hierzu Andreotti Fabio, § 11 Handel und Handelsplattformen, in: Zellweger-Gutknecht Corinne/Tschudi Dominik/MacCabe Kevin (Hrsg.), Kryptowerte, Basel 2024, Rz. 11.05 ff. (zit. Andreotti, Handelsplattformen); ferner Weber Rolf H., DLT-Handelsplattformen. Spannungsfeld von Technologie und Recht, Zürich 2022, 58 ff.; Jutzi Thomas/Abbühl Andri, Fintech und DLT. Privat- und finanzmarktrechtliche Grundlagen in der Schweiz, Bern 2023, Rz. 531 ff.

2 Mit Blick auf Transaktionen auf der Blockchain verfügt der Kryptomarkt im Vergleich zum traditionellen Finanzmarkt in aller Regel über eine erhöhte Transparenz.

3 Zur Rolle der *sozialen Medien* anschaulich Zetzsche Dirk/Woxholth Jannik, The EU Law on Cryptoassets. A Guide to European Fintech Regulation, Cambridge/New York 2025, 160 ff.; zur Frage der *Informationsungleichgewichte* im Kryptomarkt insb. Weber Rolf H., Aufklärung zur Vermeidung von Informationsasymmetrien im Kryptouniversum, SZW 2025, 108 ff., 111, 112 ff.

4 Als *Kryptowert* gilt gemäss Art. 3 Abs. 1 Ziff. 5 MiCAR *„[…] eine digitale Darstellung eines Werts oder eines Rechts, der bzw. das unter Verwendung der Distributed-Ledger-Technologie oder einer ähnlichen Technologie elektronisch übertragen und gespeichert werden kann […]“*. Mit dem Begriff *kryptobasierte Vermögenswerte* sind sodann *„[…] alle Vermögenswerte gemeint, bei denen die Verfügungsmacht ausschliesslich über ein kryptobasiertes Zugangsverfahren vermittelt wird […]“* (vgl. Botschaft des Bundesrates vom 27. November 2019 zum Bundesgesetz zur Anpassung des Bundesrechts an Entwicklungen der Technik verteilter Register, BBl 2020, 233 ff., 292). Der vorliegende Beitrag verwendet der Einfachheit halber den i.d.R. leicht umfassenderen Begriff des Kryptowerts. Im vorliegenden Beitrag umfassen

nicht direkt anwendbar.[5] Hinzu kommt der Umstand, dass der Kryptomarkt praktisch immer einen transnationalen Charakter aufweist, was Schwierigkeiten in der Rechtsdurchsetzung mit sich bringt.[6]

Ein Paradigmenwechsel fand mit dem Inkrafttreten der Markets in Crypto-Assets Regulation (MiCAR)[7] am 29. Juni 2023 statt. Die Verordnung schafft erstmals einen umfassenden und einheitlichen Regulierungsrahmen für Kryptowerte innerhalb des Europäischen Wirtschaftsraums (EWR). Die MiCAR adressiert sowohl den Primärmarkt – etwa durch Anforderungen an Whitepaper und Offenlegungspflichten – als auch den Sekundärmarkt durch die Regulierung von Anbietern von Kryptowerte-Dienstleistungen, sog. *Crypto-Asset Service Providern* bzw. CASPs. Eines der Ziele der MiCAR ist die Gewährleistung der Integrität und Stabilität des europäischen Kryptomarkts.[8] Vor diesem Hintergrund führte die Verordnung im sechsten Titel ein eigenständiges Marktverhaltensregime für den Kryptomarkt ein.[9]

Für die Schweiz stellt sich nun die rechtspolitische Frage, ob sie einen ähnlichen Weg wie die Europäische Union (EU) gehen möchte oder ob sie bewusst andere Abzweigungen wählen soll, die sich unter Umständen an den Modellen anderer Länder (insb. UK und USA) orientieren. Zwar verfügt die Schweiz mit dem DLT-Mantelerlass vom Januar bzw. August 2021 bereits über ein modernes Regelwerk für Blockchain-basierte Vermögenswerte. Allerdings ist dieses weniger umfassend als die MiCAR, und es lässt im Zusammenhang mit Kryptowerten, die nicht als Finanzinstrumente oder DLT-Effekten qualifizieren, insb. Fragen des Anleger- und Funktionsschutzes und der Marktaufsicht offen.[10] Gleichzeitig orientieren

---

sie sodann – zumindest dort, wo es um die europäische Regulierung geht – in erster Linie Token, die nach der FINMA-Kategorisierung als Zahlungs- und/oder Nutzungs-Token oder als Stablecoins mit Zahlungsmittelfunktion qualifizieren und somit nach traditionellem Verständnis nicht dem Kapitalmarkt zuzurechnen sind; mitunter stehen also tokenisierte Kapitalmarktpapiere nicht im Vordergrund des Beitrages.

5 Vgl. International Organization of Securities Commission (IOSCO), Policy Recommendations for the Regulation of Crypto and Digital Assets. Final Report, 16. November 2023, 13 ff. (zit. IOSCO, Crypto and Digital Assets).

6 Remund Cédric/Meier François, Marktmissbrauch in Kryptomärkten (Teil 1), SJZ 2025, 339 ff., 343 (zit. Remund/Meier, Teil 1).

7 Verordnung (EU) 2023/1114 des Europäischen Parlaments und des Rates vom 31. Mai 2023 über Märkte für Kryptowerte.

8 EWG 4 und 95 MiCAR.

9 Aus Sicht von *Lehmann* ist das Marktmissbrauchsrecht der praktisch wichtigste Teil der MiCAR; vgl. Lehmann Matthias, MiCAR – Gold Standard or Regulatory Poison for the Crypto Industry?, EBI Working Paper Series Nr. 160, 8. Januar 2024, 13.

10 Vgl. Eggen Mirjam, Schweizer Kryptoregulierung: Gesetzgeberischer Handlungsbedarf im Zivil- und Aufsichtsrecht, sui generis 2025, Rz. 40 ff.

sich prudenziell beaufsichtigte Finanzinstitute wie Banken und Wertpapierhäuser bereits heute an höheren Standards im Bereich des Marktverhaltens.[11] Es stellt sich somit auch die Frage, ob Erkenntnisse aus dem aktuellen Umgang mit dem Thema auch für die anstehende Diskussion neuer Regeln fruchtbar gemacht werden können.

II. Marktmissbrauch im Kryptomarkt (Fallgruppen)

1. Einleitung

Marktmissbrauch wie Insiderhandel und Kursmanipulation ist empirisch betrachtet ein häufig auftretendes Phänomen im Kryptomarkt; eine Vielzahl von Fällen aus den Bereichen des aufsichtsrechtlichen Enforcements oder der straf- oder zivilrechtlichen Gerichtspraxis veranschaulicht diese Aussage.[12] Im Folgenden werden anhand von Praxisbeispielen *drei Fallgruppen* gebildet:

2. Informationsbasierter Marktmissbrauch

Informationsbasierte Aktivitäten umfassen in erster Linie missbräuchliche Verhaltensweisen, die nicht öffentliche Informationen verwerten, um einen finanziellen Vorteil zu realisieren:

– Der erste Insiderhandelsgerichtsfall im Kryptomarkt war soweit ersichtlich der Fall *Wahi* (2023): Ein für die Zulassung neuer Token verantwortlicher Mitarbeiter der US-Handelsplattform Coinbase hatte sein Wissen über bevorstehende „Listings" entgegen einer internen Weisung über mehrere Monate an aussenstehende Drittpersonen weitergegeben. Diese Personen haben sodann auf der Basis der „Tipps" die betreffenden Kryptowerte erworben, um sie kurz nach der Handelszulassung i.d.R. mit Gewinn am Markt zu veräussern.[13] Das missbräuchliche Verhalten ist nicht

---

11 Vgl. FINMA-Rundschreiben 2013/8 „Marktverhaltensregeln".

12 Siehe in Bezug auf Kryptohandelsplattformen IOSCO, Issues, Risks and Regulatory Considerations Relating to Crypto-Asset Trading Platforms. Final Report, Februar 2020, 39 ff.; ferner in Bezug auf die Marktteilnahme von Retail-Anlegern IOSCO, Retail Market, Conduct Task Force. Final Report, März 2023, 23 ff. (zit. IOSCO, Retail Market).

13 U.S. Department of Justice (DOJ), U.S. Attorney's Office, Southern District of New York, Former Coinbase Insider Sentenced In First Ever Cryptocurrency Insider Trading Case, 9. Mai 2023, <https://www.justice.gov/usao-sdny/pr/former-coinbase-insider-sentenced-first-ever-cryptocurrency-insider-trading-case>; U.S. Securities and Exchange Commission (SEC), Former Coinbase Manager and His Brother Agree to Settle Insider Trading Charges Relating to Crypto Asset Securities, 30. Mai 2023, <https://www.sec.gov/newsroom/press-releases/2023-98>.

etwa aufgrund entsprechender Compliance-Kontrollen der Handelsplattform entdeckt worden, sondern in einem Beitrag auf Twitter, der auf die massiven, auf der Blockchain sichtbaren Zukäufe vor den Handelszulassungen aufmerksam machte.[14]

– Ähnlich gelagert war sodann der Fall eines Mitarbeiters einer bekannten US-Plattform für die Herausgabe und den Tausch von Non-Fungible Tokens (NFTs) (*Chastain*, 2023). Der Mitarbeiter hatte die Token noch vor deren Aufschalten auf der Plattform über verschiedene Wallets erworben, um sie sodann mit Gewinn an die übrigen Nutzer der Plattform zu veräussern.[15]

Zu dieser Kategorie gehören ferner Fälle der Bekanntgabe falscher oder irreführender Informationen gegenüber dem Markt und den Medien (inkl. soziale Medien), um die Preisbildung eines Vermögenswerts zu beeinflussen und daraus einen finanziellen Vorteil zu erlangen:[16]

– Ein Beispiel hierfür ist etwa der Fall *Arbitrade* (2022). Gemäss Klageschrift behaupteten verschiedene Personen aus dem Umfeld der Token, dass diese mit Goldbarren hinterlegt seien. Diese angeblich falsche Behauptung führte zu einem Preisanstieg, der von den beteiligten Personen ausgenutzt worden sei, um ihre Token am Markt zu höheren Preisen zu verkaufen.[17]

– Vergleichbar ist sodann der Sachverhalt in einer breit angelegten Aktion der US-Behörden gegen verschiedene Marktteilnehmer (*Operation Crypto Fraud*, 2024), die u.a. durch angeblich falsche und irreführende Werbeaussagen zu den mit den Token verbundenen Produkten, die teilweise gar nicht existierten, die Marktpreise der Vermögenswerte in die Höhe getrieben haben sollen.[18]

---

14 Siehe <https://x.com/cobie/status/1513874972552355846>.

15 DOJ, U.S. Attorney's Office, Southern District of New York, Former Employee Of NFT Marketplace Sentenced To Prison In First-Ever Digital Asset Insider Trading Scheme, 22. August 2023, <https://www.justice.gov/usao-sdny/pr/former-employee-nft-marketplace-sentenced-prison-first-ever-digital-asset-insider>.

16 Siehe Hanslin Marc, Marktmanipulation nach Art. 143 FinfraG, GesKR 2016, 45 ff., 46.

17 SEC, SEC Files Charges in a Crypto Asset Pump-And-Dump Scheme, 30. September 2022, <https://www.sec.gov/enforcement-litigation/litigation-releases/lr-25537>.

18 DOJ, U.S. Attorney's Office, District of Massachusetts, Eighteen Individuals and Entities Charged in International Operation Targeting Widespread Fraud and Manipulation in the Cryptocurrency Markets, 9. Oktober 2024, <https://www.justice.gov/usao-ma/pr/eighteen-individuals-and-entities-charged-international-operation-targeting-widespread>.

– Schliesslich wurde ein Verfahren wegen positiver öffentlicher Äusserungen bei gleichzeitigen Abverkäufen grosser Positionen des letztlich kollabierten LUNA-Tokens, der Teil des Terra-Universums samt algorithmischen Stablecoins UST war, mit einer Vergleichszahlung über USD 200 Millionen beigelegt (*Galaxy Digital*, 2025).[19]

3. Transaktionsbasierter Marktmissbrauch

Transaktionsbasierte Aktivitäten umfassen missbräuchliche Verhaltensweisen, die primär mittels Handelsabschlüssen und Aufträgen entweder den Marktpreis oder das Handelsvolumen eines Vermögenswerts beeinflussen, um einen finanziellen Vorteil zu realisieren:[20]

– Darunter fallen etwa *Pump-and-Dump*-Systeme (auch *Matched Orders* oder *Ramping*): Dabei handelt es sich um eine Praxis, bei welcher der Preis eines Kryptowerts durch koordiniertes Vorgehen einer Gruppe von Personen künstlich in die Höhe getrieben wird (*Pump*), worauf die Personen ihre Bestände zu überhöhten Preisen verkaufen können (*Dump*). Dieses Vorgehen führt zu einem drastischen Preisverfall, was die Mehrheit der übrigen Investoren mit Verlusten zurücklässt (z.B. *Operation Crypto Fraud*, 2024). „Pumps" werden üblicherweise von informationsbasiertem Handeln begleitet, indem nach dem Eingehen von Long- oder Short-Positionen bspw. falsche oder irreführende Informationen auf sozialen Medien gestreut werden.[21]

– Ein blosses *Pump*-System (auch *Capping* oder *Pegging*) ist sodann im koordinierten Hochdrücken und -halten eines Preises mit dem Ziel zu erkennen, günstigere Konditionen etwa für Refinanzierungen zu erhalten oder den Eindruck einer kontinuierlich hohen Nachfrage für ein Projekt zu erwecken oder dessen Stabilität vorzutäuschen. Im Falle von *Alameda/FTX* (2022) verfolgte die CEO von Alameda Research auf Anweisung von Sam Bankman-Fried, CEO der Kryptohandelsplattform FTX, das Ziel, den Preis des FTT-Token über einem bestimmten Niveau zu halten. Hintergrund: Der FTT-Token wurde von der mit Alameda verbundenen FTX her-

---

19 Siehe Attonrey General of the State of New York Investor Protection Bureau, Assurance of Discontinuance, Nr. 25-011, 27. März 2025, <https://ag.ny.gov/sites/default/files/settlements-agreements/galaxy-digital-holding-ltd-et-al-assurance-of-discontinuance-2025.pdf>.

20 Siehe Hanslin, 46.

21 Vgl. Barczentewicz Mikołaj/de Gândara Gomes André, Crypto-Asset Market Abuse Under EU MiCA, European Journal of Risk Regulation 2024, 1 ff., 12.

ausgegeben und diente als Sicherheit für die mit Kundenvermögen finanzierten Darlehen an Alameda.[22]

Schliessen kann transaktionsbasiertes Handeln auch primär volumenorientiert erfolgen: Namentlich *Wash Trading* und ähnliche Aktivitäten (z.B. *Matched Orders* oder *Painting the Tape*) von mehr oder weniger simultanen Käufen und Verkäufen durch dieselbe oder miteinander verbundene Personen, die dem Markt den falschen Eindruck einer aktiveren oder grösseren Nachfrage als unter normalen Marktbedingungen vermitteln sollen, sind gut dokumentiert:

- Der wohl bekannteste, jedoch kürzlich eingestellte Fall ist das Verfahren gegen *Binance* (2023): Der Kryptohandelsplattform wurde vorgeworfen, dass eine mit ihr verbundene Gesellschaft über Jahre gleichzeitig Kauf- und Verkaufsaufträge für Kryptowerte im Handelsbuch der Plattform platziert habe, um den übrigen Nutzern der Plattform eine hohe Liquidität vorzutäuschen.[23]
- Ähnliche irreführende Praktiken, die sich jedoch ausserhalb des Betriebs einer Handelsplattform zugetragen haben sollen, werden den verantwortlichen Personen hinter einer Kryptowährung vorgeworfen, wobei dessen Gründer seine persönlichen Bestände im Markt mit Gewinn verkauft haben soll (TRON, 2023).[24]
- Schliesslich wirft die US-Wertpapieraufsichtsbehörde mehreren Personen vor, einen eigentlichen Wash-Trading-Service für neue Token angeboten zu haben (*Market-Manipulation-as-a-Service*, 2024). Erstaunlich am Fall ist, dass die beteiligten Parteien einer eigens für die Überführung erstellten Kryptowährung der Bundespolizei FBI auf den Leim gegangen sind.[25]

Ein Kryptomarkt-Spezialfall eines transaktionsbasierten Verhaltens ist das Ausnützen von technologischen oder programmatischen Schwächen in dezentralen Anwendungen:

---

22 SEC, SEC Charges Caroline Ellison and Gary Wang with Defrauding Investors in Crypto Asset Trading Platform FTX, 21. Dezember 2022, <https://www.sec.gov/newsroom/press-releases/2022-234>.

23 SEC, SEC Files 13 Charges Against Binance Entities and Founder Changpeng Zhao, 5. Juni 2023, <https://www.sec.gov/newsroom/press-releases/2023-101>.

24 SEC, SEC Charges Crypto Entrepreneur Justin Sun and His Companies for Fraud and Other Securities Law Violations, 22. März 2023, <https://www.sec.gov/newsroom/press-releases/2023-59>.

25 SEC, SEC Charges Three So-Called Market Makers and Nine Individuals in Crackdown on Manipulation of Crypto Assets Offered and Sold as Securities, 9. Oktober 2024, <https://www.sec.gov/newsroom/press-releases/2024-166>.

– Der erste und bislang bekannteste Fall ist *Eisenberg* (2023): Im Oktober 2022 eröffnete Avraham Eisenberg zwei „Konten" auf der dezentralen Anwendung „Mango Markets" – einer dezentralen Handels- und Lending-Plattform – und finanzierte diese mit rund USDC 5 Millionen. Er erstellte gegensätzliche Long- und Short-Positionen in MNGO-Perpetuals (eine Form von unbefristeten Derivatkontrakten, die in diesem Fall auf der Blockchain abgerechnet und abgewickelt wurden) und manipulierte dann den Preis des MNGO-Tokens, indem er auf externen Handelsplattformen, die als Preis-Orakel dienten, grosse Mengen von MNGO-Tokens kaufte, was zu einer erheblichen Preissteigerung führte. Er nutzte den künstlich erhöhten MNGO-Kurs als Sicherheit, um ein Darlehen in Höhe von über USD 100 Millionen beim Protokoll aufzunehmen. Nach dem unverzüglichen Verkauf der im Preis angestiegenen MNGO-Tokens nahm er sodann auch ein Darlehen gegen die im Wert angestiegenen Short-Positionen beim Protokoll auf. Die hinterlegten Sicherheiten wurden im Liquidationsfall wie vorgesehen zwar verwertet, da aber die beim Protokoll aufgenommenen Darlehen nicht zurückbezahlt wurden, folgte aus dem Verhalten des Händlers ein Defizit für die übrigen Nutzer der DeFi-Anwendung. Ein Teil der entwendeten Mittel (etwa USD 67 Millionen) hat Eisenberg schliesslich im Rahmen einer Vereinbarung mit der dezentralen autonomen Organisation (DAO) von Mango Markets zurückgegeben, während er etwa USD 47 Millionen für sich behielt.[26] Wichtig zu erwähnen ist, dass es sich bei Eisenbergs Aktivität nicht um Hacking handelte; die dezentrale Anwendung funktionierte vermutlich zwar nicht wie von den Entwicklern beabsichtigt, jedoch als Computerprogramm einwandfrei. Im Mai 2025 wurde Eisenberg nach einer erstinstanzlichen Verurteilung wegen Betrugs und Marktmanipulation[27] von den Vorwürfen freigesprochen. Zwar

---

26 Siehe insb. DOJ, Man Charged in $110 Million Cryptocurrency Scheme, 2. Februar 2023, <https://www.justice.gov/archives/opa/pr/man-charged-110-million-cryptocurrency-scheme>; Commodity Futures Trading Commission (CFTC), CFTC Charges Avraham Eisenberg with Manipulative and Deceptive Scheme to Misappropriate Over $110 million from Mango Markets, a Digital Asset Exchange, 9. Januar 2023, <https://www.cftc.gov/PressRoom/PressReleases/8647-23; U.S. Securities and Exchange Commission>; SEC, SEC Charges Avraham Eisenberg with Manipulating Mango Markets' „Governance Token" to Steal 6 Million of Crypto Assets, 20. Januar 2023, <https://www.sec.gov/newsroom/press-releases/2023-13>; TRM Labs, Mango Markets' Exploiter Avi Eisenberg Convicted of Market Manipulation and Fraud, 17. April 2024, <https://www.trmlabs.com/resources/blog/mango-markets-exploiter-avi-eisenberg-convicted-of-market-manipulation-and-fraud>.

27 U.S. Attorney's Office, Southern District of New York, Man Convicted For $110 Million Cryptocurrency Scheme, 18. April 2024, <https://www.justice.gov/usao-sdny/pr/man-convicted-110-million-cryptocurrency-scheme>.

war mit Blick auf den Manipulationsvorwurf erstellt, dass er den relevanten „Marktpreis" manipuliert hatte, doch fehlte es nach Ansicht des Richters an der US-Gerichtsbarkeit.[28]

4. Mängel im operationellen und Kontrollbereich

Neben den eigentlichen marktmissbräuchlichen Verhaltensweisen stehen auch die Handelsplattformen sowie gewisse Marktteilnehmer im Fokus der Aufsichtsbehörden und Gerichte:

- Der Kryptohandelsplattform Binance etwa wurde vorgeworfen, dass sie keine oder bloss mangelhafte Handelsüberwachungssysteme eingesetzt habe, um Wash Trading-Aktivitäten zu verhindern, und diesbezüglich ihre Nutzer irreführte (*Binance*, 2023).[29]
- Einer Schweizer Stiftung wird in den Medien vorgeworfen, sie habe Vereinbarungen mit einem Market Marker abgeschlossen, wonach dieser nach Erreichen eines bestimmten Marktpreises die Token auf eigene Rechnung veräussern dürfe. Der damit verbundene Fehlanreiz des Market Makers, den Preis des neuen Tokens künstlich hochzutreiben, um den Token anschliessend mit Gewinn verkaufen zu können, sei dabei in Kauf genommen worden (*Movement*, 2025).[30]

5. Zwischenfazit

Die Ausführungen legen nahe, dass Marktmissbrauch im Kryptomarkt weit verbreitet ist.[31] Viele der beobachteten Praktiken entsprechen den miss-

---

28 U.S. District Court SDNY, United States of America vs. Avraham Eisenberg, Opinion and Order, Nr. 1:23-cr-00010-AS, 23. Mai 2025, 3 ff., 21 ff.

29 SEC, SEC Files 13 Charges Against Binance Entities and Founder Changpeng Zhao, 5. Juni 2023, <https://www.sec.gov/newsroom/press-releases/2023-101>.

30 Coindesk, Movement Labs Secretly Promised Advisers Millions in Tokens, Leaked Documents Show, 15. Mai 2025, <https://www.coindesk.com/tech/2025/04/30/the-protocol-inside-movement-s-token-dump-scandal>.

31 Vgl. in Bezug auf *Wash Trading* auf *zentralen Handelsplattformen* Le Pennec Guénolé/Fiedler Ingo/Ante Lennart, Wash trading at cryptocurrency exchanges, Finance Research Letters 2021, Nr. 101982, 1 ff., *passim*, und Cong Lin William/Li Xi/Tang Ke/Yang Yang, Crypto Wash Trading, Management Science 2023, 6427 ff., *passim*; betreffend *Pump-and-Dump-Schemes* auf zentralen und dezentralen Handelsplattformen Li Tao/Shin Donghwa/Wang Baolian, Cryptocurrency Pump-and-Dump Schemes, 9. November 2023, *passim*, <https://ssrn.com/abstract=3267041>; in Bezug auf *Wash Trading* und *Pump-and-Dump-Schemes* auf dezentralen Handelsplattformen Chainalysis, Market Manipulation: Suspected

bräuchlichen Praktiken, die auch in traditionellen Wertpapiermärkten beobachtet werden können. Der Gesetzgeber kann sich demnach im Grundsatz an den bewährten Vorgaben zur Verhinderung und Sanktionierung von Marktmissbrauch orientieren.[32]

Teilweise liegen indessen auch neuartige Phänomene vor, die neue spannende Rechtsfragen aufwerfen, wie etwa bei der Nutzung dezentraler Anwendungen (vgl. Fall *Eisenberg*), die sich im Spannungsverhältnis zwischen Marktmissbrauch, Softwaresicherheit und *Code-is-Law*-Argumenten bewegen. Sodann ist die Realisierung von MEV-Opportunitäten ein weiteres Beispiel neuen Marktverhaltens, das potenziell missbräuchlich ist.[33]

Schliesslich bewegen sich viele der beobachtbaren Verhaltensweisen nur am Rande des Marktmissbrauchsrechts, sondern primär im Kernstrafrecht (Betrug, Computerdelikte usw.);[34] dazu gehören etwa Schneeballsysteme (*Ponzi Schemes*), „Rug Pulls Scams" – eine Aktivität von Projektinitiatoren, sich nach einem Preisanstieg gezielt anlegerschädigend aus dem Projekt zurückzuziehen –,[35] sowie Social-Engineering- und Private-Key-Phishing-Attacken.[36] Gemäss Empfehlung der *International Organization of Securities Commissions* (IOSCO) sollten auch diese missbräuchlichen Praktiken durch das nationale Recht adressiert werden.[37]

In der Praxis lassen sich die Verhaltensweisen der drei Fallgruppen regelmässig auch in *kombinierter* Form beobachten. So kann Wash Trading samt Pump-and-Dump eines Tokens aufgrund eines internen Kontrolldefizits einer zentralen Handelsplattform länger unentdeckt bleiben. Auch auf dezentralen Handelsplattformen ist eine Kombination von Wash-Trading- und Pump-and-Dump-Aktivitäten empirisch offenbar kein seltenes Phänomen – teilweise begleitet durch ein „Rug Pulling" des DEX-Pool-Initiators.

Wash Trading on Select Blockchains May Account for Up To .57 Billion in Trading Volume, 29. Januar 2025, <https://www.chainalysis.com/blog/crypto-market-manipulation-wash-trading-pump-and-dump-2025/>; mit Blick auf *Flash Loans* und *Wash Trades* Aramonte Sirio/Huang Wenqian/Schrimpf Andreas, DeFi risks and the decentralisation illusion, BIS Quarterly Review, Dezember 2021, 21 ff., 27 f.

32 Vgl. IOSCO, Crypto and Digital Assets, 26, 57 f.

33 Siehe hierzu unten, D.

34 In diesem Zusammenhang sehr interessant sind die Ausführungen in Remund Cédric/Meier François, Marktmissbrauch in Kryptomärkten (Teil 2), SJZ 2025, 391 ff.

35 Vgl. hierzu ausführlich Sun Dianxiang et al., SoK: A Taxonomic Analysis of DeFi Rug Pulls: Types, Dataset, and Tool Assessment, Proceedings of the ACM on Software Engineering 2025, 550 ff., *passim*.

36 Vgl etwa aus einer *Cybersecurity*-Perspektive die unterschiedlichen Arten von Missbräuchen Carpentier-Desjardins Catherine et al., Mapping the DeFi crime landscape: an evidence-based picture, Journal of Cybersecurity 2025, 1 ff., 2 f., 7 ff.

37 IOSCO, Crypto and Digital Assets, 26.

Es ist angesichts der gewonnen Erkenntnisse als *Zwischenfazit* festzuhalten, dass die Rechtsordnung richtigerweise sowohl auf der Ebene der missbräuchlich agierenden Person als auch auf der Ebene des Kryptodienstleisters ansetzen sollte. Bei echten dezentralen Handelsplattformen ist nach vorliegender Ansicht demgegenüber dem Dezentralitätsparadigma angemessen Rechnung zu tragen und primär auf die Regulierung der Marktteilnehmer abzuzielen.[38]

III. Aufbau des Beitrags

Der vorliegende Beitrag widmet sich im zweiten Kapitel dem neuen europäischen Marktmissbrauchsrecht gemäss der MiCAR (B.). Im Folgekapitel wird sodann das aktuelle Schweizer Marktverhaltensrecht mit Blick auf Kryptowerte eingehender dargestellt (C.). Es folgen eine „herausgelöste" Auseinandersetzung mit dem Thema „Maximal Extractable Value" (MEV) sowie ein Versuch der Einordnung des Phänomens in den europäischen und Schweizer Rechtsrahmen (D.). Das fünfte Kapitel stellt sodann einen kurzen Vergleich der Marktmissbrauchsordnungen in der MiCAR und im Schweizer Finanzmarktrecht *de lege lata* an (E.). Der Beitrag schliesst mit einem Ausblick auf eine mögliche künftige Ordnung des Marktmissbrauchsrechts im Kryptobereich in der Schweiz (F.).

B. MiCAR-Marktmissbrauchsrecht

I. Entstehung und Zielsetzung

Die MiCAR trat nach der Verabschiedung im Europäischen Parlament und im Rat am 29. Juni 2023 in Kraft. Sie ist Teil des umfassenden Digital Finance Package der Europäischen Kommission, das bereits im September 2020 vorgestellt wurde. Ziel dieses Pakets ist es, einen einheitlichen und innovationsfreundlichen Regulierungsrahmen für digitale Finanzdienstleistungen in der EU zu schaffen.

Die MiCAR verfolgt das Ziel, Rechtsklarheit und einheitliche Standards für den Umgang mit Kryptowerten zu schaffen. Sie richtet sich an Emittenten von Kryptowerten und an Anbieter von Krypto-Dienstleistungen und soll insb.:

---

[38] Zum *Dezentralitätsparadigma* und seinen möglichen Implikationen für die Rechtsordnung ausführlich Andreotti Fabio, Dezentrale Handelsplattformen im Schweizer Finanzmarktrecht. Eine Analyse unter Erarbeitung eines Rechtsprinzips der Dezentralität, Zürich 2024, 122 f., 567 ff. (zit. Andreotti, Dezentrale Handelsplattformen).

– Anlegerschutz und Verbrauchersicherheit gewährleisten,

– Marktmissbrauch verhindern und

– die Integrität und Stabilität der Kryptomärkte fördern.

Ein zentrales Element von MiCAR ist das kryptospezifische Marktverhaltensrecht, das sich an bestehenden Regelungen des traditionellen EU-Finanzmarktrechts, namentlich an der Marktmissbrauchsverordnung (*Market Abuse Regulation*, MAR)[39] orientiert. Die MiCAR umfasst unter anderem Vorschriften zur Verhinderung von Insiderhandel und der unrechtmässigen Offenlegung von Insiderinformationen, zur Bekämpfung von Marktmanipulation sowie zur Transparenz auf Kryptohandelsplattformen (vgl. Art. 1 Abs. 2 lit. e MiCAR). Dadurch soll ein rechtlicher Rahmen geschaffen werden, der das Vertrauen in den Kryptomarkt stärken und gleiche Wettbewerbsbedingungen innerhalb der EU bzw. des EWR gewährleisten soll.

II. Rechtsgrundlagen

Das Marktverhaltensrecht der MiCAR findet sich primär im *sechsten Titel* der Verordnung (Art. 86 bis 92). Rechtsdogmatisch umfasst der Titel Legaldefinitionen (Art. 87, 89 Abs. 1, 91 Abs. 2 und 3), Verbotsnormen (Art. 89 Abs. 2 und 3, 90, 91 Abs. 1) und Offenlegungs-, Organisations- und Meldepflichten (Art. 88, 92). Ausführungsbestimmungen zu ausgewählten Bestimmungen des sechsten Titels finden sich sodann in einer Durchführungs- bzw. Delegierten Verordnung der EU-Kommission.[40] Zudem bestehen Leitlinien der European Securities and Markets Authority (ESMA), die sich mit Blick auf die Konvergenz der Finanzmarktaufsicht in den Mitgliedstaaten primär an die zuständigen nationalen Behörden richten.[41]

Ausserhalb des sechsten Titels finden sich an verschiedenen Stellen Vorgaben, die sich direkt oder indirekt mit Marktverhalten auseinandersetzen: Beson-

---

39 Verordnung (EU) 596/2014 des Europäischen Parlaments und des Rates vom 16. April 2014 über Marktmissbrauch.

40 Vgl. Art. 88 Abs. 4 MiCAR und dazugehörige Durchführungsverordnung (EU) 2024/2861 der Kommission vom 12. November 2024 sowie Art. 92 Abs. 2 MiCAR und dazugehörige Delegierten Verordnung (EU) 2025/885 der Kommission vom 29. April 2025 (vgl. auch ESMA, Draft technical Standards specifying certain requirements in relation to the detection and prevention of market abuse under the Markets in Crypto Assets Regulation (MiCA). Final Report, 17. Dezember 2024, 50 ff.; zit. ESMA, Draft Technical Standards).

41 Vgl. Art. 92 Abs. 3 MiCAR und dazugehörige ESMA, Guidelines on supervisory practices for competent authorities to prevent and detect market abuse under the Markets in Crypto Assets Regulation (MiCA). Final Report, 29. April 2025, *passim* (zit. ESMA, Supervisory Guidelines).

ders zu erwähnen sind etwa (i) die allgemeinen Verhaltensregeln in Art. 66 MiCAR, (ii) die Vorgaben zum Umgang mit Interessenkonflikten (Art. 72 MiCAR), (iii) die besonderen organisatorischen Vorgaben für Handelsplattformen, die für die Zulassung von Kryptowerten zum Handel und deren multilateralen Austausch verantwortlich sind (Art. 76 MiCAR), sowie (iv) solche für Personen, welche die Dienstleistungen der Ausführung von Aufträgen (Art. 78 MiCAR) und der Annahme und Übermittlung von Aufträgen über Kryptowerte für Kunden (Art. 80 MiCAR) erbringen. Wiederum finden sich hierzu Ausführungsbestimmungen in den Delegierten Verordnungen der EU-Kommission, so etwa im Bereich des Umgangs mit Interessenkonflikten[42] sowie der Aufzeichnung von Handelsdaten mit dem Ziel der effizienten Marktüberwachung durch Dienstleister und staatliche Behörden[43].

Soweit ersichtlich, mussten sich die europäischen *Gerichte* bislang noch nicht mit dem Marktverhaltensrecht unter MiCAR auseinandersetzen.

III. Anwendungsbereich

1. Einleitung

Die MiCAR sieht im Bereich des Marktmissbrauchsrechts eine Vollharmonisierung und die direkte Anwendbarkeit in den Mitgliedsstaaten der EU und des EWR vor (vgl. Art. 149).[44]

Der Anwendungsbereich des MiCAR-Marktverhaltensrechts wird in erster Linie in dessen Art. 86 festgelegt: Demnach gelten die Bestimmungen in Art. 87 bis 92 MiCAR für von Personen vorgenommene Handlungen im Zusammenhang mit Kryptowerten, die zum Handel zugelassen sind oder deren Zulassung zum Handel beantragt wurde (Abs. 1), und zwar unabhängig davon, ob ein Geschäft, ein Auftrag oder eine Handlung auf einer Handelsplattform getätigt wurde (Abs. 2). Die Vorgaben gelten für Handlungen und Unterlassungen in der Union und in Drittländern im Zusammenhang mit den in Abs. 1 genannten Kryptowerten (Abs. 3). Nachfolgend wird zuerst der *räumliche* Anwendungsbereich näher betrachtet.

---

42 Delegierte Verordnung (EU) 2025/1142 der Kommission vom 27. Februar 2025.

43 Vgl. etwa die Delegierte Verordnung (EU) 2025/416 der Kommission vom 29. November 2024.

44 Misterek Robin, Kapitel 18: Marktmissbrauch mit Kryptowerten, in: Miernicki Martin/Schinerl Fabian (Hrsg.), Handbuch Kryptowerte, Wien 2025, Rz. 19.

2. Räumlicher Anwendungsbereich

Das MiCAR-Marktverhaltensrecht gilt gemäss Abs. 86 Abs. 3 MiCAR für Handlungen und Unterlassungen in der Union und in Drittländern, sofern der Anwendungsbereich auch in persönlicher und sachlicher Hinsicht eröffnet ist (siehe hierzu jeweils unten).

Konkret orientiert sich die räumliche Anwendbarkeit der Bestimmungen am *Auswirkungsprinzip*, das auch unter der MAR einschlägig ist.[45] Auf den Handlungs- oder Unterlassungsort kommt es somit nicht an. Um jedoch eine allzu extraterritoriale Anwendbarkeit der Verordnung zu verhindern, ist mit der Literatur in solchen Fällen immerhin ein *hinreichender Bezug* („*genuine link*") zur EU bzw. zum EWR vorauszusetzen, wie namentlich ein gewisses Ausmass an negativen Auswirkungen auf den lokalen Kryptomarkt.[46]

Der sechste Titel von MiCAR ist nach dem Gesagten primär anwendbar, wenn die marktmissbräuchlich handelnde bzw. unterlassende Person im EWR agiert, falls der betreffende Kryptowert an einer Handelsplattform, die sich im EWR oder – nach umstrittener Ansicht –[47] in einem Drittland befindet, zugelassen wurde bzw. ein entsprechender Antrag auf Zulassung vorliegt. Sodann gelten die Bestimmungen auch, wenn die marktmissbräuchlich agierende Person die relevante Handlung bzw. Unterlassung in einem *Drittland* vornimmt, sofern wiederum ein hinreichender Bezug zum EWR-Kryptomarkt besteht.[48] Der Umstand, dass ein Kryptowert (auch) an einer Handelsplattform im EWR zum Handel zugelassen ist, dürfte darum für sich alleine die Anwendbarkeit der MiCAR noch nicht begründen. Darüber hinaus muss sich die im Ausland zutragende Handlung oder Unterlassung auch konkret negativ auf eine Handelsplattform im EWR auswirken,[49] wie etwa durch eine Verringerung der Liquidität oder eine Erhöhung der Transaktionskosten für die übrigen Marktteilnehmer.[50]

Soweit die übrigen Anwendungsbedingungen vorliegen, kann der sechste Titel von MiCAR selbst dann anwendbar sein, wenn das marktmissbräuchliche Verhalten ausschliesslich über eine *dezentrale* Handelsplattform erfolgt (vgl.

---

45 Misterek, § 18, Handbuch Kryptowerte, Rz. 19; Wutscher Claudia, Art. 86, in: Kalss Susanne/Krönke Christoph/Völkel Oliver (Hrsg), Kommentar Crypto-Assets, München 2025, Rz. 9.

46 Barczentewicz/de Gândara Gomes, 15 m.w.N.; Misterek, § 18, Handbuch Kryptowerte, Rz. 20.

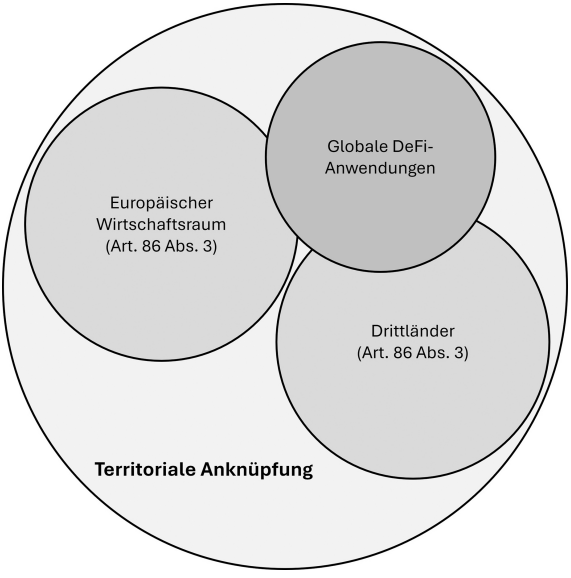
47 Siehe betreffend den *sachlichen* Anwendungsbereich unten, B.III.4.

48 Siehe Caramanica Luca/Schedler Gerhard Andreas, Kapitel 13 Grenzüberschreitende Kryptowerte-Dienstleistungen, in: Meier Johannes (Hrsg.), Handbuch MiCAR. Europäische Regulierung der Kryptowerte, Berlin 2025, Rz. 191.

49 *Gl. M. offenbar* Zetzsche/Woxholth, 164 f.; eine bloss *potenzielle* Einwirkung genügen lassend Maume Philipp, Art. 86, in: Maume Philipp (Hrsg.), MiCAR Kommentar, München 2025, Rz. 13.

50 Vgl. Misterek, § 18, Handbuch Kryptowerte, Rz. 20.

Art. 86 Abs. 2 MiCAR).[51] Dies mag überraschen, hat der EU-Gesetzgeber doch bewusst auf die inhaltliche Regulierung von (echten) DeFi-Anwendungen verzichtet.[52] Vor dem Hintergrund des weit verstandenen Auswirkungsprinzips der MiCAR ist diese Sichtweise allerdings korrekt.



3. Persönlicher Anwendungsbereich

Der persönliche Anwendungsbereich des MiCAR-Marktverhaltensrechts ist sehr offen formuliert, sodass sich grundsätzlich natürliche und juristische Personen sowie Rechtsgemeinschaften im Anwendungsbereich befinden (vgl. auch Art. 2 Abs. 1 MiCAR). Zu denken ist neben Anbietern von Kryptowerte-Dienstleistungen, deren Kunden und Mitarbeitern etwa an Emittenten und Anbieter von Kryptowerten sowie Personen, die direkt am Markt teilnehmen, ohne auf die Dienstleistungen eines Finanzintermediärs zurückzugreifen. Nicht massgeblich ist, zumal heute noch keine echte Autonomie solcher Strukturen vorliegt, ob die fragliche Person einen Smart Contract, einen computergestützten Algorithmus oder einen KI-Agenten einsetzt.[53]

---

51 Siehe betreffend den *sachlichen* Anwendungsbereich unten, B.III.4.

52 Siehe EWG 22 MiCAR: „*[…] Werden Kryptowerte-Dienstleistungen ohne eines Intermediärs in ausschließlich dezentralisierter Weise erbracht, so sollten sie nicht in den Anwendungsbereich dieser Verordnung fallen […].*“

53 Vgl. Maume, Art. 86, MiCAR Kommentar, Rz 12; ähnlich Zetzsche/Woxholth, 165; ferner EWG 96 MiCAR.

Besondere gesetzliche *Einschränkungen* des persönlichen Anwendungsbereichs bestehen in zwei Bereichen:

- Die Pflicht zur unverzüglichen Bekanntgabe von sie unmittelbar betreffenden Insiderinformationen gemäss Art. 88 Abs. 1 MiCAR (*Ad-hoc-Publizität*) gilt nur für Emittenten, Anbieter und Personen, welche die Zulassung zum Handel beantragen. Als *Emittent* gilt eine natürliche oder juristische Person oder ein anderes Unternehmen, die bzw. das Kryptowerte emittiert (Art. 3 Abs. 1 Ziff. 10 MiCAR); als *Anbieter* gilt sodann eine natürliche oder juristische Person oder ein anderes Unternehmen, die bzw. das Kryptowerte öffentlich anbietet, oder der Emittent, der Kryptowerte öffentlich anbietet (Art. 3 Abs. 1 Ziff. 13 MiCAR).
- Die Pflicht gemäss Art. 92 Abs. 1 MiCAR, wirksame Vorkehrungen, Systeme und Verfahren für die Vorbeugung und Aufdeckung von Markmissbrauch einzurichten und diesen bei begründetem Verdacht einer staatlichen Stelle zu melden, gilt nur für Personen, die beruflich Geschäfte mit Kryptowerten vermitteln oder ausführen (im Englischen: *Persons Professionally Arranging or Executing Transactions* bzw. PPAETs).[54]

Nicht im Anwendungsbereich von Art. 92 MiCAR sind nach nicht unbestrittener Ansicht hingegen die Teilnehmer am Konsensmechanismus einer Blockchain, namentlich Miner bzw. Validatoren, sowie Personen, welche die Funktion von Searchers, Builders und Relays ausüben (nachfolgend zusammen „*MEV-Agenten*").[55] Dies mag auf den ersten Blick überraschen, sind diese Personen doch nicht nur in den Prozess der Blockerstellung und -validierung einbezogen, sondern wären zumindest theoretisch auch imstande, Marktmissbrauchsaktivitäten auf der Konsensebene der Blockchain zu beobachten und entsprechende Verdachtsmeldungen zu tätigen. Allerdings scheint der aktuelle Wortlaut der MiCAR („*arranging or executing transactions*") nicht genügend Spielraum für den Einbezug dieser Funktionen zuzulassen.[56] Zumindest dann, wenn MEV-Agenten keine eigentlichen CASP-Funktionen ausüben, sollten sie nach vorliegender Ansicht nicht von Art. 92 MiCAR erfasst sein. Ob man die dazugehörigen Pflichten einem verteilten Netzwerk von Teilnehmern überhaupt überbinden will, scheint angesichts ähnlicher Diskussionen im Bereich der Fernmeldedienstanbieter und In-

---

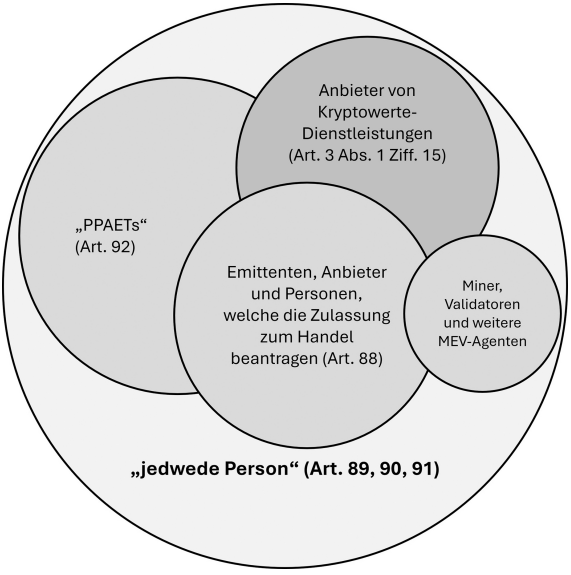
54 Zum Inhalt und Umfang der Pflichten siehe unten, B.VI.4.

55 Siehe ESMA, Draft Technical Standards, 6, 11 f.; *zustimmend* Galea Jonathan/Furcillo Vincenzo, Does MEV fall within scope of MiCA's Market Abuse provisions?, 4. September 2023, <https://blog.bcas.io/does-mev-fall-within-scope-of-micas-market-abuse-provisions>; *ablehnend* Barczentewicz/de Gândara Gomes, 9 f.

56 *Gl. M.* Misterek, § 18, Handbuch Kryptowerte, Rz. 101.

ternet Service Provider auch eine rechtspolitische Frage zu sein.[57] Es ist darum wahrscheinlich, dass für die Meinung der ESMA das Argument ausschlaggebend war, dass diese Funktionen andernfalls gänzlich ausserhalb des EWR erbracht würden.[58] In diesem Licht sollte vermutlich auch die Beschränkung des derzeit im Parlament diskutierten CLARITY Act auf „traditionelle" Krypto-Intermediäre in den USA gesehen werden.[59]

Demgegenüber scheint es ohne Weiteres möglich, dass die Gruppe von MEV-Agenten unter die übrigen Bestimmungen des Marktmissbrauchsrechts fallen kann.[60] Dies könnte etwa dann der Fall sein, wenn sie basierend auf nur ihnen zugänglichen Transaktionsdaten eigene oder fremde Transaktionen priorisieren oder Transaktionen von Blockchain-Nutzern künstlich zurückhalten, um einen eigenen Vorteil zu erlangen (siehe zum Thema „MEV" unten, D.).



57 Vgl. hierzu etwa Riordan Jaani, The Liability of Internet Intermediaries, Oxford 2016, *passim*; 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, *passim*.

58 Siehe ESMA, Draft Technical Standards, 12.

59 H.R. 3633, Digital Asset Market Clarity Act of 2025, Sec. 404 und 406, <https://www.govtrack.us/congress/bills/119/hr3633/text>, deren organisatorische Vorgaben sich an „*digital commodity exchanges*" bzw. „*digital commodity brokers*" und „*digital commodity dealers*" richten, nicht jedoch an Validatoren und andere Blockchain-Teilnehmer (vgl. Sec. 409).

60 So auch ESMA, Draft Technical Standards, 12; ferner für die USA H.R. 3633, Digital Asset Market Clarity Act of 2025, Sec. 309 und 409 jeweils *in fine*.

4. Sachlicher Anwendungsbereich

Marktmissbräuchliches Verhalten hat sich schliesslich auf *Kryptowerte* i.S.v. Art. 3 Abs. 1 Ziff. 5 MiCAR (unter Berücksichtigung der Ausnahmen gemäss Art. 2 Abs. 3 und 4 MiCAR) zu beziehen. Namentlich wird ein derartiges Verhalten mit Bezug zu Finanzinstrumenten i.S.v. Art. 4 Abs. 1 Ziff. 15 der Richtlinie 2014/65/EU (MiFID II) nicht durch die MiCAR, sondern durch die MAR erfasst, selbst wenn die Finanzinstrumente in tokenisierter Form ausgestaltet sind und somit als (von der MiCAR ausgenommene) Kryptowerte qualifizieren. Demgegenüber fallen Zahlungs- und Utility-Token sowie Stablecoins in Form von vermögenswertereferenzierten Token (ARTs) oder E-Geld-Token (EMTs) in den sachlichen Anwendungsbereich von Art. 86-92 MiCAR.

Ferner müssen die relevanten Kryptowerte einen Bezug zu einer *Handelsplattform* i.S.v Art. 3 Abs. 1 Ziff. 18 MiCAR aufweisen: Die Kryptowerte sind entweder bereits zum Handel an einer Handelsplattform zugelassen oder aber es muss zumindest ein Antrag auf eine solche Zulassung gestellt worden sein. Der Wortlaut in Art. 86 Abs. 1 MiCAR differenziert nicht, ob die fraglichen Kryptowerte zum Handel an einer Handelsplattform im EWR oder (bloss) in einem Drittland zugelassen sind.[61] Die vorherrschende Ansicht setzt allerdings zu Recht eine Handelszulassung an einer *MiCAR-regulierten* Handelsplattform oder einen diesbezüglichen Antrag bei einer solchen Plattform voraus.[62] Soweit es sich um eine EWR-Handelsplattform handelt, liegt im Regelfall ein Kryptowerte-Whitepaper gemäss den Vorgaben in der MiCAR vor.[63] Falls man hingegen der Minderheitsmeinung folgen will, würde dies bedeuten, dass den Marktverhaltensregeln der MiCAR ein nochmals grösserer extraterritorialer Anwendungsbereich zukäme, denn zumindest bedeutendere Kryptowerte sind fast immer in irgendeinem Drittland zum Handel zugelassen.[64] In diesem Fall wäre immerhin vorauszusetzen, dass die Drittstaatenplattform funktional den multilateralen Handel anbietet.[65]

---

61 *Zustimmend* Zetzsche/Woxholth, 164.

62 Siehe Maume, Art. 86, MiCAR Kommentar, Rz. 10; Misterek, § 18, Handbuch Kryptowerte, Rz. 19; Raschner Patrick, Kapitel 11 Verhinderung und Verbot von Marktmissbrauch im Zusammenhang mit Kryptowerten, in: Meier Johannes (Hrsg.), Handbuch MiCAR. Europäische Regulierung der Kryptowerte, Berlin 2025, Rz. 21; Wutscher, Art. 86, Kommentar Crypto-Assets, Rz. 6.

63 Vgl. Art. 5, 18 und 48 MiCAR sowie Art. 76 Abs. 1 UAbs. 2 MiCAR.

64 Eine Einschränkung erfolgt potenziell durch die Anwendung des *Auswirkungsprinzips*; vgl. hierzu oben, B.III.2.

65 Zetzsche/Woxholth, 164. Der Betreiber eines multilateralen Handelssystems führt die Interessen einer Vielzahl von Teilnehmern am Kauf und Verkauf von Kryptowerten innerhalb des Handelssystems zu einem Vertragsabschluss zusammen; vgl. auch Art. 22 FinfraV.

Kryptowerte, die *keinen* Bezug zu einer Handelsplattform aufweisen, befinden sich hingegen nicht im sachlichen Anwendungsbereich der Marktverhaltensregeln der MiCAR. Darunter fällt etwa ein Kryptowert, der zwar öffentlich angeboten wird und für den ggf. auch ein Whitepaper gemäss MiCAR vorliegt (vgl. Art. 4), der jedoch ausschliesslich *ausserhalb* einer Handelsplattform (insb. OTC) gehandelt wird.

Davon zu unterscheiden ist die Frage, wo die fragliche *marktmissbräuchliche Verhaltensweise* stattfindet: Diese muss gemäss Art. 86 Abs. 2 MiCAR nicht direkt auf einer Handelsplattform vorgenommen werden, sondern kann bspw. auch über einen Kryptobroker oder OTC-Desk, die selbst kein multilaterales Handelssystem betreiben, oder über eine dezentrale Handelsplattform oder gar Peer-to-Peer (P2P) erfolgen.[66]

Was das Tatbestandselement des *Marktmissbrauchs* anbelangt, verwendet die MiCAR unterschiedliche Begriffe, die grundsätzlich alle Formen von informations- und transaktionsbasierten Aktivitäten umfassen. Einerseits ist die Rede von „Geschäften" und „Aufträgen" – hierunter fallen „Insidergeschäfte" im Sinne von Art. 89 Abs. 1 MiCAR und gewisse Formen der transaktionsbasierten Marktmanipulation im Sinne von Art. 91 Abs. 2 und 3 MiCAR, die etwa Handelsabschlüsse, Aufträge zu solchen oder mit Handelsaufträgen zusammenhängende Handlungen, wie etwa Stornierungen und Änderungen, umfassen.

66 Maume, Art. 86, MiCAR Kommentar, Rz. 11.

Andererseits wird der weit zu verstehende Begriff der „Handlungen" bzw. „Unterlassungen" verwendet, der zudem die blosse Empfehlung oder Verleitung zu Insidergeschäften oder die (unrechtmässige) Offenlegung von Insiderinformationen (Art. 89 Abs. 2 und 3, Art. 90 MiCAR) oder die Verbreitung von irreführenden oder falschen Signalen bzw. Informationen gegenüber den Medien oder dem Markt (Art. 91 Abs. 2 und 3 MiCAR) umfasst.

5. Zwischenfazit

Nach dem Gesagten kann festgehalten werden, dass der räumliche, persönliche und sachliche Anwendungsbereich von Titel VI insgesamt *weiter* geht als die übrigen Bestimmungen der MiCAR.

IV. MiCAR und MAR: Gemeinsamkeiten und Unterschiede

Mit der Verordnung 596/2014/EU (Marktmissbrauchsverordnung, MAR) wird im Bereich der Finanzinstrumente ein gemeinsamer Rechtsrahmen für Insidergeschäfte, die unrechtmässige Offenlegung von Insiderinformationen und Marktmanipulation sowie für Massnahmen zur Verhinderung von Marktmissbrauch geschaffen, um die Integrität der Finanzmärkte im EWR sicherzustellen und den Anlegerschutz und das Vertrauen der Anleger in diese Märkte zu stärken (vgl. Art. 1 MAR).

Gemäss Art. 2 Abs. 1 MAR gilt die Verordnung für *Finanzinstrumente* (i.S.v. Art. 4 Abs. 1 Ziff. 15 i.V.m. Anhang 1 Abschnitt C MiFID II), wenn sie zum Handel auf einem geregelten Markt oder in einem multilateralen Handelssystem (MHS) zugelassen sind oder für sie ein Antrag auf Zulassung zum Handel auf einem geregelten Markt oder in einem MHS gestellt wurde oder wenn sie in einem organisierten Handelssystem (OHS) gehandelt werden. Ausserdem gilt die MAR für derivative und synthetische Instrumente, die sich auf vorgenannte Finanzinstrumente als Referenzwerte beziehen, jedoch nicht selbst an einem geregelten Markt, MHS oder OHS gehandelt werden. Finanzinstrumente in tokenisierter Form, wie etwa „Security Token", fallen ebenso in den sachlichen Anwendungsbereich der MAR wie bestimmte Formen von Schuldverschreibungen, strukturierten Produkten und Derivaten mit Krypto-Basiswerten (z.B. Exchange Traded Products, ETPs).[67] MAR und MiCAR ergänzen sich jedoch, wenn sowohl der organisierte Spot- als auch der organisierte Terminmarkt im Kryptobereich betroffen ist.[68]

---

67 Siehe ESMA, Guidelines on the conditions and criteria for the qualification of crypto-assets as financial instruments, 19. März 2025, 14 f.; ferner bereits EWG 97 MiCAR.

68 *Kritisch* zum fehlenden Gleichlauf Maume, Art. 86, MiCAR Kommentar, Rz. 4; ausführlich zur Zweispurigkeit der beiden Regime Misterek, § 18, Handbuch Kryptowerte, Rz. 3 ff., der auch auf mögliche Lücken hinweist

Mit Blick auf das Marktverhaltensregime der MiCAR ist die Nachahmung der MAR augenscheinlich.[69] Dies gilt zwar weniger für den Insider-, jedoch ganz besonders für den Marktmanipulationstatbestand.[70] Hinter der bewussten Nachahmung steckt die Annahme, dass Marktmissbrauch in Kryptomärkten in den Grundzügen dem in traditionellen Wertpapiermärkten Beobachtbaren entspricht.[71] Die Anlehnung bringt Vorteile für die Aufsichts- und Gerichtspraxis, birgt aber das Risiko der Über- oder Fehlregulierung der Kryptomärkte, deren Mikro- und Makrostrukturen deutlich von den traditionellen Märkten abweichen können.[72] Immerhin wird der Verhältnismässigkeitsgrundsatz in der MiCAR hervorgehoben.[73] Diskrepanzen zwischen den beiden Regimen können demgegenüber Doppelspurigkeiten für Marktteilnehmer verursachen, die über eine Zulassung als Bank oder Wertpapierfirma *und* als Anbieterin von Kryptowerte-Dienstleistungen verfügen.[74]

Die Vorgaben in der MAR sind teilweise deutlich *detaillierter* als unter der MiCAR: Die Marktmissbrauchsverordnung kennt hinsichtlich Insiderinformationen besondere Bestimmungen zu „legitimen Handlungen" (Art. 9) und Marktsondierungen (Art. 11). Im Kontext der Marktmanipulation enthält die MAR ferner die Möglichkeit der nationalen Behörde, zulässige Marktpraktiken, die den Besonderheiten des jeweiligen Marktes Rechnung trägt, zu definieren (Art. 13). Sodann werden darin auch die Massnahmen der Insiderliste und der Meldung von Eigengeschäften von Führungskräften bzw. „Directors' Dealings" (Art. 18 f. MAR) geregelt. Die vermeintlichen Vereinfachungen der MiCAR stellen in der Realität überraschenderweise allerdings Verschärfungen im Vergleich zur MAR dar.[75]

---

69 Siehe Barczentewicz/de Gândara Gomes, 1 f.; Kuhn Hans, X. Entwicklungen im Ausland, in: Weber Rolf H./Kuhn Hans (Hrsg.), Entwicklungen im Schweizer Blockchain-Recht, Basel 2021, Rz. 37; vgl. auch die Vergleichstabelle in Raschner, § 11, Handbuch MiCAR, Rz. 135; Zetzsche/Woxholth, 163 f.

70 Maume, Art. 87, MiCAR Kommentar, Rz. 1, ferner Art. 90 Rz. 1 und Art. 91 Rz. 1.

71 Vgl. ESMA, Draft Technical Standards, 7; Financial Conduct Authority (FCA), Regulating cryptoassets: Admissions & Disclosures and Market Abuse Regime for Cryptoassets, Discussion Paper DP24/4, Dezember 2024, Rz. 3.4 (zit. FCA, DP24/4).

72 *Kritisch* auch Maume, Art. 86, MiCAR Kommentar, Rz. 3; FCA, DP24/4, Rz. 3.7; offenbar *a.M.* Zetzsche/Woxholth, 170.

73 EWG 95 MiCAR: „*Da es sich bei den Emittenten von Kryptowerten und den Anbietern von Kryptowerte-Dienstleistungen jedoch sehr häufig um KMU handelt, wäre es unverhältnismäßig, sämtliche Bestimmungen der [MAR] auf sie anzuwenden.*"

74 Annunziata Filippo, An Overview of the Markets in Crypto-Assets Regulation (MiCAR), EBI Working Paper Series Nr. 158, 11. Dezember 2023, 67.

75 So Maume, Art. 89, MiCAR Kommentar, Rz. 1, 10, Art. 90 Rz. 1, 6; ebenfalls Barczentewicz/de Gândara Gomes, 5 f.

Inwieweit die MAR auch für das Aufsichtsverhalten der Behörden in Kryptomärkten von praktischer Bedeutung ist, ist noch offen.[76] Nach eigenen Aussagen der ESMA soll das MAR-Regime immerhin als Ausgangspunkt für die Vorgaben der MiCAR betrachtet werden.[77] In weiten Teilen identisch sind die Anforderungen an MAR-PPAETs, Regelungen, Systeme und Verfahren zur wirksamen Vorbeugung, Aufdeckung und Meldung von verdächtigen Aufträgen und Geschäften vorzusehen (Art. 16 MAR und Ausführungsbestimmungen[78]).[79] Ferner ist es absehbar, dass gewisse Marktverhaltensregeln, wie sie etwa für Anlageempfehlungen betreffend Finanzinstrumente gelten,[80] eine gewisse Ausstrahlungswirkung auf den Umgang der Aufsichtsbehörden mit sozialen Medien und *Finfluencern* im Kryptomarkt haben dürften –[81] ein Thema, das bekanntlich grosse praktische Bedeutung erlangt hat.[82]

V. Wesentliche Marktverhaltensregeln

1. Übersicht

Das MiCAR-Marktverhaltensregime kann im Wesentlichen in jeweils einen Abschnitt zum Umgang mit Insiderinformationen, zur Marktmanipulation und zu Organisations- und Meldepflichten von PPAETs unterteilt werden.

---

76 *Gl. M.*, teils aber skeptisch, was die ungeprüfte Übernahme anbelangt, Barczentewicz/de Gândara Gomes, 2.

77 Vgl. ESMA, Draft Technical Standards, 7, 17, 23.

78 Delegierte Verordnung (EU) 2016/957 der Kommission vom 9. März 2016.

79 ESMA, Draft Technical Standards, 7: „ESMA *proposed replicating some of the requirements imposed to PPAETs and trading venues under CDR 2016/957 in the draft RTS because most of the abusive behaviours occurring in crypto-asset markets follow patterns and schemes already observed in the traditional finance's space.*"; ferner Maume, Art. 92, MiCAR Kommentar, Rz. 2, 5, 12.

80 Art. 20 MAR; siehe etwa betreffend das Thema *Finfluencing* ESMA, Warning. For people posting Investment Recommendation on social media, 6. Februar 2024, *passim*, <https://www.esma.europa.eu/sites/default/files/2024-02/ESMA74-1103241886-912_Warnings_on_Social_Media_and_Investment_Recommendations.pdf>; hierzu auch Delegierte Verordnung (EU) 2016/958 der Kommission vom 9. März 2016.

81 Siehe EWG 96 a.E. MiCAR.

82 Vgl. IOSCO, Retail Market, 22 ff.

2. Insiderrecht

a) Begriff der Insiderinformation

Als *Insiderinformationen* gelten gemäss Legaldefinition in Art. 87 Abs. 1 MiCAR folgende Arten von Informationen:

- *Lit. a*: nicht öffentlich bekannte präzise Informationen, die direkt oder indirekt einen oder mehrere Emittenten, Anbieter oder Personen, welche die Zulassung zum Handel beantragen, oder einen Kryptowert betreffen und die, wenn sie öffentlich bekannt würden, geeignet wären, den Kurs dieses Kryptowerts oder den Kurs eines damit verbundenen Kryptowerts erheblich zu beeinflussen;
- *Lit. b*: für Personen, die mit der Ausführung von Aufträgen über Kryptowerte für Kunden beauftragt sind, bezeichnet der Begriff auch präzise Informationen, die von einem Kunden mitgeteilt wurden und sich auf die noch nicht ausgeführten Aufträge des Kunden über Kryptowerte beziehen, die direkt oder indirekt einen oder mehrere Emittenten, Anbieter oder Personen, welche die Zulassung von Kryptowerten zum Handel beantragen, oder einen Kryptowert betreffen und die, wenn sie öffentlich bekannt würden, geeignet wären, den Kurs dieses Kryptowerts oder den Kurs eines damit verbundenen Kryptowerts erheblich zu beeinflussen.

In erster Linie wird in Art. 87 Abs. 1 lit. a MiCAR zwischen *emittenten- und kryptowertbezogenen* Insiderinformationen unterschieden, wobei die Informationen sich ausnahmsweise auch auf den Anbieter oder Personen, welche die Zulassung zum Handel beantragen, beziehen können. Ferner fallen auch *marktbezogene* Informationen unter den Begriff, wenn sie nicht allgemein bekannt sind. Bei Kryptowerten ohne einen Emittenten oder Anbieter, wie etwa Bitcoin, können *de facto* nur kryptowert- und ggf. marktbezogene Informationenen tatbestandsmässig sein.[83] Denkbar wäre bei solchen Kryptowerten etwa, dass ein Softwareentwickler einen bislang unbekannten Programmierfehler entdeckt, der es einer Drittperson erlauben würde, nach Belieben neue Coins zu kreieren.[84]

Mit Art. 87 Abs. 1 lit. b MiCAR hatte der EU-Gesetzgeber den Sonderfall des *Frontrunnings* durch auftragsausführende Parteien im Blick, worunter in erster Linie Anbieter von Kryptowerte-Dienstleistungen mit einer eigenen Han-

---

[83] Ausführlich Maume, Art. 87, MiCAR Kommentar, Rz. 4 ff.

[84] Vgl. Coindesk, The Latest Bitcoin Bug Was So Bad, Developers Kept Its Full Details a Secret, 22. September 2018, <https://www.coindesk.com/markets/2018/09/21/the-latest-bitcoin-bug-was-so-bad-developers-kept-its-full-details-a-secret>.

delsabteilung fallen (vgl. die korrespondierenden Verhaltenspflichten in Art. 78 Abs. 2 und Art. 80 Abs. 3 MiCAR). Das relevante Insidergeschäft liegt im Abschluss eines Eigengeschäfts auf eigene Rechnung oder Rechnung Dritter.[85]

Die Information darf *nicht öffentlich bekannt* sein. Nicht erforderlich ist hingegen, dass sie geheim ist. Eine Insiderinformation, die einer unbestimmten Anzahl von Personen unter Ermöglichung der Kenntnisnahme zugänglich gemacht wird, worunter ein breites Anlegerpublikum am lokalen Markt zu verstehen ist, gilt als öffentlich. Eine tatsächliche Kenntnisnahme ist nicht erforderlich. Eine Publikation der Information in englischer Sprache auf sozialen Medien dürfte die Privatheit der Information entfallen lassen.[86]

Informationen sind gemäss dem nicht ganz lesefreundlichen Absatz 2 dann als *präzise* anzusehen, „*[…] wenn damit eine Reihe von Umständen gemeint ist, die bereits gegeben sind oder bei denen man vernünftigerweise erwarten kann, dass sie in Zukunft gegeben sein werden, oder ein Ereignis, das bereits eingetreten ist oder von dem man vernünftigerweise erwarten kann, dass es in Zukunft eintreten wird, und diese Informationen darüber hinaus spezifisch genug sind, um einen Schluss auf die mögliche Auswirkung dieser Reihe von Umständen oder dieses Ereignisses auf die Kurse der Kryptowerte zuzulassen. So können im Fall eines zeitlich gestreckten Vorgangs, der einen bestimmten Umstand oder ein bestimmtes Ereignis herbeiführen soll oder hervorbringt, dieser betreffende zukünftige Umstand bzw. das betreffende zukünftige Ereignis und auch die Zwischenschritte [gemäss Definition in Abs. 3] in diesem Vorgang, die mit der Herbeiführung oder Hervorbringung dieses zukünftigen Umstandes oder Ereignisses verbunden sind, in dieser Hinsicht als präzise Information betrachtet werden.*“ Vage Gerüchte und Spekulationen, die einen Emittenten oder Kryptowerte betreffen, gelten demgegenüber nicht als genügend präzise.[87]

Als *Informationen, die, wenn sie öffentlich bekannt würden, geeignet wären, den Kurs von Kryptowerten erheblich zu beeinflussen*, sind schliesslich Informationen zu verstehen, die ein verständiger (auch erst künftiger) Inhaber von Kryptowerten wahrscheinlich als Teil der Grundlage seiner Anlageentscheidungen nutzen würde (Abs. 4). Beispielhaft ist etwa an die nicht öffentliche Information über einen Stablecoin-Emittenten zu denken, dessen Geschäftsmodell nicht in Einklang mit den Zulassungsbedingungen gemäss der MiCAR steht und deshalb der Entzug der Zulassung durch die Aufsichtsbehörde überwiegend wahrscheinlich ist (z.B. aufgrund einer Unterdeckung in den Reser-

---

85 Siehe Raschner, § 11, Handbuch MiCAR, Rz. 62; Maume, Art. 87, MiCAR Kommentar, Rz. 20 f.; Barczentewicz/de Gândara Gomes, 6 m.w.H., 11.

86 Ausführlich hierzu Maume, Art. 87, MiCAR Kommentar, Rz. 12 ff.

87 Zum Ganzen Maume, Art. 87, MiCAR Kommentar, Rz. 16 ff.

ven der Emittentin und des damit zusammenhängenden Bankrun-Risikos).[88] Gemäss Wortlaut ist die Eignung zur Kurserheblichkeit ausreichend; ein Erfolg ist also nicht notwendig.[89] Abschliessend ist zu erwähnen, dass das Bild des „verständigen Inhabers von Kryptowerten" zum heutigen Zeitpunkt noch keinem einheitlichen normativen „Kryptoanlegerleitbild" folgt und Differenzen zum Anlegerleitbild unter MAR durchaus möglich sind.[90]

Die MiCAR weist nach dem Gesagten einen *weiten* Insiderinformationsbegriff auf, der es genügen lässt, dass eine Information, die (i) einen Emittenten, Anbieter oder eine Person, welche die Zulassung von Kryptowerten zum Handel beantragt, oder einen Kryptowert betrifft, (ii) nicht öffentlich bekannt und (iii) genügend präzise ist sowie (iv) geeignet wäre, den Kurs von Kryptowerten erheblich zu beeinflussen.

b) Bevorstehende Handelszulassung als Insiderinformation?

Die Erkenntnisse aus den Fällen *Wahi* und *Chastain* (siehe hierzu oben, A.II.) zeigen, dass die Information über eine bevorstehende Handelszulassung eines Tokens von grosser Relevanz für den Markt sein kann. Auch hier handelt es sich dem Wesen nach um eine Sonderform von Frontrunning von Kundenaufträgen, wobei diese anders als unter Art. 87 Abs. 1 lit. b MiCAR nur der Art nach bestimmbar sind.

Besonders Erstzulassungen von Token im organisierten Kryptomarkt sind potenziell besonders preissensitiv.[91] Marktteilnehmer, die solche Markteinführungen vornehmen, wie etwa die Emittentin selbst, aber auch der Betreiber einer Handelsplattform, haben darum ein besonderes Augenmerk auf die Vertraulichkeit des Umstands der Handelszulassung zu legen. Namentlich haben insb. Betreiber von Handelsplattformen alle geeigneten Massnahmen zu ergreifen, um Marktmissbrauch innerhalb des Unternehmens zu verhindern.[92] Das Kriterium der Kurserheblichkeit wird regelmässig auch von der Reputation und Reichweite der Handelsplattform oder des Brokers abhängen.[93] Im

---

88 Vgl. FCA, DP24/4, Rz. 3.52 ff.

89 Maume, Art. 87, MiCAR Kommentar, Rz. 7.

90 Hierzu Maume, Art. 87, MiCAR Kommentar, Rz. 10 f., ferner in Bezug auf die Marktmanipulation Art. 91 Rz. 15.

91 IOSCO, Crypto and Digital Assets, 29; ausführlich Remund/Meier, Teil 1, 340; Barczentewicz/de Gândara Gomes, 10 m.w.N.; bereits Verstein Andrew, Crypto Assets and Insider Trading Law's Domain, Iowa Law Review 2019, 1 ff., 26 ff.

92 Vgl. EWG 30 MAR.

93 Vgl. bspw. Coindesk, HBAR Surges 12% Following Robinhood Listing, Making It Top Daily Gainer Among Top 20, 26. Juli 2025, <https://www.coindesk.com/markets/2025/07/26/hbar-surges-12-following-robinhood-listing-making-it-top-daily-gainer-among-top-20>.

Sinne einer Heuristik ist sodann davon auszugehen, dass mit jeder weiteren Zulassung *desselben* Tokens zwar nicht die Vertraulichkeit, jedoch die Kurserheblichkeit der Information abnimmt. Neben dem Umstand der Zulassung eines Tokens zum Handel an einem organisierten Markt sind auch der *Ausschluss* vom Handel oder dessen *Sistierung* mögliche privilegierte Informationen, die Insiderinformationen darstellen können.

Entsprechend ist es zu begrüssen, dass die Legaldefinition der Insiderinformation unter der MiCAR (wie bereits unter der MAR) bereits die Kenntnis solcher Vorhaben erfasst.[94] Formen des Frontrunnings der Aufträge von Plattformnutzern, wie sie für Wahi und Chastain typisch waren, können somit als sanktionierbares Insidergeschäft gemäss Art. 89 Abs. 1 MiCAR qualifizieren.[95] Demgegenüber setzt der Insiderinformationsbegriff gemäss Art. 2 lit. j FinfraG[96] die *bereits* erfolgte Handelszulassung einer Effekte voraus.[97] Damit sind unter MiCAR Insiderhandelsfälle erfasst, die in der Schweiz im Effektenbereich *de lege lata* grundsätzlich nicht unterstellt sind (siehe hierzu unten, C.III.4.c)).

c) *Offenlegungspflicht (Ad-hoc-Publizität) und Bekanntgabeaufschub*

Gemäss Art. 88 Abs. 1 MiCAR *geben* Emittenten, Anbieter und Personen, welche die Zulassung zum Handel beantragen, der *Öffentlichkeit* Insiderinformationen gemäss Art. 87 MiCAR, die sie unmittelbar betreffen, unverzüglich in einer Art und Weise *bekannt*, die der Öffentlichkeit einen schnellen Zugang und eine vollständige, korrekte und rechtzeitige Bewertung ermöglicht.

Die Bestimmung ist auf den Abbau von Informationsungleichgewichten und die Gleichbehandlung der Anleger sowie auf die Verbesserung der Markteffizienz ausgerichtet.[98] Die Erfüllung der Pflicht zur Ad-hoc-Publizität lässt den Insiderhandelstatbestand entfallen, weil die Information nunmehr öffentlich bekannt ist; Insidergeschäfte sollen dadurch präventiv verhindert werden.[99]

---

94 Siehe Raschner, § 11, Handbuch MiCAR, Rz. 63.

95 In Bezug auf den NFT-Marktplatz in *Chastain* müsste man immerhin prüfen, ob ein (fungibler) Kryptowert i.S.v. MiCAR vorliegt.

96 Bundesgesetz über die Finanzmarktinfrastrukturen und das Marktverhalten im Effekten- und Derivatehandel vom 19. Juni 2015 (FinfraG, SR 958.1).

97 Statt vieler Maurenbrecher Benedikt/Hanslin Marc, Vor Art. 142 f., in: Watter Rolf/Bahar Rashid (Hrsg.), Basler Kommentar, Finanzmarktaufsichtsgesetz/Finanzmarktinfrastrukturgesetz, 3. A., Basel 2019, Rz. 54. Etwas Anderes gilt für prudenziell Beaufsichtigte gemäss FINMA-Rundschreiben 2013/8 „Marktverhaltensregeln", vgl. hierzu unten, C.VI.

98 Misterek, § 18, Handbuch Kryptowerte, Rz. 43.

99 Siehe Maume, Art. 88, MiCAR Kommentar, Rz. 2 f.; Misterek, § 18, Handbuch Kryptowerte, Rz. 43, 92.

Die *Veröffentlichung* der Insiderinformation muss in einer Art der Öffentlichkeit bekannt gegeben werden, die ihr einen schnellen Zugang und eine vollständige, korrekte und rechtzeitige Bewertung ermöglicht; dies wird regelmässig mindestens eine Bekanntgabe über die eigene Webseite und soziale Medien bedingen.[100] Die offenlegungspflichtigen Personen stellen Insiderinformationen auf ihrer Webseite für mindestens fünf Jahre bereit. Sie dürfen die Offenlegung von Insiderinformationen allerdings nicht mit der Vermarktung ihrer Tätigkeiten verbinden (Art. 88 Abs. 1 MiCAR).

Wenn die nachfolgend aufgeführten Voraussetzungen von Art. 88 Abs. 2 MiCAR kumulativ erfüllt sind, können Emittenten, Anbieter und Personen, welche die Zulassung zum Handel beantragen, auch die Bekanntgabe von Insiderinformationen *aufschieben*:

- Bei einer sofortigen Offenlegung ist davon auszugehen, dass sie die berechtigten Interessen der genannten Personen beeinträchtigt;
- der Aufschub der Offenlegung wäre nicht geeignet, die Öffentlichkeit irrezuführen; und
- die genannten Personen können die Geheimhaltung dieser Informationen sicherstellen.

Die aufschiebende Person ist für die Ergreifung angemessener Massnahmen verantwortlich; wenn erste Gerüchte am Markt auftauchen, wird sie regelmässig die Insiderinformation bekanntgeben müssen.[101] Wurde die Bekanntgabe aufgeschoben, so informieren die genannten Personen gemäss Abs. 3 die zuständige Behörde (oder alternativ auf deren Ersuchen) unmittelbar nach der Offenlegung der Informationen über den Aufschub der Offenlegung und erläutern schriftlich, inwieweit die in Abs. 2 festgelegten Bedingungen erfüllt waren.

d) Verbot von Insidergeschäften

Ein *Insidergeschäft* nach Art. 89 Abs. 1 MiCAR liegt vor, „*[…] wenn eine Person über Insiderinformationen verfügt und unter Nutzung derselben für eigene oder fremde Rechnung direkt oder indirekt Kryptowerte, auf die sich diese Informationen beziehen, erwirbt oder veräußert. Die Nutzung von Insiderinformationen in Form der Stornierung oder Änderung eines Auftrags in Bezug auf einen Kryptowert, auf den sich die Informationen beziehen, gilt auch als Insidergeschäft,*

---

100 Ausführlich dazu Durchführungsverordnung (EU) 2024/2861 der Kommission vom 12. November 2024; ferner Maume, Art. 88, MiCAR Kommentar, Rz. 11.

101 Maume, Art. 88, MiCAR Kommentar, Rz. 16.

wenn der [ursprüngliche] Auftrag vor Erlangen der Insiderinformationen erteilt wurde. Die Nutzung von Insiderinformationen schließt auch die Übermittlung, Änderung oder Zurücknahme eines Gebots durch eine Person für eigene Rechnung oder für Rechnung eines Dritten ein." Es muss ein Kausalzusammenhang zwischen der Kenntnis der Insiderinformation und dem Insidergeschäft vorliegen.[102]

Art. 89 Abs. 2 bis 4 MiCAR weisen unterschiedliche, ineinandergreifende und teils redundante Verbotsnormen auf, die sich mit dem *Handel* gestützt auf Insiderinformationen, diesbezüglichen *Empfehlungen*, der *Verleitung* bzw. *Anstiftung* zu einem solchen Handel oder der *Ausnutzung* solcher Empfehlungen oder Verleitungen befassen:

- Erstens darf niemand Insidergeschäfte tätigen oder versuchen, Insidergeschäfte zu tätigen, oder Insiderinformationen über Kryptowerte nutzen, um diese Kryptowerte, direkt oder indirekt, für eigene Rechnung oder für Rechnung eines Dritten, zu erwerben oder zu veräussern.
- Zweitens darf niemand Dritten empfehlen, Insidergeschäfte zu tätigen, oder Dritte dazu verleiten, Insidergeschäfte zu tätigen. Konkreter (so Abs. 3) darf niemand, der im Besitz von Insiderinformationen über Kryptowerte ist, auf der Grundlage dieser Insiderinformationen Dritten empfehlen oder sie dazu verleiten, (a) Kryptowerte zu erwerben oder zu veräussern oder (b) einen Auftrag, der diese Kryptowerte betrifft, zu stornieren oder zu ändern. Es muss sich um eine *eigene* Empfehlung handeln, andernfalls es sich um eine unzulässige Offenlegung der Insiderinformation gemäss Art. 90 MiCAR handelt (siehe hierzu unten); demgegenüber braucht es beim blossen Verleiten keiner kommunikativen Beziehung zwischen Insider und beeinflusster Person.[103]
- Die Nutzung von Empfehlungen oder Verleitungen gemäss Abs. 3 erfüllt ebenfalls den Tatbestand des Insidergeschäfts, wenn die Person, welche die Empfehlung nutzt oder der Anstiftung folgt (sog. *Tippempfänger*), weiss oder wissen sollte, dass diese auf Insiderinformationen beruht.

Das Insiderhandels-, Empfehlungs- und Nutzungsverbot dient jeweils dem Schutz der informationellen Chancengleichheit der Anlegerschaft und der Markteffizienz.[104]

Als taugliche Täter gelten gemäss Art. 89 Abs. 5 UAbs. 1 MiCAR insb. Mitglieder von Geschäftsführungsorganen (d.h. Geschäftsleitung und Verwaltungsrat)

---

102 Maume, Art. 89, MiCAR Kommentar, Rz. 9 m.w.H.

103 Maume, Art. 89, MiCAR Kommentar, Rz. 16 f.

104 Maume, Art. 89, MiCAR Kommentar, Rz. 3 m.w.N., 14.

von Emittenten, Anbietern oder Personen, welche die Zulassung zum Handel beantragen. Darüber hinaus kommen auch Personen infrage, die an den erwähnten Personen (qualifiziert) beteiligt sind oder aufgrund der Ausübung einer Arbeit oder eines Berufs, der Erfüllung von Aufgaben oder im Zusammenhang mit ihrer Rolle im Bereich der Blockchain (siehe hierzu sogleich unten) Zugang zu den betreffenden Informationen und darum ebenfalls über einen Zugang zu preis- bzw. kursrelevanten Informationen verfügen könnten. Neben diesen *Primärinsidern* sind grundsätzlich auch jegliche *Sekundärinsider* erfasst (Art. 89 Abs. 5 UAbs. 2 MiCAR).[105]

Anders als die MAR sieht die MiCAR keine Pflicht zur Führung von Insiderlisten und zur Meldung von Eigengeschäften von Führungskräften vor. Dass der Gesetzgeber in diesem Punkt einen zurückhaltenderen Ansatz gewählt hat, ist zu begrüssen. Dies auch darum, weil die Marktteilnehmer im Kryptomarkt regelmässig über Governance-Strukturen verfügen, die nur bedingt mit traditionellen börsenkotierten Firmen vergleichbar sind. Immerhin aber haben Emittenten von Kryptowerten bzw. die für sie im Markt handelnden Personen ein Whitepaper zu veröffentlichen, das auch Aufschluss über allfällige Interessenkonflikte geben muss.[106] Gemäss *Maume* sind sodann die Vermutungen von Art. 9 MAR, wonach trotz möglichen Besitzes von Insiderinformationen „legitime Handlungen" vorliegen, die etwa für Market Maker und zentrale Gegenparteien relevant sind, trotz Fehlens einer analogen Bestimmung auch in die MiCAR „hineinzulesen".[107]

e) Blockchain-Teilnehmer als Insider?

Ferner, und hierin weicht die MiCAR teilweise von der MAR ab, sind auch Personen als *Primärinsider* besonders exponiert, die aufgrund der Ausübung einer Arbeit oder eines Berufs, der Erfüllung von Aufgaben oder im Zusammenhang mit ihrer Rolle im Bereich der Blockchain oder einer ähnlichen Technologie Zugang zu den betreffenden Informationen haben (vgl. Art. 89 Abs. 5 UAbs. 1 lit. c MiCAR). In Bezug auf den ersten Satzteil ist v.a. an Anbieter von Kryptowerte-Dienstleistungen und deren Angestellte zu denken, die etwa die Auftragseingänge ihrer Kunden zum eigenen Vorteil ausnutzen könnten. Nach Ansicht der ESMA befinden sich sodann auch Miner, Validatoren, Searcher und Builder in einer besonderen Beziehung zu Insiderinformationen.[108]

---

105 Vgl. hierzu Zetzsche/Woxholth, 167.

106 Vgl. z.B. für „andere Kryptowerte" Art. 6 Abs. 1 i.V.m. Anhang I MiCAR.

107 Maume, Art. 89, MiCAR Kommentar, Rz. 10.

108 Bereits EWG 96 MiCAR („*[…] wobei beispielsweise […] der Rückgriff auf intelligente Verträge für die Ausführung von Aufträgen und die Konzentration von Mining-Pools zu berücksich-*

Ob dies effektiv der Fall ist, hängt von vielen Faktoren ab. Allen voran muss eine Insiderinformation im Sinne von Art. 87 MiCAR vorliegen, was bei einer Verarbeitung durch die erwähnten Personen von Transaktionen, die in einem öffentlich zugänglichen Transaktionsregister gesammelt werden, nach vorliegender Ansicht in aller Regel nicht der Fall ist. Demgegenüber könnte allerdings der Betreiber einer Full Node oder eines *Remote Procedure Call (RPC)*-Servers, der die Transaktion eines Blockchain-Nutzers zuerst und ausschliesslich sieht, die Information der Kundentransaktion durchaus zu seinen Gunsten verwerten.[109] Das Thema wird unten noch eingehender zu betrachten sein (siehe D.).

f) *Verbot der unrechtmässigen Offenlegung von Insiderinformationen*

Weil Art. 88 MiCAR die Offenlegung von Insiderinformationen gegenüber der Öffentlichkeit zum Grundsatz erklärt (*Ad-hoc-Publizität*), dürfen Insider solche Informationen nur einem sehr beschränkten Kreis von Personen zugänglich machen.[110] Laut Art. 90 Abs. 1 MiCAR darf darum niemand, der über Insiderinformationen verfügt, diese *unrechtmässig* Dritten offenlegen, es sei denn, diese Offenlegung erfolgt im Zuge der normalen Ausübung einer Beschäftigung oder eines Berufs oder der normalen Erfüllung von Aufgaben. Diese Ausnahme ist eng auszulegen und entspricht im Wesentlichen dem *Need-to-Know*-Prinzip.[111]

Die Weitergabe von (fremden) Empfehlungen oder das Verleiten anderer gemäss Art. 89 Abs. 4 MiCAR gilt als unrechtmässige Offenlegung von Insiderinformationen, wenn die Person, welche die Empfehlung weitergibt oder andere verleitet, weiss oder wissen sollte, dass die Empfehlung bzw. Verleitung auf Insiderinformationen beruht (Art. 90 Abs. 2 MiCAR).

3. Marktmanipulationsrecht

a) *Verbot der Marktmanipulation*

Niemand darf Marktmanipulation betreiben oder einen entsprechenden Versuch unternehmen (Art. 91 Abs. 1 MiCAR).

---

tigen sind.“); sodann ESMA, Draft Technical Standards, 12; ferner Maume, Art. 89, MiCAR Kommentar, Rz. 22.

109 Barczentewicz/de Gândara Gomes, 11.

110 Misterek, § 18, Handbuch Kryptowerte, Rz. 65.

111 Maume, Art. 90, MiCAR Kommentar, Rz. 7.

b) Begriff der Marktmanipulation

Neben den Verboten im Zusammenhang mit Insiderinformationen sieht MiCAR v.a. ein Verbot der Marktmanipulation vor. Gemäss Legaldefinition in Art. 91 Abs. 2 MiCAR werden folgende transaktions-, handlungs- und informationsbasierten *Marktmanipulationen* als missbräuchlich erfasst:

- *Lit. a*: den Abschluss eines Geschäfts, die Erteilung eines Handelsauftrags oder jede andere Handlung, die (i) falsche oder irreführende Signale hinsichtlich des Angebots oder des Kurses eines Kryptowerts oder der Nachfrage danach gibt oder bei der dies wahrscheinlich ist oder (ii) für einen Kryptowert ein anormales oder künstliches Kursniveau herbeiführt oder bei denen dies wahrscheinlich ist – vorausgesetzt, es liegt kein legitimer Grund für die Handlung vor;
- *Lit. b*: der Abschluss eines Geschäfts, die Erteilung eines Handelsauftrags oder eine andere Tätigkeit oder Handlung, die unter Vorspiegelung falscher Tatsachen oder unter Verwendung sonstiger Kunstgriffe oder Formen der Täuschung den Kurs eines Kryptowerts beeinflusst oder hierzu geeignet ist;
- *Lit. c*: die Verbreitung von Informationen über die Medien, einschliesslich des Internets oder auf anderem Wege, die falsche oder irreführende Signale hinsichtlich des Angebots oder des Kurses eines Kryptowerts oder der Nachfrage danach geben oder bei denen dies wahrscheinlich ist oder die für einen Kryptowert ein anormales oder künstliches Kursniveau herbeiführen oder bei denen dies wahrscheinlich ist, einschliesslich der Verbreitung von Gerüchten, wenn die Person, die diese Informationen verbreitet hat, wusste oder hätte wissen müssen, dass sie falsch oder irreführend waren.

Die MiCAR folgt wie die MAR (Art. 12) einem effekt- bzw. auswirkungsbasierten Ansatz. Besonders in Märkten, die weniger stark von Fundamentaldaten abhängen, wie etwa Geschäftsmodelle ohne regelmässige Geldflüsse (z.B. Zinszahlungen), oder solchen mit tieferer Liquidität, wie dies im Kryptomarkt häufiger der Fall sein kann, wird dieser Ansatz vor gewisse praktische Herausforderungen gestellt.[112] Wie beim Insidertatbestand gilt auch hier die Sichtweise eines objektivierten verständigen Anlegers: So liegt ein falsches oder irreführendes Signal vor, wenn das Angebots- oder Nachfrageverhalten bzw. der Preis aus Sicht des verständigen Anlegers nicht den wahren Marktverhältnis-

[112] So auch Maume, Art. 91, MiCAR Kommentar, Rz. 5, 18; Misterek, § 18, Handbuch Kryptowerte, Rz. 42, 71, 76.

sen entspricht bzw. beim verständigen Anleger eine Fehlvorstellung über die wahren Marktverhältnisse auslöst.[113]

Art. 91 Abs. 3 MiCAR enthält sodann eine *nicht abschliessende* Aufzählung an Beispielen marktmanipulatorischer Handlungen:[114]

- *Lit. a:* die Sicherung einer marktbeherrschenden Stellung in Bezug auf das Angebot an oder die Nachfrage nach einem Kryptowert, die eine unmittelbare oder mittelbare Festsetzung des Kauf- oder Verkaufskurses oder andere unlautere Handelsbedingungen bewirkt oder hierzu geeignet ist;
- *Lit. b*: die Erteilung von Aufträgen über eine Handelsplattform für Kryptowerte, einschliesslich deren Stornierung oder Änderung, mittels aller zur Verfügung stehenden Handelsmethoden (inkl. des *algorithmischen* und *Hochfrequenzhandels*), die (i) falsche oder irreführende Signale hinsichtlich des Angebots oder des Kurses eines Kryptowerts oder der Nachfrage danach gibt oder bei der dies wahrscheinlich ist oder (ii) für einen Kryptowert ein anormales oder künstliches Kursniveau herbeiführt oder bei denen dies wahrscheinlich ist, durch:
  - Störung oder Verzögerung des Betriebs der Handelsplattform für Kryptowerte oder Ausübung von Tätigkeiten, die wahrscheinlich eine solche Wirkung haben;
  - Erschwerung der Ermittlung echter Aufträge auf der Handelsplattform für Kryptowerte durch Dritte oder Ausübung von Tätigkeiten, die wahrscheinlich eine solche Wirkung haben, einschliesslich der Erteilung von Aufträgen, die zur Destabilisierung des normalen Betriebs der Handelsplattform für Kryptowerte führen; oder
  - das Setzen falscher oder irreführender Signale hinsichtlich des Angebots oder des Preises eines Kryptowerts oder der Nachfrage danach, insb. durch Erteilung von Aufträgen zur Einleitung oder Verschärfung eines Trends oder durch Ausübung von Tätigkeiten, die wahrscheinlich eine solche Wirkung haben.
- *Lit. c*: Ausnutzung des gelegentlichen oder regelmässigen Zugangs zu traditionellen oder elektronischen Medien durch Veröffentlichung von Stellungnahmen zu einem Kryptowert, nachdem zuvor Positionen in diesem Kryptowert eingegangen wurden und anschliessend aus den Auswirkun-

113 Maume, Art. 91, MiCAR Kommentar, Rz. 13 ff.

114 Ausführlich hierzu Maume, Art. 91, MiCAR Kommentar, Rz. 38 ff.

gen der Stellungnahme auf den Kurs dieses Kryptowerts Nutzen gezogen wird, ohne dass der Öffentlichkeit gleichzeitig dieser Interessenkonflikt ordnungsgemäss und wirksam bekannt gegeben wird.

Verschiedene Formen von betrügerischen Aktivitäten, die im Kryptomarkt verbreitet sind, wie etwa Pump-and-Dump-Systeme, Wash Trading und Rug Pulls, können je nach Ausgestaltung (auch) Marktmanipulation nach MiCAR darstellen.[115]

c) *Finfluencing als Marktmanipulation?*

Im Kryptomarkt kommt sozialen Medien wie X bzw. *Twitter*, *Telegram* und *YouTube* eine besondere Bedeutung zu. Darum wird die Tatbestandsvariante der informationsgestützten Marktmanipulation gemäss Art. 91 Abs. 2 lit. c MiCAR mit Blick auf den Kryptomarkt als besonders praxisrelevant angesehen.[116]

Jegliche Information, ob in Form eines Werturteils oder einer Tatsachenbehauptung, kommt grundsätzlich als „Tatobjekt" infrage.[117] So ist etwa bereits der berühmt gewordene Einzeiler-Tweet von Do Kwon eine relevante Äusserung. Darin hat der damalige CEO von Terraform Labs suggeriert, dass durch den Einsatz weiteren Kapitals die Stabilisierung des im Sinkflug befindenden algorithmischen Stablecoins UST wieder erreicht werden könne („*Deploying more capital – steady lads*").[118] Die fragliche Information muss sodann geeignet sein, falsche oder irreführende Signale herbeizuführen und dadurch den Markt zu täuschen oder aber ein anormales oder künstliches Kursniveau herbeizuführen.[119]

Das Spektrum möglicher Äusserungen im Bereich des Finfluencing ist breit: Einerseits kann es um Aussagen einer berühmten Person gehen, die ihre Vergütung durch einen Emittenten oder einen Anbieter von Kryptowerte-Dienstleistungen nicht offenlegt;[120] andererseits können Personen ganz bewusst soziale Medien dazu einsetzen, falsche Informationen mit dem Ziel eines

---

115 So etwa Barczentewicz/de Gândara Gomes, 12 f.; ferner Zetzsche/Woxholth, 168.

116 Siehe Maume, Art. 91, MiCAR Kommentar, Rz. 26 ff., 51 ff.; ausführlich Zetzsche/Woxholth, 160 ff., 170; ferner IOSCO, Retail Market, 22 ff.

117 Maume, Art. 91, MiCAR Kommentar, Rz. 27.

118 Cointelegraph, 10 crypto tweets that aged like milk: 2022 edition, 30. Dezember 2022, <https://cointelegraph.com/news/10-crypto-tweets-that-aged-like-milk-2022-edition>.

119 Maume, Art. 91, MiCAR Kommentar, Rz. 31 ff.

120 Vgl. etwa Financial Times, Binance says footballer Andrés Iniesta was paid for Twitter post, 26. November 2021, <https://www.ft.com/content/64d4cfa6-e277-4a5b-a8b7-f7def5b82e00>.

Preisanstiegs zu streuen, nachdem zuvor eigene Positionen im fraglichen Kryptowert aufgebaut worden sind (vgl. Fall von *Galaxy Digital*). Während erstere Aussage für sich alleine unter Gesichtspunkten der Marktmanipulation nicht relevant sein dürfte, wird letzterer Fall des *Scalpings* im Beispielkatalog besonders erwähnt (vgl. Art. 91 Abs. 3 lit. c MiCAR).[121]

d) Vorliegen legitimer Gründe („Safe Harbor")

Damit legitime Formen von Finanzaktivitäten nicht ungewollt verboten werden, insb. solche, in denen kein Marktmissbrauch vorliegt, ist es erforderlich, bestimmte legitime Handlungen anzuerkennen.[122] Die MiCAR enthält allerdings anders als die MAR (Art. 13) keine ausdrückliche Erwähnung *zulässiger Marktpraktiken* (ZMP).

Besonders die grundsätzlich zulässige Tätigkeit des *Market Makings*, d.h. das gleichzeitige Stellen von Kauf- und Verkaufskursen in Finanzinstrumenten bzw. Kryptowerten mit dem Ziel, den übrigen Marktteilnehmern in Einklang mit dem Preistrend Liquidität bereitzustellen,[123] kann unter gewissen Umständen Ähnlichkeiten mit unzulässigen Marktpraktiken haben.[124] Ähnliches gilt für Stabilisierungsprogramme und *Burning*-Massnahmen, die Ähnlichkeiten mit legitimen Rückkaufprogrammen von Aktiengesellschaften samt Vernichtung der Aktien aufweisen können,[125] u.U. jedoch von DAOs beschlossen werden und der Protokollstabilität dienen können.[126] Es ist wichtig, dass auch Krypto-Marktteilnehmer rechtssicher legitime Aktivitäten verfolgen können.[127]

---

121 Ein voraussichtlich vergleichbares Regime ist in den USA vorgesehen, das u.a. „*digital commodity related or affiliated persons*", die in ihrer Funktion als Promoter von der Emittentin Kryptowerte erhalten haben bzw. erhalten werden, ausdrücklich in den Anwendungsbereich der Marktverhaltensregeln aufnimmt; vgl. H.R. 3633, Digital Asset Market Clarity Act of 2025, Sec. 204; zum rechtspolitischen Hintergrund siehe Oranburg Seth, The CLARITY Act: Explaining and Analyzing How Congress Will Transform Digital Asset Markets, 11. Juni 2025, 10, 20 f., 25 ff., <https://ssrn.com/abstract=5288934>.

122 Vgl. EWG 29 MAR.

123 FINMA-Rundschreiben 2013/8 „Marktverhaltensregeln", Rz. 32.

124 Vgl. auch FINMA-Mitteilung 52, Handel im eigenen Titel mit dem Zweck der Liquiditätsbereitstellung unter den neuen Bestimmungen zur Marktmanipulation, 18. November 2013, 4 f.

125 Siehe Barczentewicz/de Gândara Gomes, 16 f.

126 Vgl. etwa CryptoSlate, MakerDAO founder proposes strict deflationary tokenomics amid rebranding process, 1. November 2024, <https://cryptoslate.com/makerdao-founder-proposes-strict-deflationary-tokenomics-amid-rebranding-process/>; ferner Allen Darcy W.E./Berg Chris/Davidson Sinclair, Buyback and Burn Mechanisms: Price Manipulation or Value Signalling?, 28. September 2022, *passim*, <https://ssrn.com/abstract=4231845>.

127 So auch FCA, DP24/4, Rz. 3.48 f.

In Ausführung von Art. 13 Abs. 2 MAR hat die EU-Kommission gemeinsame Kriterien entwickelt, welche die Festlegung von ZMP durch die nationalen Aufsichtsbehörden koordinieren soll.[128] Als Kriterien qualifizieren etwa der Grad der Markttransparenz, das Funktionieren der Marktkräfte bzw. von Angebot und Nachfrage, Marktliquidität und -effizienz, der Handelsmechanismus des betreffenden Marktes, Integritätsrisiken sowie Strukturmerkmale des betreffenden Marktes. Für die MiCAR ist ein solcher Kriterienkatalog allerdings nicht vorgesehen.

4. Organisations- und Melderegime für PPAETs

a) Begriff der PPAETs

Im Rahmen der Ausführungen zum persönlichen Anwendungsbereich des Marktverhaltensregimes der MiCAR wurde bereits auf die Unterstellung von Personen, die beruflich Geschäfte mit Kryptowerten vermitteln oder ausführen (im Englischen: „*Persons Professionally Arranging or Executing Transactions*" bzw. PPAETs), unter die Organisations- und Meldepflichten in Art. 92 MiCAR Bezug genommen.[129]

Der Kreis der PPAETs wird in der MiCAR selbst nicht näher definiert:[130] Gemäss ESMA fallen darunter beruflich tätige Personen, die eine Handelsplattform betreiben, Aufträge über Kryptowerte für Kunden annehmen und übermitteln, Aufträge über Kryptowerte für Kunden ausführen, Portfolios von Kryptowerten verwalten, Kryptowerte gegen Geldbetrag bzw. gegen Kryptowerte tauschen und solche Marktteilnehmer, die für eigene Rechnung mit Kryptowerten handeln.[131] Für Letztere gilt gemäss ESMA, dass die Tatsache, dass „*[…] they have staff or a structure dedicated to systematically deal on own account, such as a trading desk[,] are indicators to consider a person as a PPAET.*"[132] Somit werden die Pflichten von Art. 92 MiCAR auch Personen auferlegt, die nicht als Anbieter von Kryptowerte-Dienstleistungen i.S.v. Art. 3 Abs. 1 Ziff. 15 MiCAR qualifizieren und somit nicht zwingend einer prudenziellen staatlichen Aufsicht unterstehen.[133] Ferner ist es nicht ausgeschlossen, dass auch noch weitere Typen von Anbietern von Kryptowerte-Dienstleistun-

---

128 Delegierte Verordnung (EU) 2016/908 der Kommission vom 26. Februar 2016.

129 Siehe oben, B.III.2.

130 *Kritisch* Barczentewicz/de Gândara Gomes, 8 ff.

131 ESMA, Draft Technical Standards, 6.

132 ESMA, Draft Technical Standards, 6; ferner ESMA, Q&A 1149, 15. November 2022, <https://www.esma.europa.eu/publications-data/questions-answers/1149>.

133 *Kritisch* Galea/Furcillo, *passim*.

gen den Pflichtenkatalog von Art. 92 MiCAR umzusetzen haben.[134] Umstritten ist etwa die Unterstellung von reinen Wallet-Anbietern, die Transaktionen auf der Blockchain bloss technisch auslösen und deren Tätigkeit kein inhärentes Marktmissbrauchsrisiko mit sich bringt.[135]

Unbestrittenerweise ausgenommen sind hingegen Personen, die Kryptowerte lediglich gelegentlich und somit in nicht beruflicher Weise handeln, namentlich zu Absicherungszwecken.[136] Miner, Validatoren und MEV-Agenten fallen ebenfalls nicht in den persönlichen Anwendungsbereich der Bestimmung.[137] Richtigerweise muss das auch für Emittenten und Anbieter von Kryptowerten gelten, selbst wenn sie gewisse Funktionen des Smart Contracts, der für die Ausgabe der Token verwendet wird, beeinflussen können.

Ganz grundsätzlich wird in den verschiedenen Stellungnahmen zur MiCAR die ausgeprägte *Gatekeeper*-Rolle von Betreibern von *Handelsplattformen* u.a. mit Blick auf die Einhaltung der Marktverhaltensregeln durch Kunden und Geschäftspartner erkennbar.[138] Aufgrund ihrer Möglichkeit, das ganze Orderbuch einzusehen und zu überwachen, kommt ihnen tatsächlich eine wichtige Funktion in der Marktmissbrauchsbekämpfung zu. Sie unterliegen Anforderungen an die Vor- und Nachhandelstransparenz, die den Besonderheiten im Kryptomarkt angepasst sind (Art. 76 Abs. 9 und 10 MiCAR). Ausserdem haben die Betreiber solcher Plattformen ihre Gebührenstruktur so auszugestalten, dass sie keine Anreize bei ihren Kunden schaffen, Aufträge so zu platzieren, ändern oder stornieren oder Geschäfte in einer Weise so auszuführen, dass dies zu Marktstörungen oder gar Marktmissbrauch beiträgt.[139] Ein weiteres Beispiel für Gatekeeping von Plattformbetreibern ist etwa deren Pflicht, Kryptowerte einem Tokenzulassungsverfahren zu unterziehen und in diesem Rahmen bestimmte Eigenschaften und das Vorliegen eines Kryptowerte-Whitepapers zu prüfen.[140]

---

134 So ggf. Anbieter von Verwahrungs- und/oder Transferdienstleistungen; vgl. ESMA, Draft Technical Standards, 12 f.

135 Vgl. ESMA, Draft Technical Standards, 12 f.; ferner Maume, Art. 92, MiCAR Kommentar, Rz. 6.

136 Maume, Art. 92, MiCAR Kommentar, Rz. 4.

137 Siehe hierzu oben, B.III.2.

138 Art. 62 Abs. 2 lit. n und Art. 76 Abs. 7 lit. g und Abs. 8 MiCAR; vgl. dazu Maume, Art. 92, MiCAR Kommentar, Rz. 3, 5.

139 Art. 76 Abs. 13 MiCAR; vgl. hierzu Patz Anika, Art. 76, in: Maume Philipp (Hrsg.), MiCAR Kommentar, München 2025, Rz. 50 ff.

140 Art. 76 Abs. 2 MiCAR; ferner EWG 84 MiCAR; vgl. ausführlich hierzu Patz, Art. 76, MiCAR Kommentar, Rz. 6 ff.; Kaulartz Markus/Schmid Alexander, Art. 76, in: Maume Philipp (Hrsg.), MiCAR Kommentar, München 2025, Rz. 55 ff.

b) Organisationspflicht

PPAETs müssen gemäss Art. 92 Abs. 1 MiCAR in organisatorischer Hinsicht über wirksame Vorkehrungen, Systeme und Verfahren für die Vorbeugung und Aufdeckung von Marktmissbrauch verfügen. Im Vordergrund stehen dabei die organisatorischen Vorgaben zur *Handelsüberwachung*.[141] Die Erwartungen der ESMA an die zu implementierenden Systeme und Verfahren sind derweil hoch: Die Behörde geht grundsätzlich davon aus, dass Art. 16 MAR, der vergleichbare Vorgaben für traditionelle Wertpapiermärkte macht, als Ausgangspunkt zu betrachten ist.[142]

Die Anforderungen werden gemäss Delegationsnorm in Art. 92 Abs. 2 MiCAR in der Delegierten Verordnung (EU) 2025/885 der EU-Kommission konkretisiert. PPAETs haben gemäss dieser Ausführungsverordnung folgende Punkte umzusetzen:

- **Überwachung von Aufträgen und Transaktionen (Art. 2 f.)**: Aufträge und Transaktionen von Kunden sind laufend zu überwachen und zwar unabhängig davon, an welchem Ausführungsplatz (zentrale oder dezentrale Handelsplattformen oder OTC) sie ausgeführt werden.[143] Auf On-chain-Transaktionen ist dieses Erfordernis mit einer gewissen Zurückhaltung anzuwenden, da solche Transaktionen je nach Ausführungsroute nicht gleich einfach nachvollziehbar sind.[144] Die einzusetzenden Überwachungssysteme sind grundsätzlich vom Umfang, der Grösse und der Art des Geschäftsmodells der PPAET abhängig. Grundsätzlich geht die Erwartung der ESMA dahin, dass computergestützte Systeme einzusetzen sind, die im Verdachtsfall automatisch einen Alarm generieren. Wo erforderlich, sollen zudem computergestützte Analysen eingesetzt werden, die Transaktions- und Orderbuchdaten zeitnah automatisiert auslesen („*deferred automated reading*“) und auf bekannte Missbrauchsmuster (Pump-and-Dump, Wash Trades etc.) untersuchen.[145] Ausserdem soll ein Mensch in die Analyse in angemessener Weise involviert sein. Zu erwarten ist, dass Betreiber von Handelsplattformen und grössere Kryptobroker weitergehende Vorkehrungen als kleinere PPAETs zu treffen haben.[146] Die teilweise geäusserte Erwartung der ESMA, dass Marktmissbrauch

---

141 Vgl. IOSCO, Crypto and Digital Assets, 27 f.

142 ESMA, Draft Technical Standards, 7; *kritisch* Misterek, § 18, Handbuch Kryptowerte, Rz. 99 ff.

143 Maume, Art. 92, MiCAR Kommentar, Rz. 8.

144 Vgl. zur Nutzung von Private Mempools unten, D.IV.

145 Dazu v.a. Misterek, § 18, Handbuch Kryptowerte, Rz. 104.

146 Ähnlich Maume, Art. 92, MiCAR Kommentar, Rz. 11.

insb. im algorithmischen Handel in Echtzeit verhindert werden können muss, indem etwa in die (laufende) Marktausführung oder -abwicklung eingegriffen wird, geht hingegen selbst für Handelsplattformen zu weit.[147]

- **Überwachung von Aspekten der Funktionsweise einer Blockchain (Art. 2 f.)**: Sodann sind – freilich in Abweichung zur MAR – auch relevante Aspekte der Funktionsweise einer Blockchain laufend zu überwachen, was gemäss *Maume* als Einfallstor für die Berücksichtigung spezifischer Phänomene von Blockchains und DLT dienen kann.[148] Inhalt und Umfang dieser Pflicht sind besonders relevant mit Blick auf allfällige Meldungen von realisierten MEV-Opportunitäten (siehe hierzu unten, D.). Immerhin muss eine PPAET gemäss Aussage der ESMA solche Aspekte nur im Zusammenhang mit den sie tangierenden Transaktionen überwachen.[149] Dies entspricht offenbar auch der Intention der Financial Conduct Authority (FCA) in der UK, wobei die konkrete Umsetzung der Blockchain-Überwachung stärker den einzelnen Marktteilnehmern überlassen sein soll.[150]
- **Dokumentation und Audit (Art. 2)**: Die zu dokumentierenden Prozesse und Verfahren, welche die Grundlage für die Einhaltung der Organisations- und Meldepflichten bilden, sind mindestens einmal jährlich intern zu überprüfen bzw. extern überprüfen zu lassen und bei Bedarf an die veränderten Umstände anzupassen.
- **Outsourcing (Art. 3)**: Die Funktionen der Handels- und Marktüberwachung können vorbehaltlich der Einhaltung gewisser Bedingungen an einen Dritten ausgelagert werden, wobei die aufsichtsrechtliche Verantwortlichkeit für die Einhaltung von Art. 92 MiCAR bei der PPAET verbleibt.
- **Aufzeichnungen (Art. 3)**: Aufzeichnungen von Aufträgen und Transaktionen inkl. der STOR-Analyse (siehe hierzu sogleich) sind während fünf Jahren aufzubewahren und auf Anfrage an die zuständige Behörde herauszugeben.
- **Schulung (Art. 4)**: PPAETs haben schliesslich für ein regelmässiges wirksames und umfassendes Training der für die Überwachung der Marktverhaltensregeln zuständigen Personen zu sorgen.

---

147 *Kritisch* auch Maume, Art. 92, MiCAR Kommentar, Rz. 12; vgl. aber ESMA, Draft Technical Standards, 8: „*Such software should also have sufficient capacity to prevent market abuse in real-time and operate in an algorithmic trading environment.*"

148 Maume, Art. 92, MiCAR Kommentar, Rz. 2.

149 ESMA, Draft Technical Standards, 15.

150 FCA, DP24/4, Rz. 3.78.

c) *Überwachung sozialer Medien?*

Nach vorliegender Auffassung erfassen die unter Art. 92 Abs. 1 MiCAR zu ergreifenden Überwachungsmassnahmen das Verhalten von Kunden nicht, wenn es keinen Bezug zu der von der PPAET betriebenen Handelsplattform oder des von ihr unterhaltenen Auftragsbuchs aufweist.[151] Zudem fällt das Verhalten von Kunden, das nicht transaktionaler Natur ist, ohnehin nicht unter den Tatbestand. Zu denken ist etwa an blosse Äusserungen auf sozialen Medien, namentlich von Personen mit grossen Kryptopositionen (*Whales*), die auf einen potenziellen Marktmissbrauch hinweisen.

d) *Meldepflicht und* STOR

Die ESMA hat zuhanden der EU-Kommission ein standardisiertes Template für die Meldung verdächtiger Transaktionen und Aufträge gemäss Art. 92 Abs. 1 MiCAR entworfen.[152] Eine solche Meldung wird als „*Suspicious Transaction or Order Report*" (STOR) bezeichnet. Aufsichtsbehörden sind besonders bei missbräuchlichen Handelsabschlüssen, die auf einer zentralen Handelsplattform oder innerhalb des „Auftragsbuchs" eines OTC-Händlers erfolgen, auf entsprechende Meldungen der Marktteilnehmer angewiesen.[153]

PPAETs haben gemäss Art. 2 und Art. 5 ff. der einschlägigen Delegierten Verordnung der EU-Kommission Systeme und Prozesse vorzusehen, die es ihnen erlauben, einen STOR unter Verwendung des Templates *ohne Verzögerung* bei der zuständigen Behörde einzureichen. Es ist bei der Erstellung eines STOR auf ein angemessenes Mass menschlicher Analyse zu achten. Die Meldung ist gegenüber den in der Meldung erwähnten Personen, deren Verhalten als marktmissbräuchlich erscheint, vertraulich zu behandeln.

Meldepflichtig sind *Sachverhalte*, die einen Bezug zu (versuchtem) marktmissbräuchlichem Verhalten i.S. der MiCAR aufweisen. Da für eine Meldung allerdings ein begründeter Verdacht[154] in Bezug auf einen Auftrag oder ein Geschäft und andere Aspekte der Funktionsweise der Blockchain vorliegen muss, kann davon ausgegangen werden, dass primär *transaktionsbasierter* Marktmissbrauch in den sachlichen Anwendungsbereich von Art. 92 Abs. 1 MiCAR fällt.[155] Ohnehin nicht

---

151 So wohl auch ESMA, Draft Technical Standards, 15.

152 Vgl. ESMA, Draft Technical Standards, 63 ff.

153 Siehe IOSCO, Crypto and Digital Assets, 28; ferner Misterek, § 18, Handbuch Kryptowerte, Rz. 99.

154 Zur Frage des Verdachtsgrads Misterek, § 18, Handbuch Kryptowerte, Rz. 105.

155 Siehe Maume, Art. 92, MiCAR Kommentar, Rz. 10; *differenzierend* Misterek, § 18, Handbuch Kryptowerte, Rz. 102.

meldepflichtig sind rein betrügerische Aktivitäten, wie sie typischerweise bei Scams und Rug Pulls vorkommen, Cyberattacken oder Umstände, die auf Geldwäscherei oder Terrorismusfinanzierung hinweisen.[156]

Demgegenüber sieht das derzeit beabsichtigte UK-Regime eine stärkere Fokussierung auf die Rolle von Cryptoasset Trading Platforms (CATPs) und weiterer Krypto-Intermediäre vor, welche die Sachverhalte in erster Linie selbständig ohne Meldung an die FCA analysieren sollen.[157]

PPAETs unterstehen der Meldepflicht des Mitgliedstaats, in dem sie registriert sind oder ihre Haupt- bzw. Zweigniederlassung haben. In Einklang mit den Empfehlungen der IOSCO sollen Marktmissbrauchsmeldungen *grenzüberschreitend* zwischen den Aufsichtsbehörden ausgetauscht werden.[158] Die zuständigen Behörden, denen verdächtige Aufträge oder Geschäfte gemeldet werden, übermitteln diese Informationen unverzüglich den zuständigen Behörden der betreffenden Handelsplattformen (Art. 92 Abs. 1 UAbs. 2 MiCAR). Darüber hinaus regelt die Delegierten Verordnung der EU-Kommission (Art. 7 f.) *en détail* den Austausch von Meldungen bei *Cross-border*-Marktmissbrauchsfällen zwischen den unterschiedlichen Behörden. Die FCA möchte hingegen auch andere Optionen, wie etwa eine industrieeigene Plattform zwecks Austausches relevanter Informationen ohne unmittelbare Beteiligung der Aufsichtsbehörde, diskutieren.[159]

VI. Aufsicht, Sanktionen und Massnahmen

1. Einleitung

MiCAR sieht im Bereich des aufsichts- und verwaltungsrechtlichen Instrumentariums im Wesentlichen eine *Mindestharmonisierung* vor, über welche die Mitgliedstaaten hinausgehen können.[160] Die entsprechende Konkretisierung findet im nationalen Vollzugsgesetz statt.[161]

---

156 ESMA, Draft Technical Standards, 7.

157 FCA, DP24/4, Rz. 3.56 ff., 3.66 ff.

158 Siehe IOSCO, Crypto and Digital Assets, 32.

159 Ausführlich hierzu FCA, DP24/4, Rz. 3.80 ff. („*cross-plattform information sharing mechanism*").

160 Siehe Kerkemeyer Andreas/Kalbitzer Timo, Kapitel 12 Befugnisse und Sanktionsinstrumente der Aufsichtsbehörden, in: Meier Johannes (Hrsg.), Handbuch MiCAR. Europäische Regulierung der Kryptowerte, Berlin 2025, Rz. 60, 101, 104, 114; Misterek, § 18, Handbuch Kryptowerte, Rz. 108.

161 Raschner, § 11, Handbuch MiCAR, Rz. 122.

Die Vorgaben der MiCAR sind zweigeteilt in (i) gewöhnliche Aufsichtsbefugnisse und Sanktionen und Massnahmen und (ii) solche, die besonders bei Verstössen gegen das Marktmissbrauchsrecht zur Anwendung gelangen. Damit wird der regelmässig grösseren Tragweite bzw. Verwerflichkeit von Verstössen gegen Titel VI Rechnung getragen.[162]

2. Aufsicht und Zusammenarbeit

EWR-Mitgliedstaaten bezeichnen die Aufsichtsbehörden, die für die Durchsetzung der MiCAR zuständig sind (Art. 93 MiCAR). Sie statten sie mindestens mit den (weitgehenden) Aufsichts- und Untersuchungsbefugnissen aus, die in Art. 94 Abs. 1 MiCAR vorgesehen sind, wie etwa die Befugnis, Auskünfte einzuholen oder Editionen zu verlangen, die Dienstleistungserbringung auszusetzen oder gar zu untersagen, zu verlangen, dass Kryptowerte-Whitepaper oder Marketingmitteilungen angepasst werden, den Handel mit Kryptowerten auszusetzen oder Personen aus dem Leitungsorgan abzuberufen.

Art. 94 Abs. 3 MiCAR sieht sodann speziell für Marktmissbrauchstatbestände besondere (nochmals weitergehende)[163] Befugnisse der Aufsichtsbehörden vor, wie namentlich Hausdurchsuchungen, die Überweisung an die Strafverfolgungsbehörden, die Beschlagnahmung von Vermögenswerten, Berufsverbote und Berichtigungen falscher oder irreführender offengelegter Informationen.

Nationale Aufsichtsbehörden oder gar die ESMA oder die European Banking Authority (EBA) könnten ferner eine *Produktintervention* anordnen (vgl. Art. 103 ff. MiCAR), wenn sie aufgrund festgestellter systematischer Marktmanipulationen bspw. im Bereich von *Meme Coins* erhebliche Bedenken für den Anlegerschutz oder eine Gefahr für das ordnungsgemässe Funktionieren und die Integrität des Kryptomarkts haben.[164]

Art. 95 MiCAR regelt die Zusammenarbeit zwischen den Aufsichtsbehörden, der EBA und ESMA und Art. 107 MiCAR lässt Kooperationsvereinbarungen mit Drittländern zu.

3. Sanktionen und Massnahmen

Art. 111 Abs. 1 lit. e MiCAR schreibt den Mitgliedstaaten vor, Verstösse gegen die Bestimmungen in Art. 88 bis 92 MiCAR in angemessener Weise verwaltungs-

---

162 Zum Ganzen Kerkemeyer/Kalbitzer, § 12, Handbuch MiCAR, Rz. 67, 69 f., 74, 79, 86, 111.

163 Kerkemeyer/Kalbitzer, § 12, Handbuch MiCAR, Rz. 70 ff.

164 Hierzu Kerkemeyer/Kalbitzer, § 12, Handbuch MiCAR, Rz. 90 ff.

rechtlich zu *ahnden*. Dabei müssen die Mitgliedstaaten im Einklang mit dem nationalen Recht sicherstellen, dass die zuständigen Behörden zumindest die Befugnis haben, die in Art. 111 Abs. 5 MiCAR aufgeführten verwaltungsrechtlichen Sanktionen und anderen verwaltungsrechtlichen Massnahmen verhängen zu können, wie namentlich die Gewinneinziehung, (vorübergehende) Berufsverbote, Verbote von Eigengeschäften und Verwaltungsgeldbussen unterschiedlicher Höhen und bei juristischen Personen unter Berücksichtigung des konsolidierten jährlichen Umsatzes gemäss Richtlinie 2013/34/EU.

Bei der Festlegung von Art und Umfang der verwaltungsrechtlichen Sanktion und Massnahme berücksichtigen die zuständigen Behörden die in der Bestimmung aufgeführten relevanten Umstände des Einzelfalls, wie etwa die Schwere und Dauer des Verstosses oder das konkrete Verschulden (Art. 112 MiCAR).

Unbeschadet dieser Sanktionen und Massnahmen *können* Mitgliedstaaten (auch) die *strafrechtliche* Verantwortlichkeit für bestimmte Verstösse gegen die Bestimmungen des Marktmissbrauchsrechts vorsehen. Eine Pflicht hierzu besteht allerdings anders als unter MAR nicht,[165] denn eine analoge Regulierung wie die Richtlinie 2014/57/EU des Europäischen Parlaments und des Rates vom 16. April 2014 (*Marktmissbrauchsrichtlinie* bzw. *MAD II*) fehlt.[166]

4. Weitere Anordnungen

Art. 114 MiCAR sieht vor, dass nationale Behörden und Gerichte ihre Entscheidungen über verwaltungsrechtliche Sanktionen und Massnahmen auf ihrer Webseite mit oder ohne Identität der verantwortlichen Person öffentlich machen (*Naming and Shaming*), was besonders bei Finfluencers eine abschreckende Wirkung erzielen könnte.[167]

Für die Meldung von Verstössen gegen die Verordnung und den Schutz von Personen, die solche Verstösse melden, gilt gemäss Art. 116 MiCAR die Richtlinie (EU) 2019/1937 (*Whistleblowing*).[168]

---

165 Raschner, § 11, Handbuch MiCAR, Rz. 123; *kritisch* Misterek, § 18, Handbuch Kryptowerte, Rz. 113.

166 *Kritisch* wegen der besonderen Anfälligkeit des Kryptomarkts für Marktmissbrauch Maume, Art. 86, MiCAR Kommentar, Rz. 7 f.

167 Siehe hierzu Kerkemeyer/Kalbitzer, § 12, Handbuch MiCAR, Rz. 116 ff.; Misterek, § 18, Handbuch Kryptowerte, Rz. 112. Auch in der Schweiz hat die Aufsichtsbehörde mit der Veröffentlichung der aufsichtsrechtlichen Verfügung nach Art. 34 FINMAG ein ähnliches Instrument zur Hand, wenn eine schwere Verletzung aufsichtsrechtlicher Bestimmungen vorliegt.

168 Zum Zusammenspiel mit der Aufdeckung von Marktmissbrauch Misterek, § 18, Handbuch Kryptowerte, Rz. 106 f.

VII. MiCAR aus Drittstaatensicht – Bedeutung für Schweizer Marktteilnehmer

Es stellt sich aus *Schweizer* Sicht die Frage, ob die Marktmissbrauchsregeln der MiCAR auch für Personen in einem Drittland Geltung beanspruchen. Zu denken ist etwa an einen Schweizer Kryptodienstleister, dessen Mitarbeiter oder Kunden, eine Blockchain-Stiftung oder ein Proof-of-Stake (PoS)-Validator mit Domizil in der Schweiz, die jeweils marktmissbräuchlich i.S.v. MiCAR agieren.

Im Zusammenhang mit der Bestimmung des Anwendungsbereichs gemäss Art. 86 MiCAR wurde ausgeführt, dass die Handlungen und Unterlassungen von Personen in Drittstaaten unter gewissen Bedingungen durchaus erfasst sein können.[169] Wie gesehen, überschreitet die MiCAR aufgrund einer generellen extraterritorialen Ausrichtung die Grenzen des klassischen Territorialitätsprinzips.[170] Das Marktmissbrauchsregime der MiCAR basiert entsprechend auf einem weit verstandenen *Auswirkungsprinzip*, wie es auch für die MAR einschlägig ist.[171] Einschränkend ist vorauszusetzen, dass sich die betreffenden Handlungen oder Unterlassungen eines Schweizer Marktteilnehmers in relevanter Weise innerhalb eines Mitgliedstaats des EWR auswirken. In der Literatur zu MAR und MiCAR ist die Rede von einem hinreichenden Bezug („*genuine link*").[172]

Ein *Beispiel*, das mangels Auswirkungen im EWR-Kryptomarkt nach vorliegender Ansicht klar nicht von der MiCAR erfasst sein sollte, ist ein allfälliges missbräuchliches Verhalten einer Person mit Wohnsitz oder Aufenthalt in der Schweiz, das sich vollständig in der Schweiz zuträgt und sich auf einen Kryptowert bezieht, der ausschliesslich an einer Handelsplattform in den USA zugelassen wurde. Dass die Transaktionen ggf. auf deutschen Servern abgespeichert werden, ändert an der Einschätzung nichts. Ferner wäre im erwähnten Beispiel mangels negativer Auswirkungen für den EWR-Kryptomarkt der räumliche Anwendungsbereich auch dann nicht eröffnet, wenn die fragliche Handlung auf österreichischem Territorium vorgenommen würde. Ein

---

169 Siehe oben, B.III.

170 Bezeichnend der Ausdruck „Fortress Europe" in Lehmann, 20 ff.

171 Misterek, § 18, Handbuch Kryptowerte, Rz. 19; Wutscher, Art. 86, Kommentar Crypto-Assets, Rz. 9; bereits Andreotti Fabio/Taucher Joshua R., Die „Markets in Crypto-Assets"-Verordnung aus Schweizer Sicht, EIZ-Seminar Finanzmarktrecht XXI, 21. Mai 2024, 15, <https://www.flockofideas.com/wp-content/uploads/2024/05/20240521_EIZ-Tagung_MiCAR-aus-Schweizer-Sicht.pdf>; betreffend MAR Moloney Niamh, EU Securities and Financial Markets Regulation, 4. A., Oxford/New York 2023, 696; zu den unterschiedlichen Anknüpfungspunkten Tobler Simone, MiCAR – Höhenflug oder unsanfte Landung für Schweizer Krypto-Anbieter?, EuZ 04/2023, E 1 ff., E 20.

172 Siehe hierzu ausführlich oben, B.III.2.

möglicherweise *erfasstes Beispiel* ist hingegen der Plan eines Schweizer Krypto-Vereins, grössere Bestände des eigenen Tokens über einen Schweizer Krypto-Broker zu veräussern, nachdem der fragliche Verein die Handelszulassung des Kryptowerts an einer EWR-Handelsplattform beantragt bzw. über eine Drittperson beantragen lassen hat. Als Emittent bzw. Anbieter des Kryptowerts unterliegt der Verein ggf. der Pflicht nach Art. 88 MiCAR, den Tatbestand der geplanten Veräusserung vorab dem Markt offenzulegen (Ad-hoc-Publizität).

Die Geltung des auswirkungsorientierten Territorialitätsprinzips alleine sagt allerdings noch nichts über die *Durchsetzbarkeit* der anwendbaren Regeln aus. Damit wird die im Völkerrecht anerkannte Unterscheidung zwischen „*jurisdiction to prescribe*" und „*jurisdiction to enforce*" angesprochen.[173] In diesem Licht ist vermutlich auch das (beschränkte) Drittstaatenregime der MiCAR zu lesen, das etwa auf die völkerrechtlich notwendige Zusammenarbeit mit Drittländern in Art. 107 MiCAR hinweist. In diesem Zusammenhang ist anzumerken, dass die MiCAR für Drittstaaten wie die Schweiz bedauerlicherweise (zumindest derzeit)[174] keinen Mechanismus zur Anerkennung der *Gleichwertigkeit* bzw. Äquivalenz der Regulierung im Kryptobereich vorsieht.[175] Immerhin erübrigt sich damit für die Schweiz die autonome Angleichung an diejenigen MiCAR-Vorgaben, die aus verschiedenen Gründen wenig nachahmenswert sind.

Dessen ungeachtet scheint eine Sanktionierung eines Schweizer Kryptodienstleisters, der als PPAET nach MiCAR qualifizieren würde und keine angemessenen und wirksamen Systeme zur Entdeckung, Verhinderung und Meldung von Marktmissbrauch eingerichtet hat, zum Vornherein ausgeschlossen, wenn der Dienstleister seine Dienstleistungen im Einklang mit dem Drittstaatenregime in Art. 61 MiCAR (*reverse solicitation*) erbringt. Dasselbe gilt grundsätzlich für Schweizer Marktteilnehmer, die mit Kryptowerten ausschliesslich auf eigene Rechnung handeln. Die Vorgaben in Art. 92 MiCAR richten sich mit anderen Worten nur an die *nach* MiCAR zugelassenen bzw. zulassungspflich-

---

173 Siehe mit Blick auf MAR Sethe Rolf/Lehmann Matthias, § 15 Internationales Bank- und Finanzdienstleistungsrecht, in: Tietje Christian/Nowrot Karsten (Hrsg.), Internationales Wirtschaftsrecht, 3. A., Berlin/Boston 2022, Rz. 158; sodann zu MiCAR Maume, Art. 86, MiCAR Kommentar, Rz. 13; ebenfalls *zurückhaltend* Maume Philipp, § 11 Market Abuse, in: Maume Philipp/Maute Lena/Fromberger Mathias (Hrsg.), The Law of Crypto Assets, A Handbook, München/Baden-Baden/Oxford 2022, Rz. 12; für die Schweizer Sicht Remund/Meier, Teil 1, 345.

174 Vgl. Art. 140 Abs. 2 lit. v MiCAR.

175 Tobler, E 22; ausführlich hierzu Schürger Jonas/Topp Luca Anna, Kapitel 17: Grenzüberschreitende Regulierung von Kryptowerten, in: Miernicki Martin/Schinerl Fabian (Hrsg.), Handbuch Kryptowerte, Wien 2025, Rz. 191 ff.

tigen Anbieter von Kryptowerte-Dienstleistungen und die übrigen Marktteilnehmer mit Domizil im EWR, wenn sie jeweils als PPAET qualifizieren.

C. Schweizer Marktverhaltensregeln für Kryptowerte

I. Entstehung und Zielsetzung

Die Schweizer Marktverhaltensregeln finden sich im 3. Titel des FinfraG. Zu den Marktverhaltensregeln des FinfraG zählen neben den Regeln zu Derivaten, zur Offenlegung von Beteiligungen und zu öffentlichen Kaufangeboten auch die Regeln zu Insiderhandel und Marktmanipulation (5. Kapitel des 3. Titels). Nachfolgend vertieft behandelt werden die Marktmissbrauchsregeln, die nach vorliegendem Verständnis das Verbot des Ausnützens von Insiderinformationen und der Markt- bzw. Kursmanipulation umfassen und sich in aufsichtsrechtliche und strafrechtliche Bestimmungen unterteilen lassen.[176]

Während die strafrechtlichen Marktmissbrauchsregeln zeitlich bereits weiter zurückgehen,[177] fanden die verwaltungsrechtlichen Marktverhaltenstatbestände erst im Jahr 2013 Eingang ins Gesetz.[178] Vor der Einführung der aufsichtsrechtlichen Marktmissbrauchsregeln unterlag der Insiderhandel und die Marktmanipulation lediglich den aufsichtsrechtlichen Vorgaben des (alten) FINMA-Rundschreibens 08/38 „Marktverhaltensregeln“[179] und galt nur für Finanzintermediäre, die der Aufsicht der FINMA unterstellt waren.[180] In einer ähnlichen Situation finden sich aktuell von der FINMA prudenziell Beaufsichtigte mit Blick auf – gemessen am Marktanteil – die Mehrheit der Kryptowerte wieder.[181]

Die (aufsichtsrechtlichen und strafrechtlichen) Bestimmungen über den Insiderhandel und die Marktmanipulation bezwecken die Sicherstellung der Transparenz und der Gleichbehandlung sowie die Aufrechterhaltung der Funktionsfähigkeit der Effektenmärkte.[182]

---

176 Vgl. auch Hanslin, 45.

177 Die erste Schweizer *Insiderstrafnorm* fand 1988, der Straftatbestand der *Kursmanipulation* sodann 1997 Eingang ins Gesetz. Vgl. hierzu Sethe Rolf/Fahrländer Lukas, Art. 142, in: Sethe Rolf et al. (Hrsg.), Schulthess Kommentar, Finanzmarktinfrastrukturgesetz, Zürich/Genf 2017, Rz. 1 ff. m.w.H.; ferner Maurenbrecher/Hanslin, Vor Art. 142, BSK FinfraG, Rz. 11.

178 Sethe/Fahrländer, Vor Art. 142, SK FinfraG, Rz. 1 ff. m.w.H.

179 Neu FINMA-Rundschreiben 2013/8 „Marktverhaltensregeln“.

180 Sethe/Fahrländer, Vor Art. 142, SK FinfraG, Rz. 5 und 11.

181 Vgl. dazu unten, C.VI.

182 Botschaft des Bundesrates vom 3. September 2014 zum Finanzmarktinfrastrukturgesetz (FinfraG), BBl 2014, 7483 ff., 7512 f.; vgl. Art. 1 Abs. 2 FinfraG. Bei der Gleichbehandlung der Anleger handelt es sich um ein Kollektivrechtsgut, das auf den Schutz der Chancengleich-

II. Rechtsgrundlagen

Das Schweizer Recht regelt den Marktmissbrauch mit dem Verbot des Ausnützens von Insiderinformationen und dem Verbot der Marktmanipulation. Dabei werden diese Verhaltensweisen im FinfraG jeweils von aufsichtsrechtlichen und strafrechtlichen Tatbeständen adressiert: Die *aufsichtsrechtlichen* Tatbestände des Ausnützens von Insiderinformationen und der Marktmanipulation finden sich in Art. 142 und 143 FinfraG, die *strafrechtlichen* Tatbestände des Ausnützens von Insiderinformationen und der Kursmanipulation in Art. 154 und 155 FinfraG.

III. Anwendungsbereich

1. Einleitung

Aufgrund der teilweise unterschiedlichen Anwendungskriterien muss jeweils zwischen den strafrechtlichen und den aufsichtsrechtlichen Vorschriften unterschieden werden. Nachfolgend wird in einem ersten Schritt entsprechend der Anwendungsbereich geklärt, bevor die wesentlichen Marktmissbrauchsregeln inhaltlich genauer betrachtet werden.

2. Räumlicher Anwendungsbereich

Beim Kryptomarkt handelt es sich wie bereits gesehen um einen globalen Markt. Mit Blick auf die Schweizer Marktmissbrauchsregeln stellt sich entsprechend die Frage, wie weit ihr räumlicher Anwendungsbereich gefasst ist. Hierbei muss zwischen den aufsichtsrechtlichen und den strafrechtlichen Marktmissbrauchsregeln unterschieden werden:

Die *aufsichtsrechtlichen Marktmissbrauchsvorschriften* nach Art. 142 und Art. 143 FinfraG kommen dann zur Anwendung, wenn Effekten betroffen sind, die an einem Handelsplatz oder DLT-Handelssystem mit Sitz in der Schweiz zum Handel zugelassen sind. Dies ist Ausfluss des verwaltungsrechtlichen Auswirkungsprinzips.[183] Entsprechend ist es für die Anwendung der Markt-

heit der Gesamtheit der Anleger und nicht auf den Vermögensschutz des einzelnen Marktteilnehmers abzielt. Siehe Sethe/Fahrländer, Art. 142, SK FinfraG, Rz. 5; Leuenberger/Rüttimann, Art. 143, SK FinfraG, Rz. 6; Sethe/Fahrländer, Art. 154, SK FinfraG, Rz. 2.

183 Hoch/Hotz, Art. 142, BSK FinfraG, Rz. 15; Sethe/Fahrländer, Vor Art. 142, SK FinfraG, Rz. 99; siehe auch Remund/Meier, Teil 1, 345.

missbrauchsvorschriften nicht von Bedeutung, ob die in Frage stehende Handlung im In- oder Ausland erfolgt.[184]

Die *strafrechtlichen Marktmissbrauchsvorschriften* nach Art. 154 und Art. 155 FinfraG kommen dem Territorialitätsprinzip[185] folgend demgegenüber dann zur Anwendung, wenn das Delikt in der Schweiz begangen wurde.[186] Die Schweiz gilt dann als Begehungsort, wenn die marktmissbräuchliche Handlung in der Schweiz ausgeführt wird (Handlungsort) oder der Erfolg in der Schweiz eintritt (Erfolgsort).[187] Mit anderen Worten muss entweder die marktmissbräuchliche Handlung in der Schweiz erfolgen oder – beim Insiderhandel – der durch das Insiderdelikt erzielte Vermögensvorteil in der Schweiz anfallen.[188] Die strafrechtliche Kursmanipulation stellt demgegenüber ein reines Tätigkeitsdelikt dar.[189] Allerdings kann u.U. auch bei Tätigkeitsdelikten ein Erfolgsort als Anknüpfungspunkt zur Anwendung kommen.[190] Dies wäre bspw. denkbar, wenn die beabsichtigte Bereicherung bzw. Kursmanipulation in der Schweiz eintritt, auch wenn die Handlung im Ausland begangen wurde.[191]

3. Persönlicher Anwendungsbereich

a) Aufsichtsrecht

Die im FinfraG enthaltenen aufsichtsrechtlichen Marktmissbrauchsverbote gelten für sämtliche Marktteilnehmer, d.h. auch für nicht prudenziell beaufsichtigte Marktteilnehmer.[192] Erfasst werden sowohl natürliche als auch juristische Personen.[193] Der persönliche Anwendungsbereich der aufsichtsrechtlichen Marktmiss-

---

184 Maurenbrecher/Hanslin, Vor Art. 142, BSK FinfraG, Rz. 57; Sethe/Fahrländer, Vor Art. 142, SK FinfraG, Rz. 99.

185 Art. 333 Abs. 1 i.V.m. Art. 3 Abs. 1 StGB.

186 Sethe/Fahrländer, Vor Art. 142, SK FinfraG, Rz. 100; Remund/Meier, Teil 1, 344.

187 Art. 8 StGB.

188 Sethe/Fahrländer, Vor Art. 142, SK FinfraG, Rz.101 f. m.w.H.

189 Remund/Meier, Teil 1, 344 f.

190 Remund/Meier, Teil 1, 345 m.w.H.; Sethe/Fahrländer, Vor Art. 142, SK FinfraG, Rz. 102.

191 Diesbezüglich bestehen allerdings unterschiedliche Lehrmeinungen. Siehe Remund/Meier, Teil 1, 345 m.w.H.; Sethe/Fahrländer, Vor Art. 142, SK FinfraG, Rz. 102.

192 Botschaft des Bundesrates vom 31. August 2011 zur Änderung des Börsengesetzes (Börsendelikte und Marktmissbrauch), BBl 2011, 6873 ff., 6888; Maurenbrecher/Hanslin, Vor Art. 142, BSK FinfraG, Rz. 26; Sethe/Fahrländer, Vor Art. 142, SK FinfraG, Rz. 16. Siehe bspw. Medienmitteilung der FINMA, „FINMA rügt Jungfraubahn Holding AG wegen unzulässigen Marktverhaltens" vom 13. September 2018, <https://www.finma.ch/de/news/2018/09/20180913-mm-boersenmanipulation-jungfraubahnen/>.

193 Vgl. BBl 2011, 6904; Maurenbrecher/Hanslin, Vor Art. 142, BSK FinfraG, Rz. 41; Sethe/Fahrländer, Art. 142, SK FinfraG, Rz. 8; Vogel Alexander/Heiz Christoph/Luthiger Reto, Art. 142,

brauchsverbote geht damit weiter als jener der Strafbestimmungen (dazu sogleich). Handlungen, die der Insiderstraftatbestand bloss gewissen Kategorien von Insidern verbietet, wie etwa dem Primärinsider, sind aufsichtsrechtlich sämtlichen Personen untersagt.[194] Aufsichtsrechtlich ist es entsprechend auch nicht von Bedeutung, wie Informationen erlangt werden, sofern die Insiderinformation i.S.v. Art. 142 FinfraG ausgenützt, mitgeteilt oder für eine Empfehlung genutzt wird. Ein weiterer Unterschied zeigt sich sodann darin, dass aufsichtsrechtlich neben natürlichen Personen auch juristische Personen erfasst sind, während sich die Strafbestimmungen grundsätzlich bloss an natürliche Personen richten.[195]

b) Strafrecht

aa) Ausnützen von Insiderinformationen (Art. 154 FinfraG)

Als Täter kommt jede natürliche Person in Frage, die über Insiderinformationen verfügt.[196] Der Straftatbestand unterscheidet allerdings betreffend die Schwere der Strafe danach, wie jemand an die Insiderinformation gelangte.[197] Unterschieden wird zwischen Primär-, Sekundär- und Tertiärinsidern.

Zu den *Primärinsidern* gehören Personen, welche aufgrund ihrer Tätigkeit oder Beteiligung bestimmungsgemäss direkten Zugang zu Insiderinformationen haben.[198] Dazu zählen gemäss Art. 154 Abs. 1 FinfraG Personen, die als Organ oder Mitglied eines Leitungs- oder Aufsichtsorgans eines Emittenten oder einer den Emittenten beherrschenden oder von ihm beherrschten Gesellschaft tätig sind. Als Primärinsider gelten bspw. aber auch eine Leiterin einer M&A-Abteilung, der Leiter des Rechtsdienstes sowie Hilfspersonen und Beauftragte wie Assistenten und Rechtsberater.[199] Primärinsider haben entsprechend aufgrund ihrer Position die Möglichkeit, Insiderinformationen zu erzeugen oder zu beeinflussen bzw. im Vergleich zu anderen Marktteilneh-

---

Orell Füssli Kommentar (OFK), Bundesgesetz über die Finanzmarktinfrastrukturen und das Marktverhalten im Effekten- und Derivatehandel und Bundesgesetz über Bucheffekten, Zürich 2019, Rz. 3.

194 Sethe/Fahrländer, Art. 142, SK FinfraG, Rz. 6.

195 Eine subsidiäre strafrechtliche Verantwortlichkeit nach Art. 102 Abs. 1 StGB kann sich dann ergeben, wenn die Tat wegen mangelhafter Organisation des Unternehmens keiner bestimmten natürlichen Person zugerechnet werden kann. Siehe Sethe/Fahrländer, Art. 142, SK FinfraG, Rz. 8; ferner Maurenbrecher/Hanslin, Vor Art. 142, BSK FinfraG, Rz. 41.

196 BBl 2011, 6885.

197 BBl 2011, 6904.

198 BBl 2011, 6905; vgl. Wohlers/Pflaum, Art. 154, BSK FinfraG, Rz. 16.

199 BBl 2011, 6905.

mern einen besonderen Zugang zu den Insiderinformationen.[200] Der Primärinsider braucht dabei nicht zwingend beim Emittenten tätig zu sein, sondern kann auch anderweitig von Insiderinformationen des Emittenten erfahren.[201]

Sekundärinsider sind demgegenüber Personen, die eine Information direkt bzw. aktiv von einem Primärinsider erhalten (Art. 154 Abs. 3 FinfraG).[202] Als *Tertiärinsider* gelten sodann sämtliche übrigen Personen, die sich oder jemand anderem einen Vermögensvorteil verschaffen, indem sie eine Insiderinformation oder eine darauf beruhende Empfehlung ausnützen, um einen Vermögensvorteil zu erlangen.[203]

Nicht vom persönlichen Anwendungsbereich erfasst sind juristische Personen.[204]

bb) Kursmanipulation (Art. 155 FinfraG)

Beim strafrechtlichen Kursmanipulationsverbot handelt es sich um ein Allgemeindelikt, weshalb grundsätzlich jede natürliche Person als Täterin in Frage kommt.[205]

4. Sachlicher Anwendungsbereich

a) Einleitung

Marktmissbräuchliches Verhalten betreffend Kryptowerte wird grundsätzlich (vgl. zum erweiterten Anwendungsbereich für prudenziell Beaufsichtigte unten, C.VI.) nur dann von den Marktmissbrauchsvorschriften im FinfraG erfasst, wenn es sich beim Tatobjekt um *Effekten* handelt, die an einem Handelsplatz oder DLT-Handelssystem zum Handel zugelassen sind, sowie daraus abgeleitete Derivate. Die Regulierung des Effektenhandels soll dazu beitragen, dass

---

200 Sethe/Fahrländer, Art. 154, SK FinfraG, Rz. 5.

201 So bspw., wenn ein Mitarbeiter des Unternehmens A Kenntnis vom Abschluss eines Vertrages mit Unternehmen B hat und sich dieser Vertragsabschluss voraussichtlich erheblich auf den Börsenkurs von Unternehmen B auswirken wird. Siehe BBl 2011, 6905.

202 BBl 2011, 6905. Zu den Sekundärinsidern gelten auch Personen, die sich durch ein Verbrechen oder Vergehen Insiderinformationen verschafft haben (vgl. Art. 154 Abs. 3 FinfraG). Ausführlich dazu Sethe/Fahrländer, Art. 154, SK FinfraG, Rz. 63 ff.

203 Art. 154 Abs. 4 FinfraG. Sethe/Fahrländer, Art. 154, SK FinfraG, Rz. 76. Der Tertiärinsider soll im Rahmen der laufenden FinfraG-Revision allerdings abgeschafft werden; vgl. Eidgenössisches Finanzdepartement (EFD), Änderung des Finanzmarktinfrastrukturgesetzes. Erläuternder Bericht zur Eröffnung des Vernehmlassungsverfahrens, 19. Juni 2024, 21 f.

204 BBl 2011, 6905.

205 Leuenberger/Rüttimann, Art. 155, SK FinfraG, Rz. 11; Wohlers/Pflaum, Art. 155, BSK FinfraG, Rz. 12.

Marktteilnehmer ihre Entscheide für Anlagen auf Grundlage verlässlicher Mindestinformationen treffen können und der Handel fair, zuverlässig und mit effizienter Preisbildung abläuft.[206]

b) Effekten

Als *Effekten* gelten gemäss Art. 2 lit. b FinfraG vereinheitlichte und zum massenweisen Handel geeignete Wertpapiere, Wertrechte, insb. einfache Wertrechte nach Art. 973c OR und Registerwertrechte nach Art. 973d OR, sowie Derivate und Bucheffekten.

Kryptowerte fallen nur unter gewissen Voraussetzungen unter den Effektenbegriff. Um als Effekte zu qualifizieren müssen Kryptowerte

- als Wertpapier[207], Wertrechte[208], insb. einfache Wertrechte[209] oder Registerwertrechte[210], sowie Derivate[211] oder Bucheffekten[212] ausgestaltet sein;
- vereinheitlicht und zum massenweisen Handel geeignet sein; und
- über einen Bezug zum Kapitalmarkt[213] verfügen.[214]

---

206 FINMA, Wegleitung für Unterstellungsanfragen betreffend Initial Coin Offerings (ICOs), Ausgabe vom 16. Februar 2018, 3 (zit. FINMA, ICO Wegleitung).

207 Ein *Wertpapier* ist jede Urkunde, mit der ein Recht derart verknüpft ist, dass es ohne die Urkunde weder geltend gemacht noch auf andere übertragen werden kann (Art. 965 OR). Gemäss h.L. bedarf ein Wertpapier eines physischen Trägers, weshalb Kryptowerte grundsätzlich keine Wertpapiere sein können. Siehe hierzu Mauchle Yves, Tokens als Effekten, GesKR 2022, 183 ff. m.w.H.

208 Der Begriff des *Wertrechts* nach FinfraG ist dabei gemäss Botschaft nicht zwingend deckungsgleich mit jenem des Wertrechts i.S.v. Art. 973c OR und kann auch weitere Arten von Wertrechten erfassen, die nicht unter Art. 973c OR fallen (vgl. auch die Verwendung von „*insbesondere*" im Gesetzeswortlaut von Art. 2 lit. b FinfraG). Siehe BBl 2020, 262; Urteil des Bundesverwaltungsgerichts B-4185/2020 vom 16. Januar 2024, E. 4.2.1. Diese Ansicht ist allerdings in der Lehre umstritten (hierzu E. 4.2.1 m.w.H.). Vgl. zum Begriff des Wertrechts FINMA, ICO Wegleitung, 4; Mauchle, 185 f.

209 Vgl. Art. 973c OR.

210 Vgl. Art. 973d ff. OR.

211 Als *Derivate* oder *Derivatgeschäfte* gelten gemäss Art. 2 lit. c FinfraG Finanzkontrakte, deren Wert von einem oder mehreren Basiswerten abhängt und die kein Kassageschäft darstellen. Vgl. Mauchle, 186.

212 *Bucheffekten* sind vertretbare Forderungs- oder Mitgliedschaftsrechte gegenüber dem Emittenten, die einem Effektenkonto gutgeschrieben sind und über welche die Kontoinhaber nach den Vorschriften des Bucheffektengesetzes (BEG) verfügen können (Art. 3 Abs. 1 BEG). Kryptowerte können als Bucheffekten geführt werden. Vgl. Mauchle, 186 f.

213 Bei Derivaten wird bereits der Bezug zum *Finanzmarkt* als genügend erachtet.

214 Siehe Remund Cédric/Wyss Dominic, Insider Trading im digitalen Zeitalter: Neue Herausforderungen und Risiken, SZW 2023, 24 ff., 33.

Effekten gelten gemäss Art. 2 Abs. 1 FinfraV als *vereinheitlicht und zum massenweisen Handel* geeignet, wenn sie in gleicher Struktur und Stückelung öffentlich angeboten oder bei mehr als 20 Kundinnen und Kunden platziert werden, sofern sie nicht für einzelne Gegenparteien besonders geschaffen werden. Verwenden Token bspw. den ERC-20-Standard ist die Vereinheitlichung und Eignung zum massenweisen Handel üblicherweise gegeben.[215]

Ist eine Übertragung des Kryptowertes – technisch oder rechtlich – nicht möglich, liegt keine Eignung zum massenweisen Handel vor.[216] Eine bloss eingeschränkte Übertragbarkeit stellt dabei nicht zwingend ein Hindernis für die Eignung zum massenweisen Handel dar.[217]

Bei sog. *Non-Fungible Tokens* (NFTs), d.h. Kryptowerten, die nicht fungibel sind, mangelt es typischerweise an der Vereinheitlichung, da jedes NFT technisch einzigartig ist. Unter Umständen kann aber auch bei NFTs eine gewisse Vereinheitlichung vorliegen. Dies kann bspw. dann der Fall sein, wenn die NFTs zwar technisch einzigartig sind, ihnen aber wirtschaftlich eine einheitliche Funktion zukommt (z.B. wenn sie gleiche Rechte an einem Bild verkörpern).[218] Wird die Vereinheitlichung und Eignung zum massenweisen Handel im Einzelfall bejaht, ist in einem zweiten Schritt zu prüfen, ob ein Bezug zum Kapitalmarkt besteht (dazu sogleich).[219]

Zwar ergibt sich dies nicht direkt aus dem Effektenbegriff nach Art. 2 lit. b FinfraG, doch muss ein Kryptowert gestützt auf den Zweck des FinfraG für die Qualifikation als Effekte zusätzlich zur Eignung zum massenweisen Handel auch einen *Bezug zum Kapitalmarkt* aufweisen.[220] So fallen bspw. auf der Blockchain ausgegebene Gutscheine für einen Baumarkt mangels Bezugs zum Kapitalmarkt nicht unter den Effektenbegriff, auch wenn sie vereinheitlicht und an sich zum massenweisen Handel geeignet wären.[221]

---

215 Siehe FINMA, Stellungnahme betr. Unterstellungsanfrage vom 11. September 2018 i.S. WISeCoin AG, 9. Januar 2019, 3 (zit. FINMA, Stellungnahme i.S. WISeCoin AG).

216 BVGer B-4185/2020, E. 4.2.8.

217 Vgl. BVGer B-4185/2020, E. 4.2.9.

218 Siehe auch Mauchle, 187.

219 Vgl. auch Remund/Meier, Teil 1, 349 f.; Remund/Wyss, 24 ff., 35.

220 Bericht des Bundesrates über „Rechtliche Grundlagen für Distributed Ledger-Technologie und Blockchain in der Schweiz – Eine Auslegeordnung mit Fokus auf dem Finanzsektor" vom 14. Dezember 2018, 89 (zit. Bundesrat, Bericht DLT, 2018). Vgl. Bundesrat, Botschaft BEHG 1993, 1372, 1381 („*Der Anleger wird […] als Kunde des börsenmässigen Handels, d.h. als Bezüger einer Dienstleistung geschützt.*"), 1395, wo sodann darauf hingewiesen wird, dass bereits der Anleger, der Nichteffekten am Finanzmarkt erwirbt, nicht schutzbedürftig sei.

221 Siehe Bundesrat, Bericht DLT, 2018, 89.

Bei der Beurteilung, ob ein Kryptowert als Effekte qualifiziert, stellt die FINMA im Sinne einer wirtschaftlichen Betrachtungsweise auf den tatsächlichen Gehalt des Kryptowerts ab.[222] Sie folgt dabei einem *Substance-over-Form*-Ansatz, d.h., es wird auf die wirtschaftliche Funktion und den Zweck abgestellt und nicht auf formelle Kriterien.[223] So können gemäss FINMA bspw. auch nach ausländischem Recht ausgegebene Kryptowerte als Effekten qualifizieren, sofern sie mit Blick auf die nach schweizerischem Recht ausgegebenen Formen der Effekten Funktionsäquivalenz aufweisen.[224] Während die FINMA mit der ICO Wegleitung und deren Ergänzung bereits früh eine Orientierungshilfe für die Praxis schuf, ist die Qualifizierung eines Kryptowerts für die Marktteilnehmer oft mit einer gewissen Rechtsunsicherheit verbunden.[225] Diese Unsicherheit ist insb. mit Blick auf die Rechtsfolgen der Qualifizierung kritisch zu beurteilen.[226] Die FINMA unterteilt Kryptowerte grundsätzlich in drei Token-Kategorien (die sich nicht zwingend gegenseitig ausschliessen, vgl. sog. „hybride Token"):

---

222 FINMA, ICO Wegleitung, 2 ff.

223 FINMA, ICO Wegleitung, 2; FINMA, Ergänzung der Wegleitung für Unterstellungsanfragen betreffend Initial Coin Offerings (ICOs), Ausgabe vom 11. September 2019, 2; FINMA, Stellungnahme i.S. WISeCoin AG, 3; Remund/Meier, Teil 1, 347; Remund/Wyss, 24 ff., 34. Kritisch zur ökonomischen Betrachtung der Funktion eines Tokens Mauchle, 184: „*Der Ansatz […] führt zu einer ökonomischen Betrachtung der Funktion des Tokens innerhalb einer weitgehend formellen und auf zivilrechtlichen Merkmalen basierenden Legaldefinition der Effekte. Die daraus folgende typologische Kategorisierung von Token als Effekten im Sinne des Ententests oder des Prinzips ‚I know it when I see it' geben zwar der Aufsichtsbehörde einen weiten Ermessensspielraum im individuellen Fall, der bei sinnvoller Ermessensausübung zu angemessenen Resultaten führen kann. Sie scheinen aber im Lichte rechtsstaatlicher Prinzipien zweifelhaft, da sie für die rechtsunterworfenen Marktteilnehmer keine hinreichende Rechtssicherheit bezüglich ihren Pflichten schaffen.*"

224 BVGer B-4185/2020, E. 4.2. Daneben müssen sämtliche übrigen Voraussetzungen für Effekten vorliegen.

225 Zum jetzigen Zeitpunkt ist noch wenig geklärt, inwieweit Gerichte Rundschreiben, Aufsichtsmitteilungen und Wegleitungen der FINMA, wie namentlich der ICO Wegleitung, folgen werden, die in der Regel als Verwaltungsverordnungen qualifizieren und somit für die Gerichte nicht verbindlich sind. Die darin vorgenommene Auslegung der Gesetze kann durch den Richter überprüft werden, wobei die Gerichte nicht ohne triftigen Grund davon abweichen. Siehe BVGer B-4185/2020, E. 4.2.5. Zusätzliche Komplexität kann sich aus der fortlaufenden Weiterentwicklung gewisser Protokolle bzw. Projekte ergeben. Vgl. Remund/Wyss, 346 f.

226 Die Qualifikation als Effekte hat dabei nicht nur mit Blick auf die Marktverhaltensregeln Konsequenzen, sondern (u.a.) auch mit Blick auf die Anwendbarkeit der FIDLEG-Pflichten oder die Bewilligungspflicht von Finanzmarktinfrastrukturen. Vgl. hierzu auch Mauchle, 183 ff. Diese Rechtsunsicherheit könnte bspw. dadurch reduziert werden, dass die FINMA ihre Einschätzung zu (relevanten) Kryptowerten, die sie im Rahmen ihrer Aufsichtstätigkeit beurteilt (z.B. in Non-Action-Letters), publiziert.

aa) Zahlungs-Token

Der Begriff des Zahlungs-Tokens wird gleichgesetzt mit reinen „Kryptowährungen". Darunter fallen Token, die tatsächlich oder der Absicht des Organisators nach als Zahlungsmittel für den Erwerb von Waren oder Dienstleistungen akzeptiert werden oder der Geld- und Wertübertragung dienen sollen. Solche Kryptowährungen vermitteln keine Ansprüche gegenüber einem Emittenten.[227] Als Zahlungs-Token qualifiziert die FINMA insb. Bitcoin oder Ether.[228] Die FINMA behandelt Zahlungs-Token bzw. reine Kryptowährungen nicht als Effekten, da diese als Zahlungsmittel konzipiert sind und der wirtschaftlichen Funktion nach keine Analogie zu traditionellen Effekten ausweisen.[229] Diese Einstufung ist ungeachtet einer allfälligen Spekulationsabsicht der Tokenerwerber richtig.

bb) Nutzungs-Token

Als Nutzungs-Token gelten gemäss FINMA Token, die Zugang zu einer digitalen Nutzung oder Dienstleistung vermitteln sollen, welche auf oder unter Benutzung einer Blockchain-Infrastruktur erbracht wird.[230] Nutzungs-Token gelten gemäss ICO-Wegleitung dann nicht als Effekten, wenn der Token ausschliesslich einen Anspruch auf Zugang zu einer digitalen Nutzung oder Dienstleistung vermittelt und der Nutzungs-Token im Zeitpunkt der Ausgabe in diesem Sinne einsetzbar ist.[231] In diesen Fällen fehlt es an dem für Effekten notwendigen Kapitalmarktbezug, da die Realerfüllung des Anspruchs auf Zugang zur digitalen Nutzung oder Dienstleistung im Vordergrund steht.[232] Im Umkehrschluss bedeutet dies, dass gemäss FINMA Nutzungs-Token, die noch nicht im vorgesehenen Sinne einsetzbar sind, Effekten darstellen können.[233] So behandelt die FINMA Nutzungs-Token, bei denen die wirtschaftliche Funktion ganz oder teilweise in einer Anlage besteht, gleich wie Anlage-Token als Effekten.[234]

---

227 FINMA, ICO Wegleitung, 3.

228 FINMA, ICO Wegleitung, 4.

229 FINMA, ICO Wegleitung, 4.

230 FINMA, ICO Wegleitung, 3.

231 FINMA, ICO Wegleitung, 4.

232 FINMA, ICO Wegleitung, 4.

233 Hier zeigt sich, dass die Qualifizierung als Effekte sich über die Zeit ändern kann. Siehe auch Mauchle, 188.

234 FINMA, ICO Wegleitung, 4.

cc) *Anlage-Token*

Anlage-Token weisen aus Sicht des Erwerbers ein überwiegendes Anlage- oder Spekulationselement auf.[235] Als Anlage-Token gelten u.a. Token, die Vermögenswerte, wie bspw. eine schuldrechtliche Forderung gegenüber dem Emittenten oder ein Mitgliedschaftsrecht im gesellschaftsrechtlichen Sinne, repräsentieren. Wirtschaftlich betrachtet, liegen damit Parallelen zu einer Aktie, Obligation oder einem derivativen Finanzinstrument vor.[236] Ebenso als Anlage-Token gelten Token, welche physische Wertgegenstände auf der Blockchain handelbar machen.[237] Unter der Voraussetzung, dass sie die vorgenannten Voraussetzungen erfüllen, werden Anlage-Token von der FINMA als Effekten behandelt.[238] Dies gilt auch dann, wenn ein Anlage-Token ein Derivat repräsentiert, d.h. der Wert der vermittelten Forderung von einem unterliegenden Vermögenswert (Basiswert) abhängig und der Token vereinheitlicht und zum massenweisen Handel geeignet ist.[239]

Neben Effekten, die an einem Handelsplatz oder einem DLT-Handelssystem mit Sitz in der Schweiz zum Handel zugelassen sind, sind auch aus solchen Effekten abgeleitete *Derivate* von den Marktmissbrauchsregeln des FinfraGs erfasst.[240] Sofern die Derivate von an einem Handelsplatz oder DLT-Handelssystem in der Schweiz zum Handel zugelassenen Effekten abgeleitet sind, spielt es keine Rolle, ob die Derivate in der Schweiz oder im Ausland gehandelt werden.[241]

Die Qualifikation eines Kryptowertes als Effekte bzw. die Verneinung einer solchen Qualifikation ist dabei nicht zwingend in Stein gemeisselt.[242] Im sehr dynamischen Kryptobereich kommt es häufiger vor, dass sich die hinter einem Token steckenden Projekte weiterentwickeln und ein Token neue Funktionen und Eigenschaften erhält. Vor diesem Hintergrund ist es möglich, dass sich ein Kryptowert, der nicht als Effekte gilt, zu einem späteren Zeitpunkt zu einer solchen entwickelt. Auch das umgekehrte ist möglich. Dies kann bspw. der Fall sein, wenn sich die Anlagekomponente eines Kryptowerts während dessen Lebenszyklus in eine reine Nutzungskomponente wandelt.[243]

---

235 Bundesrat, Bericht DLT, 2018, 88. Bei hybriden Token kann u.U. bereits ein bloss teilweises Anlageelement genügen, um als Effekte zu qualifizieren. Siehe Remund/Meier, Teil 1, 348.

236 Vgl. Bundesrat, Bericht DLT, 2018, 88.

237 FINMA, ICO Wegleitung, 3.

238 FINMA, ICO Wegleitung, 4; vgl. auch FINMA, Stellungnahme i.S. WISeCoin AG, 3.

239 FINMA, ICO Wegleitung, 5.

240 Vgl. BBl 2011, 6903; Sethe/Fahrländer, Art. 142, SK FinfraG, Rz. 20 f. m.w.H.

241 FINMA-Rundschreiben 2013/8 „Marktverhaltensregeln", Rz. 12.

242 Vgl. Mauchle, 188.

243 FINMA, ICO Wegleitung, 4 *e contrario*. Siehe auch Mauchle, 188; Remund/Meier, Teil 1, 348 f.

c) *An einem Handelsplatz oder DLT-Handelssystem in der Schweiz zum Handel zugelassene Effekten*

Als *Handelsplatz* gelten gemäss Art. 26 lit. a FinfraG Börsen und multilaterale Handelssysteme. Als *Börse* gilt dabei, eine Einrichtung zum multilateralen Handel von Effekten, an der Effekten kotiert werden und die den gleichzeitigen Austausch von Angeboten unter mehreren Teilnehmern sowie den Vertragsabschluss nach nichtdiskretionären Regeln bezweckt (Art. 26 lit. b FinfraG). Ein *multilaterales Handelssystem* ist eine Einrichtung zum multilateralen Handel von Effekten, die den gleichzeitigen Austausch von Angeboten unter mehreren Teilnehmern sowie den Vertragsabschluss nach nichtdiskretionären Regeln bezweckt, ohne Effekten zu kotieren (Art. 26 lit. c FinfraG). Die Börse unterscheidet sich damit vom multilateralen Handelssystem dadurch, dass bei ihr auf Antrag der Emittentin Effekten kotiert[244] werden. Multilaterale Handelssysteme dagegen lassen Effekten zum Handel zu, ohne sie zu kotieren.[245]

Als *DLT-Handelssystem* gilt gemäss Art. 73a Abs. 1 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; oder (c) sie rechnet und wickelt Geschäfte mit DLT-Effekten gestützt auf einheitliche Regeln und Verfahren ab.[246]

Nicht den Marktmissbrauchsvorschriften des FinfraG unterstellt, sind Effekten, die (ausschliesslich) an einem organisierten Handelssystem gehandelt werden.[247] Als *organisiertes Handelssystem* (OHS) gilt gemäss Art. 42 FinfraG eine Einrichtung zum (a) multilateralen Handel von Effekten oder anderen Finanzinstrumenten, die den Austausch von Angeboten sowie den Vertragsabschluss nach diskretionären Regeln bezweckt, (b) multilateralen Handel von Finanzinstrumenten, die keine Effekten sind, die den Austausch von Angeboten sowie den Vertragsabschluss nach nichtdiskretionären Regeln bezweckt, oder (c) bilateralen Handel von Effekten oder anderen Finanzinstrumenten, die den Austausch von Angeboten bezweckt. Der Betrieb eines OHS bedarf allerdings

---

244 Vgl. Art. 2 lit. f FinfraG zum Begriff der Kotierung.

245 BBl 2014, 7530

246 Die FINMA hat 2025 mit der BX Digital AG das erste DLT-Handelssystem bewilligt. Vgl. Medienmitteilung der FINMA, „FINMA bewilligt erstes DLT-Handelssystem“ vom 18. März 2025, <https://www.finma.ch/news/2025/03/20250318-mm-dlt-handelssystem/>.

247 Siehe auch Hanslin, 52; Maurenbrecher/Hanslin, Vor Art. 142, BSK FinfraG, Rz. 50; Remund/Meier, Teil 1, 350.

einer Bewilligung als Bank, Wertpapierhaus, DLT-Handelssystem oder einer Bewilligung oder Anerkennung als Handelsplatz.[248] Entsprechend ist auf den Betreiber grundsätzlich das FINMA-Rundschreiben 2013/8 „Marktverhaltensregeln" anwendbar (siehe dazu unten, C.VI.).[249]

Von den Marktmissbrauchsregeln erfasst, sind bloss Effekten, die an einem Handelsplatz oder DLT-Handelssystem *mit Sitz in der Schweiz* zum Handel zugelassen sind. Aktien eines Schweizer Unternehmens, dessen Aktien ausschliesslich an einem Handelsplatz im Ausland zugelassen sind, fallen entsprechend nicht unter die Marktmissbrauchsregeln des FinfraG.[250] Mit dem Begriff der *Zulassung zum Handel* sollen auch Effekten erfasst werden, die zwar an einem Handelsplatz zum Handel zugelassen, aber nicht kotiert sind.[251] Anders als in der EU genügt somit das (blosse) Einreichen des Gesuchs um Zulassung noch nicht.[252]

Der *Primärmarkt* ist grundsätzlich nicht von den Marktmissbrauchsvorschriften des FinfraG erfasst.[253]

IV. Wesentliche Marktverhaltensregeln

1. Übersicht

Das Marktverhalten ist im 3. Titel des FinfraG geregelt. Zu den Marktverhaltensregeln zählen grundsätzlich nicht nur die vorliegend im Fokus stehenden

---

248 Vgl. Art. 43 FinfraG.

249 Siehe Sethe/Fahrländer, Art. 142, SK FinfraG, Rz. 13 f.

250 Vgl. Leuenberger/Rüttimann, Art. 155, SK FinfraG, Rz. 17; Maurenbrecher/Hanslin, Vor Art. 142, BSK FinfraG, Rz. 52. Auch hier ist u.U. das FINMA-Rundschreiben 2013/8 „Marktverhaltensregeln" anwendbar. Sodann mit Blick auf dezentrale Handelsplattformen Humbel Claude/Eckert Fabrice, Decentralized Exchanges: Grundlagen, Risiken und ausgewählte aufsichtsrechtliche Aspekte, SZW 2023, 10 ff., 21.

251 So z.B. das sog. „Sponsered Segment" der SIX Swiss Exchange. Vgl. BBl 2011, 6899. Leuenberger/Rüttimann, Art. 155, SK FinfraG, Rz. 18; Maurenbrecher/Hanslin, Vor Art. 142, BSK FinfraG, Rz. 54: „*Zeitlich ist eine Effekte zum Handel zugelassen, sobald das Zulassungsverfahren des Handelsplatzes abgeschlossen ist und sie tatsächlich von den Teilnehmern über die Handelsplatzform gehandelt werden kann.*"

252 Maurenbrecher/Hanslin, Vor Art. 142, BSK FinfraG, Rz. 54.

253 Maurenbrecher/Hanslin, Vor Art. 142, BSK FinfraG, Rz. 55; Sethe/Fahrländer, Art. 154, SK FinfraG, Rz. 96. Dies ist in der Literatur zwar teilweise umstritten, scheint aber gemäss FINMA-Rundschreiben 2013/8 „Marktverhaltensregeln" (Rz.42) *e contrario* auch dem Verständnis der FINMA zu entsprechen. Denkbar sind allerdings indirekte Sachverhalte, namentlich, wenn Verhaltensweisen auf dem Primärmarkt dazu dienen, die Preisbildung im Sekundärmarkt zu beeinflussen. Siehe Leuenberger/Rüttimann, Art. 155, SK FinfraG, Rz. 19 m.w.H.

Bestimmungen über den Insiderhandel und die Markt- bzw. Kursmanipulation, sondern u.a. auch die Bestimmungen über die Offenlegung von Beteiligungen sowie die Bestimmungen über die öffentlichen Kaufangebote. Die nachfolgenden Ausführungen beschränken sich auf den Insiderhandel und die Markt- bzw. Kursmanipulation.

2. Insiderhandel

a) Begriff der Insiderinformation

Als Insiderinformation gilt gemäss Art. 2 lit. j FinfraG eine vertrauliche Information[254], deren Bekanntwerden geeignet ist, den Kurs von Effekten, die an einem Handelsplatz oder einem DLT-Handelssystem mit Sitz in der Schweiz zum Handel zugelassen sind, erheblich zu beeinflussen.

Während Informationen bei Kryptowerten mit geringer Marktkapitalisierung tendenziell schneller zu Kursbewegungen führen können, bedarf es bei einem Kryptowert wie Bitcoin in der Regel einer bedeutenderen Information, um den Kurs zu beeinflussen. Kurserheblich könnte bspw. das Wissen über die Richtung eines grösseren Regulierungs- bzw. Deregulierungsprojekts sein.

b) Ausnützen von Insiderinformationen

Vom Verbot des Insiderhandels erfasst wird, wer Insiderinformationen dazu ausnützt, Effekten, die an einem Handelsplatz oder DLT-Handelssystem mit Sitz in der Schweiz zum Handel zugelassen sind, zu erwerben, zu veräussern oder daraus abgeleitete Derivate einzusetzen (lit. a; *Handelsverbot*); wer Insiderinformationen einem anderen mitteilt (lit. b; *Mitteilungsverbot*); und wer Insiderinformationen dazu ausnützt, einem anderen eine Empfehlung zum Erwerb oder zur Veräusserung von Effekten, die an einem Handelsplatz oder DLT-Handelssystem mit Sitz in der Schweiz zum Handel zugelassen sind, oder zum Erwerb von daraus abgeleiteten Derivaten abzugeben (lit. c; *Empfehlungsverbot*).

aa) Handelsverbot

Gemäss Gesetzestext muss die Insiderinformation dazu ausgenützt werden, um Effekten zu erwerben, zu veräussern oder daraus abgeleitete Derivate einzusetzen. Mit anderen Worten setzt der Gesetzeswortlaut eine Transaktion

---

254 Insb. mit Blick auf die Frage der Vertraulichkeit einer Information stellen sich im heutigen digital global vernetzten System gewisse Fragen. Vgl. hierzu Remund/Wyss, 24 ff., 36 ff.

voraus.[255] Entsprechend wären das Unterlassen eines Geschäfts oder das Stornieren eines bereits aufgegebenen Geschäfts nicht vom Insiderhandelsverbot erfasst. Gemäss FINMA gilt (aufsichtsrechtlich) allerdings auch das Ändern oder Stornieren eines Auftrags bezüglich einer Effekte oder daraus abgeleiteter Derivate, auf die sich die Insiderinformation bezieht als Ausnützen einer Insiderinformation, sofern die ursprüngliche Auftragserteilung vor Erlangen der Insiderinformation erfolgte.[256] *Sethe/Fahrländer* ist nicht nur darin zuzustimmen, dass dies an sich im Ergebnis zu begrüssen ist,[257] sondern auch darin, dass diese Auslegung der FINMA wohl gegen das Gesetzesmässigkeitsprinzip verstösst.[258] Dies muss umso mehr für den *strafrechtlichen* Insiderhandelstatbestand gelten.[259]

Bei der Frage, ob auch das Nichteinschreiten gegen Effektentransaktionen anderer (so bspw., wenn ein Verwaltungsrat von einem Insidergeschäft eines Mitarbeitenden weiss) vom Insiderhandelsverbot erfasst ist, muss zwischen dem aufsichtsrechtlichen und dem strafrechtlichen Tatbestand unterschieden werden: Während diese Konstellation wohl nicht unter den aufsichtsrechtlichen Tatbestand nach Art. 142 FinfraG fällt, erscheint eine Strafbarkeit nach Art. 154 FinfraG dann möglich, wenn eine Garantenstellung und Tatmacht bejaht wird.[260] Aufsichtsrechtlich kann das Nichteinschreiten allerdings ein Verstoss gegen das Gewährserfordernis darstellen, wobei als Gewährsträger sowohl natürliche Personen, wie Mitglieder des Verwaltungsrates, als auch das Unternehmen selbst in Frage kommen (vgl. dazu unten, C.VI.).[261]

Aufgrund des umfassenden Wortlauts des Handelsverbots wären grundsätzlich auch Transaktionen, die wirtschaftlich gerechtfertigt sind, erfasst.[262] Aus diesem Grund zählen die Art. 122 ff. FinfraV Verhaltensweisen auf, die zulässig sind, auch wenn sie an sich unter den Anwendungsbereich des Handelsverbots fallen.[263]

---

255 Siehe auch Sethe/Fahrländer, Art. 142, SK FinfraG, Rz. 25.

256 FINMA-Rundschreiben 2013/8 „Marktverhaltensregeln", Rz. 14.

257 Im Rahmen der laufenden FinfraG-Revision soll Art. 142 FinfraG entsprechend ergänzt werden und neu explizit auch das Abändern oder Widerrufen eines Auftrags erfassen. Siehe EFD, 48.

258 Sethe/Fahrländer, Art. 142, SK FinfraG, Rz. 26. Vgl. auch Hoch/Hotz, Art. 142, BSK FinfraG, Rz. 24.

259 Sethe/Fahrländer, Art. 154, SK FinfraG, Rz. 108.

260 Sethe/Fahrländer, Art. 142, SK FinfraG, Rz. 27; Sethe/Fahrländer, Art. 154, SK FinfraG, Rz. 110 m.w.H.

261 Sethe/Fahrländer, Art. 142, SK FinfraG, Rz. 27.

262 Vgl. BBl 2011, 6888 und 6902 f.

263 Vgl. zu den sog. „Safe Harbors" Sethe/Fahrländer, Vor Art. 142, SK FinfraG, Rz. 18 ff.

bb) Mitteilungsverbot

Mit dem Mitteilungsverbot nach Art. 142 Abs. 1 lit. b und Art. 154 Abs. 1 lit. b FinfraG soll der Kreis der Personen, die über die Insiderinformation Bescheid wissen, klein gehalten werden.[264] Im Unterschied zum strafrechtlichen Insidertatbestand erfasst das aufsichtsrechtliche Mitteilungsverbot nicht nur Primärinsider, sondern sämtliche Marktteilnehmer, die über Insiderinformationen verfügen.[265] Die Art der Mitteilung ist dabei irrelevant und kann mündlich, schriftlich oder in anderer Form erfolgen.[266] Des Weiteren ist nicht notwendig, dass der Mitteilungsempfänger die Insiderinformation verwendet.[267]

Gleich wie beim Handelsverbot enthält Art. 128 FinfraV eine Aufzählung an Mitteilungen, die zulässig sind, auch wenn sie grds. vom Wortlaut des Mitteilungsverbots erfasst sind.[268] Eine Mitteilung einer Insiderinformation an eine Person ist bspw. erlaubt, wenn diese Person zur Erfüllung ihrer gesetzlichen oder vertraglichen Pflichten auf die Kenntnis der Insiderinformation angewiesen ist.[269]

cc) Empfehlungsverbot

Das Empfehlungsverbot dient dazu, dass das Mitteilungsverbot nicht dadurch umgangen wird, dass zwar nicht die Insiderinformation an sich mitgeteilt wird, sondern (lediglich) der Erwerb oder die Veräusserung von Effekten oder der Einsatz von daraus abgeleiteten Derivaten empfohlen wird.[270] Während das aufsichtsrechtliche Empfehlungsverbot sämtliche Täter erfasst, betrifft das strafrechtliche Empfehlungsverbot nach Art. 154 Abs. 1 lit. c FinfraG lediglich Primärinsider.[271]

---

264 Sethe/Fahrländer, Art. 142, SK FinfraG, Rz. 50; Sethe/Fahrländer, Art. 154, SK FinfraG, Rz. 144.

265 *Kritisch* zum enger gefassten strafrechtlichen Mitteilungsverbot: Sethe/Fahrländer, Art. 142, SK FinfraG, Rz. 50; Sethe/Fahrländer, Art. 154, SK FinfraG, Rz. 144.

266 Sethe/Fahrländer, Art. 142, SK FinfraG, Rz. 51; Sethe/Fahrländer, Art. 154, SK FinfraG, Rz. 145.

267 Sethe/Fahrländer, Art. 142, SK FinfraG, Rz. 51; Sethe/Fahrländer, Art. 154, SK FinfraG, Rz. 145.

268 Vgl. BBl 2011, 6888 und 6902 f.

269 Siehe dazu Sethe/Fahrländer, Vor Art. 142, SK FinfraG, Rz. 47; Sethe/Fahrländer, Art. 154, SK FinfraG, Rz. 149 ff. m.w.H.

270 Sethe/Fahrländer, Art. 142, SK FinfraG, Rz. 55; Sethe/Fahrländer, Art. 154, SK FinfraG, Rz. 152.

271 *Kritisch* hierzu Sethe/Fahrländer, Art. 142, SK FinfraG, Rz. 55; Sethe/Fahrländer, Art. 154, SK FinfraG, Rz. 152.

3. Markt- bzw. Kursmanipulation

a) *Übersicht*

Die verbotene Markt- bzw. Kursmanipulation kann gemäss Art. 143 und Art. 155 FinfraG auf zwei unterschiedliche Arten erfolgen: (i) Verbreitung falscher oder irreführender Informationen (sog. *Informationstatbestand*) oder (ii) Tätigen (gewisser) manipulatorischer Geschäfte (sog. *Transaktionstatbestand*).[272]

b) *Tatbestandsvarianten*

aa) *Informationstatbestand*

aaa) *Aufsichtsrechtlicher Informationstatbestand*

Nach Art. 143 Abs. 1 lit. a FinfraG handelt unzulässig, wer Informationen öffentlich verbreitet, von denen er weiss oder wissen muss, dass sie falsche oder irreführende Signale für das Angebot, die Nachfrage oder den Kurs von Effekten geben,[273] die an einem Handelsplatz oder DLT-Handelssystem mit Sitz in der Schweiz zum Handel zugelassen sind.[274]

Der Informationsbegriff umfasst dabei sowohl (dem Beweis zugängliche) Tatsachenbehauptungen als auch (dem Beweis nicht zugängliche) Werturteile.[275] Unter öffentlicher Verbreitung ist insb. die Bekanntmachung über die in der Finanzbranche üblichen Informationskanäle, die Bekanntmachung in den Medien allgemein (mit anderen Worten auch via *social media*) wie auch im Inter-

---

272 Vgl. Hanslin, 46; Leuenberger/Rüttimann, Art. 155, SK FinfraG, Rz. 20 ff; Maurenbrecher/Hanslin, Art. 143, BSK FinfraG, Rz. 4 ff.; Vogel/Heiz/Luthiger, Art. 155, OFK FinfraG, Rz. 3.

273 Vgl. auch Hanslin, 52: „*Die Formulierung ist verunglückt. Sie legt nahe, dass auch die Verbreitung von richtigen und klaren Informationen verboten ist, falls aus ihnen falsche oder irreführende Signale abgeleitet werden können. Wer kursrelevante Informationen verbreitet, trüge damit nicht nur die Verantwortung dafür, dass seine Informationen korrekt sind, er müsste auch dafür einstehen, wie der Markt die Informationen interpretiert. Eine solche scharfe ‚Kausalhaftung' würde die Verbreitung von Börseninformationen hemmen und die Informationseffizienz des Marktes schwächen. Das wäre nicht wünschenswert. Nur die Verbreitung von falschen oder irreführenden Informationen kann tatbestandsmässig sein – unabhängig davon, welche Signale davon abgeleitet werden.*"

274 Im Rahmen der FinfraG-Revision soll explizit klargestellt werden, dass der aufsichtsrechtliche Tatbestand der informationsgestützten Marktmanipulation auch durch eine Unterlassung, also das Zurückbehalten von Informationen, begangen werden kann. Vgl. EFD, 48.

275 Hanslin, 53; Leuenberger/Rüttimann, Art. 143, SK FinfraG, Rz. 27; Maurenbrecher/Hanslin, Art. 143, BSK FinfraG, Rz. 25; Vogel/Heiz/Luthiger, Art. 143, OFK FinfraG, Rz. 4.

net zu verstehen.[276] Ein falsches oder irreführendes Signal ist dabei gegeben, wenn das Signal das Marktverhalten eines verständigen und mit dem Markt vertrauten Marktteilnehmer zu beeinflussen vermag.[277]

bbb) Strafrechtlicher Informationstatbestand

Der Kursmanipulation nach Art. 155 Abs. 1 lit. a FinfraG macht sich strafbar, wer in der Absicht, den Kurs von Effekten, die an einem Handelsplatz oder DLT-Handelssystem mit Sitz in der Schweiz zum Handel zugelassen sind, erheblich zu beeinflussen, um daraus für sich oder für einen anderen einen Vermögensvorteil zu erzielen, wider besseres Wissen falsche oder irreführende Informationen verbreitet. Der Anwendungsbereich des strafrechtlichen Informationstatbestands unterscheidet sich vom aufsichtsrechtlichen Informationstatbestand: Zum einen wird verlangt, dass der Täter eine Kursbeeinflussungsabsicht[278] hat, und zum anderen, dass zusätzlich eine Bereicherungsabsicht[279] vorliegt. Darüber hinaus verlangt der strafrechtliche Informationstatbestand, dass die Verbreitung der falschen oder irreführenden Informationen wider besseres Wissens, d.h. mit direktem Vorsatz[280], erfolgt.[281]

bb) Transaktionstatbestand

aaa) Aufsichtsrechtlicher Transaktionstatbestand

Gemäss Art. 143 Abs. 1 lit. b FinfraG handelt unzulässig, wer Geschäfte oder Kauf- oder Verkaufsaufträge tätigt, von denen er weiss oder wissen muss, dass sie falsche oder irreführende Signale für das Angebot, die Nachfrage oder den

---

276 FINMA-Rundschreiben 2013/8 „Marktverhaltensregeln", Rz. 16. Siehe auch Leuenberger/Rüttimann, Art. 143, SK FinfraG, Rz. 28; Maurenbrecher/Hanslin, Art. 143, BSK FinfraG, Rz. 41.

277 FINMA-Rundschreiben 2013/8 „Marktverhaltensregeln", Rz. 17. Vgl. BBl 2011, 6903: „*Massgebend ist, ob eine durchschnittliche Marktteilnehmerin oder ein durchschnittlicher Marktteilnehmer erkennen kann, ob eine bestimmte Information falsch oder irreführend ist.*"

278 In der Literatur ist es umstritten, ob auch ein diesbezüglicher Eventualvorsatz genügt. Siehe hierzu Leuenberger/Rüttimann, Art. 155, SK FinfraG, Rz. 37 m.w.H.

279 Siehe hierzu Leuenberger/Rüttimann, Art. 155, SK FinfraG, Rz. 43 ff.

280 Eventualvorsatz reicht diesbezüglich nicht aus. Siehe Leuenberger/Rüttimann, Art. 155, SK FinfraG, Rz. 35; Vogel/Heiz/Luthiger, Art. 155, OFK FinfraG, Rz. 11.

281 Im Unterschied zu Art. 155 Abs. 1 lit. a FinfraG ist beim aufsichtsrechtlichen Marktmanipulationstatbestand kein subjektiver Tatbestand zu erfüllen. Es ist lediglich notwendig, dass die Person weiss oder wissen muss, dass die verbreiteten Informationen falsche oder irreführende Signale für das Angebot, die Nachfrage oder den Kurs von Effekten geben. Siehe BBl 2011, 6902 f.; Leuenberger/Rüttimann, Art. 143, SK FinfraG, Rz. 43.

Kurs von Effekten geben, die an einem Handelsplatz oder DLT-Handelssystem mit Sitz in der Schweiz zum Handel zugelassen sind.

Der Transaktionstatbestand erfasst damit nicht bloss die eigentlichen Abschlüsse bzw. Transaktionen (Geschäfte[282]), sondern auch Kauf- und Verkaufsaufträge, d.h. die Eingaben in das Orderbuch.[283] So bspw., wenn Marktteilnehmer in gegenseitiger Absprache gegenläufige Kauf- und Verkaufsaufträge abgeben, um Liquidität oder Preise zu verzerren.[284] Marktmanipulation kann auch unter Verwendung algorithmischer Handelsprogramme, insb. mittels algorithmischem Hochfrequenzhandel, erfolgen.[285] Dies ist dann der Fall, wenn dadurch falsche oder irreführende Signale für das Angebot, die Nachfrage oder den Kurs für Effekten gegeben werden.[286]

Vom Transaktionstatbestand erfasst sind auch indirekte Verhaltensweisen, sofern sie sich auf in der Schweiz zum Handel zugelassene Effekten beziehen. So bspw., wenn der Preis von Rohwaren beeinflusst wird, um den Kurs daraus abgeleiteter Finanzinstrumente zu manipulieren.[287] Da es bei vielen Kryptowerten an der Qualifikation als in der Schweiz zum Handel zugelassene Effekten mangelt, erscheinen solche indirekten Verhaltensweisen im Kryptobereich unter geltendem Recht stärker im Fokus. Hängt bspw. der Preis eines in der Schweiz zum Handel zugelassenen strukturierten Produkts von einem Korb an verschiedenen Kryptowerten ab, kann die Manipulation eines Basiskryptowerts unter den Marktmanipulationstatbestand fallen.

---

282 Vgl. Hanslin, 55: „*Geschäfte meint sämtliche Verträge, die den Handel von Effekten beinhalten, insbesondere auch Leerverkäufe oder Sicherungsgeschäfte wie Treuhandschaften oder Verpfändungen und Leihgeschäfte.*"

283 Leuenberger/Rüttimann, Art. 143, SK FinfraG, Rz. 35; Maurenbrecher/Hanslin, Art. 143, BSK FinfraG, Rz. 54 ff.; siehe auch FINMA, Erläuterungsbericht zur Totalrevision des FINMA RS 08/38 – Rundschreiben 2013/xy „Marktverhaltensregeln", 12 (zit. Erläuterungsbericht FINMA RS 2013/xy): „*Orderbucheingaben müssen mit echter Kauf- oder Verkaufsabsicht erfolgen […]. Das Verursachen eines Überhangs sowie das Platzieren von Aufträgen, um den Anschein von Marktaktivität zu erwecken und Preise zu beeinflussen, sind nicht zulässig. Ein nachhaltiges Missverhältnis zwischen Abschluss- und Orderbuchvolumen in einer bestimmten Effekte weist auf Marktmanipulation hin.*"

284 FINMA-Rundschreiben 2013/8 „Marktverhaltensregeln", Rz. 24, mit weiteren Beispielen von gegen Art. 143 FinfraG verstossenden Verhaltensweisen.

285 FINMA-Rundschreiben 2013/8 „Marktverhaltensregeln", Rz. 18.

286 FINMA-Rundschreiben 2013/8 „Marktverhaltensregeln", Rz. 18.

287 Erläuterungsbericht FINMA RS 2013/xy, 12; siehe Leuenberger/Rüttimann, Art. 143, SK FinfraG, Rz. 39 ff. und 58.

bbb) Strafrechtlicher Transaktionstatbestand

Der strafrechtliche Transaktionstatbestand ist enger gefasst als der aufsichtsrechtliche Transaktionstatbestand.[288] Nach Art. 155 Abs. 1 lit. b FinfraG macht sich (bloss) strafbar, wer in der Absicht, den Kurs von Effekten, die an einem Handelsplatz oder DLT-Handelssystem mit Sitz in der Schweiz zum Handel zugelassen sind, erheblich zu beeinflussen, um daraus für sich oder für einen anderen einen Vermögensvorteil zu erzielen, Käufe und Verkäufe von solchen Effekten tätigt, die beidseitig direkt oder indirekt auf Rechnung derselben Person oder zu diesem Zweck verbundener Personen erfolgen. Erfasst werden somit bloss gewisse Transaktionen, nämlich sog. *Wash Sales* und *Matched Orders*.

Unter *Wash Sales* werden Effektengeschäfte verstanden, welche beidseitig direkt oder indirekt auf Rechnung der gleichen Person erfolgen.[289] Es findet dabei keine Vermögensverschiebung statt.[290] Als *Matched Orders* werden Effektengeschäfte verstanden, welche beidseitig direkt oder indirekt auf Rechnung zu diesem Zweck verbundener Personen erfolgen.[291] Anders als bei *Wash Sales* kommt es damit zwar zu einer Vermögensverschiebung, aber es liegt eine Absprache verbundener Personen vor.[292] Es handelt sich um Scheingeschäfte, die dazu dienen, eine gewisse Marktaktivität hervorzurufen, um den Kurs von Effekten zu beeinflussen.[293] Solche Scheingeschäfte sind im Kryptomarkt wie gesehen stark verbreitet (siehe oben, A.II.).

Andere Geschäfte, wie bspw. *echte* Transaktionen mit manipulatorischem Charakter, sind nicht vom strafrechtlichen Transaktionstatbestand erfasst.[294] Entsprechend ist der Anwendungsbereich des strafrechtlichen Transaktionstatbestands deutlich enger als der aufsichtsrechtliche. Dies zeigt sich auch auf der subjektiven Tatbestandsseite: Verlangt wird, dass der Täter eine Kursbeeinflussungs-[295] und Bereicherungsabsicht[296] hat. Im Unterschied zum straf-

---

288 Im Rahmen der FinfraG-Revision soll der strafrechtliche Tatbestand der Kursmanipulation ausgeweitet und an das aufsichtsrechtliche Verbot der Marktmanipulation angeglichen werden. Vgl. EFD, 50.

289 Leuenberger/Rüttimann, Art. 155, SK FinfraG, Rz. 31 m.w.H.

290 Leuenberger/Rüttimann, Art. 155, SK FinfraG, Rz. 31.

291 Leuenberger/Rüttimann, Art. 155, SK FinfraG, Rz. 31.

292 Leuenberger/Rüttimann, Art. 155, SK FinfraG, Rz. 31.

293 Leuenberger/Rüttimann, Art. 155, SK FinfraG, Rz. 31; Vogel/Heiz/Luthiger, Art. 155, OFK FinfraG, Rz. 10.

294 BBl 2011, 6886; Leuenberger/Rüttimann, Art. 155, SK FinfraG, Rz. 32 m.w.H. Dies soll im Rahmen der laufenden FinfraG-Revision allerdings geändert werden; vgl. EFD, 21.

295 In der Literatur ist es umstritten, ob auch ein diesbezüglicher Eventualvorsatz genügt. Siehe hierzu Leuenberger/Rüttimann, Art. 155, SK FinfraG, Rz. 37 m.w.H.

296 Siehe hierzu Leuenberger/Rüttimann, Art. 155, SK FinfraG, Rz. 43 ff.

rechtlichen Informationstatbestand ist beim Transaktionstatbestand Eventualvorsatz ausreichend.[297]

V. Ahndung

Die Verletzung der *aufsichtsrechtlichen* Marktmissbrauchsvorschriften wird von der FINMA im Aufsichtsverfahren geahndet.[298]

Während es für den persönlichen Anwendungsbereich keine Rolle spielt, ob eine Person von der FINMA beaufsichtigt ist oder nicht, hat dies einen Einfluss auf die Ahndung der Handlung: Gegenüber den *Beaufsichtigten* stehen der FINMA grundsätzlich sämtliche im FINMAG vorgesehenen aufsichtsrechtlichen Massnahmen zur Verfügung.[299] Bei *nicht beaufsichtigten Personen*, unabhängig davon, ob es sich um natürliche oder juristische Personen handelt, kann die FINMA gestützt auf Art. 145 FinfraG die folgenden Aufsichtsinstrumente einsetzen: Auskunftspflicht (Art. 29 Abs. 1 FINMAG), Anzeige der Eröffnung eines Verfahrens (Art. 30 FINMAG), Feststellungsverfügung (Art. 32 FINMAG), Veröffentlichung der aufsichtsrechtlichen Verfügung (Art. 34 FINMAG) sowie Einziehung des Gewinns (Art. 35 FINMAG).[300]

Die Verfolgung und Beurteilung der *strafrechtlichen* Marktmissbrauchsvorschriften nach Art. 154 und Art. 155 FinfraG unterstehen gemäss Art. 156 Abs. 1 FinfraG der Bundesgerichtsbarkeit. Zuständig sind somit die Strafbehörden des Bundes, d.h. die Bundesanwaltschaft und das Bundesstrafgericht.[301] Als anwendbares Verfahrensrecht gilt die Strafprozessordnung (StPO).[302]

VI. Aufsichtsrechtliche Ausdehnung der Marktverhaltensregeln

1. Gewährserfordernis und FINMA-Rundschreiben

Wie vorne aufgezeigt, sind viele Kryptowerte mangels Qualifikation als in der Schweiz zum Handel zugelassene Effekte nicht von den Marktmissbrauchsvorschriften des FinfraG erfasst.

---

297 Leuenberger/Rüttimann, Art. 155, SK FinfraG, Rz. 35.

298 Vgl. BBl 2011, 6889.

299 BBl 2011, 6889.

300 BBl 2011, 6889; Jutzi/Schären, Art. 145, SK FinfraG, Rz. 16 m.w.H.

301 Mráz, Art. 156, SK FinfraG, Rz. 5.

302 Mráz, Art. 156, SK FinfraG, Rz. 7.

Zumindest mit Blick auf prudenziell Beaufsichtigte kommt es aber (bereits unter geltendem Recht) zu einer aufsichtsrechtlichen Ausdehnung der Marktverhaltensregeln des FinfraG. Gemäss FINMA-Rundschreiben 2013/8 „Marktverhaltensregeln" (Rz. 41 ff.) gelten für prudenziell Beaufsichtigte „*[z]ur Beurteilung der Gewähr für eine einwandfreie Geschäftstätigkeit […] die Bestimmungen zum Umgang mit Insiderinformationen und zur Marktmanipulation […] nicht nur hinsichtlich von an schweizerischen Handelsplätzen zum Handel zugelassenen Effekten, sondern sinngemäss insbesondere auch bezüglich des Effektenhandels im Primärmarkt, nur an einem ausländischen Handelsplatz zum Handel zugelassener Effekten und daraus abgeleiteter Derivate sowie der Geschäftstätigkeit in anderen Märkten als dem Effektenmarkt (bspw. Rohwaren-, Devisen- und Zinsmärkte), insbesondere im Zusammenhang mit Benchmarks.*"[303]

Die besonders verantwortungsvolle Position der prudenziell beaufsichtigten Personen im Finanzmarkt rechtfertigt es nach Ansicht der FINMA, von ihnen via das Gewährserfordernis eine Organisation zu verlangen, die das rechtzeitige Erkennen und Verhindern marktmissbräuchlichen Verhaltens erleichtert und fördert.[304] Die Gewähr hat neben der generellen Einhaltung der anwendbaren Rechtsordnung insb. auch den Grundsatz von Treu und Glauben im Geschäftsverkehr zum Inhalt; dies umfasst nach Ansicht der FINMA die Einhaltung von Verhaltenspflichten, die „*berufsspezifisch und nicht notwendigerweise in materiell-gesetzlichen Bestimmungen festgelegt sind*"[305].

Dieser Ansicht ist in der Sache (insb. mit Blick auf die eigenen Aktivitäten der Beaufsichtigten) zuzustimmen, wäre es doch stossend, wenn prudenziell Beaufsichtigte sich marktmissbräuchlich verhalten könnten, bspw. durch das Ausnutzen von Insiderinformationen, bloss weil die in Frage stehenden Kryptowerte nicht als Effekten qualifizieren. Es fragt sich jedoch, ob die Ausdehnung der Bestimmungen zum Umgang mit Insiderinformationen und zur Marktmanipulation durch deren sinngemässe Anwendung auf diverse andere Sachverhalte, insb. dort, wo nicht das eigene Handeln der Beaufsichtigten im Fokus steht, sondern die ihnen auferlegten Organisationspflichten zur Verhinderung von Marktmissbrauch von Dritten, nicht gegen das Legalitätsprinzip verstösst.[306]

---

303 Der Begriff des „Benchmarks" wird im FINMA-Rundschreiben nicht definiert. Vgl. hierzu Maurenbrecher/Hanslin, Vor Art. 142, BSK FinfraG, Rz. 71 (mit Verweis auf Art. 3 Abs. 1 Ziff. 29 MAR).

304 Erläuterungsbericht FINMA RS 2013/xy, 8.

305 Erläuterungsbericht FINMA RS 2013/xy, 12.

306 Gl. M. Vogel/Heiz/Luthiger, Art. 142, OFK FinfraG, Rz. 5. Dies ist insb. vor dem bewussten Entscheid des Gesetzgebers, ausschliesslich den Effektenhandel an Schweizer Handelsplätzen und DLT-Handelssystemen den Marktmissbrauchsvorschriften zu unterstellen, beachtlich. Siehe Maurenbrecher/Hanslin, Vor Art. 142, BSK FinfraG, Rz. 64 f.

Während für die strafrechtlichen und aufsichtsrechtlichen Marktmissbrauchsregeln des FinfraG stets ein Bezug zu Effekten vorliegen muss, die in der Schweiz zum Handel zugelassen sind, gelten die Bestimmungen zum Umgang mit Insiderinformationen und zur Marktmanipulation für prudenziell Beaufsichtigten – wie soeben gesehen – via die Anforderungen an eine einwandfreie Geschäftstätigkeit (Gewähr) sinngemäss auch für weitere Sachverhalte und Märkte.[307] Als solcher Markt ist potenziell auch der *Kryptomarkt* erfasst.[308]

Dies hat zweierlei zur Folge: Einerseits dürfen sich prudenziell Beaufsichtigte selbst nicht marktmissbräuchlich verhalten. Andererseits müssen sie mit Blick auf die Verhinderung marktmissbräuchlichen Verhaltens gewisse Organisationspflichten beachten. Entsprechend konkretisiert das Rundschreiben (i) zum einen die Verbotstatbestände zum Marktverhalten gemäss FinfraG (Art. 142 und Art. 143 sowie Art. 122 bis 128 FinfraV) sowie (ii) zum anderen das Erfordernis der Gewähr für eine einwandfreie Geschäftsführung im Bereich des Marktverhaltens, indem es Vorgaben zur Organisation von Beaufsichtigen statuiert, die der Verhinderung und der Aufdeckung unzulässigen Marktverhaltens dienen sollen.[309]

Die konkreten Anforderungen an die Organisation hängen von der spezifischen Geschäftstätigkeit, Grösse und Struktur des Beaufsichtigten ab.[310] Zur Ermittlung der für sie einschlägigen Anforderungen haben Beaufsichtigte nach Bedarf, mindestens aber einmal jährlich, eine Risikoanalyse durchzuführen.[311] Gestützt auf diese Risikoanalyse sind die zur Einhaltung der Gewähr für eine einwandfreie Geschäftsführung notwendigen organisatorischen Massnahmen

---

307 Erläuterungsbericht FINMA RS 2013/xy, 12; FINMA-Rundschreiben 2013/8 „Marktverhaltensregeln", Rz. 41.

308 Siehe auch Remund/Meier, Teil 1, 351.

309 FINMA-Rundschreiben 2013/8 „Marktverhaltensregeln", Rz. 2. Während die konkretisierenden Ausführungen zu Insiderhandel und Marktmanipulation nach Art. 142 und Art. 143 FinfraG für sämtliche natürlichen und juristischen Personen gelten, die hinsichtlich an schweizerischen Handelsplätzen zum Handel zugelassener Effekten als Marktteilnehmer auftreten, sind die Ausführungen zur Gewähr für eine einwandfreie Geschäftsführung im Bereich des Marktverhaltens bloss für von der FINMA prudenziell beaufsichtigte Personen zu beachten. Siehe FINMA-Rundschreiben 2013/8 „Marktverhaltensregeln", Rz. 4 f.; vgl. insb. die Auflistung der vom Geltungsbereich des Rundschreibens erfassten prudenziell Beaufsichtigten in Rz. 4.

310 FINMA-Rundschreiben 2013/8 „Marktverhaltensregeln", Rz. 45; Erläuterungsbericht FINMA RS 2013/xy, 13.

311 Diese Risikoanalyse und die getroffenen Massnahmen sind von den geschäftsleitenden Organen der Beaufsichtigten zu genehmigen. FINMA-Rundschreiben 2013/8 „Marktverhaltensregeln", Rz. 46; Erläuterungsbericht FINMA RS 2013/xy, 13.

zu treffen. Hierzu sind gemäss Rundschreiben insb. die nachfolgenden Massnahmen zu prüfen:

a) Umgang mit marktmissbräuchlichen Geschäften

Sofern offensichtliche Anzeichen bestehen, dass Kundengeschäfte mit den Anforderungen von Art. 142 und Art. 143 FinfraG nicht zu vereinbaren sein könnten, haben Beaufsichtigte die Hintergründe abzuklären und sich gegebenenfalls der Mitwirkung am Geschäft zu enthalten.[312] Das Rundschreiben spricht dabei von „*offensichtliche[n] Anzeichen*", das marktmissbräuchliche Verhalten muss damit ins Auge springen.[313] Eine systematische Überwachung wird dabei – zu Recht – nicht verlangt.[314] Entsprechend wird auch nicht verlangt, dass Beaufsichtigte ausserhalb ihres Geschäftsbereichs den Markt auf solche Anzeichen durchkämmen.

b) Informationsbarrieren / Vertraulichkeitsbereiche

Die Beaufsichtigten haben den Umgang mit allfälligen Insiderinformationen so zu organisieren und überwachen, dass aufsichtsrechtlich unzulässiges Marktverhalten verhindert und aufgedeckt werden kann.[315] Zur Verhinderung von unzulässigem Verhalten können sich insb. die Schaffung von Vertraulichkeitsbereichen durch Ergreifen von räumlichen, personellen, funktionalen, organisatorischen und informationstechnologischen Massnahmen aufdrängen.[316]

c) Überwachung von Mitarbeitergeschäften

Da Geschäfte von Mitarbeitern, die Zugang zu Insiderinformationen haben, erhöhte Risiken mit sich bringen, sind Massnahmen zur Überwachung der

---

312 FINMA-Rundschreiben 2013/8 „Marktverhaltensregeln", Rz. 47 f. Geschäfte, die mit Art. 142 oder Art. 143 FinfraG im Widerspruch stehen und sich wesentlich auf die Risiken eines Beaufsichtigten oder des Finanzplatzes auswirken könnten, sind der FINMA zu melden (Art. 29 Abs. 2 FINMAG).

313 Es genügt dabei, dass deutliche Anzeichen eines Verstosses gegen die Marktverhaltensregeln vorliegen; der Verstoss muss nicht erwiesen sein. Siehe Erläuterungsbericht FINMA RS 2013/xy, 14.

314 FINMA-Rundschreiben 2013/8 „Marktverhaltensregeln", Rz. 47; siehe auch Erläuterungsbericht FINMA RS 2013/xy, 15. Im Rahmen der FinfraG-Revision soll mit Art. 143a FinfraG allerdings eine neue Bestimmung eingeführt werden, mit welcher Beaufsichtigte i.S.v. Art. 3 FINMAG, die gewerbsmässig Geschäfte in Finanzinstrumenten vermitteln oder ausführen, dazu verpflichtet werden, sich so zu organisieren, dass sie Insiderhandel und Marktmanipulation erkennen können. Siehe EFD, 48.

315 FINMA-Rundschreiben 2013/8 „Marktverhaltensregeln", Rz. 49.

316 FINMA-Rundschreiben 2013/8 „Marktverhaltensregeln", Rz. 51; vgl. Hoch/Hotz, Art. 142, BSK FinfraG, Rz. 62.

Mitarbeitergeschäfte zu prüfen. Solche Massnahmen müssen geeignet sein, den Missbrauch von Insiderinformationen für eigene Transaktionen der Mitarbeiter zu verhindern bzw. aufzudecken.[317]

Während dies Beaufsichtigte bereits im traditionellen Bereich vor Herausforderungen stellt, ist eine Überwachung von Mitarbeitergeschäften im Kryptobereich aufgrund der globalen Natur und einfachen technischen Zugänglichkeit dezentraler Anwendungen zusätzlich erschwert. Die Überwachung der Mitarbeitergeschäfte sollte sich am Ergebnis der Risikoanalyse orientieren und dem Grundsatz der Verhältnismässigkeit folgen.[318]

d) Führen von Watch Lists und Restricted Lists

Watch Lists enthalten Angaben über die bei einer Beaufsichtigten vorhandenen Insiderinformationen über Emittenten, Informationsträger und über den Zeitrahmen der Vertraulichkeit.[319] *Restricted Lists* geben eine Übersicht über die Verbote oder Beschränkungen von spezifischen Geschäftsaktivitäten, wie z.B. Transaktionssperren.[320] Erscheint das Führen solcher Listen aufgrund der Geschäftstätigkeit, Grösse oder Struktur der Beaufsichtigten nicht notwendig, kann die Beaufsichtigte darauf verzichten.[321]

e) Aufzeichnungspflichten

Die Aufzeichnungspflicht gilt in zweierlei Hinsicht: Einerseits sind Geschäfte zu dokumentieren, die aufgrund offensichtlicher Anzeichen nicht mit den Anforderungen von Art. 142 und Art. 143 FinfraG vereinbar sind.[322] Andererseits sind externe und interne Telefongespräche aller im Effekten- und – wenn dies gestützt auf die Risikoanalyse angezeigt ist – auch im Kryptohandel tätigen Mitarbeiter aufzuzeichnen und elektronische Korrespondenz aufzubewahren.[323]

---

317 FINMA-Rundschreiben 2013/8 „Marktverhaltensregeln", Rz. 53; siehe auch Erläuterungsbericht FINMA RS 2013/xy, 16 f.

318 So können Beaufsichtigte bspw. verschiedene Mitarbeiterkategorien bilden und ein abgestuftes Massnahmenkonzept vorsehen. Siehe Hoch/Hotz, Art. 142, BSK FinfraG, Rz. 64.

319 FINMA-Rundschreiben 2013/8 „Marktverhaltensregeln", Rz. 57; siehe auch Erläuterungsbericht FINMA RS 2013/xy, 17.

320 FINMA-Rundschreiben 2013/8 „Marktverhaltensregeln", Rz. 58.

321 Hoch/Hotz, Art. 142, BSK FinfraG, Rz. 68.

322 FINMA-Rundschreiben 2013/8 „Marktverhaltensregeln", Rz. 59; siehe auch Erläuterungsbericht FINMA RS 2013/xy, 17.

323 FINMA-Rundschreiben 2013/8 „Marktverhaltensregeln", Rz. 60 f.

f) Hochfrequenzhandel / Algorithmischer Handel

Betreiben Beaufsichtigte algorithmischen Handel, muss durch wirksame Systeme und Risikokontrollen sichergestellt werden, dass dadurch keine falschen oder irreführenden Signale für das Angebot, die Nachfrage oder den Kurs für Kryptowerte ausgelöst werden können.[324]

2. Umsetzung der Anforderungen

Beaufsichtigte können komplett oder teilweise auf die vorgängig beschriebenen Massnahmen verzichten, wenn sie im Rahmen der Risikoanalyse zum Schluss kommen, dass diese Risiken bei ihnen nicht einschlägig sind.[325] Ein solcher Verzicht ist allerdings zu begründen (*comply or explain*).[326]

Mit Blick auf andere Märkte (wie bspw. den Kryptomarkt) stellt die FINMA klar, dass eine sinngemässe Anwendung des Rundschreibens voraussetzt, dass das fragliche Handeln auch dort verpönt ist, wo es stattgefunden hat. Die entsprechenden Situationen müssen entsprechend vergleichbar sein, d.h., es müssen in diesen anderen Märkten Gegebenheiten vorliegen, welche Insiderhandel und Marktmanipulation grundsätzlich ermöglichen.[327] Anders als Insiderhandel und Marktmanipulation bezüglich von in der Schweiz gehandelten Effekten sind solche Verhaltensweisen mit Blick auf andere Märkte wie den Kryptomarkt nicht per se gewährswidrig.[328] Die Beurteilung der Gewähr hat vielmehr im Einzelfall zu erfolgen.[329] Marktmissbrauchssachverhalte im Kryptobereich sind – wie einleitend gesehen – allerdings nicht immer ohne Weiteres mit den Verhaltensweisen im traditionellen Effektenhandel vergleichbar. Die sinngemässe Anwendung des FINMA-Rundschreibens birgt deshalb für prudenziell Beaufsichtigte in der Praxis oft Auslegungsschwierigkeiten und eine gewisse Rechtsunsicherheit.[330]

---

324 FINMA-Rundschreiben 2013/8 „Marktverhaltensregeln", Rz. 62; siehe auch Erläuterungsbericht FINMA RS 2013/xy, 17.

325 Erläuterungsbericht FINMA RS 2013/xy, 13; Sethe/Fahrländer, Vor Art. 142, SK FinfraG, Rz. 53.

326 Erläuterungsbericht FINMA RS 2013/xy, 13.

327 Bericht der FINMA über die Anhörung vom 27. März bis zum 13. Mai 2013 zum totalrevidierten Rundschreiben „Marktverhaltensregeln" vom 29. August 2013, 26 (zit. FINMA, Anhörungsbericht 2013).

328 Vgl. Maurenbrecher/Hanslin, Vor Art. 142, BSK FinfraG, Rz. 62, wonach Marktmissbrauch bloss dann gewährsrelevant erscheint, wenn dieser in direktem Zusammenhang mit der Ausübung der *prudenziell beaufsichtigten* Tätigkeit erfolgt.

329 FINMA, Anhörungsbericht 2013, 26.

330 Siehe Maurenbrecher/Hanslin, Vor Art. 142, BSK FinfraG, Rz. 65.

Die Organisationsanforderungen in Bezug auf andere Märkte gehen sodann mit erhöhtem Aufwand und erhöhten Kosten für die Beaufsichtigten einher. Dies kann einen Einfluss haben auf die Wettbewerbsfähigkeit der Beaufsichtigten im Vergleich zu Anbietern von Dienstleistungen, die den umfassenden Organisationspflichten nicht unterstehen. Mit Blick auf den Grundsatz des *level playing field* wäre in diesem Bereich eine gesetzliche Angleichung unter verhältnismässiger Berücksichtigung der konkreten Geschäfts- und Reputationsrisiken wünschenswert. Im Gegenzug kann die direkte Beaufsichtigung auch Vorteile, bspw. reputationeller Natur, mit sich bringen, die den erhöhten Aufwand wirtschaftlich kompensieren.

VII. Zwischenfazit

Die aktuellen Marktverhaltensregeln des FinfraG bieten aufgrund ihres Anwendungsbereichs bloss einen beschränkten Schutz für den Kryptomarkt. Kryptowerte sind von den Marktverhaltensregeln des FinfraG nur erfasst, wenn sie (i) entweder selbst als eine in der Schweiz an einem Handelsplatz oder DLT-Handelssystem zum Handel zugelassene Effekte qualifizieren (z.B. in Form von Aktientoken) oder (ii) als Basiswert einer solchen Effekte dienen (z.B. ein Exchange Traded Product mit Bitcoin als Basiswert), wobei in diesem Fall der Kurs der Effekte das „geschützte" Objekt ist.[331] Entsprechend sind viele Kryptowerte nicht von den Marktmissbrauchsvorschriften des FinfraG erfasst. Zahlungs-Token, wie Bitcoin und Ether, fallen ebenso wenig wie reine Nutzungs-Token unter den Effektenbegriff. Als Effekte qualifizieren demgegenüber Anlage-Token und gewisse hybride Token, sofern sie eine Anlagekomponente aufweisen und die übrigen Merkmale einer Effekte erfüllen (wobei die Verkörperung einer Rechtsposition durch den Token regelmässig fraglich ist). Zusammenfassend kann festgehalten werden, dass der durch die Marktmissbrauchsvorschriften bezweckte Schutz aufgrund des engen Anküpfungspunkts der „Effekte" im Kryptomarkt bloss sehr beschränkt greift.[332]

Sodann fallen – gleich wie beim traditionellen Effektenhandel – weder der Krypto-Primärmarkt noch Effektentoken, die nur an einem OHS gehandelt werden, in den Anwendungsbereich der Marktmissbrauchsregeln.

Der enge Anwendungsbereich der Marktmissbrauchsregeln des FinfraG wird für prudenziell Beaufsichtigte durch die sinngemässe Anwendung gemäss

---

331 Ebenfalls erfasst können Kryptowerte sein, deren Basiswert eine Effekte ist (insb. in Form von tokenisierten Derivatekontrakten). Siehe auch Remund/Meier, Teil 1, 351.

332 Vgl. auch Remund/Meier, Teil 1, 351; ferner bereits Reutter Thomas U./Raun Daniel, Insider Trading and Market Manipulation in Tokens, CapLaw-2018-43, die das aufsichtsrechtliche Marktverhaltensrecht als „*preliminary measure*" für anwendbar erklären.

FINMA-Rundschreiben 2013/8 „Marktverhaltensregeln" auf den Kryptomarkt teilweise korrigiert. Zur Einhaltung der Gewähr für eine einwandfreie Geschäftsführung haben prudenziell Beaufsichtigte ihre Anforderungen an die Organisation gestützt auf eine Risikoanalyse zu ermitteln und die notwendigen Massnahmen zur Verhinderung von Marktmissbrauch auch im Kryptobereich zu ergreifen.

D. MEV als Form des Marktmissbrauchs?

I. Einleitung

Die *Maximal Extractable Value* (MEV)[333] ist eine besondere Erscheinung in öffentlichen Blockchain-Systemen, die in dieser Form in traditionellen Märkten und Infrastrukturen nicht existiert.[334] MEV ist innerhalb der Kryptogemeinschaft seit dem erstmaligen Verzeichnis ein in hohem Masse kontroverses Thema: Die Ansichten gehen je nach Betrachter von „*ethisch fragwürdig*" über „*notwendiges Übel*" bis hin zu „*für das Funktionieren des Konsensmechanismus unabdingbar*".[335]

Ausgehend von verschiedenen Publikationen internationaler Organisationen[336] haben die Diskussionen inzwischen die Rechtsliteratur erreicht: Das Thema wird besonders unter der MiCAR, aber auch im US-amerikanischen und UK-Finanzmarktrecht und kürzlich auch mit Blick auf die Schweizer Rechtsordnung eingehender untersucht.[337] Ob MEV oder gewisse Formen da-

---

333 Ursprünglich als *Miner Extractable Value* (MEV) und neuerdings auch als *Blockchain Extractable Value* (BEV) bezeichnet.

334 Bank for International Settlements (BIS)/Basel Committee on Banking Supervision (BCBS), Novel risks, mitigants and uncertainties with permissionless distributed ledger technologies, Working Paper Nr. 44, 28. August 2024, 5 f.

335 Vgl. erstmals pmcgoohan, Miners Frontrunning, 11. August 2014, <https://www.reddit.com/r/ethereum/comments/2d84yv/miners_frontrunning/>; sodann 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>; Daian Philip, MEV… wat do?, 15. April 2021, <https://pdaian.com/blog/mev-wat-do/>.

336 Siehe IOSCO, Policy Recommendations for Decentralized Finance. Final Report, Dezember 2023, 20, 34 f. (zit. IOSCO, DeFi); Auer Raphael/Frost Jon/Pastor Jose Maria Vidal, Miners as intermediaries: extractable value and market manipulation in crypto and DeFi, BIS Bulletin Nr. 58, 16. Juni 2022, *passim*; International Monetary Fund (IMF)/Financial Stability Board (FSB), IMF-FSB Synthesis Paper: Policies for Crypto-Assets, 7. September 2023, 15.

337 Vgl. EBA/ESMA, Recent developments in crypto-assets (Article 142 of MiCAR). Joint Report, 16. Januar 2025, 27 ff., 63 ff. (zit. EBA/ESMA, Crypto-Assets); The President's Working Group on Digital Asset Markets, Strengthening American Leadership in Digital Financial Technology, 30. Juli 2025, 27, <https://www.whitehouse.gov/crypto/>; Galea/Furcillo, *passim*; Barczentewicz/de Gândara Gomes, 11 f., 15, 17; Barczentewicz Mikołaj/Sarch Alex/Vasan Natasha, Block-

von marktmissbräuchlich im finanzmarktrechtliche Sinne sind und, falls ja, welche der Tatbestände des Marktmissbrauchs gegebenenfalls erfüllt sein könnten, ist umstritten.[338] Gewisse Literaturmeinungen schlagen sodann eine Weiterentwicklung des bestehenden Marktverhaltensrechts vor.[339] Andere Meinungen sehen aufgrund der Inhärenz des MEV-Phänomens in öffentlichen (permissionless) Blockchains in erster Linie ökonomische und technische Massnahmen als geeignetere Lösungsansätze an.[340] Schliesslich gibt es in der Branche auch Anstrengungen, *Fairnessprinzipien*, wie namentlich Transparenz und Netzwerkneutralität, im Umgang mit dem Thema mit dem Ziel zu definieren, die öffentliche Natur von Blockchains zu bewahren.[341] Nachfolgend wird in einem ersten Schritt dargelegt, worum es sich bei MEV genau handelt, bevor eine rechtliche Einschätzung vorgenommen wird.

---

chain Transaction Ordering as Market Manipulation, Ohio State Technology Law Journal 2023, 1 ff., 40 ff.; Banaei B. Salman, Response to Blockchain Transaction Ordering as Market Manipulation, Ohio State Technology Law Journal 2023, 89 ff., 103 ff.; Ji Yan/Grimmelmann James, Regulatory Implications of MEV Mitigations, Financial Cryptography and Data Security. FC 2024 International Workshops 2024, 335 ff., 341 ff.; Momberg Tom/Angelovska-Wilson Angela, Regulating the unseen: Limiting the potential for negative externalities from MEV realization, Blockchain & Cryptocurrency Laws and Regulations 2025, *passim*, <https://www.globallegalinsights.com/practice-areas/blockchain-cryptocurrency-laws-and-regulations/regulating-the-unseen-limiting-the-potential-for-negative-externalities-from-mev-realization/>; Raschner, § 11, Handbuch MiCAR, Rz. 62 ff.; von Essen Frederik/Hofert Eduart, Maximum Extractable Value (MEV) in Blockchains in the Light of Market Abuse Law, ZdiW 2023, 59 ff., *passim*; Misterek, § 18, Handbuch Kryptowerte, Rz. 63 m.w.H.; Maume, Art. 87, MiCAR Kommentar, Rz. 22 f., Art. 89 Rz. 6; Müller Vaïk, Les règles de conduite sur le marché à l'épreuve de la Market Extractable Value, GesKR 2025, 96 ff., 97, 101 ff.; ferner für die UK Financial Conduct Authority (FCA), Review of Maximal Extractable Value & Blockchain Oracles, Research Note, Februar 2024, 5 f., 20 f. (zit. FCA, Research Note).

338 Vgl. etwa die Diskussion in IOSCO, Crypto and Digital Assets, 57 f. ferner Auer/Frost/Pastor, 4 f.; Gramlich Vincent/Jelito Dennis/Sedlmeir Johannes, Maximal extractable value: Current understanding, categorization, and open research questions, Electronic Markets 2024, Nr. 34:49, 1 ff., 14 ff. m.w.N.; Barczentewicz Mikołaj, MEV on Ethereum: A Policy Analysis, ICLE White Paper 2023-01-23, 23. Januar 2023, 20 ff.; Momberg/Angelovska-Wilson, *passim*; mit Verweis auf die *Transparenzrisiken* aus Nutzersicht Andreotti, Dezentrale Handelsplattformen, 289 ff.; Müller, 101 ff.

339 So etwa Müller, *passim*; Ji/Grimmelmann, 347, wonach die regulatorische Verantwortlichkeit von MEV-Agenten davon abhängen soll, ob die *Absichten* des Blockchain-Nutzers, Transaktionen in bestimmter Weise zu übermitteln oder gewisse Informationen nicht zu verwerten, respektiert worden sind.

340 *Zurückhaltend* etwa Barczentewicz/Sarch/Vasan, 78 ff.; ebenso Banaei, 98 f.; ferner Momberg/Angelovska-Wilson, *passim*, die einen „*flexible, principles-based approach*" unter Beizug der Industrie und bei Beachtung von Marktprinzipien befürworten.

341 Siehe etwa Proof of Stake Alliance (POSA), MEV Principles, 24. Juni 2024, 24 ff., <https://www.proofofstakealliance.org/posa-mev-principles>.

II. Definition von MEV

In der Literatur wird unter MEV der mögliche *monetäre Gesamtwert* verstanden, den eine Person, die in relevanter Weise in die Verarbeitung von Transaktionen in einem Blockchain-Netzwerk involviert und somit in einer „privilegierten" Position ist, extrahieren kann, indem sie vor deren Aufnahme in einen Block die Reihenfolge der Transaktionen bestimmen und ändern oder Transaktionen ignorieren bzw. zensieren kann.[342] Allgemeiner formuliert: „*[…] the maximum value that can possibly be realized from a given block as a result of the most optimal and efficient contents and order of messages within that block.*"[343] Die privilegierte Position ergibt sich typischerweise aus der vorübergehenden „Monopolisierung" des Konsensmechanismus durch Zuweisung der Blockerstellung an einen bestimmten Teilnehmer (typischerweise einen Miner oder Validator).

In der Theorie richtet sich die Verarbeitung von Transaktionen in einem Block „strikt" nach der Höhe der durch die *Blockchain-Nutzer* bezahlten Transaktionsgebühren.[344] Minern und Validatoren steht es allerdings frei, andere (willkürliche) Faktoren zu berücksichtigen.[345]

Eine *zeitliche* Priorisierung, wie namentlich nach dem *First-in, First-out (FIFO)-Prinzip*,[346] das etwa im traditionellen Wertpapierhandel dem Standard entspricht, bei Marktteilnehmern zu eigentlichen Wettkämpfen um die geringste Latenz geführt hat[347] und teils rechtlich vorausgesetzt wird[348], ist in öffentlichen Blockchains hingegen nicht gleichermassen praktikabel, sehen die Netzwerkteilnehmer (Nodes) die Transaktionen der Blockchain-Nutzer doch

342 Siehe Daian et al., Flash Boys 2.0: Frontrunning in Decentralized Exchanges, Miner Extractable Value, and Consensus Instability, 2020 IEEE Symposium on Security and Privacy 2020, 910 ff., *passim*; Gramlich/Jelito/Sedlmeir, 6 m.w.H.

343 POSA, 2.

344 Siehe etwa Antonopoulos Andreas M., Mastering Bitcoin. Programming the Open Blockchain, 2. A., Sebastopol 2017, 127; Antonopoulos Andreas M./Wood Gavin, Mastering Ethereum. Building Smart Contracts and DApps, Sebastopol 2019, 316; Berentsen Aleksander/Schär Fabian, Bitcoin, Blockchain und Kryptoassets. Eine umfassende Einführung, Basel 2017, 215 f.

345 Arvind Narayanan et al., Bitcoin and Cryptocurrency Technologies. A Comprehensive Introduction, Princeton/Oxford 2016, 131, 136.

346 Auch als *First-come, First-served (FCFS)*-Mechanismus bezeichnet.

347 Zum Ganzen: Fox Merritt B./Glosten Lawrence R./Rauterberg Gabriel V., The New Stock Market: Law, Economics, and Policy, New York 2019, 95 ff.

348 Vgl. etwa Art. 20 Abs. 2 lit. b FIDLEV; ausdrücklicher noch SBVg, Verhaltensregeln für Effektenhändler bei der Durchführung des Effektenhandelsgeschäfts 2008, Art. 10; hinsichtlich der *Börsenausführung* Handelsreglement der SIX Swiss Exchange AG, 21. April 2023, Ziff. 11.1.1 f.; ausführlich zur *Preis-Zeit-Priorität* im Börsenhandel Weisung 3: Handel der SIX Swiss Exchange AG, 11. Dezember 2024, Ziff. 6; ferner für Deutschland § 69 WpHG.

zu unterschiedlichen Zeitpunkten;[349] das Netzwerk unterliegt aufgrund seines globalen verteilten Charakters keiner einheitlichen Zeitregelung.[350] Dieser Umstand ist zentral für die MEV-Diskussion.[351] Einen anderen Ansatz können demgegenüber *Layer-2-Protokolle* wählen, denen es möglich ist, insb. solange sie noch stärker zentralisiert sind, Transaktionen etwa nach Zeitpriorität zu ordnen.[352]

Im Kontext von MEV wird wiederum ausschliesslich der *monetäre* Faktor priorisiert: Dies geschieht dadurch, dass die involvierten Personen nicht nur diejenigen Transaktionen auswählen, die hohe Nutzergebühren mit sich bringen, sondern auch weitergehende finanzielle Opportunitäten im Zusammenhang mit unterschiedlichen Aktivitäten im Kryptoökosystem berücksichtigen.[353]

III. Beteiligte („MEV-Agenten")

Als MEV-*Agenten* qualifizieren alle Personen, die in relevanter Weise in die Transaktionsverarbeitung inkl. Blockerstellung in einem Blockchain-Netzwerk eingebunden sind. Im „Urzustand" eines Blockchain-Protokolls handelt es sich dabei um die Miner bzw. Validatoren.

Dazu gehören mit Blick auf die Ethereum Blockchain und *mev-boost* – ein Zusatzprotokoll, das Teilnehmer bei Bedarf ausführen können – die Funktionen von *Searcher*, *Builder*, *Relays* und *Proposer* (bzw. PoS-Validatoren). Vereinfacht gesagt, suchen *Searcher* auf verschiedenen Kanälen nach Transaktionen mit MEV-Opportunitäten und bündeln diese zu einem „Paket", *Builder* strukturieren sodann die gebündelten Transaktionen zu einem Blockvorschlag, *Relays* speichern den strukturierten Blockvorschlag[354] ab und übertragen ihn an die *Proposer*, wobei diese die Transaktionen samt MEV-Opportunitäten in den nächsten Block aufnehmen, bevor der Block durch andere Validatoren gemäss den Ethereum-Protokollregeln attestiert wird. Die unterschiedlichen Rollen können theoretisch von derselben Person ausgeübt werden. In der Praxis

---

349 Siehe Annessi Robert, Can First Come First Served-Based Transaction Ordering Prevent Front-Running?, 8. September 2022, *passim*, <https://writings.flashbots.net/fcfs-and-front-running>.

350 Siehe Antonopoulos, 163 f.; ferner Arvind Narayanan et al., 213.

351 Vgl. EBA/ESMA, Crypto-Assets, 28, 36.

352 Vgl. Alipanahloo Zeinab/Hafid Abdelhakim Senhaji/Zhang Kaiwen, Maximal Extractable Value Mitigation Approaches in Ethereum and Layer-2 Chains: A Comprehensive Survey, arXiv:2407.19572, 28. Juli 2024, 4 ff.

353 Siehe hierzu unten, D.V.

354 In der Praxis wird nur eine Summe (*Header*) aller Transaktionen im Block an den Proposer übertragen; siehe hierzu Mohan Vijay/Khezr Peyman, Blockchains, MEV and the knapsack problem: a primer, arXiv:2403.19077, 28. März 2024, 24 f.

wird jedoch besonders das Searching und das Block-Building von spezialisierten Anbietern angeboten. Nach Umsetzung des *Proposer-Builder-Separation* (PBS)-Vorschlags soll zudem die Rolle der heute „trusted" Relays künftig direkt in das Ethereum-Protokoll integriert werden.[355] In Proof-of-Work (PoW)-Protokollen geht es bei MEV hingegen primär um die Rolle der Miner bzw. von Mining-Pools.

Am Ende des „Extraktionsprozesses" steht die Aufnahme der Transaktionen und somit auch der MEV-Opportunitäten in den nächsten Block der Blockchain; beabsichtigt ist die dauerhafte Speicherung der Transaktionen und damit die Realisierung des MEV. Builder, die den *Block-Building*-Prozess übernehmen, bieten zu diesem Zweck in einem Auktionsprozess um einen Platz im nächsten Block eines Proposers.[356] Die Proposer haben mit anderen Worten einen finanziellen Anreiz, MEV zuzulassen, wobei sie je nach Präferenz Relays mit unterschiedlichen Filtereinstellungen verwenden können.[357]

Die Realisierung von MEV ist dabei nur eine der möglichen finanziellen Quellen, die eine am Konsensmechanismus beteiligte Partei erschliessen kann: In PoW- und Proof-of-Stake (PoS)-Blockchains erhalten Miner bzw. Validatoren in der Regel auch neue vom Protokoll emittierte Protokoll-Token sowie Transaktionsgebühren, die Nutzer der Blockchain für die Verarbeitung ihrer Transaktionen bezahlen (zusammen *Mining* bzw. *Staking Rewards*).[358]

IV. Wirtschaftlicher und funktionaler Hintergrund

MEV ist, wie eingangs erwähnt, ein Blockchain-spezifisches Phänomen, das im Rahmen der regulären transaktionalen Nutzung der Blockchain sowie der Interaktion mit Smart Contracts entsteht. Hierzu gehören auch Preisupdates

---

355 Vgl. Ethereum, Proposer-builder separation, 13. Februar 2024, <https://ethereum.org/en/roadmap/pbs/>; ferner Koegler Maxwell, SoK: Current State of Ethereum's Enshrined Proposer Builder Separation, arXiv:2506.18189, 22. Juni 2025, 6 ff.

356 In *mev-boost* erfolgt die Auktion indirekt über die Relays; vgl. <https://docs.flashbots.net/flashbots-auction/overview#how-does-it-work>; POSA, 9 f.; Garimidi Pranav/Bonneau Joseph, MEV explained, 15. Mai 2025, <https://a16zcrypto.com/posts/article/mev-explained/>; ausführlich zur Auktion Wu Fei et al., To Compete or Collude: Bidding Incentives in Ethereum Block Building Auctions, ICAIF '24: Proceedings of the 5th ACM International Conference on AI in Finance 2024, 813 ff., 813 f.

357 In diesem Zusammenhang interessant ist die Untersuchung in Brownworth Anders et al., Regulating Decentralized Systems: Evidence from Sanctions on Tornado Cash, SNB Working Papers 9/2024, Juli 2024, 4 f.

358 Siehe SBF, Zirkular 2023/01 Staking, Version 3.0, 28. Mai 2025, 7; Andreotti Fabio/Zimmermann Stephan/Prantl Florian, Custodial Staking. Eine Einordnung in das Schweizer Finanzmarktrecht, GesKR 2023, 333 ff., 334.

durch Orakel-Netzwerke, die direkt auf der Blockchain an DeFi-Anwendungen wie Lending-Protokolle übermittelt werden.[359] MEV-Opportunitäten müssen vor diesem Hintergrund von den MEV-Agenten regelrecht „aufgespürt" werden, bevor sie allenfalls einen materiellen Vorteil realisieren können. Dabei bilden insb. die folgenden Faktoren die Grundlage für das Auftreten von MEV:

- Das Ziel von Blockchain-Protokollen ist es, eine einheitliche verbindliche Datensicht innerhalb eines verteilten Netzwerks anonymer Teilnehmer mit teilweise gegensätzlichen Interessen und Zielen zu schaffen. Trotz dezentraler Natur ist es darum notwendig, einer bestimmten Person (Minern bzw. Validatoren) ein *zeitlich befristetes Entscheidungsmonopol* zu überlassen. Die datenverarbeitende Rolle in verteilten Blockchain-Systemen ist somit anders als bei traditionellen Finanzmarktinfrastrukturen nicht dauerhaft bei einer einzigen Person konzentriert.
- Dazu kommt, dass das vorübergehende Entscheidungsmonopol *by design* gewissen *Kapazitätsgrenzen* bezüglich Aufnahme, Verarbeitung und Speicherung von Daten unterliegt. Die Protokollregeln müssen darum die Rahmenbedingungen für den Umgang mit Transaktionen und Smart-Contract-Operationen und somit letztlich die Netzwerkeffizienz unter Berücksichtigung möglicher *Trade-offs* festlegen.[360]
- Blockchain-Protokolle verfügen normalerweise über Transaktionsregister, in denen die nutzerseitig ausgelösten, aber netzwerkseitig noch nicht in einen Block aufgenommenen Transaktionen gesammelt werden. Diese als *Public Mempools* bezeichneten Register sind grundsätzlich für alle Nutzer und Teilnehmer einer Blockchain ohne Weiteres einsehbar.[361] Public Mempools existieren programmatisch etwa in Bitcoin[362] und Ethereum[363]. Es gibt auch Blockchain-Protokolle, wie namentlich Solana, die nicht über das Konzept eines zentralen Public Mempools verfügen. Dessen ungeachtet ist es jedoch den Teilnehmern möglich, alle zu verarbeitenden SOL-Transaktionen in eigenen Mempools zu rekonstruieren.[364]

---

359 Generell zum Thema „*Oracle Extractable Value (OEV)*" als Unterfall von MEV Chainlink, Introducing Smart Value Recapture (SVR): A Chainlink-Powered MEV Recapture Solution For DeFi, 23. Dezember 2024, <https://blog.chain.link/chainlink-smart-value-recapture-svr/>.

360 Ausführlich POSA, 18 ff.; ferner Momberg/Angelovska-Wilson, *passim*.

361 EBA/ESMA, Crypto-Assets, 28.

362 Siehe etwa <https://mempool.space/>.

363 Siehe etwa <https://etherscan.io/txspending>.

364 Vgl. Helius, Solana MEV Report: Trends, Insights, and Challenges, 15. Januar 2025, <https://www.helius.dev/blog/solana-mev-report>.

– Demgegenüber existieren auch *Private Mempools*, die nur einem beschränkten Kreis von Personen zugänglich sind. Die Motivation für die Nutzung von privaten Kommunikationskanälen kann insb. in der schnelleren Ausführung und der vorübergehenden Wahrung der Vertraulichkeit von Transaktionen bestehen. In Ethereum existiert mit dem Zusatzprotokoll *mev-boost* ebenfalls ein Private Mempool, weshalb die Transaktionsdaten mit Ausnahme der beteiligten Searcher und Builder bis zur Aufnahme in einen Block grundsätzlich vertraulich bleiben.[365] Grundlage des Protokolls ist ein arbeitsteiliges Modell, bei dem neben den Validatoren die bereits erwähnten MEV-Agenten in einen strukturierten Transaktionsverarbeitungsprozess eingebunden werden: Die Searcher und Builder beziehen die Transaktionsdaten typischerweise aus öffentlichen und privaten Quellen;[366] die Relays sehen ebenfalls noch den vollen Datensatz;[367] demgegenüber erlangen die Proposer erst nach deren Aufnahme in einen Block Einsicht in die Transaktionsdaten.[368]

– Miner und Validatoren können im Rahmen des oben erwähnten Entscheidungsmonopols schliesslich *frei bestimmen*, welche Transaktionen in den nächsten Block aufzunehmen und welche zu ignorieren sind.[369] Zwar steht die Teilnahme an mev-boost grundsätzlich jeder Person offen, die bereit ist, die dazugehörige Software auszuführen und die vorgegebenen formalen Standards einzuhalten.[370] In Bezug auf die inhaltlichen Verarbeitungskriterien ist mev-boost hingegen neutral,[371] sodass Proposer nach eigenem Ermessen Relays mit unterschiedlichen Transaktions-

---

365 <https://docs.flashbots.net/flashbots-auction/overview#searchers>.

366 <https://docs.flashbots.net/flashbots-mev-boost/block-builders>.

367 <https://docs.flashbots.net/flashbots-mev-boost/relay>.

368 <https://docs.flashbots.net/flashbots-mev-boost/block-proposers>.

369 EBA/ESMA, Crypto-Assets, 28.

370 Ein spannender Rechtsfall trägt sich derzeit in den USA zu, wo das DOJ Anklage gegen zwei Brüder erhoben hat, die gemäss Anklageschrift einen *Softwarefehler* in der Relay-Funktion von mev-boost zu ihren Gunsten ausgenutzt haben sollen. Inhaltlich geht es gemäss Anklageschrift wie so oft in solchen Fällen nicht um einen Verstoss gegen Marktverhaltensregeln, sondern um Betrug und Geldwäscherei; vgl. DOJ, Two Brothers Arrested for Attacking Ethereum Blockchain and Stealing $25 M in Cryptocurrency, 15. Mai 2024, <https://www.justice.gov/archives/opa/pr/two-brothers-arrested-attacking-ethereum-blockchain-and-stealing-25m-cryptocurrency>; vgl. hierzu Momberg/Angelovska-Wilson, *passim*.

371 Wie zu erwarten (und erwünscht), ist jedoch ein primär monetär motivierter Markt der Transaktionsverarbeitung zwischen Builders und Proposers entstanden; vgl. <https://docs.flashbots.net/flashbots-mev-boost/introduction>.

filtern verwenden können.[372] Teilnehmer in Blockchain-Netzwerken sind üblicherweise aber finanziell motiviert und werden darum den möglichen Ertrag maximieren.[373] Einen anderen Ansatz zu wählen, würde bedeuten, das kryptoökonomische Fundament öffentlicher (permissionless) Blockchains zu hinterfragen.[374]

V. Formen

MEV entsteht, wie bereits angedeutet, im Rahmen der regulären transaktionalen Nutzung einer Blockchain; „extrahiert" wird der Wert jedoch durch diejenigen Personen, die über die Reihenfolge der Transaktionen in Blocks bestimmen können. Das Potenzial für MEV ist bei einfachen Transaktionen eher gering; entsprechend wenig wird das Thema für die Bitcoin Blockchain diskutiert, die bewusst auf eingeschränkte Programmierbarkeit setzt.[375] Demgegenüber entstehen MEV-Opportunitäten v.a. im Kontext von komplexen Anwendungsfällen, wie sie für Decentralized Finance (DeFi) typisch sind.[376]

Vorab sind zwei Formen von MEV zu erwähnen, die gemeinhin als eher *positiv* wahrgenommen werden:

- Dezentrale Handelsplattformen (DEX), die auf dem Automated Market Maker (AMM)-Modell basieren, sind systembedingt auf *Arbitrageure* angewiesen, deren Handelsaktivitäten die Preise auf unterschiedlichen zentralen und dezentralen Handelsplattformen angleichen.[377] MEV-Agenten können durch Beobachtung von Mempools allfällige Ungleichgewichte in AMM-Pools frühzeitig erkennen und diese bereits im selben Block wie die Transaktion des regulären AMM-Nutzers ausgleichen.
- Dezentrale Lending-Protokolle sind ebenfalls auf Marktteilnehmer angewiesen, damit die eingegangenen „Schuldpositionen" bei (drohender) Unterbesicherung möglichst schnell *liquidiert* werden. Andernfalls droht ein grösserer Verlust nicht nur dem regulären Nutzer der dezentralen An-

372 In Bezug auf die Umsetzung von OFAC-*Sanktionen* durch Relays vgl. <https://www.mev-watch.info/>.

373 EBA/ESMA, Crypto-Assets, 28.

374 So auch Momberg/Angelovska-Wilson, *passim*.

375 Siehe River, What Is MEV? Does it Apply to Bitcoin Mining?, undatiert, <https://river.com/learn/what-is-mev-does-it-apply-to-bitcoin-mining/>.

376 Siehe EBA/ESMA, Crypto-Assets, 27 f., 63 f. Eine hilfreiche Aufbereitung samt Livestream von MEV-Aktivitäten in Ethereum findet sich auf <https://eigenphi.io/>.

377 Andreotti, Dezentrale Handelsplattformen, 210 f.

wendung, der den Kredit erhalten hat, sondern im Extremfall steht das ganze Lending-Protokoll „unter Wasser".

In beiden Fällen kommt das MEV in Form eines Arbitrage- bzw. Liquidationsgewinns den MEV-Agenten zugute. Aus Sicht der Nutzer und des Gesamtmarktes verbessern diese Aktivitäten die Markteffizienz und die Funktionsweise der betreffenden DeFi-Anwendungen; mithin Ziele, die auch durch die Marktmissbrauchsvorschriften verfolgt werden. Beide Formen von MEV können darum als nützlich und aus Systemsicht sogar als notwendig angesehen werden.[378]

Als demgegenüber tendenziell *schädliches* MEV werden Frontrunning und Sandwich Attacks betrachtet:[379]

- Beim *Frontrunning* platziert ein MEV-Agent typischerweise seine eigene Transaktion z.B. durch Erhöhung der Transaktionsgebühren vor derjenigen des regulären Blockchain-Nutzers. Letzterer ist unmittelbar mit schlechteren Ausführungsbedingungen konfrontiert, wenn der Preis durch die vorgeschobene Transaktion innerhalb der von ihm angesetzten Ausführungstoleranz (*Slippage*)[380] angehoben wird.
- Eine Spielart des Frontrunnings ist *Sandwiching*, bei welchem der Transaktion des regulären Nutzers nicht nur eine Transaktion vorgeschoben, sondern im gleichen Block auch eine Transaktion nachgeschoben wird. Die nachgeschobene (Verkaufs-)Transaktion dient typischerweise der Gewinnmitnahme aufgrund des inzwischen eingetretenen Preisanstiegs.[381] Mit anderen Worten schliesst der MEV-Agent die eingegangene Position wirtschaftlich im gleichen Block wieder.

Diese Formen von MEV werden gemeinhin als eher *negativ* betrachtet: Dabei werden direkte finanzielle Nachteile für die Blockchain-Nutzer (aus Ökosys-

---

378 *Gl. M.* ESMA, Maximal Extractable Value Implications for crypto markets, ESMA TRV Risk Analysis, 1. Juli 2025, 10 (zit. ESMA, MEV); EBA/ESMA, Crypto-Assets, 33; POSA, 5 f. m.w.H.

379 Ausführlich zum Ganzen Gramlich/Jelito/Sedlmeir, 8 ff.; POSA, 5 m.w.H., worin von „*targeted trading*" gesprochen wird; ebenfalls Momberg/Angelovska-Wilson, *passim*.

380 *Slippage* ist die Differenz zwischen dem Preis, zu dem ein Auftrag für einen Kryptowert aufgegeben wird, und dem Preis, zu dem er effektiv ausgeführt wird. Da die Preise für Kryptowerte ständig schwanken, ist es bei Verwendung einer DEX notwendig, für jeden Trade eine *Slippage-Toleranz* festzulegen, die es den Nutzern ermöglicht, zum Zeitpunkt der Ausführung einen etwas höheren oder etwas niedrigeren Preis für ihren Auftrag zu akzeptieren. Zum *praktischen* Problem, dass die Slippage-Toleranz nicht einfach auf „null" gesetzt werden kann, Zhou Liyi et al., High-Frequency Trading on Decentralized On-Chain Exchanges, IEEE Symposium on Security and Privacy 2020, 428 ff., 430, 443 f.

381 Vgl. zu Unterspielarten des Frontrunnings ESMA, MEV, 6.

temsicht ein Nullsummenspiel darstellend: Was der MEV-Agent gewinnt, verliert der Nutzer.) sowie negative Externalitäten, wie v.a. die Aushöhlung der Marktintegrität oder gar der Sicherheit und Stabilität der Blockchain, unterschieden.[382]

Neben dieser (vereinfachten) Darstellung möglicher MEV-Erscheinungsformen gibt es in der umfangreichen Literatur weitere Abgrenzungsversuche, die bspw. zwischen der Ausnutzung öffentlicher und privater Informationen oder risikobehafteten und risikolosen MEV-Aktivitäten unterscheiden.[383]

VI. Herausforderungen und Lösungsvorschläge

Das Ausmass von MEV korrekt zu messen, ist mit konzeptionellen und praktischen Herausforderungen verbunden: Gewisse Aktivitäten, die Ähnlichkeiten zu Frontrunning oder Sandwiching aufweisen, können auf echte Präferenzen der Marktteilnehmer zurückzuführen sein, etwa eine Transaktion schneller ausführen zu können, oder zulässigen Market-Making-Praktiken entsprechen.[384] *Backrunning* hat sodann allgemein grosse Ähnlichkeiten mit Arbitrage, die den Preisfindungsmechanismus eines Marktes unterstützt.

Ferner ist die Datenlage in Anbetracht der Mehrschichtigkeit des Phänomens sehr komplex: MEV-Opportunitäten existieren aufgrund der Verbreitung derselben Kryptowerte auf unterschiedlichen Plattformen und Blockchain-Ebenen nicht nur *on-chain*, sondern auch *off-chain* (d.h. insb. an zentralen Handelsplattformen) und können sich in horizontaler und vertikaler Hinsicht über mehrere Blockchains bzw. deren unterschiedlichen Layers verteilen.[385]

Nach dem Gesagten ist es dennoch wahrscheinlich, dass Frontrunning und damit verwandte Aktivitäten in wohlfahrtsökonomischer Hinsicht unerwünschte Resultate produzieren. Als Reaktion auf diese Erkenntnis werden in der Literatur drei mögliche Massnahmen diskutiert, die sich teils ergänzen und teils ausschliessen:[386]

---

382 Siehe ESMA, MEV, 10 f.; EBA/ESMA, Crypto-Assets, 32 f.

383 Siehe ESMA, MEV, 6 f. m.w.N.; Barczentewicz, 10 ff.; ferner Chen Eugene et al., A Tale of Two Arbitrages, 21. Juni 2023, <https://frontier.tech/a-tale-of-two-arbitrages>.

384 EBA/ESMA, Crypto-Assets, 30.

385 Ausführlich EBA/ESMA, Crypto-Assets, 29 ff.

386 Ausführlich Gramlich/Jelito/Sedlmeir, 12 ff.; Ji/Grimmelmann, 337 ff.; Yang Sen et al., SoK: MEV Countermeasures, DeFi '24: Proceedings of the Workshop on Decentralized Finance and Security 2024, 21 ff., 21 f.; EBA/ESMA, Crypto-Assets, 33 ff., insb. 36; ESMA, MEV, 12.

1. *Ökonomische* Massnahmen, die insb. auf Änderungen an den Parametern des Auktionsmodells öffentlicher Blockchains oder die Vernichtung von MEV durch einen *Burn*-Mechanismus abzielen;
2. *technische* Massnahmen, wie etwa *Fair Ordering*-Mechanismen, neue Designs von Private Mempools, die nur einen Teil der Transaktionsdaten offenlegen bzw. diese vor Aufnahme in einen Block verschlüsseln, die Auslagerung des „*Sequencing*" an Dritte, wie etwa ein Orakel-Netzwerk, oder die Möglichkeit, den extrahierten Wert an die betroffenen Nutzer zurückzuerstatten;[387] und
3. *rechtliche* Massnahmen (hierzu sogleich).

VII. Rechtliche Einschätzung

1. Vorbemerkungen

Das wohlfahrtsökonomisch und ethisch fragwürdige Resultat gewisser MEV-Aktivitäten wirft die Frage nach deren rechtlicher und regulatorischer Unterstellung auf. Die rechtliche Einordnung von MEV steht jedoch noch am Anfang. Zentrale offene Frage ist die rechtliche Definition von MEV aus Sicht des Marktverhaltensrechts und gegebenenfalls darüber hinaus. Eine verbindliche Einordnung durch den Gesetzgeber sowie die Aufsichtsbehörden fehlt bislang, ebenso wie Klarheit darüber, ob eine allgemeine oder anwendungsbezogene Regulierung erforderlich ist.

Ein gutes Beispiel für die bestehende Rechtsunsicherheit ist die MiCAR: Auf Gesetzesebene wird MEV nicht ausdrücklich erfasst. Art. 92 Abs. 1 MiCAR setzt immerhin voraus, dass PPAETs „*[…] jeden begründeten Verdacht [von Marktmissbrauch] in Bezug auf einen Auftrag oder ein Geschäft, einschließlich […] anderer Aspekte der Funktionsweise der Distributed-Ledger-Technologie wie des Konsensmechanismus […]*" den zuständigen Behörden melden. Besonders der Verweis auf „andere Aspekte der Funktionsweise" einer Blockchain könnte den Einbezug von MEV als meldepflichtigen Tatbestand nahelegen. In den begleitenden Ausführungen der ESMA zu Art. 92 Abs. 2 MiCAR finden sich sodann

---

387 Vgl. etwa die Initiative „*MEV-Share*" von Flashbots <https://docs.flashbots.net/flashbots-mev-share/introduction>; Breidenbach Lorenz et al., Chainlink 2.0: Next Steps in the Evolution of Decentralized Oracle Networks, 15. April 2021, 43 ff., <https://research.chain.link/whitepaper-v2.pdf>; sodann zu *Anti-Frontrunning*-Technologien auch Andreotti, Dezentrale Handelsplattformen, 292 ff.; IOSCO empfiehlt, dass nationale Regulatoren bereits im Blockchain-Design MEV-*minimierende* Elemente voraussetzen sollten; vgl. IOSCO, DeFi, 35.

ausdrückliche Hinweise zu MEV.[388] Der sich auf die „Draft Regulatory Technical Standards" stützende finale Entwurf der Delegierten Verordnung der EU-Kommission enthält aber weder eine Definition noch eine ausdrückliche Regelung von MEV – angesichts der vielen Rückmeldungen aus Industrie und Rechtspraxis überrascht dies doch ein wenig.[389] Dasselbe gilt für die gestützt auf Art. 92 Abs. 3 MiCAR erlassenen Aufsichtsrichtlinien der ESMA, die sich ohnehin primär an die Aufsichtsbehörden richten.[390] ESMA macht aber deutlich, dass die Extrahierung von MEV marktmissbräuchlich sein *kann*, weshalb MEV-Agenten sich aufsichts- und ggf. strafrechtlich verantwortlich machen können; für PPAETs bedeutet das zudem eine mögliche Pflicht zur Überwachung und Meldung solcher Vorgänge unter Art. 92 MiCAR. Die genauen Konturen sind jedoch in beiden Fällen unklar.

Aus *Schweizer* Perspektive könnte für prudenziell Beaufsichtigte u.U. bei *offensichtlichen* Anzeichen, dass ein Kryptogeschäft nicht mit den Anforderungen von Art. 142 und Art. 143 FinfraG zu vereinbaren ist, eine Abklärungspflicht und gegebenenfalls eine Enthaltung der Mitwirkung am entsprechenden Kryptogeschäft in Frage kommen.[391] Anders als im Fall, den die FINMA in diesem Zusammenhang wohl vor Augen hat, ist allerdings kaum je das Verhalten des eigenen Kunden potenziell missbräuchlich, sondern jenes einer Drittpartei, die bei der Transaktionsverarbeitung mitwirkt. Hinzu kommt, dass es in solchen Fällen wohl häufig an offensichtlichen Anzeichen mangeln wird. Wenn bei Kundengeschäften keine systematische Überwachung und Abklärung von Effekten bzw. Kryptogeschäften verlangt ist,[392] muss dies u.E. umso mehr für Handlungen von an der Transaktionsverarbeitung beteiligten Personen gelten.

2. Insiderhandel

An erster Stelle steht die Frage, ob gewisse Formen von MEV-Aktivitäten gegen das Insiderhandelsverbot verstossen könnten. Dies setzt das Vorliegen *nicht öffentlich bekannter* bzw. vertraulicher Informationen voraus. Ob dieses Erfordernis erfüllt ist, hängt von der konkreten Datenquelle und deren Zugänglichkeit für Netzwerkteilnehmer im Einzelfall ab.[393]

---

388 ESMA, Draft Technical Standards, 12, wo die ESMA im Rahmen der Beantwortung der Frage, ob Miner und Validatoren im persönlichen Geltungsbereich von Art. 92 MiCAR sind, einige wenige Ausführungen zu MEV macht.

389 Siehe ESMA, Draft Technical Standards, 34 f., 36.

390 ESMA, Supervisory Guidelines, 15, 16.

391 FINMA-Rundschreiben 2013/8 „Marktverhaltensregeln", Rz. 47.

392 FINMA-Rundschreiben 2013/8 „Marktverhaltensregeln", Rz. 47.

393 Siehe betreffend *Konzept* der Öffentlichkeit von Informationen in Blockchain-Netzwerken Barczentewicz/Sarch/Vasan, 19 ff.

Transaktionsdaten, soweit sie im Public Mempool gesammelt werden, sind in der aktuellen Ausprägung von Blockchains grundsätzlich *öffentlicher* Natur.[394] Der Datensatz ist grundsätzlich auch für gewöhnliche Blockchain-Nutzer zugänglich.[395] Dass die breite Masse der regulären Blockchain-Nutzer die Transaktionsdaten des Public Mempools nicht regelmässig ausliest bzw. zur Kenntnis nimmt, ändert nach vorliegender Ansicht nichts daran, dass die Informationen insgesamt genügend Personen, namentlich allen Netzwerkteilnehmern, die einen Full Node betreiben, bekannt sind bzw. sein können.[396] Bei solchen Daten handelt es sich nach vorliegender Ansicht in aller Regel weder nach europäischer noch nach Schweizer Rechtsauffassung um Insiderinformationen.

Demgegenüber könnte es sich bei *ausschliesslich privat übermittelten* Transaktionen, wie etwa im Fall der direkten Kommunikation zwischen Nutzern und Validatoren, oder bei Transaktionsdaten, die in Private Mempools gesammelt werden, die nur einem ausgewählten Kreis von MEV-Agenten zugänglich ist, um Insiderinformationen im rechtlichen Sinne handeln – in dieser Konstellation ist die Situation nicht unähnlich zu derjenigen, in welcher eine Bank Kundenaufträge an einen vertraglich verbundenen Broker übermittelt und dieser seine eigenen Transaktionen den von der Bank übermittelten Kundenaufträgen voranstellt.[397]

Im Grenzbereich finden sich Transaktionen, die *privat* an eine Node oder einen *Remote Procedure Call* (RPC)-Server übermittelt werden, jedoch noch *vor* Transaktionsverarbeitung öffentlich gemacht werden.[398] Selbst Transaktionen, die bloss für einen kurzen Moment zurückgehalten werden, gelten gemäss gesetzlicher Fiktion nach ihrer Bekanntgabe an den übrigen Teil des Netzwerks als öffentlich bekannt. Solange andere MEV-Agenten die realistische Möglichkeit besitzen, derartige Informationen selber zu verwerten, handelt es sich auch hier *de lege lata* um öffentlich bekannte Informationen und somit nicht um Insiderinformationen.

---

394 In Bitcoin: z.B. <https://mempool.space/>; in Ethereum: z.B. <https://etherscan.io/txspending>.

395 *Kritisch* hingegen ESMA, MEV, 11.

396 Zur Frage der (*einfachen*) *Zugänglichkeit* von Insiderinformationen ausführlich Remund/Wyss, 38 ff.; *a.*A. als hier Maume, Art. 87, MiCAR Kommentar, Rz. 6, 23 m.w.N.; skeptisch auch Müller, 102.

397 Zur Relevanz einer „trust relationship" unter US-amerikanischem Recht insb. Barczentewicz/Sarch/Vasan, 66 ff.; zu den Unterschieden zwischen EU- und US-Insiderrecht Ventoruzzo Marco, in: Ventoruzzo Marco/Mock Sebastian (Hrsg.), Market Abuse Regulation. Commentary and Annotated Guide, 2. A., Oxford 2022, A.2.11 ff., B.10.44 f.

398 Vgl. Barczentewicz/Sarch/Vasan, 20.

Ferner muss die Insiderinformation geeignet sein, den Kurs eines Kryptowerts erheblich zu beeinflussen (*Kursrelevanz*). Bei volumenmässig kleineren Aufträgen, die zudem über eine tiefe *Slippage*-Toleranz verfügen, wird die Kurserheblichkeit nur ausnahmsweise gegeben sein. Bei grösseren Transaktionen oder systematischen MEV-Aktivitäten, welche sich die Bündelung vieler kleinerer Transaktionen zunutze machen, kann hingegen eine kursrelevante Insiderinformation vorliegen.[399]

3. Marktmanipulation

Sodann ist die Anwendbarkeit der Vorgaben zur Marktmanipulation auf MEV-Aktivitäten zu prüfen:

Im Vordergrund steht primär die *transaktionsbasierte* Marktmanipulation:[400] Durch das Einschieben eigener oder fremder Transaktionen verzerren MEV-Agenten möglicherweise den Erwerbs- oder Verkaufspreis für reguläre Blockchain-Nutzer. Bei Frontrunning- und Sandwiching-Aktivitäten entsteht dadurch unter Umständen ein „*anormales oder künstliches Kursniveau*" (vgl. Art. 91 Abs. 2 lit. a (ii) MiCAR) – ein „*künstliches Kursniveau*" liegt gegebenenfalls vor, weil MEV-Extraktion dazu führt, dass der Auftrag von regulären Blockchain-Nutzern innerhalb der vorbestimmten *Slippage*-Toleranz kostspieliger ausgeführt wird. Aus *FinfraG*-Sicht stellt sich die Frage, ob die Geschäfte oder Aufträge falsche oder irreführende Signale für das Angebot, die Nachfrage oder den Kurs von Kryptowerten geben, die als Effekten qualifizieren.

Es scheint ferner nicht ausgeschlossen, dass bei ausschliesslich privat übermittelten Transaktionen der Tatbestand von Art. 91 Abs. 2 lit. b MiCAR erfüllt ist, weil der MEV-Agent eine Handlung vornimmt, die unter Vorspiegelung falscher Tatsachen oder unter Verwendung sonstiger Kunstgriffe oder *Formen der Täuschung* den Kurs eines Kryptowerts beeinflusst oder hierzu zumindest geeignet ist.[401]

Ebenfalls könnte eine *marktbeherrschende* Stellung im MEV-Markt v.a. bezüglich Block-Building als Marktmanipulation qualifizieren (vgl. Art. 91 Abs. 3 lit. a MiCAR), wenn diese dominante Stellung dazu missbraucht wird, unlautere

---

399 Ähnlich Maume, Art. 87, MiCAR Kommentar, Rz. 23 m.w.N.

400 A.M. offenbar Müller, 104 f., der im Verhalten v.a. informationsbasierte Manipulation erkennt.

401 Vgl. hinsichtlich der Diskussion einer „trust relationship" zwischen Blockchain-Nutzern und MEV-Agenten Barczentewicz/Sarch/Vasan, 67 f.

Handelsbedingungen für die übrigen Nutzer herbeizuführen.[402] Ähnliches könnte bei *Suppression Attacks* gelten, welche die Ausführung von Transaktionen verhindern oder zumindest zeitlich verzögern, um eigene Transaktionen des Angreifers zu bevorzugen (vgl. die Ähnlichkeiten zu den Handlungen in Art. 91 Abs. 3 lit. b (i) und (ii) MiCAR).[403] Diese Form der Manipulation könnte etwa bei Orakelpreisen, die durch vorübergehende Unterdrückung nicht rechtzeitig an die DeFi-Anwendungen übermittelt werden können, zentral sein. Ausserdem können die erwähnten Aktivitäten auch Berührungspunkte mit dem Wettbewerbs- und Kartellrecht aufweisen.

Ein Angriffsvektor mit besonderen MEV-Opportunitäten stellt die *Manipulation von Orakelpreisen* dar.[404] Im Fall *Eisenberg* etwa wurden sowohl On-chain- als auch Off-chain-Preisquellen manipuliert, sodass die dezentrale Anwendung Mango Markets verzerrte Preise bezogen hat, was dem Angreifer die Entnahme einer zu hohen Darlehenssumme ermöglichte. Es ist nicht ausgeschlossen, dass die Manipulation von Preisquellen, die als „Benchmarks" in DeFi dienen, durch MEV-Agenten (aber auch durch andere Marktteilnehmer)[405] trotz fehlender ausdrücklicher Regelung in MiCAR[406] den Tatbestand der Marktmanipulation erfüllen kann.[407]

Soweit hingegen *legitime* MEV-Geschäftsmodelle infrage stehen, wie etwa bei Preisarbitrage inkl. Backrunning-Strategien, sofern sie darauf ausgerichtet sind, das Preisniveau auf einer Plattform an den Rest des Marktes anzugleichen, sowie DeFi-Liquidationen, soweit MEV-Agenten damit nicht Aktivitäten

---

402 Ähnlich Maume, Art. 91, MiCAR Kommentar, Rn 40 a.E., 44; ferner Barczentewicz/Sarch/Vasan, 71 f.; sodann in Bezug auf „large liquidity pools" Zetzsche/Woxholth, 165.

403 Vgl. zu den *Suppression Attacks* Gramlich/Jelito/Sedlmeir, 12; POSA, 5 Fn. 12, worin diese Form als „*censorship*" bezeichnet wird; ähnlich zu *Distributed-Denial-of-Service* (DDoS) *Attacks* Misterek, § 18, Handbuch Kryptowerte, Rz. 63.

404 Siehe Barczentewicz, 12 ff.; ausführlich zum Spezialfall von „*Multi-Block MEV*" Mackinga Torgin/Nadahalli Tejaswi/Wattenhofer Roger, TWAP Oracle Attacks: Easier Done than Said?, 2022 IEEE International Conference on Blockchain and Cryptocurrency (ICBC) 2022, 1 ff., *passim*.

405 Es handelt sich dabei nicht nur um ein MEV-Thema; vgl. etwa Duley Chanelle et al., The oracle problem and the future of DeFi, BIS Bulletin Nr. 76, 7. September 2023, 1 ff., *passim*.

406 Vgl. demgegenüber Art. 2 Abs. 2 lit. c i.V.m. Art. 12 Abs. 1 lit. d MAR (Referenzwerte); betreffend Meldepflicht von Benchmark-Administratoren bei Verstössen im traditionellen Bereich Art. 14 Verordnung (EU) 2016/1011 des Europäischen Parlaments und des Rates vom 8. Juni 2016; zur Rechtslage unter MAR Sajnovits Alexander, Financial Benchmarks. Manipulation von Referenzwerten wie LIBOR und EURIBOR und deren aufsichts- und privatrechtlichen Folgen, Berlin 2018, 135 ff.; ferner unter *Schweizer* Recht FINMA-Rundschreiben 2013/8 „Marktverhaltensregeln", Rz. 44; Härtner Stefan, Referenzwertmanipulationen aus zivilrechtlicher Perspektive, Zürich 2022, *passim*.

407 So auch Barczentewicz/de Gândara Gomes, 8, 14.

ähnlich zu *Stop-Loss-Hunting* betreiben, um etwa Liquidationen von Schuldpositionen künstlich herbeizuführen,[408] sollte nach vorliegender Ansicht nicht von Marktmanipulation ausgegangen werden.[409]

4. Best Execution von Kundenaufträgen

Aus Sicht der Kryptodienstleister stellt sich die Frage, wie sie mit MEV mit Blick auf Kundentransaktionen umgehen, und zwar nicht nur in ihrer allfälligen Rolle als PoS-Validator bzw. Block-Proposer, sondern auch aufgrund der den Kunden regelmässig geschuldeten *Best Execution* (BEX) bei Ausführung ihrer Aufträge.[410] Praktisch relevant ist dies v.a. bei Ausführung und Abwicklung von Kundentransaktionen direkt auf der Blockchain, d.h. über dezentrale Handelsplattformen (DEX) und andere DeFi-Anwendungen.

Unter MiCAR müssen Anbieter von Kryptowerte-Dienstleistungen, wenn sie Kundenaufträge *ausführen*, alle erforderlichen Massnahmen ergreifen, um bei der Ausführung das bestmögliche Ergebnis für ihre Kunden zu erzielen; sie berücksichtigen dabei die Faktoren Preis, Kosten, Schnelligkeit, Wahrscheinlichkeit der Ausführung und Abwicklung, Umfang, Art der Auftragsausführung und Bedingungen der Verwahrung von Kryptowerten sowie jegliche sonstigen für die Auftragsausführung relevanten Faktoren (Art. 78 Abs. 1 MiCAR). Die BEX-Regelung in Art. 18 FIDLEG ist demgegenüber auf den Handel der vorliegend interessierenden Zahlungs- und Nutzungs-Token nicht anwendbar, wenn sie keine Finanzinstrumente sind, was dem absoluten Regelfall entspricht.[411]

Es ist schliesslich auch zu prüfen, ob Gesetzgeber und Aufsichtsbehörden BEX-Praktiken insb. bei Ausführung über eine DEX unter Berücksichtigung von Slippage, dynamischen Transaktionsgebühren und potenziellen MEV-be-

---

408 Vgl. hierzu Lee Joseph/Schu Lukas, Market abuse in the crypto-assets market: same risks, same activities, and same regulatory outcomes?, in: Lee Joseph/Darbellay Aline (Hrsg.), A Research Agenda for Financial Law and Regulation, Cheltenham/Northampton 2025, 157 ff., 160 ff.

409 Vgl. auch die Ausnahmen vom Verbot des Insiderhandels und der Marktmanipulation (sog. Safe Harbor-Regeln) in Art. 122 ff. FinfraV, die *de lege ferenda* u.U. ausgeweitet werden müssten.

410 Die Frage ebenfalls aufwerfend Auer/Frost/Pastor, 4; FCA, Research Note, 20; Momberg/Angelovska-Wilson, *passim*; ferner Müller, 103, der eine generelle Ausdehnung der *FIDLEG-Verhaltensregeln* anregt.

411 Siehe Abegglen Sandro/Andreotti Fabio, Best Execution gemäss FIDLEG. Eine privat- und aufsichtsrechtliche Betrachtung, GesKR 2020, 36 ff., 46; ferner Vogel Alexander/Heiz Christoph/Luthiger Reto, Art. 3, Orell Füssli Kommentar (OFK), Bundesgesetz über die Finanzdienstleistungen und Bundesgesetz über die Finanzinstitute, Zürich 2020, Rz. 46. Eine Pflicht des Anbieters von Kryptowerte-Dienstleistungen, das bestmögliche Ergebnis für ihre Kunden zu erzielen, kann sich allerdings auch aus dem Privatrecht ergeben.

dingten Preisauswirkungen womöglich in Abweichung zu „traditionellen" BEX-Standards festzulegen haben.

VIII. Zwischenfazit

MEV ist ein Blockchain-spezifisches Phänomen, das komplexen soziotechnischen Annahmen unterliegt. Dabei geht es allen voran um die Beantwortung der Frage, welcher monetäre Wert regulären Blockchain-Nutzern, die dem System durch ihre Transaktionen erst Relevanz verleihen, und welcher monetäre Wert Netzwerkteilnehmern, die das System in Übereinstimmung mit den Protokollregeln unterhalten und dafür auch entschädigt werden sollten, zukommen soll.[412] In ökonomischer Hinsicht geht es sodann um Markteffizienz, und in ethischer Hinsicht um Fairness im Kryptomarkt. Der Gesetzgeber und die Marktaufsichtsbehörde haben mit Blick auf den Anleger- und Funktionsschutz[413] eine ausgewogene Lösung zu finden, die nach vorliegend vertretener Ansicht unbedingt auch ökonomische und technische Ansätze berücksichtigen sollte.[414]

E. Vergleich: MiCAR vs. Schweizer Marktverhaltensregeln *de lege lata*

Mit der MiCAR wurde im EWR ein umfassendes *kryptospezifisches* Marktverhaltensregime eingeführt, um die im Kryptomarkt beobachteten Marktmissbräuche zu adressieren. Im Zusammenspiel mit dem MAR-Regime sind nunmehr die relevanten Formen des Marktmissbrauchs in Bezug auf unterschiedliche Typen von Kryptowerten vergleichbaren Marktverhaltensregeln unterstellt.

Mit Ausnahme für Effektentoken, die in der Schweiz zum Handel an einem Handelsplatz oder DLT-Handelssystem zugelassen sind, verfügt die Schweiz demgegenüber über kein Marktmissbrauchsregime für Kryptowerte. Entspre-

412 Ebenfalls auf das Spannungsverhältnis zwischen Netzwerksicherheit und Kollektivschutz von Nutzern hinweisend Momberg/Angelovska-Wilson, *passim*.

413 Vgl. Meirich David, Regulatorische Einordnung von Decentralized Finance, Zürich 2023, N 528 ff., der sodann auch den Schutz der *Reputation* des Finanzplatzes im Kontext von DeFi betont.

414 Eine interessante Betrachtungsweise von MEV in Blockchains ergibt sich aus der Perspektive der Untersuchung von *Gemeingütern*, vgl. Poux Philémon/De Filippi Primavera/Deffains Bruno, Maximal Extractable Value and the Blockchain Commons, 23. August 2022, 15 ff., <https://ssrn.com/abstract=4198139>. Daraus folgt grundsätzlich auch die Erkenntnis, dass rein ökonomische und rein rechtliche Massnahmen für sich alleine ungenügend sein dürften.

chend werden zahlen- und volumenmässig nur wenige Kryptowerte *de lege lata* durch die Marktmissbrauchsregeln erfasst. Der sehr enge Anwendungsbereich des FinfraG wird allerdings dadurch ausgedehnt, dass die Vorgaben für prudenziell Beaufsichtigte gestützt auf das FINMA-Rundschreiben 2013/8 „Marktverhaltensregeln" in der Aufsichtspraxis auch auf andere Märkte als den Effektenmarkt, wie insb. den *Kryptomarkt*, sinngemässe Anwendung finden. Banken, Wertpapierhäuser und andere prudenziell Beaufsichtigte haben demnach analog zu den für den Effektenhandel relevanten Bestimmungen gewisse organisatorischen Massnahmen zu ergreifen, um auch Marktmissbrauch mit Kryptobezug zu verhindern.

Die MiCAR adressiert sodann nicht nur den Sekundärmarkt, sondern sieht auch Pflichten auf dem *Primärmarkt* vor, so insb. Anforderungen an Whitepaper und Offenlegungspflichten im Zusammenhang mit Insiderinformationen (Ad-hoc-Publizität gemäss Art. 88 MiCAR). In der Schweiz fehlen solche kryptospezifischen Bestimmungen für den Primärmarkt – vorbehaltlich der bereits gemachten Ausführungen zu prudenziell Beaufsichtigten.

Die MiCAR folgt in Bezug auf den *Insiderinformationsbegriff* der Regelung in der MAR und erfasst insb. auch (noch) nicht öffentliche Informationen über eine bevorstehende Handelszulassung. Das Schweizer Regime sieht keine solche Regelung für Effekten vor (vgl. Art. 2 lit. j FinfraG). Eine Erweiterung des FinfraG auf solche Sachverhalte scheint sich angesichts des besonderen potenziellen Missbrauchspotenzials im Kryptomarkt anzubieten.

Schliesslich knüpft die Anwendung des MiCAR-Marktverhaltensregimes an die Zulassung eines Kryptowerts an einer im EWR bewilligten Handelsplattform mit multilateralem Matching an. Rund zehn Plattformen dieser Art sind inzwischen in der EU bewilligt.[415] Die Schweiz war demgegenüber bislang kein Land der multilateralen Kryptohandelsplattformen,[416] wobei Ende 2023 immerhin sechs Banken und Wertpapierhäuser ein OHS für kryptobasierte Vermögenswerte (vermutlich primär für Effektentoken) betrieben haben sollen.[417]

---

415 Vgl. die online verfügbare Liste der ESMA unter <https://www.esma.europa.eu/esmas-activities/digital-finance-and-innovation/markets-crypto-assets-regulation-mica#InterimMiCARegister>.

416 So bereits Andreotti, Handelsplattformen, Rz. 11.05.

417 FINMA, Jahresbericht 2023, 33.

F. Ausblick: Schweizer Marktverhaltensregeln *de lege ferenda*

Der vorliegende Beitrag hat aufgezeigt, dass der Kryptomarkt von marktmissbräuchlichen Verhaltensweisen nicht verschont bleibt. Ferner hat er herausgearbeitet, dass die Schweizer Marktverhaltensordnung im Kryptobereich gewisse Lücken aufweist. Diese Lücken ergeben sich aus der Anknüpfung der Marktverhaltensregeln einerseits an den Effektenbegriff und andererseits an die Zulassung der Effekten an einem Handelsplatz oder DLT-Handelssystem. Die sinngemässe Unterstellung des Kryptomarktes unter das Marktverhaltensrecht erscheint darum aus regulatorischer Sicht grundsätzlich als wünschenswert.[418] Darüber hinaus sollten wohl auch gewisse Formen des Insiderhandels künftig erfasst werden (*Wahi* und *Chastain*), die derzeit nicht einmal im Effektenbereich reguliert sind.

Gestützt auf die aktuelle Rechtslage, insb. mit Blick auf das FINMA-Rundschreiben 2013/8 „Marktverhaltensregeln", gibt es *de lege ferenda* grundsätzlich zwei Möglichkeiten, den Geltungsbereich der Marktverhaltensregeln auszuweiten: (i) über eine Ergänzung beim Anknüpfungspunkt der Effekten um (gewisse) Kryptowerte[419] und eine Erweiterung der erfassten Handelsplattformen im Kryptobereich oder (ii) über eine Unterstellung gewisser Kryptodienstleistungen unter eine neue Bewilligungsart, die direkt von der FINMA beaufsichtigt wird (wodurch die Marktmissbrauchsregeln via Gewährsanforderungen wiederum sinngemäss zur Anwendung gelangen würden). Nach vorliegender Ansicht ist eine „Regulierung" bloss über das FINMA-Rundschreiben 2013/8 „Marktverhaltensregeln" aus rechtsstaatlichen Überlegungen jedoch abzulehnen.

Auch mit Blick auf das laufende Gesetzesprojekt des SIF[420] stellt sich also die Frage, inwieweit das Marktverhalten im Kryptobereich *gesetzgeberisch* sinnvoll erfasst werden könnte. Ein künftiges Marktmissbrauchsregime im Kryptobereich könnte nach Ansicht der Autoren folgende Eckpunkte umfassen:

---

418 Vgl. für die USA H.R. 3633, Digital Asset Market Clarity Act of 2025, Sec. 302, wonach die Rechtsprechung und Praxis zu „*securities transactions*" für „*digital commodities*" und „*permitted payment stablecoins*" zu übernehmen sei; weniger weitgehend in der UK hingegen FCA, DP24/4, Rz. 3.7, worin von einem „*pragmatic approach… in the near-term*" die Rede ist.

419 Denkbar, aber aus gesetzessystematischen Gründen abzulehnen, wäre auch die *Erweiterung des Effektenbegriffs*, um relevante Kryptowerte miteinzubeziehen.

420 Staatssekretariat für internationale Finanzfragen (SIF), Anpassung des Finanzmarktrechts im Hinblick auf innovative Geschäftsmodelle der Finanzinstitute, 27. März 2024, <https://www.sif.admin.ch/de/finanzmarktrechts-innovative-geschaeftsmodelle-finanzinstitute>.

- Die heutige Anknüpfung an Effekten sollte um eine Anknüpfung an *Kryptowerte mit eindeutigem Kapitalmarktprofil* (d.h. Finanzierungs- und/oder Anlagezweck) ergänzt werden, die *de lega lata* mangels Verkörperung einer Rechtsposition in aller Regel keine Effekte darstellen.
- Für die Eröffnung des Anwendungsbereichs müssten derartige Kryptowerte an einem neu zu regelnden „*Krypto-MHS*" (FinfraG), das auch nicht prudenziell beaufsichtigte Personen als Teilnehmer zulässt, und/oder „*Krypto-OHS*" (FinfraG bzw. BankG/FINIG) mit jeweils Sitz in der Schweiz zum Handel zugelassen sein. Da reguläre OHS *de lege lata* nicht Anknüpfungspunkt für das Marktverhaltensrecht sind, wäre die Ausgestaltung der regulatorischen Konturen eines Krypto-OHS insb. unter Berücksichtigung des Gleichbehandlungsgrundsatzes eingehend zu prüfen. Auf jeden Fall wäre der Kreis der Betreiber über die heute vorgesehenen prudenziell Beaufsichtigten hinaus zu erweitern. Dies würde eine generelle Anpassung der (prudenziellen) Regulierung von „Krypto-Instituten" in der Schweiz nahelegen.
- Um der Relevanz solcher Vorgänge im Kryptomarkt Rechnung zu tragen, ist zu prüfen, ob der Insiderinformationsbegriff künftig bereits den Sachverhalt der *Handelszulassung* von Kryptowerten abdecken sollte.
- Je nach künftiger Regulierung der Krypto-Institute sind organisatorische Vorgaben im Zusammenhang mit der *Überwachung* der eigenen Handelstätigkeit bzw. des eigenen Handelssystems vorzusehen. Allerdings ist zu verhindern, dass unrealistische oder unverhältnismässige Anforderungen an die Überwachung des Marktes durch Krypto-Institute gestellt werden, zumal die Rollenverteilung nicht derart sein sollte, dass die Marktteilnehmer faktisch zum verlängerten Arm der Aufsichtsbehörde und der Strafverfolgungsbehörden mutieren. Folglich ist eine umfangreiche „Whistleblowing-Pflicht", wie sie in der MiCAR vorgesehen ist,[421] grundsätzlich abzulehnen.[422]
- Ob eine Direktunterstellung von Krypto-Instituten unter die *Aufsicht* der FINMA notwendig ist oder ob die Aufsicht durch eine Aufsichtsorganisation (AO) genügt, wie sie für Vermögensverwalter und Trustees gilt, oder ob sogar eine neue spezialisierte „*Krypto-Selbstregulierungsorganisation*" (Krypto-SRO) als Aufsichtsorgan in Betracht zu ziehen ist, sollte mit Blick

---

421 So etwa mit Blick auf das Melderegime in Art. 92 MiCAR Zetzsche/Woxholth, 169.

422 Im Rahmen der laufenden FinfraG-Revision soll abhängig von der Grösse und Komplexität des Geschäftsmodells *„[…] nicht in jedem Fall eine systematische Überwachung […]"* vorgeschrieben sein; vgl. EFD, 48.

auf den Verhältnismässigkeitsgrundsatz sowie eine wirksame Marktaufsicht geprüft werden.

- Es ist schliesslich zu prüfen, ob Emittenten von Kryptowerten dem Markt ein Mindestmass an Informationen zur Verfügung stellen sollen. Kryptowerte-Whitepaper gemäss der MiCAR sollten in einem allfälligen Schweizer „*Krypto-Prospektregime*" zudem ohne Einschränkungen wiederverwendet werden dürfen. Schliesslich ist auch die Einführung einer Ad-hoc-Publizitätspflicht solcher Emittenten auf Stufe der Handelsplattformen (Selbstregulierung) zu prüfen. Von solchen Pflichten vollständig ausgenommen sollten hingegen Kryptowerte sein, die ohne eindeutige Emittentin in dezentraler Weise programmatisch herausgegeben werden (und zwar selbst dann, wenn sie ein eindeutiges Kapitalmarktprofil aufweisen sollten).
- Bis auf Weiteres sollte sich die Schweiz mit einer Regulierung gewisser (negativer) Formen von MEV zurückhalten und sich in internationalen Gremien für Blockchain-basierte wirtschaftliche und technische Lösungen einsetzen. Die unhinterfragte Übernahme des traditionellen Marktverhaltensregimes basierend auf dem „*same activity*, *same risk*, *same rules*"-Ansatz in diesem Bereich wäre angesichts der materiellen Unterschiede zu traditionellen Infrastrukturen wahrscheinlich unverhältnismässig und zudem „handwerklich" falsch.[423] Ausserdem wäre zu diskutieren, ob über das Marktmissbrauchsrecht hinaus besondere Vorgaben für Personen oder Gruppen von miteinander verbundenen Personen, welche die Funktionsweise von Blockchains in relevanter Weise beeinflussen können, eingeführt werden sollen.[424]

Eine Ausweitung der Marktverhaltensregeln in der Schweiz auf den Kryptomarkt muss in jedem Fall sachgerecht und verhältnismässig erfolgen und darf u.a. nicht zu einer Überregulierung des Kryptomarkts im Vergleich zu anderen

---

423 So offenbar auch Global Finance & Technology Network (GFTN), Market Abuse in Crypto Markets, August 2025, *passim*, <https://gftn.co/insights/market-abuse-in-crypto-markets>, wobei es sich beim Dokument um einen Bericht über einen Roundtable u.a. mit Beteiligung der FINMA handelt.

424 Vgl. etwa für die USA den Begriff der „*blockchain control person*" in H.R. 3633, Digital Asset Market Clarity Act of 2025, Sec. 411, unter dessen Offenlegungs- und Verhaltensregime eine Vorgabe zur erwünschten (*progressiven*) Dezentralisierung eines anfänglich noch zentral gemanagten Blockchain-Protokolls gesehen werden kann. Betreffend Erkenntnis, dass Regulierung ein *Dezentralisierungstreiber* sein kann, siehe Andreotti, Dezentrale Handelsplattformen, 659 f.

Märkten, wie bspw. den Rohwaren-, Devisen- und Zinsmärkten, führen.[425] Mit anderen Worten soll eine Ausweitung der Marktverhaltensregeln bloss dort erfolgen, wo eine empirische Notwendigkeit – insb. für den Schweizer Markt – nachgewiesen worden ist.[426]

425 Als solche Überregulierung, die über das hinausgeht, was gemeinhin noch als finanzmarktnah bezeichnet werden kann, kann bspw. die (generelle) Unterstellung von „Utility-Token" unter die MiCAR genannt werden. Vgl. Art. 3 Abs. 1 Ziff. 9: „*[…] einen Kryptowert, der ausschließlich dazu bestimmt ist, Zugang zu einer Ware oder Dienstleistung zu verschaffen, die von seinem Emittenten bereitgestellt wird[.]*"

426 Siehe auch Swiss Blockchain Federation (SBF)/Bitcoin Association Switzerland (BAS)/ Crypto Valley Association (CVA), Zwölf Punkte zur Stärkung der Innovation des Schweizer Finanzplatzes, 6. Mai 2025, Empfehlung 2, <https://blockchainfederation.ch/wp-content/uploads/2025/05/SBF_Manifest_DE.pdf>.

EuZ
ZEITSCHRIFT FÜR EUROPARECHT

27. Jahrgang

Herausgeber

Europa Institut an der
Universität Zürich
Hirschengraben 56
8001 Zürich
Schweiz
eiz@eiz.uzh.ch

Institut für deutsches und
europäisches Gesellschafts-
und Wirtschaftsrecht der
Universität Heidelberg
Friedrich-Ebert-Platz 2
69117 Heidelberg
Deutschland

LL.M. Internationales
Wirtschaftsrecht
Universität Zürich
Hirschengraben 56
8001 Zürich

Redaktion
Dr. Tobias Baumgartner, LL.M., Rechtsanwalt (Leitung)
MLaw Sophie Tschalèr
Dr. Wesselina Uebe, Rechtsanwältin

Cover-Foto: Marek Piwnicki, Unsplash

Erscheinungsweise
EuZ – Zeitschrift für Europarecht erscheint zehnmal jährlich online. Die Leitartikel werden zu Beginn des Folgejahres zusätzlich in Form eines Jahrbuchs als eBook sowie im Wege des print on demand veröffentlicht.

Zitierweise
EuZ, Ausgabe 7/2025, G 1.

ISSN
1423-6931 (Print)
2813-7833 (Online)

Kontakt
EIZ Publishing c/o Europa Institut an der Universität Zürich
Dr. Tobias Baumgartner, LL.M., Rechtsanwalt
Hirschengraben 56
8001 Zürich
Schweiz
eiz@eiz.uzh.ch

Version 1.02-20250904

DOI
Fabio Andreotti, Joshua R. Taucher, Marktmissbrauch im Kryptomarkt, https://doi.org/10.36862/74WK-0D9Q