|  |
| --- |
| 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 | BCAS |
| Activity | Audit/Legal/Individual |
| Are you representing an association? |[ ]
| Country/Region | Malta |

**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>

ESMA's analysis rightly extends the scope to include crypto-asset service providers (CASPs) operating a trading platform as persons professionally arranging or executing transactions (PPAETs). Moreover, the inclusion of CASPs providing services of reception or transmission of orders for crypto-assets on behalf of clients and/or execution of orders for crypto-assets on behalf of clients is aligned with the interpretation of the definition of persons professionally arranging or executing transactions (PPAETs) under MAR’s Article 3(28).

However, the inclusion of CASPs providing custody and administration of crypto-assets on behalf of their client seems contrary to the idea behind MiCA’s Article 92. The definition of custody and administration service under MiCA - the safekeeping or controlling, on behalf of clients, of crypto-assets or of the means of access to such crypto-assets, where applicable in the form of private cryptographic keys – does not typically include or denote activities that constitute professional arrangement and/or execution of transactions; for instance, a CASP providing custody and administration as a service does not always additionally provide the ancillary service of reception and transmission of orders as a service, which would typically be seen as a form of transaction arrangement. Therefore, where a CASP solely provides custody and administration services, such an activity should not be considered as equivalent to a PPAET, and should therefore fall outside the scope of Article 92.

In addition, BCAS strongly disagrees with the proposed inclusion, even by way of an example, of miners and validators under the definition of PPAETs, which should remain limited to CASPs and persons who are not involved in ensuring the proper functioning of distributed ledger technology (DLT) networks. Miners and validators do not execute transactions, as transactions are only executed after validation resulting from the network’s collective consensus. Additionally, miners and validators are not always responsible for 'arranging' transactions in blocks, as their roles may differ depending on the network in question.

Miners and validators play a crucial role in securing the running of permissionless DLT networks. Under point 63 of its second Consultation Paper ‘Technical Standards specifying requirements of MiCA’ (5 October 2023, ESMA75-453128700-438), ESMA considered that such networks are to be excluded from the possibility of outsourcing arrangements under MiCA because *"no formal contractual relationship (such as a service level agreement) is required to interact with permissionless blockchains”*. Crucially, ESMA mentioned that *“permissionless DLT networks may be considered a form of "common good" resource"*. Based on this interpretation, it is safe to state that miners and validators play a vital role in ensuring the proper running of a “common good” resource, a marked departure and difference from the ‘traditional’ role attributed to PPAETs, which provide no services that may be deemed to support a "common good" resource.

As outlined in point 19 of the present consultation, ESMA’s questioning around the potential inclusion of miners and validators under the definition of PPAETs seems based on the concept of Maximum Extractable Value (MEV) and the idea that all MEV activities suggest the existence of market abuse. This is far from a correct picture; MEV activities – which refer to the value block proposers can extract by reordering, excluding, or including transactions while proposing a new block – are also sometimes beneficial for the functioning of permissionless DLT networks.

For instance, back-running is a type of MEV activity consisting of executing a transaction right after a targeted transaction. Such activity is often performed on lending platforms, where anyone can perform liquidations in exchange for a percentage of the liquidation fee to keep loans over-collateralised. In this scenario, back-running activities allow MEV operators to profit from the liquidation fee while rendering service to lending platforms by enabling them to operate safely and maintain financial health for the protocol in question. Contrary to a common yet misconceived understanding of front-running, front-running can actually help level out crypto-asset prices across multiple AMMs or DEXes, making it a form of arbitrage that prevents users from acquiring crypto-assets at significantly different prices across various decentralised forms of trading venues. Front-running often occurs when users increase the standard slippage rates by an amount which would consider a disparity in prices for the crypto-assets; it is up to the users to accept the risk coming from increased slippage, which is what leads to arbitrage opportunities.

In any case, it is extremely difficult to differentiate between beneficial instances of MEV, and potentially harmful ones. Even if one were to consider imposing obligations on operators of MEV, namely *searchers, relayers, and builders* (as miners/validators, depending on the network, may not even have the opportunity to engage in MEV), it is almost impossible to enforce such obligations, as: a) the identity of any such participants who may be using MEV in a malicious manner for their own benefit is often not known/not possible to be known and b) integrating any systems to detect, prevent and report market abuse would just inhibit their ability to perform their functions versus other searchers/relayers/builders not located in the EU/EEA, likely to result in the ousting of such entities, and therefore harming the Union’s prospects in remaining as technologically relevant in the industry of crypto-assets.

In summary: from a technological perspective, MEV keeps blockchains running in the most efficient manner possible by incentivising block producers to act in competition. Therefore, ESMA’s attempt to prevent or limit MEV by including miners and validators in the definition of PPAETs, or any other operators involved in MEV, is tantamount to a disproportionate measure that would hamper the efficiency of the decentralised markets, rather than increase their level of protection against malicious participants – which in any case are likely to be located around the world, including outside of the Union.

<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>

The guidelines stipulate that ESMA considers that CDR 2016/957 can be taken as a precedent for this mandate, considering the similarities between the empowerments received under Article 92(2) MiCA and Article 16(5) MAR. Moreover, the proposed technical standard should add elements related to the specific nature of crypto-asset transactions, such as the effective and ongoing monitoring of the functioning of the DLT, including the consensus mechanism.

While BCAS agrees with the proposed elements that constitute appropriate arrangements, systems, and procedures to detect and prevent market abuse, BCAS also underscores the importance of ensuring that the size, nature and scale of the business activity are taken into consideration, including flexibility in the time allowed between one review and another as suggested under point 42. In the spirit of the principle of proportionality outlined in point 25, it would be equitable to extend the review period to a maximum of 18 months for smaller PPAETs, while retaining it at 12 months for larger PPAETs, with the difference & thresholds established on the basis of the aforementioned criteria of size, nature, and scale of the business activity.

<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>

BCAS agrees with the proposed STOR template as presented in the RTS Annex. The suggested template is comprehensive and covers each type of information required for the competent authorities to adequately understand the nature of the suspicions and effectively investigate the reported behaviour. However, Section 2 mentions that the report must include a description of the distributed ledger subject of the STOR, including its name and type. The latter may create confusion among participants, considering that a distributed ledger can only be of two types: permissioned and permissionless. Furthermore, since ESMA does not refer to the consensus mechanism but rather to the type of the distributed ledger, which can create some logistical issues on whether CASPs must report market abuse regarding permissioned DLTs, considering that certain permissioned DLTs may not make it possible to collect all the information required in the STOR when it comes to this specific type of DLT.

<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>

BCAS is of the opinion that parameters and naming conventions in the STOR template need flexibility and ongoing monitoring to accommodate new types of transactions. Currently, the suggested approach is comprehensive and adapted in regard to other applicable frameworks within the Union, notably the AMLD5, which also presents clear parameters for the identification of suspicious activities regarding AML/CFT risks and KYC obligations.

<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>

BCAS is of the opinion that while including 'location' data, such as the IP addresses, could theoretically be retrieved, the inherent characteristics of permissionless DLTs, as well as the use of VPNs and other anonymising technologies, may severely limit the effectiveness of such information. Therefore, the concept of ‘location’ is unlikely to be applicable to a permissionless distributed ledger; but it may be applied to permissioned/private networks.

<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>

BCAS views the provided template as rather comprehensive, though additional information that could be considered includes interactions with smart contracts, as these can significantly influence market behaviour. Details regarding the execution of smart contracts, any associated events, or the calling of specific functions could provide insights into potential market manipulation or abuse.

<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>

N/A

<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>

BCAS agrees with ESMA's approach of applying the suitability regime under MiFID II and applying it similarly within MiCA. However, differently to MiFID II, the technical understanding of a client should additionally be taken into consideration when assessing the suitability of crypto-assets in their regard, since this is an important factor that, contrarily, is not relevant for financial instruments.

<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>

BCAS is of the opinion that the draft guidelines should be amended to better fit crypto-assets and the relevant crypto-asset services, specifically in relation to the use of a DLT. The suitability assessment should not be limited to the assessment of the level of knowledge of clients and prospective clients on the crypto-asset or the type of crypto-asset they invest in but should rather also include a specific assessment in relation to the DLT used to transact and transfer the said crypto-asset. An assessment focusing specifically on the level of knowledge regarding crypto-assets or a specific type of crypto-asset would not necessarily cover the specificity that this type of asset represents and would hence require an amendment to the draft guidelines.

In addition to the above, one of the main risks that investors in the crypto-asset market are exposed to, besides the financial risk due to the volatility of financial markets, is the risk of permanently losing access to their assets or permanently losing the asset while transferring the asset(s) to another DLT address or account. Crypto-assets entail a particular risk when stored insecurely or being transferred negligently to other DLT networks using different technical standards. Moreover, they are unable to receive an asset that does not match the type of token transacted in this network. Therefore, crypto-assets specificity resides in the technology used to store and transfer these assets more than in the characteristics of the asset itself. Suitability assessment should ensure that clients and prospective clients have a clear understanding of how crypto-assets are stored and transferred, rather than solely focusing on the financial risk inherent to such assets.

<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>

BCAS agrees with the proposed approach.

This said, BCAS believes that the necessity for the service provider to provide evidence that their clients have accessed a valuation at least once during the relevant quarter should be redefined. BCAS acknowledges that legitimate doubt exists pertaining to the type of information service providers should assess to determine if this specific criterion is met. Most of the entities providing portfolio management services provide their clients with a web application/mobile platform that clients may access at any given time. However, clients may also opt to follow their portfolio and its valuation through separate applications or platforms, notably by configuring an Application Programming Interface (API) to receive and collect information from the application/platform that clients use, provided by the CASP.

On this note, ESMA does not specify if a CASP can evidence access to an up-to-date valuation of their portfolio through the use of APIs and diverse applications/platforms. In instances where the application/platform is provided by the issuer, not every action may be performed by the user that can be assimilated to accessing an updated valuation. For instance, for entities providing a mobile platform to their clients, the logs they collect on their user activities mostly relate to the signing-in activities within the platform itself but do not necessarily identify which actions have been performed by the client once on the platform except for certain specific actions such as requesting the purchase or sale of one of their asset(s). Therefore, BCAS opines to define further how this point can be evidenced, considering the wide range of platforms and applications that can be provided by CASPs or used by clients on their own exclusive initiative.

<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>

Arguably, the following types of information that have the most value for clients of entities providing transfer services are: the technical impossibility of reverting transactions processed on a DLT network; the specific DLT network used for the transfer of the crypto-asset; the approximative execution time, including a maximum execution time over which the CASP must require the client to reiterate its consent for the transfer to be processed; and the information related to the fee or rate that applies to the targeted transfer.

<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>

While the draft guidelines make significant strides in addressing the risks related to on-and off-DLT crypto-asset transfers, continuous monitoring and updating of these guidelines will be necessary to keep pace with the technological developments and emerging market practices. For instance, providing information to clients on the functioning of the DLT network and its consensus mechanism, specifically regarding block validation, could also include a comprehensive description of why a transfer may be rejected, returned or suspended. This level of information requested from the CASP could sufficiently facilitate covering the risks of on- and off-DLT crypto-asset transfers.

<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>

BCAS wishes to highlight the following:

Firstly, BCAS emphasises the relatively broad scope of the terms 'information of precise nature' and uncertainty regarding the criteria provided in Article 87(2), specifically 'reasonable expectation of an event or a circumstance to take place' and 'ability for a conclusion to be drawn in relation to the price of the crypto-asset in question'. Currently, the explanation in place is arguably vague and does not account for instances where it is naturally difficult to predict an event or circumstance to take place, moreover, whether the information would affect the price of the crypto-asset. Therefore, it is recommended that more information is provided to define these terms.

Secondly, a point that should be addressed further is in relation to the information provided to clients in regards to the fees of rates applicable to their transfer of crypto-assets; such information should be presented in a clear and understandable way so that it notably enables clients to differentiate the fees charged by the provider to the gas fees charged within the DLT network itself. It is important to ensure that CASPs are providing clear information regarding the gas fees incurred when transacting through the relevant DLT network and the fees they charge for their services. The reference to "all costs relating to the transfer for crypto-assets" under point 114 covers both DLT network gas fees and service fees applied by the CASP and thus requires emphasis.

<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>

BCAS supports ESMA's interpretation of the term 'systems'.

The terms appear to be the most acceptable interpretation to clarify the scope of Article 14(1)(d) of MiCA. When referring to ICT systems, ESMA refers to information and communication technologies that already encompass a wide range of tools used by CASPs, such as online platforms and mobile applications. Oppositely, the term 'business processes', as mentioned under point 128, is rather largely undefined, which means that it would inadvertently blur the spectrum of which systems or processes should be updated in compliance with the Union laws. In this context, BCAS is of the opinion that it would be more appropriate to refer to ICT systems, besides the fact that other processes potentially fall under the scope of other articles under the Regulation.

<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>

No

<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>

BCAS does not have any comments on this point.

<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>

BCAS agrees with the inclusion of cryptographic key management under Guideline 5 and, therefore, opines that cryptographic keys are relevant as a system or as a security access protocol. If cryptographic keys are rather close to the latest term, they cover a certain specificity in that they allow direct access to all crypto-assets held by the provider and, therefore, involve a higher level of risks that cannot be compared to other ICT. Moreover, BCAS is of the opinion that the promotion of a specific policy on encryption and cryptographic controls that clients can easily access at any time would be highly beneficial, specifically in instances when custody services are provided or when the offeror or person seeking admission to trading holds crypto-assets within their reserve of assets.

Secondly, paragraph 29 implies that cryptographic keys can be replaced, with which BCAS does not fully agree and opine that this guideline should be reformulated to emphasise scenarios where cryptographic keys are compromised, offerors and persons seeking admission to trading should update their system, prevent fraudulent transfers and assume the cost and expense of migration of the crypto-assets to newly generated cryptographic keys.

<ESMA\_QUESTION\_MIC4\_17>