|  |
| --- |
| Reply form to the Consultation Paper on 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 |
|  |

**Responding to this paper**

ESMA invites comments on all matters in this consultation paper and in particular on the specific questions. Comments are most helpful if they:

* respond to the question stated;
* indicate the specific question to which the comment relates;
* contain a clear rationale; and
* describe any alternatives ESMA should consider.

ESMA will consider all comments received by **25 June 2024.**

**Instructions**

In order to facilitate analysis of responses to the Consultation Paper, respondents are requested to follow the below steps when preparing and submitting their response:

1. Insert your responses to the questions in the Consultation Paper in the present response form.
2. Use this form and send your responses in Word format (**pdf documents will not be considered except for annexes**);
3. Please do not remove tags of the type <ESMA\_QUESTION \_MIC4\_1>. Your response to each question has to be framed by the two tags corresponding to the question.
4. If you do not wish to respond to a given question, please do not delete it but simply leave the text “TYPE YOUR TEXT HERE” between the tags.
5. When you have drafted your response, name your response form according to the following convention: ESMA\_MIC4\_nameofrespondent\_RESPONSEFORM. For example, for a respondent named ABCD, the response form would be entitled ESMA\_MIC4\_ABCD\_RESPONSEFORM.
6. Upload the form containing your responses, **in Word format**, to ESMA’s website (www.esma.europa.eu under the heading “Your input – Open Consultations” -> Consultation Paper on guidelines on conditions and criteria for the classification of crypto-assets as financial instruments”).

**Publication of responses**

All contributions received will be published following the close of the consultation, unless you request otherwise. Please clearly and prominently indicate in your submission any part you do not wish to be publically disclosed. A standard confidentiality statement in an email message will not be treated as a request for non-disclosure. A confidential response may be requested from us in accordance with ESMA’s rules on access to documents. We may consult you if we receive such a request. Any decision we make not to disclose the response is reviewable by ESMA’s Board of Appeal and the European Ombudsman.

**Data protection**

Information on data protection can be found at [www.esma.europa.eu](http://www.esma.europa.eu) under the heading [Legal Notice](http://www.esma.europa.eu/legal-notice).

**Who should read this paper**

# All interested stakeholders are invited to respond to this consultation paper. In particular, ESMA invites crypto-assets issuers, crypto-asset service providers and financial entities dealing with crypto-assets as well as all stakeholders that have an interest in crypto-assets.

**General information about respondent**

|  |  |
| --- | --- |
| Name of the company / organisation | Kiln SAS |
| Activity | Non-financial counterparty |
| Are you representing an association? |[ ]
| Country/Region | France |

**Questions**

1. 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.

<ESMA\_QUESTION\_MIC4\_1>

We strongly support market abuse prevention and detection to ensure market integrity and consumer protection outcomes are met. However we are concerned that the Consultation implies that Maximum Extractable Value (MEV) is inherently abusive and seeks to combat market abuse through disproportionate measures which in many instances will be impossible to comply with if miners, validators and custodians are bought within scope, and will not achieve the desired policy outcomes. **We urge ESMA to:**

* **clarify that MEV is not inherently abusive and should not in many instances result in the filing of a STOR** and
* **ensure that miners, validators and custodians are not brought within PPAET scope** **with ongoing market surveillance obligations**

A phased and proportionate approach should be taken in relation to market abuse prevention and ongoing monitoring requirements (for example when it comes to CASP assessment and treatment of MEV). Failure to do so will result in negative impacts for the European market including worse execution outcomes for users and inhibiting innovation, growth, regulatory oversight and therefore consumer protection within the EU market, as activity is pushed offshore.

**MEV is not inherently abusive**

In paragraph 19 of the consultation, ESMA notes that ‘*MiCA is clear when indicating that orders, transactions, and other aspects of the distributed ledger technology may suggest the existence of market abuse e.g., the well-known Maximum Extractable Value (MEV) whereby a miner/validator can take advantage of its ability to arbitrarily reorder transactions to front-run a specific transaction(s) and therefore make a profit.*’

**MEV is a nuanced term that refers to the value that can be extracted from block production in addition to the standard gas fees, by including, excluding, or ordering transactions within a block.** It can result in many benefits for market structure and users alike and in only certain instances result in negative outcomes. Common examples of positive outcomes include arbitraging swaps on decentralized exchanges or identifying opportunities to liquidate DeFi positions. **Failure to accommodate non toxic MEV would have a significant impact on the security, efficiency and economics of a network.** It is, in the main, a positive outcome of the architecture of decentralized systems’ technical and economic architecture.

It will be critical for more research to be done and a clear taxonomy created for “non-toxic” healthy MEV vs “toxic” or market abusive MEV. The defining toxic vs non-toxic MEV is still an ongoing discussion and research topic within the Ethereum community. The Ethereum community recognizes the importance of addressing toxic MEV and is actively engaged in devising solutions. In addition, there are a number of arguments that MEV “frontrunning”, is not in itself abusive nor would it be illegal in traditional markets the way it is conducted on blockchains today. This is because in a blockchain environment “front running” is equivalent to “trading ahead” but does not rely on non-public information and therefore does not breach a duty to a client or use of non-public information to ill effect (<https://www.barczentewicz.com/papers/MEV_Response_to_IOSCO_2023.10.19.pdf>). We wanted to highlight this paper by Proof of Stake Alliance (POSA) which highlights key MEV principles (<https://www.proofofstakealliance.org/posa-mev-principles>), and we urge ESMA to continue their engagement with the wider community and research discussions on this important topic before a regulatory position on MEV is taken.

**MEV is an inherent feature of decentralised public blockchain design**

MEV capabilities arise owing to market microstructures, enabled by public blockchain design. It is therefore necessary to consider two junctures when it comes to blockchain transactions and value extraction 1/ Execution of a transaction when a block is created (eg. gas fees), and 2/ Transaction ordering within a block (eg MEV).

It is critical to highlight that there is no baseline order or set “queue” in which transactions are included within a block. Instead, “sequencers” eg validators or blockbuilders, have access to a set of pending transactions, and transactions are then selected for inclusion in a block based on competitive “fee” weighting. As there is no inherent ordering for transaction within a block this technology facilitates a way for participants and users alike to benefit from ordering or sequencing that enables the most value to be extracted (see below for benefits).

**MEV, in many instances, leads to beneficial user outcomes**

Examples of benefits offered by the market microstructure enabled by MEV include:

* Aiding price discovery, **creating more efficient markets** across centralised and DEX platforms, across chains and tapping into other off-chain liquidity sources such as private counterparties - creating tighter spreads across various networks and enabling users to access the prices and liquidity of off-chain venues while staying on-chain
* Enabling **arbitrage** between decentralized exchanges leading to **price convergence**
* Enabling **liquidations to happen more quickly to protect lenders**
* **Reducing gas costs**, **transaction latency, conditional transaction execution** and offering  the possibility of strengthening security (via distributed participation in the network).
* Enabling user optionality to **access faster transaction execution** (particularly beneficial for high frequency traders / more price-insensitive users). Options to avoid market slippage are available in wallets and dApps, so users can elect to execute their transactions without “slippage” protection by paying  a higher execution price, as an alternative to setting high gas fees.
* Providing **end users rebates**, in certain instances, where a portion of rewards received by participants such as searchers are passed back to the end user.

In general it is broadly accepted that without non-toxic MEV many decentralised market efficiency gains would be lost (including making price discovery even more difficult with very different prices from one venue to another resulting in a lot of uncertainty as to the real price of tokens). It is therefore critical that MEV is not treated as a blanket term denoting market abusive activity but instead that a more nuanced approach is taken considering relevant factors could include the intent behind the MEV, the information advantages employed, and the effects on market efficiency and integrity. We stand ready to support ESMA and other regulators and policymakers in this endeavor to help provide further market insights and developments on this important topic.

**Ongoing surveillance and reporting obligations in relation to market abuse should sit with CASPs (specifically brokers/exchanges) and not validators, miners and custodians**:

We generally agree market intermediaries (e.g. brokers and exchanges) are best placed to observe and therefore report suspicious market abuse activity on a proportionate basis (although for reasons discussed below we do not think it is possible for these obligations to extend to MEV monitoring and STOR reporting). We urge ESMA to ensure that validators, miners and custodians remain out of scope of Art. 92 and PPAET scope.

**1/ Validators and miners do not meet the definition of PPAET** as they validate transactions they do not execute transactions on the instructions of a user. They are not CASPs under MiCA and do not technically directly “arrange or execute crypto-assets transactions” (Art 92, MiCA), a necessary tenant for the obligation to arise. Their primary function is technical and operational in nature, to ensure the security and integrity of the network. They do not hold, manage or transfer assets on behalf of others, execute instructions or have direct relationships with end users.

**2/ Including validators and miners within PPAET scope would not achieve the desired policy outcome** of protecting consumers and market integrity by preventing market abuse as in many instances it will be **impossible to comply with and highly disproportionate to the risks posed** for the following reasons.

Validators will not be privy to the relevant data required to assess whether toxic MEV has been executed (this is further complicated by the fact there is no current consensus as to what is defined as toxic MEV). It is therefore not possible to conclude whether an action amounts to abusive behaviour. Validators will not have access to the majority of information required for a STOR due to blind signature and proposer-builder separation: the proposer (or validator) only receives the header of the block from the relayer, and can only see the content and the transactions inside it after signing the header. Even if it was possible through extensive blockchain analytics to access relevant information to file a STOR, it will result in a flood of ineffectual STOR reports that are only partially complete (given limitations in accessing necessary information), as blocks are created every ~12 seconds. This will detract resources away from combating true market abuse. Furthermore, different protocols have different consensus mechanisms so it would be impossible to deploy a blanket approach to detecting and reporting abuse, therefore increasing levels of complexity. For validators and miners to establish and maintain market surveillance programs it would be highly costly and resource intensive and will unlikely uncover abusive practices (given information limitations).

Further, the decentralised nature of the technology will make it impossible to determine which validators / miners and which transactions should be captured within the regulatory perimeter as it will be highly impractical and in some instances impossible to know the precise location or IP addresses of validators or miners within the EU and/or the location of the end users. Further, in some instances validators are fully decentralised and controlled by multiple operators across a number of different jurisdictions, an implementation called Distributed Validators Technology.

Bringing these types of participants within the scope of market surveillance obligations, could also have the undesired effect of pushing validator/miner activity offshore, weakening regulatory oversight and consumer protection with detrimental impact on innovation within EU digital asset market infrastructure.

**MEV involves a wide range of participants**

We urge ESMA to work with industry to map the different types of MEV and risk profiles and participants involved before taking steps to place regulatory burdens on certain participants.

Outlined below are the key participants involved in a transaction within a block, with a high-level description of the value they provide to the network, in the context of the Ethereum blockchain:

Wallets and dApps, the main access points for end users interacting on decentralised networks, compete on (1) optimal execution and (2) end users fees. When users express an intent to perform an action on a decentralised network (e.g. spot trade, buy an NFT, deploy assets on a lending protocol), the wallet or dApp submits the transaction to a memory pool (mempool), where searchers will look for the optimal ordering of transactions.

There are currently two types of mempools:

* **Public mempool** - The public mempool is a default implementation of Ethereum and is a list of pending transactions (publicly available) waiting for validation from a node before it is committed to a block on the blockchain.
* **Protected/Private mempool** - The protected (also called “private”) mempool is where access is only given to searchers who agree to reordering transactions in a way that does not have a negative impact on a given target transaction (i.e. non-toxic MEV). Searchers gain access to the transaction order flow from private pools through an order-flow auction (OFA), aggregating user transactions into a market where searchers can assess the value of including specific transactions based on the fees users are willing to pay and the intrinsic value of their transactions, and the builders’ ability to meet those intents. Searchers get access to private mempools based on criteria decided by the private mempool and bid through a first-price sealed-bid auction. It is important to note that end users may benefit directly from this process by getting a part of the auction price paid by the searcher to the OFA.

Searchers will then find the optimal sequence of transactions found in the public mempool and protected mempools they have access to. This sequencing results from arbitrage opportunities found in connecting various liquidity sources (DEX, CEX, private counterparties, cross-chain arbitrage) and submit a new transaction to be exposed to a part of the value created, as a fee for the re-ordering proposed. The submitted result found by a searcher is called a bundle.

Then, block builders compete to combine bundles (using bundle merging algorithms) in the most efficient way and create the block with the most value for the network, and send their blocks to relayers as a finalised block. Relayers compare the blocks built by builders and choose the most efficient one, and finally send it to the proposer (validator) chosen by the network to push the block.

It is important to note that the proposer doesn’t know the content of the block until after the block is created (having pushed it to the network). This concept is called “proposer-builder separation” (currently implemented on top of the Ethereum protocol) and enables higher consensus-layer security since proposers would have no incentive to rewrite past blocks (a threat previously identified as a “time-bandit attack”) as they have already validated the most efficient block as found by a set of highly specialised players (namely builders and relayers), and also since proposers have no ability to re-order a transaction within a block and include their own transaction due to this ability sitting upstream with searchers and block builders.

The market microstructure relies on order competition at several layers (mempools, searchers, block builders, relayers) to provide users with optimal execution by abstracting away the complexity of accessing and optimising blockspace, and sharing part of the efficiencies found through better execution conditions through user rebates.

**CASPs providing custody and administration of crypto assets should not be subject to market surveillance obligations under MiCA**

A custodian or administrator's role does not involve managing or executing trade transactions. These participants do not interact with the market dynamics in a way that could influence market integrity or transparency. They are therefore not best placed to observe or report on market abuse. Whilst it is appropriate for brokers and exchanges to be subject to broader market surveillance observations, it is worth noting that many CASPs operate in a centralised manner. In a centralised off chain environment, MEV does not occur and as such it would be not possible or relevant for CASPs to monitor it. We would therefore suggest a phased and proportionate approach should be taken in relation to market abuse prevention and ongoing monitoring requirements (for example when it comes to CASP assessment and treatment of MEV).  A better outcome would be to increase education around MEV and integrate tools that decrease levels of malicious MEV activity.

<ESMA\_QUESTION\_MIC4\_1>

1. 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.

<ESMA\_QUESTION\_MIC4\_2>

TYPE YOUR TEXT HERE

<ESMA\_QUESTION\_MIC4\_2>

1. Do you agree with the proposed STOR template as presented in the Annex of the RTS?

<ESMA\_QUESTION\_MIC4\_3>

TYPE YOUR TEXT HERE

<ESMA\_QUESTION\_MIC4\_3>

1. Is there any parameter or naming convention that in your view should be modified to facilitate the identification of suspicious orders/transactions/behaviours involving crypto-assets?

<ESMA\_QUESTION\_MIC4\_4>

TYPE YOUR TEXT HERE

<ESMA\_QUESTION\_MIC4\_4>

1. In Section II of the Annex, would the concept of ‘location’ be applicable to a distributed ledger? For instance, would the IP address of miners/validator nodes in the network be useful in a context where it can be masked through VPNs?

<ESMA\_QUESTION\_MIC4\_5>

TYPE YOUR TEXT HERE

<ESMA\_QUESTION\_MIC4\_5>

1. Is there any other element or information relevant to crypto-asset markets that in your view should be included in the template? Please explain.

<ESMA\_QUESTION\_MIC4\_6>

TYPE YOUR TEXT HERE

<ESMA\_QUESTION\_MIC4\_6>

1. Please provide information about the estimated costs and benefits of the proposed technical standard, in particular in relation to the arrangements, systems and procedures to prevent and detect market abuse.

<ESMA\_QUESTION\_MIC4\_7>

TYPE YOUR TEXT HERE

<ESMA\_QUESTION\_MIC4\_7>

1. Do you agree with ESMA’s approach regarding consistency between the MiCA and MiFID II suitability regimes? If you think that the two regimes should diverge, where and for which reasons?

<ESMA\_QUESTION\_MIC4\_8>

TYPE YOUR TEXT HERE

<ESMA\_QUESTION\_MIC4\_8>

1. Do you think that the draft guidelines should be amended to better fit crypto-assets and the relevant crypto-asset services? In which regard? Please justify your answer.

<ESMA\_QUESTION\_MIC4\_9>

TYPE YOUR TEXT HERE

<ESMA\_QUESTION\_MIC4\_9>

1. Do you agree with the approach followed by ESMA regarding periodic statements provided in relation to portfolio management of crypto-assets?

<ESMA\_QUESTION\_MIC4\_10>

TYPE YOUR TEXT HERE

<ESMA\_QUESTION\_MIC4\_10>

1. Do you agree with the approach taken by ESMA in the draft guidelines for crypto-asset service providers providing transfer services for crypto-assets on behalf of clients as regards procedures and policies, including the rights of clients? Please also state the reasons for your answer.

<ESMA\_QUESTION\_MIC4\_11>

TYPE YOUR TEXT HERE

<ESMA\_QUESTION\_MIC4\_11>

1. Do you think that the draft guidelines address sufficiently the risks for clients related to on- and off-DLT crypto-asset transfers? Please justify your answer.

<ESMA\_QUESTION\_MIC4\_12>

TYPE YOUR TEXT HERE

<ESMA\_QUESTION\_MIC4\_12>

1. Are there any additional comments that you would like to raise and/or information that you would like to provide, for example, on whether other relevant points or clients’ rights should be considered?

<ESMA\_QUESTION\_MIC4\_13>

TYPE YOUR TEXT HERE

<ESMA\_QUESTION\_MIC4\_13>

1. Do you support ESMA’s interpretation of the term, ‘systems’ in the mandate? If not, please explain your understanding of the term (and provide examples if possible).

<ESMA\_QUESTION\_MIC4\_14>

TYPE YOUR TEXT HERE

<ESMA\_QUESTION\_MIC4\_14>

1. Are there other ‘appropriate Union standards’ beyond those identified in the consultation paper that you consider relevant for this mandate? If yes, please list them and provide a rationale for why they would be relevant.

<ESMA\_QUESTION\_MIC4\_15>

TYPE YOUR TEXT HERE

<ESMA\_QUESTION\_MIC4\_15>

1. Do you agree with the inclusion of minimal administrative arrangements in Guideline 2 (i.e., no reference to implementing a risk management framework)? If no, please explain whether you would consider either *fewer* or *more* administrative arrangements appropriate.

<ESMA\_QUESTION\_MIC4\_16>

TYPE YOUR TEXT HERE

<ESMA\_QUESTION\_MIC4\_16>

1. Do you support the inclusion of Guideline 5 on ‘cryptographic key management’? Do you consider cryptographic keys relevant as either a ‘system’ or a ‘security access protocol’? Is this guideline fit for purpose (i.e., can cryptographic keys be ‘replaced’ as implied in paragraph 29 of the draft guidelines)?

<ESMA\_QUESTION\_MIC4\_17>

TYPE YOUR TEXT HERE

<ESMA\_QUESTION\_MIC4\_17>