European Journal of Risk Regulation (2024), 1–18
doi:10.1017/err.2024.80

ARTICLE

Crypto-Asset Market Abuse Under EU MiCA

Mikołaj Barczentewicz[1] and André de Gândara Gomes[2]

[1]University of Surrey, Guildford, UK and [2]Uría Menéndez, Lisbon, Portugal
Corresponding author: Mikołaj Barczentewicz; Email: m.barczentewicz@surrey.ac.uk

Abstract

The new EU Markets in Crypto-Assets Regulation ("MiCA") emphasises the prevention of market abuse as one of its five main objectives. This paper critically analyzes MiCA's provisions on market abuse (Title VI), applying the new rules to the primary categories of crypto-asset market integrity risks to provide a coherent interpretation. In doing so, we consider both the pre-existing legal framework for protecting market integrity, chiefly the Market Abuse Regulation ("MAR"), and the unique features of crypto-asset markets. We find that by largely replicating MAR, MiCA presents "new wine in old bottles" challenges, as crypto-assets introduce novel issues that the legislator attempts to address with a subset of existing tools. The extent to which "decentralized finance" (DeFi) activities will incur liability under MiCA's anti-market abuse provisions remains unclear, particularly regarding various blockchain network participants. Furthermore, classifying MEV strategies as market abuse may prove difficult. The absence of certain safe-harbor provisions present in MAR, such as those for self-insiders and buy-back and stabilisation schemes, may create uncertainty and potentially chill legitimate market behavior under MiCA.

Keywords: crypto-assets; market abuse; markets in crypto-assets regulation

I. Introduction

The Markets in Crypto-Assets Regulation ("MiCA")[1] puts prevention of market abuse as one of its five main areas of focus (Article 1(2)(e)). The bulk of MiCA's anti-market abuse rules is in its Title VI (Articles 86-92). Those rules are inspired by the Market Abuse Regulation ("MAR"),[2] which already applies to crypto-assets that constitute financial instruments under MiFID II.[3] Filling the gap left by MAR, MiCA applies to crypto-assets, which are not financial instruments (Article 2(4)(a)).[4]

Despite being inspired by MAR, MiCA does not fully replicate it. The reason for this is given in Recital 95: "as issuers of crypto–assets and crypto-asset service providers are very often SMEs, it would be disproportionate to apply all the provisions of" MAR. However,

[1] Regulation EU 2023/1114 of the European Parliament and of the Council of 31 May 2023 on Markets in Crypto-assets.

[2] Regulation EU 596/2014 of the European Parliament and of the Council of 16 April 2014 on market abuse (Market Abuse Regulation).

[3] Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments (MiFID II); ESMA, "Advice on Initial Coin Offerings and Crypto-Assets" (2019) ESMA50-157–1391 18–21 <https://www.esma.europa.eu/sites/default/files/library/esma50-157-1391_crypto_advice.pdf>.

[4] There are crypto-assets which are not financial instruments to which MiCA — including its anti-market abuse rules – does not apply, e.g. Non-Fungible Tokens ("NFTs"). See below Section II.3.

https://doi.org/10.1017/err.2024.80 Published online by Cambridge University Press

MiCA's substantive provisions on insider dealing, unlawful disclosure of inside information, and market manipulation follow the example of MAR very closely.

This relationship between MiCA and MAR suggests that MAR can be used to assist in interpreting MiCA's anti-market abuse provisions. For example, MiCA uses terms clearly borrowed from MAR (like a "person professionally arranging or executing transactions" in Article 92), which are defined in MAR (see Article 3(1)(28) MAR) but are not defined in MiCA, potentially creating interpretative difficulties. However, it should also be noted that, neither in its recitals, nor in the main text, does MiCA explicitly set MAR as a point of reference for interpretative purposes. Moreover, even the obvious borrowing of content from MAR is not strictly speaking explicitly acknowledged in MiCA (an implicit acknowledgment can be found in the already cited Recital 95).

The purpose of this paper is to critically analyse MiCA's provisions on market abuse (Title VI). We apply the new rules to the main categories of crypto-asset market integrity risks, aiming to provide a coherent interpretation. While doing so, we have in mind both the pre-existing legal framework for protecting market integrity (chiefly: MAR) and the special features of the markets in crypto-assets. We begin, in Section II, by considering the scope of application of MiCA's Title VI. We note that the rules will apply broadly, both in a geographic sense (outside the EU) and in terms of subject matter. In particular, "DeFi" (decentralised finance) is not excluded, and this may also be true, at least indirectly, for some trading in non-fungible tokens (NFTs) and in crypto-assets not admitted to trading and with no request for admission. In the following Section III, we introduce MiCA's provisions on inside information, market manipulation, as well as monitoring and reporting of market abuse. In Section IV, we apply the new rules to key risks of crypto-asset market abuse, including, among others, private information about orders to trade, crypto investment scams (like "rug pulls"), pump-and-dump schemes, wash trading, and "oracle" manipulation. Section V is devoted to some of the important aspects of crypto-asset markets, which will require more research and debate before their status under MiCA's Title VI becomes settled. Here, we discuss "MEV extraction" and buy-back and stabilisation mechanisms. Section VI concludes.

II. The scope of application of MiCA's Title VI

1. DeFi not excluded

It seems to be commonly expected that MiCA will not apply to decentralised finance ("DeFi").[5] This expectation is based on a misunderstanding, both regarding what kind of activity counts as crypto-asset services covered by MiCA and with respect to the scope of MiCA's anti-market abuse rules. In this paper, we set aside the former issue and focus exclusively on the latter.

In terms of the scope of application of its anti-market abuse provisions, MiCA inherited the broad approach adopted in MAR (Article 2(3) MAR)). Accordingly, MiCA's anti-market abuse rules from Title VI apply

> (. . .) to acts carried out by any person concerning crypto-assets that are admitted to trading or in respect of which a request for admission to trading has been made.[6]

And:

[5] See Recital 22, according to which MiCA does not apply to crypto-asset services "provided in a fully decentralised manner without any intermediary." Also, see Recital 93, which provides that crypto-asset "transfer" services do not include the actions of "the validators, nodes or miners that may be part of confirming a transaction and updating the state of the underlying distributed ledger."

[6] Art 86(1) MiCA.

https://doi.org/10.1017/err.2024.80 Published online by Cambridge University Press

> (. . .) to any transaction, order or behaviour concerning crypto-assets (. . .), irrespective of whether such transaction, order or behaviour takes place on a trading platform.[7]

Importantly, the rules apply to "acts carried by any person." Had the legislator intended the scope of Title VI to be limited only to the persons mentioned in Article 2(1) MiCA ("natural and legal persons and certain other undertakings that are engaged in the issuance, offer to the public and admission to trading of crypto-assets or that provide services related to crypto-assets in the Union"), the reference to "any person" would have been superfluous. Such a reading would conflict with the interpretative principle that the legislator is a rational actor.[8] The better reading is then that the personal scope of Title VI is not limited to the persons listed in Article 2(1), but indeed covers "any person" that carries out acts concerning crypto-assets admitted to trading or with a request for admission.

Moreover, the rules apply to any "transaction, order or behaviour" *irrespective of where it takes place*. In other words, the prohibitions of market abuse are not limited to activities on MiCA-regulated "trading platforms" or even where any crypto-asset service provider is involved. Hence, conduct constituting unlawful insider dealing or market manipulation may be prohibited even if it occurs on a fully decentralised market (e.g. a fully decentralised exchange operating as a smart contract on the Ethereum blockchain). What is important is whether the crypto-assets involved are admitted to any trading platform under MiCA or are under a request for such admission. In a recent document, the European Securities and Markets Authority (ESMA) confirmed this interpretation by referencing "MEV" activities as a potential avenue for market abuse covered by MiCA.[9]

2. *Unlisted crypto-assets with no request for admission made*

MiCA excludes from market abuse provisions assets not admitted to trading platforms or without pending admission requests (*a contrario* Article 86(1)). Interestingly, this exclusion deviates from MAR's approach to market abuse.[10]

MAR considers market abuse possibilities involving non-listed instruments impacting admitted ones. In contrast, MiCA does not expressly address non-admitted assets affecting listed assets. This gap could enable manipulation of listed assets through non–listed assets.

For example, asset-referenced tokens reference other collateral tokens to maintain value stability. If a collateral token is not admitted (or pending admission) and faces manipulation, MiCA seemingly does not address resulting price impacts on the listed reference token. Hence an asset's non-covered collateral could undergo manipulation leading to covered asset price distortions. However, an alternative interpretation exists. Manipulating non-covered asset X to affect covered asset Y could constitute direct manipulation of Y. Manipulation of X may signal false demand for Y or impact Y through the relationship between X and Y. Thereby manipulation of X to manipulate Y could fit the prohibition against disseminating false information to manipulate the market price of crypto-assets.

[7] Art 86(2) MiCA.

[8] See e.g. Koen Lenaerts and José A Gutiérrez-Fons, "To Say What the Law of the EU Is: Methods of Interpretation and the European Court of Justice" (2013) 20 Columbia Journal of European Law 3, 17.

[9] See Section V.1 below.

[10] Recital 10 MAR. See also Art 2(1)(d) MAR.

https://doi.org/10.1017/err.2024.80 Published online by Cambridge University Press

3. Other exclusions—NFTs

The scope of the application of MiCA's rules on market abuse is defined not only by Article 86(1) but also by the general provisions on the scope of MiCA's application, chiefly Article 2. We already noted that Article 2(4)(a) excludes crypto-assets that are financial instruments from the scope of MiCA. Among other exclusions in Article 2(4) are, for instance, "deposits, including structured deposits" and "funds, except if they qualify as e-money tokens."

Here, we wish to highlight the exclusion of "crypto-assets that are unique and not fungible with other crypto-assets" (Article 2(3)), i.e., the exclusion of Non-Fungible Tokens ("NFTs"). Firstly, not all crypto-assets referred to as NFTs in practice may be excluded from the scope of MiCA. As stated in Recital 11:

> The issuance of crypto-assets as non-fungible tokens in a large series or collection should be considered an indicator of their fungibility. (. . .) This Regulation should also apply to crypto-assets that appear to be unique and non-fungible, but whose *de facto* features or whose features that are linked to their *de facto* uses, would make them either fungible or not unique.

Secondly, NFTs that constitute financial instruments are outside the scope of MiCA, but in the scope of MAR.

Nevertheless, even with those qualifications, excluding NFTs may create market integrity issues. NFTs have been subject to certain forms of market manipulation, such as wash sales (wash trading),[11] and insider trading.[12] Wash trading in NFTs reportedly reached a volume of over $30 billion in 2022.[13] This kind of wash trading is normally done by trading NFTs for other, fungible crypto-assets, which may be in the scope of MiCA. The question then arises whether such wash trading could be illegal under MiCA if the NFTs concerned are not on their own in the scope of MiCA. One reason why such wash trading may be outside of the scope is that it could be directed solely at creating false signals about the demand of the out-of-scope NFT asset without manipulating (e.g. by creating appreciable false signals) the in-scope asset. However, if the volume of NFT wash trading is significant enough relative to other trading activity of the non-NFT asset, then perhaps this could constitute market manipulation of the non-NFT asset, irrespective of the intent of those engaged in wash trading.

4. Territorial scope

Like MAR (Article 2(4) MAR), MiCA's Title VI applies "to actions and omissions, in the Union and in third countries with regard to the crypto-assets referred to in paragraph 1."[14] Thus, Title VI applies, in principle, globally. For instance, trading on a centralised exchange outside the EU between persons who are neither EU residents nor EU citizens could still be

[11] Chainalysis, "Crime and NFTs: Chainalysis Detects Significant Wash Trading and Some NFT Money Laundering In this Emerging Asset Class" (2 February 2022) < https://blog.chainalysis.com/reports/2022-crypto-crime-report-preview-nft-wash-trading-money-laundering/ >.

[12] US Attorney's Office, Southern District of New York, "Former Employee Of NFT Marketplace Charged In First Ever Digital Asset Insider Trading Scheme" (1 June 2022) < https://www.justice.gov/usao-sdny/pr/former-employee-nft-marketplace-charged-first-ever-digital-asset-insider-trading-scheme >; James Fanelli, "Ex-OpenSea Worker Found Guilty in First NFT Insider-Trading Case" (The Wall Street Journal, 3 May 2023) < https://www.wsj.com/articles/ex-opensea-worker-found-guilty-in-first-nft-insider-trading-case-6872b4b6 >.

[13] Rosie Perper, "Over $30B of NFT Trading Volume on Ethereum Is Wash Trading, Research Suggests" (*CoinDesk*, 23 December 2022) < https://www.coindesk.com/web3/2022/12/23/over-30b-of-nft-trading-volume-on-ethereum-is-wash-trading-research-suggests/ >; Hildobby, "Ethereum NFTs Wash Trading" < https://dune.com/hildobby/nfts-wash-trading >.

[14] Art 86(3).

https://doi.org/10.1017/err.2024.80 Published online by Cambridge University Press

covered by MiCA's anti-market abuse rules. However, there may be some limitations to the territorial scope. As has been suggested regarding MAR, arguably MiCA should only apply to situations with a "genuine link" to the EU.[15] One way to show that an act or omission outside the EU may have such link with the EU is that it "affects or is likely to affect the price" of a crypto-asset on a trading platform regulated by MiCA or affect any other MiCA-regulated service (in Title V).[16]

III. MiCA's provisions on market abuse

This section discusses MiCA's provisions on market abuse, beginning with issues related to inside information and information on clients' orders, followed by market manipulation, and concluding with the rules on market abuse monitoring, detection and reporting. Examples of actions that would likely violate those provisions are considered in the following section.

1. Inside information

MiCA's rules related to inside information consist of its definition (Article 87), rules on proper disclosure of inside information (Article 88), a prohibition of insider dealing (Article 89), and a prohibition of unlawful disclosure of inside information (Article 90).

a. Definition of "inside information"

"Inside information" is defined in MiCA analogously to how it is defined in MAR:

> (a) information of a precise nature, which has not been made public, relating, directly or indirectly, to one or more issuers, offerors or persons seeking admission to trading, or to one or more crypto-assets, and which, if it were made public, would likely have a significant effect on the prices of those crypto-assets or on the price of a related crypto-asset.[17]

For those "charged with the execution of orders for crypto-assets on behalf of clients" inside information also means information on "the client's pending orders."[18]

As we discuss below, MiCA contains separate rules on the misuse of information about clients" orders by certain categories of CASPs, which do not specify whether they apply only to inside information (Articles 78(2) and 80(3)). This may raise a possibility that those rules apply even to such information related to clients' orders which would not be classified as inside information under Article 87.

Moreover, MiCA did not adopt MAR's institution of insider lists.[19] MiCA also lacks a safeguard clause for legitimate behaviours in the context of insider dealing or unlawful disclosure of inside information.[20] This suggests that the actions that could be classified as insider dealing, or unlawful disclosure of inside information are broader under MiCA than

[15] Marco Ventoruzzo and Sebastian Mock (eds), *Market Abuse Regulation: Commentary and Annotated Guide* (2nd edn, Oxford University Press 2022) B.2.15.

[16] Compare ibid.

[17] Art 87(1)(a) MiCA. Compare Art 7(1)(a) MAR.

[18] Art 87(1)(b) MiCA. Compare Art 7(1)(d) MAR.

[19] Compare Art 18 MAR.

[20] Compare Art 9 MAR.

https://doi.org/10.1017/err.2024.80 Published online by Cambridge University Press

under MAR. Unlike MAR, MiCA lacks provisions excluding some "self-insiders."[21] MAR acknowledges self-inside dealing" exists but considers it, in principle, legitimate behaviour not warranting prohibition.[22] In contrast, under MiCA there is no similar exclusion for self-insiders. This difference may have significant consequences. For example, major DAO governance token holders could trade ahead of likely market-moving DAO decisions they can influence. Someone may know a decision they help make may materially impact an asset's price and trade based on that exclusive knowledge. Absent MAR-style carve-outs, such scenarios arguably constitute insider dealing under MiCA. The lack of self-insider provisions could profoundly affect behaviours previously deemed acceptable. The implications of omitting MAR's conceptual delineation of self-inside information require further examination given crypto governance dynamics.

b. Prohibition of misuse of order information (including front-running)

As quoted above, for CASPs executing orders on behalf of clients, MiCA expressly defines some information related to pending clients' orders as inside information.[23] For this category of CASPs, MiCA also includes a duty to prevent the misuse of information relating to client orders by CASP employees.[24] An analogous duty is imposed on CASPs that receive and transmit orders on behalf of clients.[25]

"Front-running" is the chief example of activity prohibited by those provisions.[26] Front–running takes place when a trusted service provider, like a broker-dealer, uses their knowledge about an order that a client submitted to that service provider to trade ahead of the clients' order.

Interpretative challenges may arise as MiCA does not restrict misuse of order information to *inside* information about orders. There is no explicit cross-reference between provisions on misusing orders (Article 78(2)) and those on inside information on pending orders (Article 87(1)(b)). This raises the question of whether MiCA prohibits misuse of *public* order information by certain CASPs. For example, trading ahead of publicly known DeFi orders is common, and some operators transmitting such orders may qualify as CASPs. However, it is unclear if this would constitute information "misuse."[27]

[21] The "self-insiders" excluded from the prohibition on the use of inside information in Art 9(5) MAR are the ones who use their "own knowledge that [they have] decided to acquire or dispose of financial instruments." Note that even under MAR, "self-insiders" could be liable due to Art 9(6), which turns Art 9(5) into a kind of a rebuttable presumption. The notion of "self-insiders" could also be defined more broadly to cover all who have "autonomously produced the inside information" and use "this inside information for trading"; see Stefano Lombardo, "Some Reflections on the Self-Insider and the Market Abuse Regulation – The Self-Insider as a Monopoly-Square Insider" (2021) 18 European Company and Financial Law Review 2.

[22] Ibid.

[23] Art 87(1)(b) MiCA.

[24] Art 78(2) MiCA.

[25] Art 80(3) MiCA.

[26] The label "front-running" is unhelpfully used in DeFi to refer to a different phenomenon, more accurately described as "trading ahead," because it does not necessarily involve any service provider acting on information about their client's orders. See Mikołaj Barczentewicz, "MEV on Ethereum: A Policy Analysis" (*International Center for Law & Economics White Paper 2023–01-23*, 2023) <https://ssrn.com/abstract=4332703>; Mikołaj Barczentewicz, Alex F Sarch and Natasha Vasan, "Blockchain Transaction Ordering as Market Manipulation" (2024) 20 Ohio State Technology Law Journal 1; Mikołaj Barczentewicz, Alex F Sarch and Natasha Vasan, "Battle of the Crypto Bots: Automated Transaction Copying in Decentralized Finance" (2024) 26 University of Pennsylvania Journal of Business Law 672.

[27] For an argument that trading ahead in DeFi is not necessarily market manipulation, see Barczentewicz (n 26); Barczentewicz, Sarch and Vasan (n 26).

https://doi.org/10.1017/err.2024.80 Published online by Cambridge University Press

The rules on inside information on pending orders and on misuse of order information only apply to CASPs executing or transmitting orders, not those operating platforms.[28] This contrasts with the older rule from Regulation 2017/565 on which MiCA provisions were modelled.[29] Consequently, it is ambiguous if trading based on non-public order information is illegal for other persons. One could argue such order information meets the general definition of inside information (Article 87(1)(a)), but that could render Article 87(1)(b) redundant. Moreover, CASPs handling client orders may be in special positions of trust, distinguishing them from other parties. However, CASPs operating platforms or transmitting orders could be comparably positioned regarding order information.

In any case, Article 66(1) requires all CASPs to act honestly and in clients" best interests. So even if insider dealing prohibitions or information misuse provisions do not apply, overarching conduct standards still constrain CASP behavior regarding client orders.

c. Prohibition of insider dealing

Insider dealing – trading based on inside information – is prohibited in Article 89. Like MAR, MiCA prohibits not only directly engaging in insider dealing but also attempting to engage, recommending that others engage, and inducing others to engage in insider dealing.[30] We consider the implications of this provision below in Section IV.1.

Notably, the scope of the prohibition of insider trading under US law is narrower than the prohibition of insider dealing in EU law, at least under MAR.[31] Under US law, liability for insider trading requires that a breach of a fiduciary duty or "misappropriation" of non-public information occurs. In comparison, no such requirement exists under the EU "parity-of-information" approach.[32] Like in MAR, MiCA's prohibition of insider dealing extends beyond the direct use of inside information, also covering tippers (providers of inside information) and tippees (receivers of inside information).[33] The key condition of liability for a tippee is that they know or ought to know that the tipper's recommendation is based on inside information. Unlike in US law, there is no additional requirement of a breach of fiduciary duty or misappropriation of the information (including a quid pro quo between a tippee and a tipper).

d. Prohibition of unlawful disclosure of inside information

Article 90 prohibits unlawful disclosure of inside information, while Article 88 regulates proper disclosure of inside information. The general principles of disclosure closely follow MAR:[34] informing the public as soon as possible and "in a manner that enables fast access and complete, correct and timely assessment of the information by the public." One

[28] CASPs operating trading platforms are likely to be considered as distinct from the other two categories of CASPs. Compare ESMA's notes on reception and transmission of orders in 'Consultation Paper On ESMA's Opinion on the Trading Venue Perimeter' (2022) ESMA70-156–4978 <https://www.esma.europa.eu/sites/default/files/library/esma70-156-4978_consultation_paper_on_the_opinion_on_trading_venue_perimeter.pdf> [13]–[14].

[29] MiCA's provisions on misuse of order information are modelled on an analogous provision of Art. 67(3) of Regulation 2017/565 supplementing MiFID II. Notably, Regulation 2017/565 includes a recital (110) clarifying the issue of misuses of information relating to a pending client order, whereas no such clarification is included in MiCA. Moreover, unlike the MiCA analogue, the rule on misuse of order information in Regulation 2017/565 explicitly applies to all "investment firms," thus including operators of trading venues, investment advisors, and portfolio managers; see also Annex I, Section A, MiFID II.

[30] Compare Articles 8 and 14 MAR.

[31] See e.g. Ventoruzzo and Mock (n 15) A.2.14, B.10.44-45.

[32] Ibid A.2.17.

[33] Art 8(3)-(4) MiCA.

[34] Art 17 MAR.

https://doi.org/10.1017/err.2024.80 Published online by Cambridge University Press

notable difference is that MAR refers to the officially appointed mechanism for disclosure of information,[35] whereas such mechanisms are not contemplated in MiCA. Like MAR, MiCA tasks the European Securities and Markets Authority (ESMA) with preparation of draft implementing technical standards for disclosure and for delaying of disclosure.[36]

2. Market manipulation

MiCA's prohibition of market manipulation also closely follows MAR in substance, despite editorial differences.[37] What is missing in MiCA in comparison with MAR is a specific prohibition of "transmitting false or misleading information or providing false or misleading inputs in relation to a benchmark."[38] Despite the omission of this example, it can be argued that at least some benchmark manipulation is covered by MiCA, especially by the prohibition of behaviour which "gives, or is likely to give, false or misleading signals as to the supply of, demand for, or price of, a crypto-asset"[39] or the prohibition related to employing a "fictitious device or any other form of deception or contrivance."[40] This interpretation may be particularly relevant for so-called "oracle manipulation" discussed below (Section IV.5). A list of examples that "shall, inter alia, be considered as market manipulation" is included in Article 91(3).

3. Abuse monitoring, detection, and reporting

As indicated in Recital 95, MiCA's approach is to impose lower compliance costs than under the regime applicable to financial instruments. MiCA does not require regulatory reporting of all transactions,[41] but only submitting suspicious transaction and order reports (STOR). Additionally, CASPs that operate trading platforms, as well as any person professionally arranging or executing transactions, are obligated to put in place effective systems, procedures, and arrangements to prevent or detect market abuse.[42]

There may be some confusion regarding who exactly is subject to this duty because Article 92 copied MAR's language referring to persons "professionally arranging or executing transactions," which is inconsistent with MiCA's other terminology.[43] MiCA defines a category of crypto-asset service providers who execute "orders" (not "transactions" like in Article 92) without mentioning "arranging" (of either orders or

[35] Art 21 of Directive 2004/109/EC of the European Parliament and the Council.

[36] Compare Commission Implementing Regulation (EU) 2016/1055 of 29 June 2016 laying down implementing technical standards with regard to the technical means for appropriate public disclosure of inside information and for delaying the public disclosure of inside information in accordance with Regulation (EU) No 596/2014 of the European Parliament and of the Council.

[37] Art 91(2). As to the editorial differences, e.g. MAR contains a separate provision defining market manipulation (Art 12 MAR) and a separate provision prohibiting it (Art 15 MAR).

[38] Art 12(1)(d) MAR.

[39] Art 91(2)(a)(i).

[40] Art 91(2)(b).

[41] Unlike in the case of regulatory transaction reporting under Art 26 MiFIR; Regulation (EU) No 600/2014 of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments and amending Regulation (EU) No 648/2012 (MiFIR).

[42] Arts 76(7)(g) and 92(1) MiCA.

[43] See Art 16(2) MAR and Art 2(1) of the Commission Delegated Regulation (EU) 2016/957 supplementing Regulation (EU) No 596/2014 of the European Parliament and of the Council with regard to regulatory technical standards for the appropriate arrangements, systems and procedures as well as notification templates to be used for preventing, detecting and reporting abusive practices or suspicious orders or transactions (Regulation 2016/957).

https://doi.org/10.1017/err.2024.80 Published online by Cambridge University Press

transactions).[44] In contrast, MAR includes a specific definition of a "person professionally arranging or executing transactions."[45]

In its *Third MiCA Consultation Paper*, covering Article 92, the European Securities and Markets Authority (ESMA) referenced its interpretation of the analogous MAR rule from its *MAR Q&A*. That interpretation stresses that the rules do not cross refer to other definitions of service providers.[46] On ESMA's view, the scope of the relevant MAR rule "is not only limited to firms or entities providing investment services under MiFID."[47] It includes also buy side firms (investment management firms, proprietary traders, direct electronic access providers) and some non-financial firms, for instance, those with trading desks. This interpretation is also consistent with the text of the Regulation 2016/957 on "suspicious transaction and order reports" (STOR), which explicitly refers to trading on own account.[48] Moreover, this interpretation has also been adopted by at least one MAR commentary.[49]

In the cited MiCA *Consultation Paper*, ESMA proposed to read Article 92 as covering both some CASPs and "persons dealing on own account in crypto-assets on a professional basis or as part of their business activity."[50] Before the *Third Consultation Paper* was published, Galea and Furcillo suggested a narrower interpretation, arguing that Article 92 should only apply to CASPs otherwise regulated by MiCA.[51] Their key argument appears to be that because Article 92 only applies to professional activity, it must only apply to CASPs. However, we believe that ESMA's position is better founded.

First, as we argued above and as Galea and Furcillo also accept, MiCA's Title VI has a broader scope than the rest of MiCA and applies to "any person," not only to CASPs and others listed in Article 2(1).[52] Second, neither Article 92, nor even the more detailed MAR definition of a "person professionally arranging or executing transactions" include any reference to the provision of services. The MAR definition refers only to "a person professionally engaged in the reception and transmission of orders for, or in the execution of transactions in, financial instruments."[53] This can be contrasted, for example, with MiCA's narrower concepts crypto-assets services of "reception and transmission of orders for crypto-assets *on behalf of clients*" or "execution of orders for crypto-assets *on behalf of clients*."[54] Of the two concepts: (1) professionally arranging or executing transactions and (2) professionally arranging or executing transactions *on behalf of clients*, the first one is broader than the second and only the first one is to be found in Article 92. Clearly, some professionally arrange or execute transactions on their own account, including non-financial firms with trading desks and so on, as ESMA noted in its *MAR Q&A*'s and as provided for in Regulation 2016/957.

Hence, we agree with ESMA that a better reading of Article 92 is that it covers "persons dealing on own account in crypto-assets on a professional basis or as part of their business

[44] Art 3(16)(e), (g) MiCA.

[45] Art 3(1)(28) MAR.

[46] ESMA, "Draft technical standards and guidelines specifying certain requirements of the Markets in Crypto Assets Regulation (MiCA) on detection and prevention of market abuse, investor protection and operational resilience – third consultation paper" (25 March 2024) < https://www.esma.europa.eu/sites/default/files/2024-03/ESMA75-453128700-1002_MiCA_Consultation_Paper_-_RTS_market_abuse_and_GLs_on_investor_protection_and_operational_resilience.pdf > (Third Consultation Paper); ESMA "MAR Q&A" (version 17, last updated on 15 November 2022), 6.1 < https://www.esma.europa.eu/sites/default/files/library/esma70-145-111_qa_on_mar.pdf >.

[47] Ibid.

[48] Art 7(2)(a) of the Regulation 2016/957.

[49] Ventoruzzo and Mock (n 15) para. B.3.40.

[50] ESMA, "Third Consultation Paper," paras 37–38.

[51] Jonathan Galea and Vincenzo Furcillo, "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 >.

[52] See Section II.1 above.

[53] Art 16(2) MAR.

[54] Arts 2(21) and 2(23) MiCA.

https://doi.org/10.1017/err.2024.80 Published online by Cambridge University Press

activity." *Contra* Galea and Furcillo, this means that some of those who professionally engage in "MEV searching" or "block building" may not only be covered by the general prohibitions on market abuse, but also have the specific duty of market abuse prevention and detection imposed by Article 92.[55]

IV. Key risks of crypto-asset market abuse covered by MiCA

1. Insider dealing and misuse of inside information

a. Private information about the asset or its issuer

One simple kind of insider dealing in crypto-assets, which already has provoked enforcement actions in the United States, is insider dealing in connection to crypto-assets takes place in the context of a listing of an asset on a prominent crypto-asset exchange.[56] An opportunity for illicit gains arises in such a case because it is common that when it becomes public that a crypto-asset will be listed by a well-known exchange, the price of that asset rises significantly. Hence, if someone knows about such a listing announcement before others, they can buy the asset (or tip others to buy) and then sell it after the announcement has its effect on prices.

What is specific to this kind of scenario in crypto-asset markets is that the illicit trading may happen entirely on an on-chain ("decentralised") blockchain exchange.[57] This kind of trading does not guarantee anonymity but requires novel methods of surveillance to identify insider dealing. Also, even if the trading is being done on a centralised exchange, some exchanges may have less mature insider dealing monitoring and detection processes.

Perhaps the best-known enforcement action against this kind of conduct was the successful prosecution of a former employee of the Coinbase exchange by the US Department of Justice[58] and the SEC.[59] The SEC claimed that the former employee ran a scheme with other individuals, whereby he would trade crypto-assets before they were about to be listed on the exchange. This way he exploited access to material inside information, being aware which assets will be listed on the exchange before non-insiders. Another notable example is that, according to press reports, Alameda Research – a hedge fund under common ownership with Sam Bankman-Fried's FTX exchange – likely traded on non-public information about upcoming listings of crypto-assets on FTX.[60]

As we noted earlier, the scope of the prohibition of insider trading under US law is more circumscribed than in EU law.[61] This may suggest that a broader array of cases could be considered as prohibited in the EU, than in the US.

[55] On MEV, see also section V.1 below.

[56] See, e.g. Andrew Verstein, "Crypto Assets and Insider Trading Law's Domain" (2019) 105 Iowa L. Rev. 1; Ester Félez-Viñas, Luke Johnson and Tālis J Putniņš, "Insider Trading in Cryptocurrency Markets" [2022] SSRN <https://ssrn.com/abstract=4184367>.

[57] We put "decentralised" in quotation marks because not all so-called "decentralised exchanges" (DEX) may be fully decentralised in the meaning of MiCA's Recital 22 and hence some DEX-es may be in the scope of MiCA.

[58] US Attorney's Office, Southern District of New York, "Former Coinbase Insider Pleads Guilty In First-Ever Cryptocurrency Insider Trading Case: Ishan Wahi Tipped His Associates Regarding Crypto Assets That Were Going To Be Listed On Coinbase Exchanges" (7 February 2023) < https://www.justice.gov/usao-sdny/pr/former-coinbase-insider-pleads-guilty-first-ever-cryptocurrency-insider-trading-case>.

[59] SEC Charges Former Coinbase Manager, Two Others in Crypto Asset Insider Trading Action (21 July 2022) <https://www.sec.gov/news/press-release/2022-127>.

[60] Stacy Elliott, "Alameda Research Was Frontrunning FTX Token Listings: Report" *Decrypt* (15 November 2022) <https://decrypt.co/114622/alameda-research-frontrunning-ftx-token-listings>.

[61] See above Section III.1.c.

https://doi.org/10.1017/err.2024.80 Published online by Cambridge University Press

b. Information about orders (including front-running)

As discussed above (Section III), MiCA contains two kinds of provisions regarding illicit use of information about pending orders to trade: prohibitions on "misuse" of any (?) such information in Articles 78(2) and 80(3), as well as a prohibition of insider dealing in *private* information about orders. We also mentioned that "front-running" constitutes the chief example of activity prohibited by those provisions.[62]

We are not aware of enforcement actions specifically for this kind of activity in respect to crypto-assets, but some of the allegations against FTX and Alameda Research made by the US CFTC may suggest that this special exchange-hedge fund relationship involved at least an opportunity for misuse of (private) information about orders submitted by FTX's clients. The CFTC alleged that FTX gave exclusively to Alameda faster access to FTX's trading system (to its API), which perhaps may have allowed Alameda to see at least limit orders before any other market participant (i.e. before the existence of such limit orders could have been considered public information).[63] Such an exclusive arrangement should be distinguished from, for example, a trading venue offering collocation services on a non-exclusive basis.

c. More novel issues: insider dealing based on DLT information

A special case of insider dealing worth discussing here is trading based on non–public information which is accessible to some privileged operators in blockchain networks. For example, on the Ethereum network, almost all new blockchain transactions, including those that contain orders to trade crypto-assets, are initially non-public information possessed only by the user who submitted an order and the operator of the server to which the user sends their blockchain transaction.[64] It is at least possible that the operator of that server will use that non–public information, for example, to trade ahead of a large pending order to trade. If not disclosed to and accepted by the customer, this could be analogised to front-running of a customer by a broker–dealer.

MiCA recognises that the use of blockchains may come with new insider dealing challenges. In Recital 96, it explicitly states that factors like "the use of smart contracts for order executions and the concentration of mining pools" should be taken into account in the context of preventing market abuse. Moreover, Article 89(5)(c) provides that the prohibition of insider dealing applies in particular to any person who possesses inside information as a result of "having access to the information through the exercise of an employment, profession duties or in *relation to its role in the DLT or similar technology*" (emphasis added).

The fact that some operators may have privileged access or even exclusive control over routing of user orders creates a possibility for the development of arrangements similar in some ways to "payment for order flow" in traditional finance.[65] Due to technical differences between crypto markets and traditional markets, it may be possible to develop payment for order flow schemes which do guarantee the best execution and benefit customers overall. Thus, this issue warrants further research and debate.

As we discussed above in Section III.1, several questions require further scrutiny, such as the concept of "misuse" of information provided by client orders, the scope of the

[62] See supra, n 26 and the accompanying text.

[63] CFTC v Samuel Bankman-Fried, FTX Trading Ltd, and Alameda Research LLC, <https://www.cftc.gov/media/7986/enfftxtradingcomplaint121322/download> para. 61.

[64] By the server to which the user sends transactions we mean "RPC" services, as described in more detail in Barczentewicz (n 26); Barczentewicz, Sarch and Vasan (n 26). See also Verstein (n 56) 30.

[65] Payment for order flow refers to "a payment that an 'internaliser' makes to a broker in exchange for the broker routing her retail clients' orders to the internaliser, who can then execute trades against those orders"; Barczentewicz (n 26) 21–22.

https://doi.org/10.1017/err.2024.80 Published online by Cambridge University Press

definitions of CASPs engaged in "executing orders for crypto-assets on behalf of clients," and "receiving and transmitting orders for crypto-assets on behalf of clients," as well as whether Article 92 refers to those or other persons. Particularly, it is unclear which, if any, blockchain operators (network participants) could be considered as CASPs subject to obligations related to non-public information.[66] Moreover, it may also be that liability for insider dealing based on private information about pending blockchain transactions could be grounded in the general prohibition of insider dealing and thus attach even to actors who are expressly indicated in MiCA as such.

2. "Rug pulls" and other investment scams

"Rug pull" is a label used in crypto-asset markets for a kind of investment scam, which often directly leverages hidden functions of on-chain applications – that is, smart contracts. According to a compliance services provider Chainalysis, rug pulls amount for a very significant proportion of all stolen or defrauded crypto-assets – 36 per cent ($2.8 billion out of $7.8 billion) in 2021.[67]

A rug pull usually involves creation and promotion of a crypto-asset. Once the asset gains sufficient market value and liquidity, or if sufficient value of assets is sent to a smart contract controlled by the scheme's orchestrators, then the orchestrators perform an "exit scam."[68] For example, the orchestrators may be able to use a hidden function in a smart contract which allows them to withdraw all the locked funds.

What makes detection and prosecution of rug pulls more difficult is that they can happen mostly on on-chain markets.

Hopefully, MiCA will contribute to alleviating the issue of rug pulls through the requirements that it imposes on admitting assets on trading platforms (this assumes that investors will be less likely to invest in assets that are not admitted to MiCA-regulated trading platforms). However, MiCA's anti-market abuse rules may apply to rug pull schemes even if the assets involved are not admitted on any MiCA-regulated trading platform, if a *request for admission* on a trading platform has been made in respect to any such asset (Article 86(1)). If a rug pull scheme affects a crypto-asset in the scope of Title VI MiCA, then the scheme is likely to be classified under Article 91(2)(b) and (c), but given the role of private information, it may also constitute insider dealing (Article 89).

3. Pump-and-dump and trash-and-cash schemes

Pump-and-dump and trash-and-cash schemes are well-known outside of crypto-assets, but they do have some special characteristics in this context.[69] Schematically speaking, a scheme of this sort involves three phases: (1) buying (or shorting) an asset, (2) spreading misleading information to affect the price, (3) selling the asset (or closing a short). Under MiCA, they are likely to constitute market manipulation under Article 91(1)(a)-(b), but they may also violate the prohibition of insider dealing from Article 89.[70]

[66] See Mikołaj Barczentewicz, 'Blockchain Infrastructure Operators Under EU MiCA: Are Miners Regulated?'

[67] Chainalysis, "Crypto Crime Trends for 2022" <https://blog.chainalysis.com/reports/2022-crypto-crime-report-introduction/>. See also Lin William Cong and others, "The Dark Side of Crypto and Web3: Crypto-Related Scams" [2023] SSRN <https://ssrn.com/abstract=4358572>.

[68] See e.g. US Attorney's Office, Southern District of New York, "Two Defendants Charged in Non-Fungible Token ("NFT") Fraud And Money Laundering Scheme" (24 March 2022) < https://www.justice.gov/usao-sdny/pr/two-defendants-charged-non-fungible-token-nft-fraud-and-money-laundering-scheme-0 >.

[69] Felix Eigelshoven, Andre Ullrich and Douglas A Parry, "Cryptocurrency Market Manipulation: A Systematic Literature Review," *International Conference on Information Systems* (2021) 8.

[70] Compare Ventoruzzo and Mock (n 15) 350 fn 19, 412. See also Commission Delegated Regulation (EU) 2016/522, Annex II.

https://doi.org/10.1017/err.2024.80 Published online by Cambridge University Press

The special characteristics of these schemes in crypto-asset markets include, first, the way in which the scheme participants are organising themselves. This takes place on messaging apps like Telegram and WhatsApp. Second, the misleading information is spread on social media[71], for example on Twitter. Third, it may be that all or most of the trading – both by the pump group and by the victims – will be done on on-chain exchanges. And finally, such schemes may be very short-lives – lasting as little as several minutes.[72]

Several particularly widely discussed cases of pumps-and-dumps took place due to the promotional activity on the entrepreneur's John McAfee's Twitter profile in 2017–18. For some of those schemes, the US Commodity Futures Trading Commission successfully prosecuted a McAfee associate.[73] But there were also allegations that some other schemes took place due to someone hacking the McAfee twitter account, without the involvement of McAfee or his associates.[74]

4. Wash trading (wash sales)

Wash trading (wash sales) can be classified as a market practice potentially leading to false or misleading signals and secure prices at abnormal or artificial levels under MiCA 91(1)(a) (analogously to Article 12(1)(a) MAR)[75], as users – or simply one user operating different wallets or accounts – trade the same asset again and again. Perhaps due to the perception that crypto-asset markets are unregulated, wash trading has been a significant phenomenon in those markets.[76] It is true that, to some extent, it may be harder to monitor and detect wash trading on on-chain crypto-asset exchanges, but the difficulty is not insurmountable and good estimates of how much of it is taking place exist. Those estimates suggest a large amount of wash trading: even 30 to 70 per cent of trading volume in some markets.[77] As we noted earlier (see Section II.3), significant wash trading in NFTs has been observed, but it remains an open question which NFTs will be considered in the scope of MiCA.

In a recent example of a wash trading enforcement action, the US Securities and Exchange Commission claimed that a well-known entrepreneur Justin Sun breached US securities regulations by artificially boosting the trading volume of a crypto-asset Tronix (TRX) in the secondary market. Between April 2018 and February 2019, Sun allegedly directed over 600,000 wash trades, involving daily trading of 4.5 to 7.4 million TRX, using accounts he controlled.[78]

[71] Again, see Recital 96 which refers to the use of social media as an element that may have an impact on market abuse.

[72] Eigelshoven, Ullrich and Parry (n 69) 9.

[73] CFTC, "Federal Court Orders Texas Man to Pay Over $290,000 for Manipulative and Deceptive Digital Asset Pump-and-Dump Scheme" (18 July 2022) < https://www.cftc.gov/PressRoom/PressReleases/8558-22 >.

[74] Arnab Shome, "John McAfee Twitter Handle Hack Results in Pump and Dump of Multiple Coins" (28 December 2017) < https://www.financemagnates.com/cryptocurrency/news/john-mcafee-twitter-handle-hack-results-pump-dump-multiple-coins/ >.

[75] Ventoruzzo and Mock (n 15) 411.

[76] Eigelshoven, Ullrich and Parry (n 69) 9. See also Anirudh Dhawan and Tālis J Putniņš, 'A New Wolf in Town? Pump-and-Dump Manipulation in Cryptocurrency Markets' [2022] Review of Finance, forthcoming.

[77] See e.g. Chainalysis, "Can On-chain Data Help Us Spot Fake Exchange Trading Volumes?" (15 November 2019) < https://blog.chainalysis.com/reports/fake-trade-volume-cryptocurrency-exchanges/ >.

[78] SEC, "SEC Charges Crypto Entrepreneur Justin Sun and His Companies for Fraud and Other Securities Law Violations" (22 March 2023) < https://www.sec.gov/news/press-release/2023-59 >; *Securities and Exchange Commission v. Sun* (1:23-cv-02433) < https://www.courtlistener.com/docket/67071330/1/securities-and-exchange-commission-v-sun/ >.

https://doi.org/10.1017/err.2024.80 Published online by Cambridge University Press

5. "Oracle" (inter-trading venue/cross-product) manipulation

Markets for crypto-assets, especially the on-chain or "decentralised" exchanges,[79] involve benchmark mechanisms and other kinds of relations between assets across venues and across different assets. "Oracle" is a name used for software that provides data access or benchmarking mechanisms. This creates opportunities for influencing the price on one market, to profit from the effect on another market.[80]

A notable example is the strategy deployed by Avraham Eisenberg on the Mango Markets service, who is being prosecuted in the US.[81] Reportedly, this involved a successful attempt to raise prices both on off-chain (FTX) and on-chain (Raydium) markets.[82] Eisenberg bought the MNGO token across multiple trading platforms where the oracle received its pricing inputs. By manipulating this benchmark, he was able to affect the operation of a separate product relying on it, and thus drain Mango's resources.[83]

Oracle manipulation often (though not necessarily) involves manipulation of a lending system. According to Recital 94, MiCA "does not address lending and borrowing in crypto-assets." However, we should remember the breadth of the scope of application of MiCA's provisions on market abuse. Hence, inter-trading venue or cross-product manipulation schemes that involve a lending product or arrangement may still violate Article 91's prohibition of market manipulation.

6. Manipulation of trading infrastructure

Crypto-asset markets, and especially on-chain markets, are vulnerable to profit-motivated attacks on the infrastructure. Such manipulative strategies may leverage distributed denial-of-service (DDoS) attacks,[84] 51 per cent attacks,[85] time bandit attacks,[86] or controlling multiple blockchain blocks.[87] The kind of strategy that Avraham Eisenberg reportedly executed against Mark Markets (an "oracle manipulation") may be especially easy and almost risk-free, if the perpetrator can control the contents of several consecutive blocks on a blockchain.[88] A capacity for that is not just theoretical – some actors arguably already possess it, even on Ethereum. To use such an opportunity could constitute a prohibited deceptive contrivance or scheme under Article 91(2)(b).

[79] See supra, n 57.

[80] Barczentewicz (n 26). See also Torgin Mackinga, Tejaswi Nadahalli and Roger Wattenhofer, "TWAP Oracle Attacks: Easier Done than Said?" *2022 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)* (2022) 2.

[81] CFTC, *CFTC Charges Avraham Eisenberg with Manipulative and Deceptive Scheme to Misappropriate Over $110 million from Mango Markets, a Digital Asset Exchange* (9 January 2023), https://www.cftc.gov/PressRoom/PressReleases/8647-23; SEC, *SEC Charges Avraham Eisenberg with Manipulating Mango Markets" "Governance Token" to Steal $116 Million of Crypto Assets* (20 January 2023), https://www.sec.gov/news/press-release/2023-13.

[82] Khor Win, *Insights and Implications of the Mango Squeeze*, CoinGecko (21 November 2022), https://www.coingecko.com/research/publications/insights-and-implications-of-the-mango-squeeze.

[83] Louis Husney, *Mango Markets Madness: A Case Study on the Mango Markets Exploit*, <https://infotrend.com/mango-markets-madness-a-case-study-on-the-mango-markets-exploit/>.

[84] See, e.g., Amir Feder and others, "The Impact of DDoS and Other Security Shocks on Bitcoin Currency Exchanges: Evidence from Mt. Gox" (2018) 3 Journal of Cybersecurity 137; Eigelshoven, Ullrich and Parry (n 69) 10.

[85] Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System" (2008) <https://bitcoin.org/bitcoin.pdf>.

[86] Philip Daian and others, "Flash Boys 2.0: Frontrunning, Transaction Reordering, and Consensus Instability in Decentralized Exchanges" (2019) 2 <https://arxiv.org/abs/1904.05234>.

[87] See, e.g., Mackinga, Nadahalli and Wattenhofer (n 80).

[88] ibid. See also Barczentewicz (n 26) 12–13.

7. Order book manipulation: spoofing, painting the tape and stuffing

Finally, we ought not to forget that centralised exchanges of crypto-assets work in similar ways to analogous trading venues for financial instruments.[89] Thus, potentially manipulative activities like spoofing, painting the tape, and stuffing, may also happen there and be prohibited by MiCA's Title VI, likely Article 91(1)(a).[90] As an example, it has been alleged that one particular actor engaged in spoofing was responsible for significant movements in the price of Bitcoin in 2017.[91]

V. Market practices requiring further study

1. MEV strategies

Among the crypto-asset market practices that require further study, the most prominent are the various "MEV" strategies.[92] MEV is clearly a relatively significant market phenomenon: according to one estimate, in 2022, the volume traded on on-chain exchanges on the Ethereum blockchain was $666 billion. At the same time, the volume of funds involved in MEV extraction was $328 billion – nearly 50 per cent of all trading volume, which was affected in some way, by MEV extraction.[93]

"MEV" originally referred to "maximal" or "miner extractable value." A helpful metaphor for it is a landowner charging rents from those wanting to use their land. Similarly, blockchain validators control piece of blockspace – the blocks which batch transactions. Validators choose which transactions to include and their order of execution. Unlike in traditional finance, there is no natural order for transaction execution in blockchains like Ethereum. Imposing first-in-first-out could negatively impact markets. The lack of natural order means "front-running" (better termed "trading ahead") may not necessarily constitute market abuse. If one controls the block, one can place any transaction ahead of another. Section IV.1 discussed likely abusive trading ahead based on non-public order information – arguably a form of insider dealing. However, trading ahead of publicly observable orders is more legally ambiguous.[94] Any participant can execute such strategies by observing pending transactions. There are other MEV strategies beyond trading ahead, e.g. arbitrage and loan liquidations. Many are likely lawful open market trading activities.

In the *Third Consultation Paper* cited earlier, ESMA referred to MEV in the context of market abuse covered by MiCA, giving an example of a miner or validator using their privileged position to "front-run" a transaction.[95] ESMA's comment is not detailed, and it does not follow from it that ESMA suggested that all MEV activities constitute market abuse. As we mentioned above, given the breadth of the scope of the term "MEV," it is clearly not the case that all activities classified under this label are likely to be market abuse.[96]

[89] Eigelshoven, Ullrich and Parry (n 69) 9–10.

[90] Compare Art 12(1)(a) MAR and Annex I, section A(d)-(f) MAR; see also Commission Delegated Regulation (EU) 2016/522, Annex II.

[91] Bitfinex'ed, "Meet 'Spoofy.' How a Single entity dominates the price of Bitcoin." < https://medium.com/hackernoon/meet-spoofy-how-a-single-entity-dominates-the-price-of-bitcoin-39c711d28eb4 >.

[92] For in-depth literature on legal classification of various MEV strategies, see supra, n 26.

[93] https://twitter.com/EigenPhi/status/1630266577894375425

[94] Barczentewicz, Sarch and Vasan (n 26). See also other references supra, n 26.

[95] ESMA, "Third Consultation Paper," para 19.

[96] See also supra, n 26.

https://doi.org/10.1017/err.2024.80 Published online by Cambridge University Press

2. Buy-back and stabilisation programs

While MAR provides a safe harbour for legitimate buy-back and stabilisation programs, acknowledging their potential market impact and economic purposes, MiCA lacks such provisions. [97] In the crypto context, "buy-back" programs serve various purposes. They may be considered integral to protocol functions,[98] approved by DAO governance,[99] or employed by centralised entities to drive up token prices by reducing circulating supply.[100] In turn, stabilisation programmes aim to facilitate orderly markets by alleviating selling pressures.[101] For example, Curve Finance founder Michael Egorov provided liquidity to repay some decentralised loans collateralised by the CRV token to avoid liquidations cascades.[102] His actions aimed to stabilise CRV's price after code exploit drained supply.[103]

While we make no judgment on the lawfulness of any specific case, both buy-backs and stabilisation programmes may raise questions regarding the liability for market manipulation under Article 91(2)(a)(i) MiCA. This provision prohibits creating "false or misleading signals as to the supply of, demand for, or price of, a crypto-asset." Stabilisation programmes, in particular, could be seen as creating such signals by relieving market pressure that would otherwise reflect the natural interplay of supply and demand. When someone in a privileged position, like an issuer, tries to counteract this pressure – especially using privileged tools like inside information – it could be considered an attempt to give a "false or misleading" signal.

There are a few difficulties in applying this theory of liability to crypto-asset buy-back and stabilisation programmes. They include whether DAOs qualify as legal "persons,"[104] if a look-through approach applies, and which DAO members could be liable.

The differences with MAR we discuss here do not entail illegality for crypto-assets buy-back and stabilisation programmes. However, MiCA's lack express carve-outs may lead to heightened scrutiny of those practices, market uncertainty and over-compliance. Further examination is needed regarding, for instance, when price stability may call for buy-backs and what disclosure practices should be adopted.

3. Burning mechanisms

Burning mechanisms are usually coupled with "buy-back" programmes. Burning is the process by which a crypto-asset is permanently removed from circulation.[105] As a result,

[97] See Art 5(2) and (4).

[98] See, for example, Frax and its protocol implementation for buy-back of FXS: "(. . .) Frax Protocol will use Fraxswap for: buying back and burning FXS with AMO profits, minting new FXS to buy back and burn," <https://docs.frax.finance/fraxswap/technical-specifications>.

[99] See, for example, Maker DAO's Smart Burn Engine, which allocates excess DAI stablecoins from Maker's surplus buffer to purchase MKR, <https://forum.makerdao.com/t/introduction-of-smart-burn-engine-and-initial-parameters/21201>.

[100] Binance Coin Whitepaper, <https://www.exodus.com/assets/docs/binance-coin-whitepaper.pdf>; Philipp Schulz "Buyback-and-burn: How it works and why it's effective," <https://medium.com/invao/buyback-and-burn-how-it-works-and-why-its-effective-cb2c7d9b9297>.

[101] See Art 3(2)(d) MAR and Recital 6 of Commission Delegated Regulation EU no. 2016/1052 of 8 March 2016.

[102] Curve's Egorov turns to notable counterparties to bail out his DeFi positions <https://blockworks.co/news/curve-egorov-exit-defi-positions>.

[103] Vulnerability in Curve Finance Vyper Code Leads to Multi-Million Dollar Hack Affecting Several Liquidity Pools <https://blog.chainalysis.com/reports/curve-finance-liquidity-pool-hack>.

[104] For a discussion of DAO classification as general or civil partnerships, see António Garcia Rolo, "Challenges in the legal qualification of Decentralised Autonomous Organisations (DAOS): The rise of the crypto-partnership" <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3417900>.

[105] By being sent to a "burn" address, which makes it impossible for anyone to control them; Darcy Allen, Chris Berg and Sinclair Davidson, "Buyback and Burn Mechanisms: Price Manipulation or Value Signalling?" <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4231845>.

https://doi.org/10.1017/err.2024.80 Published online by Cambridge University Press

token holders who didn't participate in the buy-back own a larger proportion of the total supply without changing their token count. The economic nature of burning is in a way similar to the cancellation of shares in a company, which also may accompany buy-back and stabilisation programmes in traditional markets. There is some controversy to what extent, if at all, burning affects prices over and above the effect of the associated buy-backs.[106] But if burning does affect prices, then like buy-backs, it could be considered as giving a "false or misleading" signal and thus constitute market abuse under Article 91(2)(a)(i) MiCA. Nevertheless, just like with buy-backs and stabilisation, there may be good economic arguments for considering burning as legitimate under some circumstances.[107] Moreover, it may be worth considering, for future legislation, applying to crypt-asset burning some of the features of the legal rules applicable to the cancellation of shares.

VI. Conclusions

The crypto-asset market is sometimes seen by its participants as the wild west, where laws do not, or should not, apply. From this perspective, market integrity could only be ensured by technical and self-regulatory solutions. Although non-state solutions have merits, the EU legislator decided legal intervention was needed to ensure market integrity, hence MiCA's Title VI.

By largely replicating MAR, MiCA created "new wine in old bottles" problems, since crypto-assets present novel challenges while the legislator decided to address them with a subset of old tools. For instance, the absence in MiCA of MAR's definition of "persons professionally arranging or executing transactions" creates uncertainty about which entities are subject to the duty to monitor and report market abuse under Article 92. Similarly, prohibitions on misuse of information about client orders in Articles 78(2) and 80(3) raise questions of whether they apply only to inside information as defined in Article 87 or more broadly. The different technical features and common practices of crypto-asset markets, such as on-chain order execution and the lack of a natural order for transactions on blockchains, make it ambiguous how concepts like front-running and market manipulation apply. Strategies like MEV extraction, which are specific to crypto-asset markets, are difficult to fit into the market abuse categories defined based on traditional financial markets.

Overall, the extent to which DeFi activities will lead to liability for breaches of MiCA's anti-market abuse provisions remains unclear, especially regarding various blockchain network participants. Classifying MEV strategies as market abuse may be particularly difficult.

Moreover, there are potentially significant differences between MiCA and MAR beyond the issues arising from the novel features of markets in crypto-assets. As we discussed, MAR includes safe-harbour provisions, which are absent in MiCA, like that for self–insiders and for buy-back and stabilisation schemes. Should this exclusion mean a stricter approach under MiCA? In the case of buy-backs, we suggested that this is not necessarily the case: buy-backs and stabilisation may still constitute trading for a "legitimate reason." However, a safe-harbour may be important for providing clarity and thus preventing a chilling effect on legitimate market behaviour. So, the absence of a safe-harbour – especially in the context of its presence in MAR – may create that chilling effect, irrespective of what legal interpretation may suggest.

[106] See Joel Monegro, "Stop Burning Tokens – Buyback and make instead," <https://www.placeholder.vc/blog/2020/9/17/stop-burning-tokens-buyback-and-make-instead>.

[107] Darcy Allen and others (n 92).

https://doi.org/10.1017/err.2024.80 Published online by Cambridge University Press

To some extent, ESMA may address those issues in their draft regulatory technical standards (e.g. under Articles 88(4) and 92(2)) and guidance may come from national authorities, but some questions will likely be left for scholars, practitioners, and eventually the courts.

Acknowledgment. The authors thank Natasha Vasan for comments and discussion.

Competing interests' declaration. The first author received an Ethereum Foundation grant, which is indirectly related to this paper.

Cite this article: M Barczentewicz and A de Gândara Gomes, "Crypto-Asset Market Abuse Under EU MiCA". *European Journal of Risk Regulation.* https://doi.org/10.1017/err.2024.80