coinbase

To:

Verena Ross
Chair, ESMA
201-203 Rue de Bercy
75012 Paris

25 June 2024

ESMA's third consultation on MiCA

Coinbase Global, Inc. and its EU subsidiary Coinbase Europe Limited. (together, **Coinbase**) welcome the opportunity to respond to ESMA's third consultation on "Technical Standards specifying certain requirements of the Markets in Crypto Assets Regulation (MiCA)" (the **Consultation**).

Coinbase started in 2012 with the idea anyone, anywhere, should be able to send and receive Bitcoin easily and securely. Today, we are publicly listed in the US and provide a trusted and easy-to-use platform relied on by millions of verified users in over 100 countries to access the broader crypto economy.

We are committed to the EU as one of our largest international markets outside of the US. Coinbase has a crypto license in Germany, EMI license in Ireland and a number of registrations in national markets across the EU. We believe we are well placed to transition to a MiCA license, and we are excited by the opportunities presented across the region. The EU has taken a leadership role globally with MiCA, introducing the most comprehensive regulatory framework in the world. With fit-for-purpose regulation, the EU will be well positioned to capitalise on this new wave of technological innovation towards Web3, and to achieve its competitiveness ambitions by attracting inward investment.

The consultation and the questions posed demonstrate ESMA's desire to draft regulation that reflects the unique features of crypto-assets and crypto-asset markets. We appreciate this thoughtful approach ESMA is taking to regulating the sector and we stand ready to support it in this important work.

Yours sincerely,

Tom Duff Gordon, Vice President, International Policy, Coinbase

Scott Bauguess, Vice President, Global Regulatory Policy, Coinbase

coinbase

Introduction

ESMA's third consultation on MiCA addresses points that are critical to market integrity and consumer protection: market abuse, suitability, disclosures, and security. The proposed guidelines borrow heavily from regulatory approaches used in traditional financial markets. But, as the preamble to MiCA correctly notes, crypto-assets are not financial instruments. An overarching theme to our response is that additional regulatory nuance is required to account for both the consumptive nature of crypto-assets, and the unique technical features of DLT.

While crypto-assets may be purchased as an investment, that is not always inherent to their design; it is typically a byproduct of their anticipated future utility. The use cases for crypto-assets centre on networks and applications for which they are designed; they serve as building blocks for the next generation of the internet and as a faster way to transfer value. Similarly, while certain features of crypto-asset markets are reminiscent of traditional financial markets, distributed ledger technology is an innovation that operates in fundamentally different ways and promises a better, more efficient and more open global financial system.

We commend ESMA for seeking to draft fit-for-purpose regulation and for asking how these proposed guidelines should be amended to appropriately reflect the distinct features of crypto-assets and crypto-asset markets. In addition to providing general feedback on the proposed guideline, our response below highlights several unique features of crypto-assets and crypto-asset markets that warrant a different approach.

Preventing Market Abuse

Preventing and detecting market abuse is critical to ensuring the integrity of markets and earning user trust. For that reason, Coinbase has long been a leader in this area. Our surveillance team operates a best-in-class system that improves upon the tools developed for traditional markets while leveraging the unique features of 24/7 markets.

Crypto markets are truly global. Trading activity in one market will impact prices in another. While this is a positive feature and helps ensure price discovery and efficient markets, it means that effective surveillance for market abuse requires mechanisms for cross-market surveillance and cross-border cooperation involving various market participants and regulators.

When solving for cross-market surveillance, proportionality of rules is paramount. It would be disproportionate to require CASPs or persons professionally arranging or executing

transactions (**PPAETs**) to regularly monitor market participation beyond their functional operations and where they do not exert control. We also believe it would be inappropriate and inconsistent with MiCA to place market surveillance obligations on miners, validators, or custodians who are beyond MiCA's remit. In the case of miners and validators, this would undermine the neutrality of the blockchain and those entities do not otherwise have the expertise and funding to carry out surveillance.

In addition to our general views on the importance of market surveillance in crypto markets, there are three areas where we urge ESMA to further consider the unique features of crypto markets when interpreting Article 92: Maximum Extractable Value (**MEV**), requirements for ongoing monitoring of distributed ledger technology, and the growing role of AI in market surveillance.

MEV is an inescapable characteristic of well-functioning crypto markets.

While the Consultation discusses MEV in only one place, and without a lot of detail, the implication is that ESMA may believe it to be a manipulative or abusive activity.[1] We strongly disagree with the classification of MEV in this way, as MEV describes a wide variety of activities, many of which are vital for well functioning crypto markets. We urge ESMA to clarify that MEV is not inherently abusive and should not, in the ordinary course, trigger a STOR.

It is important to recognise that it is likely impossible to build a blockchain without MEV. Whenever the ordering of transactions matters, including in most blockchain-based applications, there is opportunity for MEV. This is because there is no "correct" ordering of transactions. Blockchain transactions are prioritised by block proposers (miners and validators) based on the amount of fees they can earn for including this activity in a block, with the most valuable being included first. This auction mechanism is critical for blockchains to efficiently allocate a scarce resource (block space) without being overwhelmed by economically irrelevant transactions (i.e., spam).

If there are 10 people initiating a trade in the same pool (e.g., ETH/USDC), some of which are selling and some of which are buying, each buyer would prefer to buy at the lowest price possible, while each seller would prefer to sell at the highest price possible. This expression of user preferences and resulting competition for transaction inclusion is an inherent part of blockchains.

MEV encompasses a wide range of activities, such as arbitrage and DeFi loan liquidations, that are clearly not manipulative or abusive. They keep DeFi operating effectively while contributing to the security and stability of the underlying blockchain.

[1] ESMA, Technical Standards specifying certain requirements of the Markets in Crypto Assets Regulation (MiCA), (25 Mar. 2023), p.10.

Arbitrage is the essential ingredient for price discovery, convergence, and efficiency in blockchain-hosted digital asset markets, especially across decentralised exchanges (**DEXs**). Arbitrageurs – often through use of algorithms (a.k.a "bots") – close price differentials among various assets across different centralised or decentralised exchanges by competing for block space. The best arbitrage opportunities are served first by way of higher fees and greater MEV. This makes crypto markets extremely efficient without any need for complicated order routing rules that characterise securities markets.[2]

Of course, it is also important to recognise that some forms of MEV are less desirable, such as sandwiching of trades within a proposed block. This is a form of front running, where one user offers a higher fee to place transactions on either side of another user's transaction, within the same block, for a risk free profit opportunity. The result is a higher price paid by a user seeking to buy an asset from a decentralised exchange, made possible because pending DeFi transactions are visible for all to see in a mempool.

Optimising MEV

Activities such as sandwiching have led some to inappropriately believe that MEV is broadly undesirable. In reality, the undesirable features of MEV activities are economically similar to practices in traditional finance, where some market participants routinely seek to profit from the anticipated behaviours of other market participants. Some remedies are also similar – i.e. cloaking buy and sell behaviour – while others are new and unique.

The crypto-asset ecosystem already offers protection against potentially manipulative behaviour. Most notably, users can engage with a centralised exchange like Coinbase, where orders are matched offchain, through a central limit order book, and therefore not subject to sandwiching on a per transaction basis.

Users also have access to protections on decentralised exchanges. For example, when a user initiates a trade on an automated market maker like Uniswap, they can select the level of slippage (post-order price movement) they are willing to accept, which is akin to specifying the bid-ask spread of a market order in a securities transaction. Users can also choose larger liquidity pools or use private mempools, both which limit the ability of other users to profit from their actions. Users' transactions can only be included in a block if a user's preferences – relating to more than just price – are met. This is a key differentiator of blockchain technology. Only valid transactions that are executed according to the selected preferences of the user can be included in blocks, regardless of their sequencing within the block.

Importantly, these tools offer greater flexibility to crypto-asset users than what currently exists for securities markets investors, where abuses of order routing practices have led to almost three decades of continuous regulatory optimisation. We strongly encourage

[2] See ETH ETP Comment Letter of Paul Grewal, Chief Legal Officer, Coinbase Global, Inc., (21 Feb. 2024).

ESMA to support continued industry efforts to leverage these technologies to minimise the negative externalities of MEV. As we discuss below, in our response to question 2, the industry is actively making progress in several ways.

MEV and decentralisation

The efficiency, stability, and security of blockchains such as Bitcoin and Ethereum depends on a central assumption: that block proposers – e.g. miners and validators – propose the most profitable block possible at any given moment. The first reason for this, mentioned above, is spam prevention.

The second is that if a block proposer followed any other strategy than profit maximisation (including MEV) in assembling their blocks, they would be less profitable than their peers, which over time would diminish their competitiveness on the network. They would fall behind their peers in their hash power on Bitcoin or staked assets on Ethereum, and as a result, would produce fewer blocks as their presence on the network would shrink over time and become irrelevant. Furthermore, as block proposers' revenues decrease, the likelihood of a 51% attack on a blockchain increases.

Regulation to curtail MEV, e.g. through restrictions or punitive regulatory requirements imposed on miners and validators within a jurisdiction, would have the unintended consequence of providing an incentive for remaining participants to locate outside what could otherwise be a well-regulated jurisdiction.

There is empirical evidence to support this claim. China used to have 70%+ of the hashrate on Bitcoin, before briefly banning it in 2021. They've now fallen to about 21% hashrate,[3] with America's share increasing to 40% given the favourable regulatory treatment in Texas and other states. On the other hand, America's disfavourable regulatory treatment of developers has caused its share of global crypto developers to fall from 40% in 2018 to only 26% in 2023.[4] Punitive MEV-related requirements on miners and validators would result in similar migrations, and would be inappropriate for MiCA objectives.

Summing up

The consequence of the current crypto-asset market design is that, even without fully implemented regulatory frameworks, they are already more efficient in many respects than traditional financial markets. As we shared with the United States Securities and Exchange Commission, Bitcoin[5] and Ethereum[6] already demonstrated higher market

[3] Statista, Distribution of Bitcoin mining hashrate from September 2019 to January 2022, by country (May 2022).
[4] Electric Capital, 2023 Crypto Developer Report, slide 173 (17 Jan. 2024).
[5] See Bitcoin ETP Comment Letter of Paul Grewal, Chief Legal Officer, Coinbase Global, Inc., (3 Mar. 2022).
[6] See ETH ETP Comment Letter of Paul Grewal, Chief Legal Officer, Coinbase Global, Inc., (21 Feb. 2024).

quality than the largest U.S. equity securities. If these markets were subject to the complicated order routing rules that have been promulgated in certain jurisdictions, notably the United States under Regulation NMS, we would likely see crypto markets that are similarly plagued by inefficiencies and an inability to get the execution that traders desire.

More generally, it is important to recognise that blockchain activity is public and transparent, meaning anyone can examine all current and past blocks and transactions. All transacting parties have equal visibility into onchain activity with no privileged actors designed into the system. This is in stark contrast to the opacity and exclusivity of roles built into current global market infrastructure. The tradeoffs of an open architecture offer many improvements over the proprietary and closed systems we use today.

Efficient and Effective Ongoing Monitoring

It is with the open architecture of blockchains in mind, and as we explain in more detail below, that ESMA should more carefully think about the roles CASPs play in market surveillance. In particular, to the degree that there is a desire for STORs based on onchain activity, our recommendation is to task those responsibilities to entities that are already monitoring blockchains, such as law enforcement agents. Put differently, CASPs or PPAETs should have the responsibility of surveilling their own systems and their interactions with the ecosystem, but should not have the responsibility of monitoring the entire ecosystem.

Requiring CASPs or PPAETs to have in place mechanisms for ongoing monitoring of the underlying distributed ledger or its consensus mechanism would be extremely costly and resource intensive, even for the most established market participants, and it is unlikely that it would uncover abusive practices. The vast majority (92% as of May 2024 as reported by an independent third party)[7] of spot crypto trading and price formation occurs off chain, and we wholeheartedly agree that ongoing monitoring by the centralised markets of transactions on their platforms is both necessary and appropriate. However, in most cases, onchain activity – including MEV – is not relevant to preventing or identifying misconduct in centralised markets.

Automation

Finally, we note that automation – in particular machine learning (**ML**) technology – will increasingly play a significant role in effective market surveillance. We applaud ESMA's recognition of this trend. Today, Coinbase's market surveillance function uses machine learning to provide 24/7/365 monitoring, vastly exceeding what can be achieved using manual tracking alone. This technology provides us with real-time insights and allows us to act quickly, which is imperative in crypto markets.

[7] The Block, DEX to CEX Spot Trade Volume (%) (last updated 19 Jun. 2024) (showing centralized exchanges accounting for 92.01% of spot trading volume in May 2024).

Successful use of ML technology requires human calibration and intervention. As it is designed to improve based on repeated use, we expect that the "appropriate level of human analysis" with respect to setting parameters or reviewing the alerts generated by such software will evolve over time. We encourage ESMA to continue to work with market participants to make sure that surveillance rules keep up with, but don't stifle, technological innovation.

Suitability

We agree with the approach taken by ESMA in this consultation insofar as it limits the application of suitability assessments to persons providing investment advice or portfolio management services in respect of crypto-assets. In this context, as with traditional financial instruments, suitability requirements can protect against unscrupulous actors seeking to put investors into products that don't match their investment profile.

We caution, however, against the blanket adoption of suitability requirements designed for financial instruments and securities markets. This is because crypto-assets are also used for consumptive purposes, and it would be inappropriate for suitability assessments to cover consumer preferences as they relate to the utility of a crypto-asset – e.g. how it is used in a network or protocol in exchange for a service.

This difference is well illustrated by comparing Apple to Ethereum. You don't need a share of Apple to use an iPhone, but you need an Ether (**ETH**) token to operate on the Ethereum network. If a market actor is advising a client to 'invest' in ETH because the value of the network will increase with time, that decision is materially different than another actor advising a client to purchase ETH for the purpose of actively participating in the Ethereum network.

Suitability assessments may be appropriate in the first instance – where persons are solely providing investment advice – but not in the second. Many crypto-assets are designed to be consumed on a network or protocol in exchange for a service, in a manner similar to how a traveler can redeem frequent flier miles in exchange for a plane ticket. Many also can be used as a generalised means of payment. Just because such a crypto-asset has value does not mean it was purchased as an investment. When a crypto-asset is purchased for its consumptive use, a suitability determination would be no more appropriate than seeking advice from an investment professional in the context of buying airline miles.

Of course, understanding client intent – investment v. consumption – for the same asset can be a challenge, and may not always be separable, so any suitability requirement should account for this nuance. Recognising that a client may have consumptive intent when holding crypto-assets is essential to avoid impeding web3 innovation in the EU.

As an example, Blackbird is a crypto application that uses the FLY token similarly to airline points, but for restaurants. Similar to a rewards program, users can earn FLY for dining at

restaurants or spend FLY on merch, rewards, and other perks. FLY can also be traded on decentralised exchanges if users desire to do so.

As a general guide to this determination, crypto intermediaries should not have the power nor the responsibility to determine which consumptive uses of a crypto-asset are open to the public or impair an end-user's ability to decide how to participate in the crypto-asset ecosystem. Users should generally be free to interact with protocols as they see fit – such activity is not inherently financial, and the application of investment suitability-like requirements in this context is inappropriate.

Transfer services

A core element of Coinbase's mission is to update the financial system leveraging the speed and accessibility of crypto-assets. We offer simple-to-use services that allow instant value transfers between users anywhere in the world, and believe that real-time settlement of this nature will power significant portions of our future online activities, including across borders. The speed and broad accessibility of crypto is already driving the value of projects being developed by many of our users who are builders in the crypto-asset ecosystem.

We want our users to be empowered. We support and encourage requirements to provide understandable user instructions, education about services offered by CASPs, as well as clear information about a user's rights and obligations. We already make various educational materials available on our website and explain our users' rights and obligations in our user agreement. If other market participants are not already doing this, we believe they should, and ESMA is right to focus on this.

We are concerned, however, with the requirement to provide certain information "in good time" before entering into the user agreement. This term is left undefined in the consultation and could unnecessarily slow down and complicate a process that is intended to be simple and efficient.

We recommend ESMA revise its guidelines to clarify that necessary information be readily available to users prior to a transfer, but without any delay unrelated to the accessibility of such disclosures. To the extent that such disclosure be made via a durable medium – which we note is inconsistent with the general user preference for digital recordkeeping of onchain activity – this should be done once at the time of initial customer onboarding and not on a per transaction or asset basis.

We further recommend that information provided should focus on the unique characteristics of the service provider and the manner in which it provides the services, as opposed to information about the technology or assets themselves, which is already publicly available. Moreover, to the extent that a CASP bundles transfer services with other services where the majority of the contemplated information will already have been provided, we encourage ESMA to streamline the disclosure and informational

requirements so as to minimise redundancy and thereby maximise the operational efficiency of CASPs.

Finally, we understand para. 19 of Guideline 2 to apply only to the originating CASP and we urge ESMA to make this clear. The receiving CASP may not have all the information included in para. 19, such as the name of the originator. While many jurisdictions have in place Travel Rule regulations that require the collection and transmission of such information, this is not consistent globally. For instance, CASPs may receive transfers that do not contain the originator's name because the originating CASP is located in a jurisdiction that does not yet require it to transmit Travel Rule information. If, however, para. 19 is intended to apply to the receiving CASP, we ask ESMA to clarify that the receiving CASP is only obligated to comply with para. 19 to the extent the receiving CASP has the relevant information.

As we discuss further below, we are also concerned by the reference in Question 12 to "off-DLT transfers." We do not believe that these kinds of transactions are in scope of MiCA, nor are they contemplated in the guidelines – since the guidelines appear to be drafted for onchain transfers, as would be expected. ESMA should clarify that its intent with the guidelines is not to encompass off chain transactions. If off chain transactions are intended to be captured by the scope of these guidelines, then significant amendments would be required for the guidelines to appropriately reflect the different (and more limited) considerations raised by off chain transfers and ESMA should consider the costs and benefits of doing so.

Systems and security

We generally agree with the approach taken by ESMA with respect to systems and security requirements for offerors and persons seeking admission to trading. We reiterate our view that the term "offeror" should not be read so broadly as to capture decentralised protocols, who are not only outside of the scope of MiCA but would also be unable to comply with the Guidelines. We urge ESMA to make this explicit.

Targeted Responses

Chapter 3 - detecting and reporting suspected market abuse in crypto-assets

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.

We agree that entities that are within the remit of MiCA (i.e. exchanges and brokers) should be considered within the scope of Article 92. However, Recital 2 of the draft RTS clearly ties the obligations on market abuse to specific authorisations under MiCA, and we recommend that ESMA reflect this in the Articles. In particular, these obligations should be limited to those persons that are covered under MiCA. It is not appropriate to include crypto miners, validators and other entities that are not within the MiCA perimeter.

Exceeding the MiCA perimeter by including miners and validators would violate the neutrality of their role in serving a blockchain's consensus mechanism. If validators and miners were required to assess the transactions being sequenced for market abuse, disagreements could arise among validators as to whether a certain transaction is abusive and whether it should be included in a block. These types of disagreements would hinder consensus and could result in forks and even blockchain halts, severely undermining the core functionality of blockchain technology.

It is critical to recognise that crypto miners and validators are purely technology providers and they should remain that way; it would not be appropriate to task them with the responsibilities expected of financial intermediaries, including the requirement to collect, process, store, or assess PII associated with any transacting market participant – i.e., commensurate with maintaining a compliance trade monitoring program covered under Article 92. Miners and validators have no way of obtaining this information as they only see the transaction contents. They have no ability to know where these transactions are originating from, who sent them, or even the capability to ask for additional information.

We similarly do not believe that custodians should be considered a PPAET to the extent they do not provide a means for their customers to interact directly with CEXs/DEXs. In these instances, where custodians just offer safekeeping services, we encourage ESMA to retain the principle of proportionality, given that the rules are drafted broadly and would impose a wide range of obligations that are not relevant to a custodian's ordinary

course operations. Proportionality should be applied in practice by the NCAs, and ESMA should monitor this application to ensure that the standards set across member states on proportionality are harmonised as much as possible.

Proportionality is also relevant when considering obligations placed on brokers, who generally will not have access to the same level of information as exchanges. We urge ESMA to revise Article 2(3)(a) to more directly state that the obligations of a PPAET depend on the information that the PPAET receives in the ordinary course of operating its business. We also encourage ESMA to amend Article 3(2)(a) to ensure that own-account trading is not included in scope of the obligation – only those "trading activities" where there is a professional arranging or executing of a transaction. Own-account trading on its own does not implicate the same concerns that justify obligations when customer trading activities are involved.

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.

While we agree with the aim of the proposed requirements, they are too broad and without sufficient granularity for us to fully assess their appropriateness. ESMA is correct to not be overly prescriptive in its requirements, but providing a broad set of obligations without specificity leaves open how ESMA intends for NCAs to incorporate the principle of proportionality. We encourage ESMA to provide further guidance to the NCAs on harmonising expectations around arrangements, systems, and procedures and the application of the principle of proportionality.

Specific requirements notwithstanding, we recommend ESMA require all CASPs and PPAETs operating a trading platform to apply the same minimum standards. These standards should include: real-time or near-real-time monitoring, in-house or third party surveillance software that is appropriately tested and capable of identifying all relevant abusive or manipulative trading behaviours, periodic reviews and tests of alerts settings / parameters, adequate staffing, monitoring for employee or insider trading, and policies and procedures that require an annual review of market abuse risk.

Obligations for other PPAETs should be viewed through the lens of proportionality, subject also to minimum standards that are appropriate for the type of business the relevant category of PPAET operates. For example, actors such as brokers will not have the same access to information as do CASPs that operate trading platforms and their obligations should be considered through that lens.

To reiterate the discussion above, CASPs and PPAETs should not be charged with ongoing monitoring of the underlying distributed ledger or its consensus mechanism. CASPs and PPAETs should only be responsible for surveilling their own systems and their

interactions with the ecosystem, but should not have the responsibility of monitoring the entire ecosystem.

Finally, given the relationship between MEV and blockchain market structure and security, ESMA should allow those who have the necessary technical expertise to continue working towards solutions that minimise MEV's negative externalities. Developers are already exploring many models for transaction sequencing, including auctions, first-come-first-serve, encrypted mempools, preference matching, and many other methodologies.

A growing array of products in the market already attempt to minimise MEV. For example, Uniswap X and CoW Swap seek to provide users with better execution on trades by matching their orders with those of other users or market makers without exposing them to the public mempool (i.e. a "pre-trade" cloaking solution). This reduces multiple forms of MEV by eliminating frontrunning and reducing arbitrage profits since users get a more accurate price. Flashbots Protect is a service that allows bot operators to interact with user transactions through a process of backrunning. This is a MEV strategy whereby the user receives a portion of the generated MEV for successful transactions (i.e. the bot shares the arbitrage profit). Using Protect, a user is strictly always the same or better off than if they had submitted their transaction to the blockchain themselves.

These examples demonstrate that there is no one-size-fits-all solution. The market structure for MEV is dependent on the technology of the underlying blockchain. For example while frontrunning and sandwiching is possible on Layer 1 blockchains like Ethereum, it is likely impossible to frontrun or sandwich a user on a Layer 2 blockchain like Base (incubated by Coinbase). This is because transactions that are waiting to be included in a block on Base are not publicly viewable and therefore cannot be acted upon by other actors.

Blockchain technology creates MEV and it is technology that must minimise the negative externalities of MEV on users, block proposers, and blockchains. Designing a market structure that leverages policy to solve this problem would result in serious negative consequences for the stability and security of blockchains, while pushing the prohibited activities offshore to actors and regions not beholden to MiCA regulation.

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

STOR filings for crypto-assets, like with traditional financial transactions, can be an important tool for NCAs to identify and mitigate market abuse when it occurs. However, STOR filings will only be an efficient tool if they allow for quick identification and reporting of suspicious activity by CASPs.

As currently presented in the Annex of the RTS, the STOR template contains significantly more information than is necessary to make a determination on market abuse. This includes information that is not standardised, that a CASP may not have at its disposal or information that is simply unnecessary for an NCA to appropriately begin an investigation. As a result, completing a STOR filing could be unnecessarily delayed by several hours (collecting unnecessary information) to as long as multiple days (searching for immediately unavailable information). This would be a bad policy outcome. We recommend that ESMA streamline the STOR template to ensure that CASPs are able to quickly report enough information to allow NCAs to make a determination on market abuse.

We recognise that the proposed STOR is based on the STOR developed by ESMA under its mandate within Art 16(5) of Regulation (EU) No 596/2014 of the European Parliament and of the Council of 16 April 2014 on market abuse. While this is a good baseline, there are several reasons for ESMA to take a different and incremental approach for crypto-assets. STORs in traditional markets are efficient to compile because of the significant standardisation in trade data, identifiers, order types, and onboarding information collected. This does not yet exist in crypto-asset markets, as the regulatory regime is just beginning to take shape. As a result there are a number of elements in the proposed STOR that would significantly extend the time needed to respond while providing NCAs with little immediate benefit.

For example, CASPs will have unique ways of identifying clients internally and providing such information to NCAs will not be helpful unless those identifiers are standardised across the industry. In addition, some of the information in the STOR may not be immediately available to CASPs or may be unnecessary for initiating an effective investigation. An example of immediately unavailable information in the current STOR template is the requirement to provide certain relevant additional information including historical trading patterns of the suspected entity/person, which would seemingly require information beyond the trading activity that triggered the suspicion of abusive behaviour. An example of unnecessary information in the STOR template is the description of the crypto-asset and a description of the distributed ledger. This information is publicly available and already known by NCAs for assets that are trading within their regulatory framework.

Including informational requirements that are not possible to provide, or not relevant for the initial phase of an investigation, will unnecessarily delay this important process. CASPs may also spend time unnecessarily providing non-critical information that, while available to them, is not readily available. Delaying a STOR is not warranted unless that information is critical.

We believe ESMA, to comply with its own objective of avoiding delay of “the submission of a report in order to incorporate further suspicious orders, transactions or other aspects of

the functioning of the distributed ledger technology," should adopt a more streamlined approach to STOR filing requirements that privileges speed over unnecessary details.

As ESMA correctly notes, a CASP is always able to submit additional information. We recommend that ESMA amend the STOR template to expressly delineate what information is critical and required to be provided with each initial filing, what information is optional or may be provided at a later date, and to delete requirements to provide publicly available information. ESMA and NCAs, after evaluating a quickly and efficiently delivered STOR, can subsequently work with the CASP to collect additional, relevant information as required to further the investigation. In this way, ESMA can privilege reporting speed without sacrificing an ability to collect all other possible information it could require.

We also urge ESMA to work with the industry to create standardisation across inputs to further enhance the efficiency of completing STORs. We welcome the opportunity to engage with ESMA in this regard. The Annex to our response sets out our recommendations in more detail.

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?

We believe it is important to make clear that CASPs should not be responsible for broadly policing onchain activity. Blockchains are inherently transparent and allow for direct monitoring by anyone, including regulatory authorities, and requiring CASPs to monitor for market abuse outside of activity on their own trading platform or platform the CASP provides access to should be considered outside of their regulatory obligations.

With this in mind, our response to this question is specific to the STOR template, as CASPs would file it with respect to off chain activity only. As we discuss in response to Question 3, and illustrate in the Annex to our submission, we suggest that ESMA significantly streamline the list of parameters in the template. Naming conventions in the template itself are appropriate and do not need to be modified to address suspicious orders, transactions, or behaviours involving crypto-assets. Spoofing, front-running, and other common terms apply to abusive behaviour regardless of the type of assets traded.

However, we suggest that ESMA engage with the industry and release a sample populated STOR, so that CASPs can better understand the naming conventions that ESMA associates with specific behaviour. In addition, releasing this sample STOR would help clarify the level of detail that ESMA expects in the filings.

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?

As we explained above in our response to Question 1 and elsewhere, we don't believe it is appropriate for there to be regulatory requirements imposed on validators and miners. As technology providers, it would not be appropriate to task them with the responsibilities expected of financial intermediaries, including the requirement to collect, process, store, or assess PII associated with any transacting market participant. To this end, knowing their location has little bearing on knowing whether regulatory requirements of MiCA registrants are being satisfied.

There would, however, be value in knowing the location of technology providers for the purpose of understanding the economic relevance of crypto-asset activity within a particular jurisdiction. The measure of a workable regulatory framework will be heavily influenced by whether market participants chose to operate within that jurisdiction. Nevertheless, as this question correctly implies, location is a complex topic, especially in the context of masking. To the extent activity is being conducted by a bad actor, it is very likely that the IP information collected will be unhelpful in leading to the identity of that actor.

For offchain activity, IP addresses are not additive. The STOR requires CASPs to provide other identifying information, which should be sufficient.

Q6: Is there any other element or information relevant to crypto-asset markets that in your view should be included in the STOR? Please explain.

As we discussed in our response to Question 3, we believe the expediency of STOR reporting should lead it to being as streamlined as possible. We recommend that ESMA remove, rather than add, information from the STOR template, requiring only the immediately available and necessary information to begin an investigation. Of course, CASPs should have the option to include additional relevant investigative information including, e.g., relevant wallet addresses as the situation merits. Similarly, regulators should have the ability to request additional information as their investigation ultimately merits.

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.

Please see our discussion in the questions 1-4 above, as well as our proposed revisions to the STOR in the Annex.

Chapter 4 - suitability requirements applicable to the provision of advice and portfolio management in crypto-assets

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?

As we note above, the concept of suitability is only relevant when a user purchases crypto-assets as an investment and should not be used as a gating mechanism for interactions with the web3 ecosystem. Any suitability requirement should take into consideration that a user may have a consumptive intent.

When appropriately limited to circumstances where a user seeks to invest in crypto-assets, many of the concerns that underpin a suitability assessment for investments in traditional financial products should apply to investments in crypto-assets. However, even in an investment context, we urge ESMA to calibrate the assessment requirements to the unique features of crypto markets.

For example, any suitability assessments and determinations should reflect the risks of the services being provided. The risks of crypto-asset custody differ from the risks of crypto-asset brokerage activity and suitability assessments should take into account the different degrees and types of risk that an end user is exposed to. In addition, requirements to collect information relating to a customer's suitability preferences should consider the relevant inputs for crypto-assets. Finally, consistent with treating consumer uses of crypto-assets differently than investment uses, ESMA should make clear that providing educational or technical details about a specific asset, both of which are necessary to understanding the asset's utility, will not trigger a suitability assessment. Nor should the provision of technical details be treated as providing investment advice.

We also disagree with ESMA's statement that it is less relevant to vary the extent of an investment firm's suitability requirements based on the specific features of a crypto-asset on the basis that "there is no such thing as a 'safe' crypto-asset." While crypto-assets can be volatile, volatility does not make an asset inherently "unsafe". Volatility merely reflects the uncertainty of an asset's future value, and crypto-asset volatility behaves no differently than the volatility of a typical security, many of which have greater volatility than BTC or ETH. And to reiterate a point we make above, certain crypto markets currently have as high, if not higher, market quality than the largest U.S. equity securities.[8] Finally, as we note in our responses to the US Securities and Exchange Commission's request for comments on the proposed rule changes filed by NYSE Arca, Inc. to list and trade shares of the Grayscale Bitcoin Trust (the **BTC ETP Comment Letter**) and the Grayscale Ethereum Trust (the **ETH ETP Comment Letter**), the consensus mechanisms,

[8] BTC ETP Comment Letter of Paul Grewal, Chief Legal Officer, Coinbase Global, Inc., (3 Mar. 2022).

decentralisation and security features of the world's largest blockchains protect the corresponding assets from manipulation and security risks.[9]

Just like with traditional financial instruments, investment firms should be able to apply different suitability criteria to these assets than to crypto-assets with a riskier profile. The Guidelines should be future proof. As the crypto-asset markets grow, more and more crypto-assets will resemble U.S. equity securities in terms of being "safe" and investment firms should be able to take that into account when fulfilling their suitability obligations.

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.

Please see response to Question 8.

Chapter 5 - transfer services for crypto-assets

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.

As noted above, the draft Guidelines are overly prescriptive as to how and when certain information should be provided. Crypto is designed to be fast and easy to use, especially so for transfer services. CASPs providing transfer services should have flexibility in how they provide customers with the relevant information, so long as customers receive or are made aware that they can access the relevant information prior to making a transfer. For example, Guideline 1 does not take into account that transfer services will, much more often than not, be provided as part of a wider integrated exchange solution. Therefore, the guidelines should expressly allow for the information required to be provided to be capable of being delivered via various different means, as much of the information required to be disclosed will be disclosed as a matter of course during the client's wider relationship with the CASP.

In addition, many of the items to be addressed by paragraph 12 of Guideline 1 may not be relevant to a user as a disclosure prior to onboarding, and would be more useful and easier to digest if presented by other means. For example, the guidelines propose requiring a CASP that supports transfer services for hundreds of digital assets to provide information related to each asset prior to onboarding a client. It is highly unlikely that any

[9] *Id.*; ETH ETP Comment Letter of Paul Grewal, Chief Legal Officer, Coinbase Global, Inc., (21 Feb. 2024).

user would meaningfully process this information if provided in such a form, defeating the purpose of the requirement. Users are more likely to seek these types of details in an FAQ or similar resource once onboarded.

We recommend that ESMA provide additional clarity on what it means by requirement to disclose: "*the means of communication, including the technical requirements for the client's equipment and software, agreed between the parties for the transmission of information or notifications related to the crypto-asset transfer service*". It is not clear what ESMA is referring to here. Further guidance should recognise and accommodate that messaging on transfer services will occur within the client's online account opened with the CASP, generally provided via a web-based application, or mobile application. It is in our view highly unlikely that any specific technical requirements for the client's equipment and software will be relevant to a client making an informed transaction decision.

The guidelines require the creation of risk-based policies and procedures around when transfer requests should be refused or rejected, due to the Travel Rule or other issues. We would note this is somewhat duplicative of the requirements of the Travel Rule under Level 1 and the EBA's (currently draft) Travel Rule Guidance. We encourage ESMA to provide further clarity on the interaction between this requirement and those contained in Travel Rule legislation and guidance.

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.

As we note in question 11, the proposed requirements go beyond what is required to address risks for clients relating to on-DLT crypto transfers. It should be noted that on-DLT crypto transfer services are a common feature of the crypto industry and are generally highly reliable from a technical point of view. The core complexity that generally arises with on-DLT transfers is where users incorrectly input information (for example an incorrect wallet address). Coinbase deals with that risk through education, warnings and other confirmation processes. Otherwise, generally the operation of on-DLT transfers is relatively standardised and most providers offer education to ensure that users understand the risks, timing and process of those transactions.

In our view, off-DLT transfers are not captured by "transfer services," which refers to the provision of a service to transfer crypto-assets "from one distributed ledger address or account to another"[10]. An off-DLT transfer is a "books and records" transfer between clients of the same provider, which would not be effected via an on-DLT transaction. The

[10] Article 3(1)(26) of MiCA.

requirements in the guidelines relate to on-DLT transfers (e.g., requiring information to be provided around the sending and receiving wallet addresses, confirming block confirmations required to consider a transaction as settled, etc). We would therefore ask ESMA to confirm that off-DLT transfers are not included within this requirement. If they are included, we ask that ESMA make that clear and better reflect in the guidelines the significantly reduced requirements that should exist for an off-DLT transfer (effected via books and records).

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?

We have nothing further to add beyond our answers to the questions above and in the introduction to our response.

Chapter 6 - maintenance of systems and security access protocols

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).

We are generally supportive of ESMA's interpretation of the term "systems" as it appropriately matches the scope of the mandate in MiCA. This narrower interpretation is better suited to the types of entities captured as "offerors and persons seeking admission to trading" who, as ESMA correctly points out, do not "pose risks to the stability of the crypto-asset market nor to investors" on the same scale as CASPs.

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.

No.

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.

Yes. Consistent with our response to question 14, we agree that offerors and persons seeking admission to trading are more appropriately subject to minimal administrative arrangements related to the maintenance of ICT systems and mitigation of related risks.

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)?

We agree with the inclusion of Guideline 5 on cryptographic keys. We consider keys to be a "system access protocol" rather than a "system" because 'cryptographic keys' facilitate the access and management of funds by granting the holder(s) the ability to authenticate, authorise, and execute actions such as signing a transaction. The guideline is generally fit for purpose, and we note that keys can be replaced in certain circumstances, for example in the event of a suspected or actual compromise or when transitioning to stronger cryptographic standards. However keys that are truly lost cannot be replaced if backups are not maintained. From a maintenance perspective some environments may perform regular key renewal to prevent keys from being used beyond their secure lifespan.

ANNEX

STOR template

In addition to information identifying the person submitting the STOR, we recommend that ESMA limit the initial STOR filing obligation to immediately available, critical information that is dipositive to a regulator's ability to open an investigation: i) the name of the base crypto-asset and quote asset (i.e. trading pair),[11] ii) a description of the suspicious activity, including the date and time, and iii) the name, National Identification Number (where applicable and collected), and type of user engaging in the activity, and iv) any other readily available information that the CASP deems relevant.

We include below our suggested revisions to the STOR, noting which information is critical and which information is optional. We have also suggested ESMA delete certain information fields, as they are publicly available.

We have marked suggested critical fields with an *, noted suggested additions or comments in bold, and struck out suggested deletions.

SECTION 1 — IDENTITY OF ENTITY/PERSON SUBMITTING THE STOR Persons professionally arranging or executing transactions in crypto-assets — Specify in each case:	
Name of the natural person*	[First name(s) and surname(s) of the natural person in charge of the submission of the STOR within the submitting entity.]
Position within the reporting entity*	[Position of the natural person in charge of the submission of the STOR within the submitting entity.]

[11] Base Asset means the Asset being traded on the Order Book; i.e., the first Asset in the Trading Pair. Quote Asset means the Asset in which trading is denominated on the Order Book; i.e., the second Asset in the Trading Pair. For example, on the BTC-EUR Order Book, BTC is the Base Asset and EUR is the Quote Asset.

Name of the reporting entity*	[Full name of the reporting entity, including for legal persons: — the legal form as provided for in the register of the country pursuant to the law of which it is incorporated, where applicable, and — the Legal Entity Identifier (LEI) code in accordance with ISO 17442 LEI code, where applicable.]
Address of the reporting entity*	[Full address (e.g. street, street number, postal code, city, state/province) and country.]
Acting capacity of entity with respect to the orders, transactions or behaviour related to the functioning of the distributed ledger technology that could constitute market abuse*	[Description of the capacity in which the reporting entity was acting with regards to the order(s), transaction(s) or behaviour(s) related to the functioning of the distributed ledger technology that could indicate the existence of market abuse, e.g. executing orders on behalf of clients, dealing on own account, operating a trading platform...]
Type of trading activity (market making, arbitrage etc.) and type of crypto-asset traded by the reporting entity, **if applicable***	[Description of any corporate, contractual or organisational arrangements or circumstances or relationships, if available]
Contact for additional request for information*	[Person to be contacted within the reporting entity for additional request for information relating to this report (e.g. compliance officer) and relevant contact details: — first name(s) and surname(s), — position of the contact person within the reporting entity, — professional e-mail address.]

SECTION 2 — TRANSACTION/ORDER/BEHAVIOUR AND OTHER ASPECTS RELATED TO THE FUNCTIONING OF THE DISTRIBUTED LEDGER TECHNOLOGY

Description of the crypto-asset **or trading pair, including Base Asset and Quote Asset***	Describe the crypto-asset(s) **or trading pair**s which **are** the subject of the STOR, specifying: — the full name (including Digital Token Identifier (DTI) in accordance with ISO 24165-2, where applicable) or description of the crypto-asset in the absence of DTI. ~~— the type of crypto-asset (asset-referenced token (ART), e-money token (EMT), other crypto-asset) and for ARTs and EMTs, the value, right or official currency (or combination thereof) which the crypto-asset references in order to maintain a stable value. If the suspicious behaviour involves a trading pair, please list both crypto-assets in the pair.~~
~~Description of the distributed ledger (where the STOR refers to the functioning of the distributed ledger technology):~~	~~[Describe the distributed ledger, which is the subject of the STOR, specifying the full name and type of the underlying distributed ledger technology~~
Date and time of transactions, orders or behaviour related to functioning of the distributed ledger technology that could indicate the existence of market abuse *	[Indicate the date(s) and time(s) of the order(s), transaction(s) or behaviour(s). Dates and times should be reported in UTC per the format in ISO 8601.]
Trading platform where order was placed or the transaction was executed*	[Specify name and Market Identifier Code (MIC) in accordance with ISO 10383 to identify the trading platform where the order was placed or the transaction was executed. If the order/transaction was not identified in a trading platform, please mention 'outside a trading platform' and the LEI of the CASP(s) that carried out the transaction if applicable.]

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

Description of the order, transaction or suspicious behaviour related to the functioning of the distributed ledger technology*	[Describe at least the following characteristics of the order(s) or the transaction(s) reported — transaction reference number/order; reference number (where applicable),**[we note that this information is not standardised across the market and may not be useful to NCAs absent the development of standards]** — settlement date and time, **[we note that settlement is near instant on centralised exchanges and will not be additive]** — purchase price/sale price, — volume/quantity of crypto-assets. [Where there are multiple orders or transactions that could constitute market abuse the details on the prices and volumes of such orders and transactions can be provided to the competent authority in an Annex to the STOR.] — information on the order submission, including at least the following: — type of order (e.g. 'buy with limit EUR x'), — the way the order was placed, — the person that actually received the order **(if applicable; note: trading is often self-directed)**, — the means by which the order is transmitted. — Information on the order cancellation or alteration (where applicable) including:

	— the nature of the alteration (e.g. change in price or quantity) and the extent of the alteration, [Where there are multiple orders or transactions that could constitute insider dealing, market manipulation or attempted insider dealing or market manipulation, the details on the prices and volumes of such orders and transactions can be provided to the competent authority in an Annex to the STOR.] — the means to alter the order (e.g. via e-mail, phone, etc.). In case of reporting a suspicious behaviour related to the functioning of the distributed ledger, please provide as much detail as possible, including the impact it had on the validation of transactions and the method used to alter the functioning of the distributed ledger (where known).
SECTION 3 — DESCRIPTION OF THE NATURE OF THE SUSPICION	
Nature of the suspicion*	[Specify the type of breach the reported order(s), transaction(s), behaviour related to the functioning of the distributed ledger functioning, could constitute market abuse.]

Reasons for the suspicion*	[Description of the activity (transactions and orders, way of placing the orders or executing the transaction and characteristics of the orders and transactions that make them suspicious, behaviours related to the functioning of the distributed ledger functioning) and how the matter came to the attention of the reporting person and specify the reasons for suspicion. For crypto-assets admitted to trading on/traded on a trading platform, a description of the nature of the order book interaction/transactions that could constitute market abuse.]
SECTION 4 — IDENTIFICATION OF PERSON(S) RESPONSIBLE FOR THE ORDERS, TRANSACTIONS OR BEHAVIOUR RELATED TO THE FUNCTIONING OF THE DISTRIBUTED LEDGER TECHNOLOGY THAT COULD CONSTITUTE MARKET ABUSE ('SUSPECTED PERSON')	

Name (where applicable and where known)*	[For natural persons: the first name(s) and the last name(s).] [For legal persons: full name including legal form as provided for in the register of the country pursuant to the laws of which it is incorporated, if applicable, and Legal Entity Identifier (LEI) code in accordance with ISO 17442, where applicable.]
National Identification Number (where applicable and where known)*	[Where applicable in the concerned Member State.] [Number and/or text.] [If the National Identification Number is not applicable or known, provide a date of birth (for natural persons only).] [yyy-mm-dd]
Optional Identifying Information to be Provided on NCAs' Request **[The following information may be provided where applicable and known]**	

Address (where applicable and where known)	[Full address (e.g. street, street number, postal code, city, state/province) and country.]
Information about the employment: — Place — Position (where applicable and where known)	[Information about the employment of the suspected person, from information sources available internally to the reporting entity (e.g. account documentation in case of clients, staff information system in case of an employee of the reporting entity).]
Account number(s) (where applicable and where known)	[Numbers of the cash and securities account(s), any joint accounts or any Powers of Attorney on the account the suspected entity/person holds.] **[We note that this is unlikely to be known if accounts are not held with the CASP]**
Client identifier (where applicable and where known)	[In case the suspected person is a client of the reporting entity.] **[Client identifiers are internal and would not be consistent with identifiers used by other market participants]**
Relationship with the issuer of the crypto-asset concerned (where applicable and where known)	[Description of any corporate, contractual or organisational arrangements or circumstances or relationships]
~~SECTION 5 — ADDITIONAL INFORMATION~~ Background or any other information considered by the reporting entity relevant to the report	
[The following list is **indicative** ~~not exhaustive~~.] — The position of the suspected person (e.g. retail client, institutions),	

— The nature of the suspected entity's/person's intervention (on own account, on behalf of a client, validator of transactions in a distributed ledger system, other),
— The size of the suspected entity's/person's portfolio,

— The date on which the business relationship with the client started if the suspected entity/person is a client of the reporting person/entity,

— The type of activity of the trading desk, if available, of the suspected entity,

— Trading patterns of the suspected entity/person. For guidance, the following are examples of information that may be useful:

— trading habits of the suspected entity/person,

— comparability of the size of the reported order/transaction with the average size of the orders submitted/transactions carried out by the suspected entity/person for the past 12 months,

— habits of the suspected entity/person in terms of crypto-assets it has traded for the past 12 months, in particular whether the reported order/transaction relates to a crypto-asset which has been traded by the suspected entity/person for the past year.

— Other entities/persons known to be involved in the orders or transactions of which could constitute market abuse:

— Names,

— Activity (e.g. executing orders on behalf of clients, dealing on own account, operating a trading platform, validating transactions).]

— Relevant wallet addresses

SECTION 6 — DOCUMENTATION ATTACHED

[List the supporting attachments and material together provided with this STOR.

Examples of such documentation are e-mails, recordings of conversations, order/transaction records, distributed ledger technology records, confirmations, broker reports, Powers of Attorney documents, and media comment **in each case** where relevant **to information provided in the STOR.**

Where the detailed information about the orders/transactions/behaviours related to the functioning of the distributed ledger technology referred to in Section 2 of this template is provided in a separate annex, indicate the title of that annex.]