Blockchain for Europe Response to ESMA's consultation on certain requirements in the Markets in Crypto Assets Regulation (MiCA) on detection and prevention of market abuse, investor protection and operational resilience – third consultation paper

Q1 Do you agree with ESMA's analysis on the personal scope of Article 92 of MiCA? Are there other types of entities in the crypto-asset markets that should be considered as a PPAET (e.g. miners/validators)? Do you believe that CASPs providing custody and administration of crypto-assets on behalf of clients should also be considered as PPAETs for the purpose of this RTS? Please elaborate.

As Blockchain for Europe (BC4EU), we appreciate the opportunity to respond to ESMA's consultation on its Draft RTS related to the prevention of market abuse. While we agree with the goal of preventing market abuse in crypto-markets, we have concerns about ESMA's references to certain activities. Thus, our response focuses on questions related to Maximum Extractable Value (MEV), which is crucial for blockchain networks' functionality and sustainability. We note that many CASPs, operating in centralised environments, are unsuitable for monitoring MEV, as it does not occur in such settings. Therefore, it is neither proportionate nor appropriate to consider miners or validators as professional participants in the crypto-asset ecosystem (PPAETs) and subject them to market surveillance obligations under MiCA.

Expanding the obligations of Article 92 of MiCA to include entities like miners or validators could lead to unintended consequences. Validators typically do not know the transactions in their blocks before committing to them, making it impractical to ensure no market abuse occurs. This could drive such entities out of the market, reducing decentralisation and creating inefficiencies in crypto-asset transactions processing. Moreover, individual validators running software from their homes would face disproportionate burdens compared to entities captured by traditional financial regulations, inhibiting decentralisation, individual participation, and innovation. It would be akin to requiring a restaurant's cooking team to make judgments about each customer's order based on their health and dietary needs, which is impossible. Therefore, imposing these obligations on miners and validators is not feasible and would hinder the positive aspects of blockchain ecosystems.

ESMA's Categorization of MEV as Market Abuse

In paragraph 19, ESMA notes that MiCA indicates the potential for market abuse through activities like Maximum Extractable Value (MEV), where miners or validators reorder transactions to front-run specific trades for profit. However, we believe that categorizing all types of MEV activities as market abuse is misleading and inaccurate. ESMA provides no evidence of pervasive harm, fails to discuss market forces that mitigate MEV's effectiveness, and does not acknowledge differences in MEV practices across blockchains. While some types of MEV are indeed extractive and harmful, many forms of MEV promote healthy market functioning and efficiency.

As always, when dealing with new concepts and activities, it is important to ensure there is a clear and common understanding of such concepts. This is why initiatives like the "MEV Fair Market Principles" being developed by the Proof of Stake Alliance (POSA) are crucial to ensure a core understanding of these key concepts across the industry and among regulators. POSA's set of definitions and principles around MEV are a great resource and starting point to understand MEV, as their paper seeks to explain how block construction on public blockchains works, as well as the various incentives that motivate behavior in the market for blockspace. The paper is now open for public consultation and input from other industry players, as consistent and informed practices industry-wide will ultimately help to ensure blockchain networks are not only secure and efficient but also safe.

Distinguishing Good MEV from Adversarial MEV

Good MEV includes activities such as enabling arbitrage between decentralized exchanges (leading to price convergence), facilitating quick liquidations to protect lenders, and generally reducing gas costs. Adversarial MEV, on the other hand, includes sandwich attacks (where a bot places orders before and after a victim's trade to extract value), time-bandit attacks (involving block reorganization for personal gain), and using inside information from dark pools or private mempools. It is generally accepted that without the beneficial forms of MEV, decentralized markets would be far less efficient. Given the difficulty in clearly defining and identifying all forms of adverse MEV that constitute market abuse, ESMA should clarify that not all forms of MEV are inherently manipulative. For instance, nearly 50% of all trading volume on decentralized exchanges in 2022 was influenced by MEV extraction. It is crucial for the development and optimization of crypto markets to maintain flexibility in transaction ordering without broadly labeling it as market abuse. We respectfully ask ESMA to provide evidence regarding specific MEV activities considered market abuse, considering factors like the intent behind the MEV, the information advantages used, and the impact on market efficiency and integrity.

Q2 Do you agree with the proposed elements that should constitute appropriate arrangements, systems and procedures to detect and prevent market abuse? If not, please specify the article of the draft RTS and elaborate.

BC4EU acknowledges the necessity of establishing effective arrangements, systems, and procedures to detect and prevent market abuse within the framework of MiCA. However, we have substantial concerns regarding several proposed elements outlined in the draft RTS, which we believe could impose disproportionate burdens on entities within the blockchain industry.

Firstly, a critical issue lies in the inclusion of validators and miners under stringent market surveillance compliance obligations. These entities play crucial roles in blockchain ecosystems by validating transactions and securing networks. However, the nature of their activities, such as Market Extractable Value (MEV), which encompasses various order-sequencing activities, differs significantly from traditional market abuse scenarios in centralised financial markets.

MEV, while sometimes associated with negative behaviours like "sandwich attacks," is also integral to enhancing network participation and transaction efficiency in decentralised finance (DeFi) environments. For instance, MEV can help resolve price discrepancies across different protocols, contributing to more accurate pricing and tighter spreads for users. Requiring validators and miners to monitor and report on MEV-related activities would not only impose unnecessary regulatory burdens but also hinder the development and optimization of blockchain technologies.

The broad definition of entities subject to extensive monitoring systems poses significant practical challenges, particularly for smaller crypto firms. These firms may lack the resources to develop and maintain sophisticated systems capable of real-time analysis, order book data replay, and detection of potential market abuse. For example, implementing systems capable of analysing historical transaction data and generating alerts for suspicious activities across decentralised platforms can be prohibitively complex and resource-intensive.

Moreover, the requirement to include aspects of DLT operations in STORs introduces additional complexities. Blockchain transactions are inherently transparent and decentralised, making it impractical to pinpoint the precise location or IP addresses of validators or miners involved in potential market abuse. Such requirements could lead to a disproportionate regulatory burden without commensurate benefits in enhancing market integrity.

Finally, we are also concerned about the extensive personal information potentially required in STORs, such as detailed client information and employment details. This raises significant privacy issues without clear evidence that such information would significantly aid in detecting or preventing market abuse in blockchain contexts. Moreover, the practicality of collecting and securely managing such sensitive data poses challenges, particularly in decentralised environments where maintaining confidentiality and preventing unauthorised access are paramount.