25 March 2024
ESMA75-453128700-1012

# 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 under the heading 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 | ADAN |
| Activity | Regulatory and Public Affairs |
| Are you representing an association? | ☒ |
| Country/Region | France and Belgium |

## Questions

**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.**

<ESMA_QUESTION_MIC4_1>

We strongly support combating market abuse and agree that brokers/exchanges ought to be within the scope of market surveillance obligations. However, we strongly disagree that miners, validators, and custodians should be considered PPAETs.

**A. Adan strongly disagrees with considering validators and miners PPAETs for important reasons**

**1st) Miners and validators do not meet the requirements laid down in Article 92 of MICA**

*1. Any person **professionally arranging or executing transactions in crypto-assets** shall have in place effective arrangements, systems, and procedures to prevent and detect market abuse. That person shall be subject to the rules of notification of the **Member State where it is registered or has its head office or, in the case of a branch, the Member State where the branch is situated**, and shall without delay report to the competent authority of that Member State any reasonable suspicion regarding an order or transaction, including any cancellation or modification thereof, and other aspects of the functioning of the distributed ledger technology such as the consensus mechanism, where there might exist circumstances indicating that market abuse has been committed, is being committed or is likely to be committed.*

Article 92 of MICA lays down 2 conditions on the definition of PPAETs: First) Those should be persons who arrange or execute crypto-assets transactions. Second) they should perform those activities on a professional basis.

Miners and Validators do not meet either of the requirements.

Regarding the first condition, it would not be accurate to deem miners and validators persons that arrange or execute crypto-assets transactions.

While miners and validators play critical roles in blockchain networks, their functions are primarily technical and operational in nature, focused on maintaining network integrity and security. They do not have decision-making authority over the transactions they process.

Technically, they process data in order to transfer the asset. Their role is to validate transactions based on predefined consensus rules and cryptographic algorithms. They do not have the discretion to arrange or execute transactions on behalf of others in the same way as traditional financial intermediaries.

**2nd) Imposing PPAET rules on validators/miners is unlikely to be successful as they are not market operators, therefore it is practically impossible for them to effectively meet these requirements. This approach would not effectively achieve the policy objective of combating market abuse.**

It is worth noting that in its recital 93, MiCA excludes validators and miners from its obligations stating:

> *A provider of transfer services for crypto-assets should be an entity that provides for the transfer, on behalf of a client, of crypto-assets from one distributed ledger address or account to another.* ***Such transfer service should not include the validators, nodes or miners that might be part of confirming a transaction and updating the state of the underlying distributed ledger. This might also be the case in payments transitions, where validators are indeed needed****.*

The aforementioned recital acknowledges that although validators and miners might be part of confirming a transaction, they do not perform transfers of crypto-assets type of services under MICA, and that is why they are scoped out of the regulatory regime.

Considering them as ''Persons professionally arranging or executing transactions'' (PPAETs) may not accurately reflect the nature of their activities and could lead to regulatory challenges that may not be appropriate given their role within the blockchain ecosystem.

Miners and validators are not per se legal persons or natural persons acting on a professional basis either under MICA's meaning of article 92..

They do not engage in direct relationships with end-users or customers in the same manner as financial intermediaries, providing financial services to clients.

Typically, they do not hold, manage or transfer assets on behalf of others. This distinguishes them from traditional financial intermediaries who hold and manage customer funds and which characterize entities falling under MICA purview.

Crucially, the geographical scope of enforcement presents significant challenges when considering validators and miners under Article 92 of MiCA. Validators and miners typically do not have visibility into the locations of end-users, making it inherently difficult to ascertain whether regulatory requirements specific to the EU should apply. This ambiguity not only stretches the intended regulatory perimeter of MiCA but also introduces considerable legal uncertainty. Moreover, if MiCA's regulations were to be strictly imposed on technology stacks based in the EU, there is a substantial risk that such activities could be relocated to jurisdictions with less stringent regulations. This potential shift could undermine the effectiveness of the regulatory framework and inadvertently encourage the migration of blockchain and crypto-asset activities outside of the European Union.

**3nd) Miners and validators do not hold the capacity to reorder transactions. Making them comply with market abuse rules is technically unfeasible.**

To provide the necessary explanations, Adan would like to provide, in parallel, clarifications regarding the points raised on the Maximal extractable value (MEV) in paragraph 19.

Some important aspects of MEV are inaccurately described.

As a reminder, Maximal Extractable Value (MEV) refers to the maximum value that can be extracted from block production in excess of the standard block reward and gas fees by including, excluding, or reordering transactions within a block.

The paragraph states that ''*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*''.

As a consequence, the paragraph suggests that MEV is inherent to all Distributed Ledger Technologies (DLTs). This is incorrect.

1. MEV is primarily relevant to DLTs that utilize Proof-of-Stake (PoS) consensus mechanisms. **While transaction reordering for MEV extraction is technically possible in PoW systems, it is not a practice on PoW blockchains,** like Bitcoin, due to the lack of a DeFi ecosystem. However, blockchains with a developed DeFi ecosystem, like Ethereum prior to its transition to PoS a few years ago, could potentially have seen miners exploiting MEV through transaction reordering. In PoS systems, where MEV exists, only validators (not miners) are involved in the execution of transactions.
2. In PoW systems, the order of transactions within a block is crucial for maintaining the integrity and consistency of the blockchain. Miners must include transactions in the order they are received to ensure that the chronological sequence of transactions is preserved. **Reordering transactions within a block would disrupt the continuity of the blockchain and lead to inconsistencies in the transaction history**. **Any attempt to reorder transactions or manipulate block content would result in an invalid block that is rejected by the network.**
3. In PoS, Validators are typically blind to the content of transactions before they are included in a block. Transactions are propagated across the network, and validators independently verify their validity based on the information provided in the transaction data. **Validators do not have access to the content of transactions until they are included in a block and presented for validation. This blind validation process prevents validators from selectively reordering transactions.** The ability to re-order the transactions does not fall on validators but on the so-called searchers. They often utilize sophisticated software tools and bots to scan for specific patterns and arbitrage opportunities within the mempool (pool of pending transactions) to identify profitable MEV scenarios. In practical terms, MEV is not inherently abusive; rather, it involves complex strategies where validators or specialized actors known as 'searchers' may exploit available re-ordering opportunities within a blockchain's mempool (the collection of all pending transactions). These searchers use sophisticated algorithms to predict and execute the optimal reordering of transactions before they are finalized in a block.

**Toxic Vs non-toxic MEV**

Adan would also like to bring to your attention clarifications about MEV specifics that are relevant to its treatment as a risk-prone activity.

We encourage the distinction between operations that intentionally or unintentionally harm consumers and those that bring balance to the system (Non-toxic Vs. Toxic MEV). Recognizing this distinction clarifies that MEV itself isn't inherently abusive, but the way it's utilized can be.

However, certain implementations of MEV can lead to what is termed 'Toxic MEV,' where the practices employed harm the blockchain ecosystem, such as by disadvantaging other users through front-running or by destabilizing the network. In other words, toxic MEV refers to applications that make use of MEV to perform practices that create market abuse. It's crucial to distinguish between non-toxic MEV, which contributes positively or neutrally to the ecosystem by ensuring efficiency and liquidity, and toxic MEV, which can undermine fairness and transparency.

Categorizing MEV as inherently abusive behavior may overlook its essential role in maintaining a healthy and efficient crypto market. MEV is a neutral tool. It's the strategy behind it that determines whether it's abusive or beneficial.

MEV incentivizes validators to identify and exploit price discrepancies across different markets. This arbitrage activity helps push prices closer to their true market value, reflecting a more accurate picture of supply and demand. The potential for MEV profits can make staking more attractive, encouraging more users to participate while a larger pool of validators strengthens the network's security by making it more resistant to attacks.

We welcome that the STOR regime obliges reporting only where the PPAET has identified situations of risks of market abuse. However, it must also be noted that in the context of CeFi exchanges, where a significant portion of transactions occur off-chain, the impact of toxic MEV can be challenging to assess due to the limited visibility of on-chain activities. Since the on-chain footprint is limited, distinguishing between legitimate value extraction strategies and potentially harmful MEV behaviors would be a complex task, as the full context of transaction sequencing and prioritization may not be readily apparent.

**Adan strongly supports efforts to strengthen the supervision of market abuse activities to ensure consumer protection. However, MEV is a complex technical topic that merits further examination, and in any case, should not be automatically labeled as market abuse. We encourage the ESMA and European Regulators more broadly to monitor it as the market develops and to provide guidance on where to consider toxic and non-toxic MEV**.

**B. Regarding whether CASPs providing custody and administration of crypto-assets on behalf of clients should be classified as Persons Professionally Arranging or Executing Transactions (PPAETs), Adan highlights that it is important to differentiate based on the nature of services they provide**

Adan recalls that to safeguard against market abuse, Article 92(1) of MiCA compels persons to establish effective preventative and detective measures when they arrange or execute transactions in crypto-assets.

In determining which entities qualify as PPAETs and thus subjecting them to the STOR regime, we underscore the paramount importance of the proportionality principle. Proportionality ensures a calibrated approach by considering the nature and scale of an entity's business activities when assigning PPAET status. This approach recognizes that PPAETs are able to effectively prevent and detect suspicious activity due to their inherent involvement in transaction execution, ultimately enabling them to fulfill their reporting obligations to the relevant National Competent Authority in a timely manner.

According to the above, if a CASP is solely offering custody services, they should not be subject to market surveillance obligations under MiCA, as their role does not involve managing or executing trade transactions. Indeed, these providers do not interact with the market dynamics in a way that could influence market integrity or transparency.
However, if a CASP also has permission to execute trading activities, such as operating as a broker or an exchange, then it is appropriate for them to be considered under the PPAET category. This classification aligns with ESMA's existing regulatory framework which anticipates that brokers and exchanges will be included due to their active role in trading. Adan supports this approach as it rightly subjects those with the potential to impact market

dynamics to appropriate regulatory scrutiny, thereby safeguarding the market against abuse while ensuring that purely custodial services are not unnecessarily burdened with compliance obligations that do not align with their operational functions.

### C. Additional comments to paragraphs 18 to 21 on the Material scope of the prevention and detection mechanism

Adan advocates for a materiality risk-based approach to market abuse, focusing on the weight or importance of the transactions compared to the overall market activity. For instance, if a CASP executes less than 0.0001% of the total transactions or of the valuation for a crypto-asset, the potential risk of market abuse would be insignificant.

Transactions that represent a negligible percentage of the overall market volume or valuation are less likely to have a significant impact on market dynamics or price manipulation, reducing the risk of abusive behavior.

Thus, establishing a threshold, such as executing less than 0.0001% of total transactions or market valuation, could provide a quantitative benchmark for assessing the materiality of crypto-asset transaction activities. Transactions falling below this threshold would be deemed to have minimal influence on market outcomes, suggesting a lower likelihood of market abuse or manipulation associated with such activities.

<ESMA_QUESTION_MIC4_1>

**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.**

<ESMA_QUESTION_MIC4_2>

Adan agrees that it is important to ensure that systems, arrangements, and procedures developed by PPAETs are proportionate and appropriate to comply with the STOR regime.

This proportionality approach would ensure that systems can be adequate to the size, nature and scale of the business activity carried out by PPAETs and therefore to the risk dimension of the activities carried out. Proportionality ensures the implementation of the proposed systems in a way that allows the correct allocation of resources without compromising the ability to prevent and detect market abuse situations.

The proposed technical obligations are likely to create technical difficulties for smaller players leading to disparities in resources and implementation capabilities between market participants; market inequalities; and potentially unfair competition. Indeed, larger players have greater resources and implementation capabilities, unlike smaller players who might struggle to meet these new requirements due to a lack of human and financial means. The strict implementation of such measures could therefore result in an unequal and discriminatory situation.

While ESMA states that has developed its draft RTS and guidelines having due regard to the principle of proportionality, being mindful of the possible costs the obligations they contain would create for market participants, the proposed standards do not specify in concrete terms what a "proportionate" approach requires or enables the various players.

It would be useful to have more operational details on what is meant by "proportionate", including more precise indications on how companies should adapt their provisions, systems , and procedures to their size, the nature of their activities, and their risk profile. In our view, it does not seem appropriate to impose equivalent rules on a CASP operating a trading platform and on a "broker"-type CASP, which only acts as an intermediary between the customer and the trading platform.

**Thus, Adan recommends establishing a common set of rules for all players subject to the requirements, enabling even small/medium-sized businesses to put in place appropriate measures, while at the same time setting up additional measures for players carrying a significant risk in terms of their activity and volumes.**

Likewise, Adan agrees with the delegation of the prevention and detection of market abuse activity allowed by the RTS.

Adan believes that there is value in a regime that allows for the specialization in the conduct of preventing, monitoring, and detecting market abuse activity, including through the use of innovative technologies.

Specialization can both increase effectiveness and decrease costs. Increased effectiveness will help better counter market abuse, and decreased cost will help reduce the margin of the price of goods and services constituted by regulatory compliance costs. These benefits would be particularly impactful for smaller and more innovative businesses, which are less likely to have the budget, bandwidth, or in-house expertise to conduct those procedures. Thus, outsourcing can help small and medium-sized businesses (SMBs) and start-ups in Europe compete with larger, more established competitors – without compromising on essential efforts to counter market abuse.

**Therefore, Adan recommends excluding from the obligation to develop such systems to Small and Medium Enterprises (SMEs) as defined in the EU recommendation 2003/361. The burden of implementing such systems could make it substantially overwhelming for them to operate in the Union.**

**To promote a tailored-based approach that considers company size, activity type, and inherent risk, Adan recommends that ESMA provide more specific guidance on how firms could adapt their compliance provisions, systems, and procedures.**

**To this end, Adan advocates for a two-pronged approach: establishing a base rule set applicable to all players, which would allow small and medium-sized businesses to implement proportionate and appropriate measures. Additional requirements could be imposed on actors carrying a significant risk in terms of their activity and volumes.**

<ESMA_QUESTION_MIC4_2>

**Q3** **Do you agree with the proposed STOR template as presented in the Annex of the RTS?**

<ESMA_QUESTION_MIC4_3>

Regarding the STOR template, Adan reiterates the elements described in Questions 5 and 6.

Regarding the means of transmission, Adan suggests the implementation of a dedicated portal making any declaration easier and homogeneous for the declarants.
<ESMA_QUESTION_MIC4_3>

**Q4** **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>

Adan recommends the use of standardisation to effectively identify and report suspicious activities in crypto-asset markets in order to enhance transparency, improve data analysis, and strengthen regulatory oversight. Rather than recommend specific parameters or name conventions, collaboration is going to be needed between regulators and industry stakeholders in order to define and implement these standards and naming conventions. Ultimately, standardisation will lead to more effective detection of market abuse in the crypto-asset sector.

<ESMA_QUESTION_MIC4_4>

**Q5** **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>

In a DLT, transactions are propagated and validated by nodes distributed across the network. The concept of "location" of a transaction in a DLT may not correspond then to a physical or geographical location, but it can still be interpreted in terms of node identity, transaction path, and chronological sequence within the decentralized network.

In permissioned DLTs, where only authorized participants can join the network, nodes can be more easily identified as participants typically require approval and provide some form of identity information during onboarding. This could support locating the person running the node.

However, in permissionless DLTs, open to anyone to join, nodes are typically identified by their cryptographic addresses (which don't directly link to an official identity).

In this context, the "location" of a transaction could refer to the specific nodes that participate in the transaction validation process. Entities that run a node in the network have a Public Address. Public addresses are unique numbers that serve to identify the node, similar to a phone number or bank account. Through them, its user can send, request, or receive funds. Such an address could be considered the "location" of the transaction within the distributed ledger system.

In parallel, in a DLT system, data is replicated and stored across the multiple nodes in the network. The concept of "location" can refer to the specific nodes or servers where copies of the ledger are stored.

While generally, it is not possible to identify the geographical location of the node, it could be possible to do so for the server that stores off-chain data. This could be the case, for example, when an APP is used.

However, specifically for the case of miners and validators do not necessarily interact in the network through APPs.
<ESMA_QUESTION_MIC4_5>

**Q6 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>

Based on the aforementioned elements, we suggest the following amendments to the STOR template:

| | |
|---|---|
| Location ~~**(country)**~~ | [Full name of the country **(if available)** and the ISO 3166-1 two-character country code.]<br>[Specify:<br>— **Public address from** where the order is given **and location** (if available), — where the order is executed,<br><br>—**Public address and location** where the behavior related to functioning of the distributed ledger technology takes place (if available).] |

<ESMA_QUESTION_MIC4_6>

**Q7 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>

Cost is a significant concern in the implementation of MiCA. We estimate that the necessary additional investments to meet the current technical standards to prevent and detect market abuse are likely to vary widely depending on the level of sophistication and size of the firm, ranging from €40-50,000 to €300,000+. Some costs are one-off and others will be on an ongoing basis. These costs have to be added to the minimal capital requirements, the licensing requirement costs which are likely to range from €100,000 to €250,000 depending on the jurisdiction (not including technology or staff), and to other service provider costs such as travel rule solutions, etc.

As a result, a careful balance must be struck so as to protect the integrity of these growing markets but not stifle innovation which would ultimately affect the EU's competitiveness. As stated in our response to Q2, it is critical to further develop the concept of proportionality.

However, it should also be noted that for SMEs, developing an internal solution appears complex and expensive, making outsourcing a potentially preferred option; but the lack of clear solutions and identified external providers for CASP makes it difficult to accurately assess the costs associated with outsourcing. Beyond the financial costs, SMEs also need specific skills and expertise to implement and manage an anti-market abuse solution. These requirements can represent an additional burden for SMEs, limiting their ability to adapt effectively to new obligations.

Given these difficulties, it is therefore crucial to adopt a proportionate approach to obligations. This means, tailoring systems and procedural requirements to the capabilities and risk profile of different regulated entities, particularly SMEs.
<ESMA_QUESTION_MIC4_7>

**Q8 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>

Adan agrees with the proposed Guidelines. The alignment between MiCA and MiFID II on the assessment of suitability regimes, is crucial for ensuring consistency and harmonization in the treatment of investment services and activities in Europe.

Both MiCA and MiFID II aim to protect investors and ensure the integrity and transparency of financial markets and therefore, the same principles can be applicable to both.

By aligning their approaches to the assessment of suitability regimes, regulators can maintain consistent standards for evaluating the appropriateness of investment products, services, and advice, regardless of whether they involve traditional financial instruments or crypto-assets falling under MiFID II or MICA purview. This consistency enhances investor confidence, makes more consistent their investor experience, and reduces the risk of regulatory arbitrage or confusion.

By leveraging existing frameworks, principles, and best practices from MiFID II, regulators can streamline the implementation of suitability assessments for crypto-assets, reducing duplication of efforts, compliance costs, and administrative burdens for market participants.

This alignment also facilitates cross-border supervision and enforcement, as regulators can rely on established standards and procedures for assessing suitability across different jurisdictions.
<ESMA_QUESTION_MIC4_8>

**Q9 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>

Adan refers to question 8 response.
<ESMA_QUESTION_MIC4_9>

**Q10 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>

Periodic statements are key to enhancing transparency and accountability in portfolio management of crypto-assets, fostering trust of investors and among market participants.

By providing investors with regular updates on the performance, composition, and valuation of their crypto-asset portfolios, investors are able to track their investments, understand the risks involved, and hold portfolio managers accountable for their actions.

They provide valuable insights into the performance, risk profile, and diversification of crypto-asset portfolios, enabling investors and portfolio managers to make informed decisions and adjustments based on accurate and up-to-date information.

Additionally, and in line with our response to Question 8, this is a practice that would offer consistency with the MiFID II framework under which a similar obligation exists for portfolio management services.
<ESMA_QUESTION_MIC4_10>

**Q11 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>

Adan believes that by providing clients with essential information on the conditions of the service beforehand, clients can assess the risks, costs, terms, and conditions associated with the transfer of crypto-assets, enabling them to evaluate whether the service aligns with their investment objectives, risk tolerance, and preferences.

This is also a common practice within the traditional financial industry.

This way, CASPs empower clients to make informed decisions about engaging with the service. This clarity helps prevent misunderstandings, disputes, and legal issues down the line.

We would nevertheless bring ESMA's attention to one specific point in relation to the scope of transfer services.

In MiCA, transfer services are defined as "*providing services of transfer, on behalf of a natural or legal person, of crypto-assets* ***from one distributed ledger address or account to another***". We understand from the extract in bold that the definition of transfer services intends at covering two different types of on-chain transfers, depending on the DLT used:

- The reference to distributed ledger "address" is intended to capture blockchain address relying on **UTXO-based blockchains**;
- The reference to a distributed ledger "account" is intended to capture blockchain addresses relying on **account-based blockchains**.

Hence, it is very clear from the definition of transfer services contained in MiCA that transfer services are intended to cover **on-chain transfers** facilitated by a CASP, i.e. where crypto-assets move from one blockchain address to another.

This contrasts with Regulation (EU) 2023/1113 on information accompanying transfers of funds and certain crypto-assets ("**TFR**") in which transfer services are defined in a different manner:

> *'transfer of crypto-assets' means any transaction with the aim of moving crypto-assets from one distributed ledger address,* ***crypto-asset account*** *or other device allowing the storage of crypto-assets to another, carried out by at least one crypto-asset service provider acting on behalf of either an originator or a beneficiary, irrespective of whether the originator and the beneficiary are the same person and irrespective of whether the crypto-asset service provider of the originator and that of the beneficiary are one and the same;*

The transfer definition in TFR contains a reference to "crypto-asset account", which is further defined in TFR:

> *'crypto-asset account' means* ***an account held by a crypto-asset service provider*** *in the name of one or more natural or legal persons and that can be used for the execution of transfers of crypto-assets;*

The crypto-asset account definition is a clear reference to off-chain accounts managed by CASPs and which allow users to interact with digital asset products. TFR therefore clearly applies to off-chain transfers executed between crypto-asset accounts.

By contrast, it is clear from the definition of transfer services under MiCA that transfer services shall not apply to pure off-chain transfers within the internal systems of a CASP. However, it appears that the draft RTS are confusing on this point as there seems to be a reference to

crypto-asset accounts in the text of the draft RTS. In particular, point 19 of the draft RTS indicates that:

> *Crypto-asset service providers should establish, implement and maintain adequate policies and procedures (including appropriate tools) to ensure that, after execution of individual transfers for crypto-assets, the crypto-asset service provider provides the client with at least the following information:*
> ● *the names of the originator and the beneficiary*
> ● *the originator's distributed ledger address or* ***crypto-asset account number;***
> ● *the beneficiary's distributed ledger address or* ***crypto-asset account number;***

This reference to crypto-asset account number here seems to be imported from TFR but does not make sense in the context of transfer services under MiCA. These two bullet points should read "***the originator's distributed ledger address or account***".

This interpretation is moreover in line with the rest of the draft RTS which systematically refer to data in relation to on-chain transfers. For instance, CASPs are entitled to indicate "the number of block confirmations needed for the transfer of crypto-assets to be irreversible on the DLT, or sufficiently irreversible in case of probabilistic settlement, for each DLT network", information which can only be provided in the case of an on-chain transfer.

Further clarification from ESMA in the RTS to specify that the transfer services under MiCA only refer to on-chain transfers would be welcomed.

<ESMA_QUESTION_MIC4_11>

**Q12 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>

As indicated above, Adan believes that the RTS should not deal with off-chain transfers as the transfer service under MiCA does not encompass off-chain transfers.

Other than the above, Adan believes that draft guidelines address more than sufficiently the risks for clients related to on- and off-DLT crypto-asset transfers.

CASPs must provide clients with detailed, clear, and comprehensive information about the terms and conditions of the transfer services before any agreement is made.

Prior to execution, clients should be informed about the irreversibility of the transaction and all associated charges. Post-execution, clients should receive a reference identifier for the transaction, the amount and type of crypto-assets transferred, and detailed cost information. CASPs are also required to implement risk-based procedures for handling situations of market abuse where a transfer is rejected, returned, or suspended.
Customers must be promptly informed of the reasons for such actions and given guidance on how to address the issues causing the rejection or suspension.

For those reasons, the draft guidelines presented by ESMA appear more than sufficiently balanced to address the risks.

In addition, it appears correct that the ESMA has aligned this information with the requirements applied for payment transactions.

Both the guidelines and PSD2 share a common goal: consumer protection through transparency. This transparency empowers users to choose the most suitable provider for crypto-asset transfers and payment services, respectively. As a result, similar principles can be applied to both regulatory frameworks.

<ESMA_QUESTION_MIC4_12>

**Q13 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>

Adan believes that the draft guidelines address in a very comprehensive way the information to be provided to clients. This offers a level of transparency which ensures that clients are fully informed about the risks, costs, and implications of transferring crypto-assets on and off DLT platforms. By empowering clients with this information, they can make informed decisions.
<ESMA_QUESTION_MIC4_13>

**Q14 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>

Adan agrees with the clarification of the term 'systems' in the mandate as ICT systems. Indeed, the term 'system' is quite broad and without sufficient clarification, could capture other processes and procedures being implemented by obliged entities that do not necessarily have to do with requirements concerning the security of network and information systems supporting the business processes of financial entities.

By clarifying the scope, the guidelines are also aligning them with the Digital Operational Resilience Act (DORA).

ICT systems encompass the hardware, software, networks, databases, and technologies that support the operations, data processing, and communication functions of financial entities.

The clarification of the term systems helps to avoid ambiguity and ensures that the regulatory focus is directed toward the technology infrastructure that is critical for maintaining the security and resilience of financial operations.
<ESMA_QUESTION_MIC4_14>

**Q15 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>

Adan would like to bring to your attention the Cyber Resilience Act.

The Regulation lays down cybersecurity requirements for economic operators in relation to the design and manufacturing of products with digital elements for making available on the market such products in the EU.

Software or hardware and its remote data processing solutions, including software or hardware components to be placed on the market separately are considered products with digital elements under the regulation.

Manufacturers of open-source software are also subject to cybersecurity requirements where made available in the course of a commercial activity.

Therefore, tokens such as NFTs, Blockchain protocols, Smart Contracts, CASPs, Dapps, crypto assets wallets, and other types of Web3 products would be subjected to the CRA.

Manufacturers shall ensure that that product has been designed, developed, and produced in accordance with essential cybersecurity requirements, and shall undertake an assessment of the cybersecurity risks and take the outcome of that assessment into account during the design, development and maintenance phases of the product..

When placing a product with digital elements on the market, the manufacturer shall include the cybersecurity risk assessment in the technical documentation together with the mandatory CE marking.

The manufacturer shall notify any actively exploited vulnerability contained in the product and any vulnerability as well as cyber threats that could affect the risk profile of a product.

<ESMA_QUESTION_MIC4_15>

**Q16 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>

Adan would recommend that Guideline 2 explicitly mention the need for a risk management framework. Although minimal administrative arrangements could facilitate ease of compliance, this does not remove the need for a risk management framework, particularly when all categories of risk (operational, regulatory, market, etc) in crypto-asset markets are subject to evolution in technology. Minimal administrative arrangements could quickly become redundant in such a fast-moving environment but this can be mitigated by an appropriate risk management framework.

<ESMA_QUESTION_MIC4_16>

**Q17 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>

Adan supports the inclusion of 'cryptographic key management' in Guideline 5 as they are relevant to ICT systems and security access protocols. Cryptographic keys are integral to the overall ICT systems. They are used to safeguard communications, protect data integrity, and ensure the authenticity of transactions within these systems. They serve as a fundamental part of security access protocols by controlling access to sensitive data and systems, thereby ensuring that only authorized entities can decrypt and access the information.

The guideline addresses key aspects such as generating, renewing, storing, backing up, archiving, retrieving, transmitting, retiring, revoking, and destroying cryptographic keys, which are essential for preventing unauthorized access and ensuring data confidentiality and integrity. However, it is crucial to ensure that the methods for replacing keys are robust and secure to prevent any potential vulnerabilities during the transition period.
<ESMA_QUESTION_MIC4_17>