15 December 2022

Financial Stability Board
Centralbahnplatz 2
CH-4002 Basel
Switzerland

Re: International Regulation of Crypto-asset Activities

ConsenSys Software Inc. respectfully submits this letter in response to the Financial Stability Board's (FSB) consultation on the proposed framework for the international regulation of crypto-asset activities, dated 11 October 2022. Our response covers questions 6, 7, 8 and 10 of the consultation.

ConsenSys is the leading Ethereum software company. We enable developers, enterprises, and people worldwide to build next-generation applications, launch modern financial infrastructure, and access the decentralised web. Our software suite, composed of MetaMask, Infura, Quorum, Truffle, Codefi, and Diligence, is used by millions and supports billions of blockchain calls. Ethereum is the largest programmable blockchain in the world, leading in developer community, user activity, and business adoption. On this trusted, open source foundation, people around the world are building the digital economies and online communities of tomorrow.

As the FSB works on formulating its proposed recommendations, we encourage policymakers in all jurisdictions to pay attention to the innovation in the programmable blockchain ecosystem. This ecosystem not only offers the opportunity for economic growth but also the potential to make the internet more open, egalitarian, private, and secure.

We view this comment letter as an invitation to converse further regarding the ongoing development of Ethereum and other programmable blockchain ecosystems. We hope to engage with you in greater depth on the summarised points set forth below. We appreciate the opportunity to collaborate with you on the important task of bolstering innovation while mitigating the risks that new technologies may present. You may contact us at GATF@ConsenSys.net at your convenience.

ConsenSys' response

Should there be a more granular differentiation within the recommendations between different types of intermediaries or service providers in light of the risks they pose? If so, please explain. (Question 10)

We strongly support a more granular differentiation between different types of intermediaries and service providers in light of the risks they pose. In our view, the differentiation should be done on the basis of (i) the *type* of risks posed, and (ii) the *amount or severity* of risks posed. In respect of both points, a distinction should be drawn between what is commonly referred to as Centralised Finance (CeFi) and Decentralised Finance (DeFi). The Consultative Document does not seem to make this distinction.

(I) Differentiation based on the type of risks posed

There are different types of risks pertaining to DeFi and CeFi, as discussed in the recently published report commissioned by the European Commission and written by Prof. Tarik Roukny.[1] In his report, Roukny identifies distinct features of DeFi and how it differs from traditional finance. CeFi (as this term is often used to centralised crypto exchanges, custodians, and centralised trading platforms among others) has many of the features of traditional finance mentioned below, with the key feature being the existence of a centralised intermediary. Roukny identifies the following unique features of DeFi:

- "Universal access: No single entity has authority to bar entry of any participant. This applies to all sides of a financial service including users, developers, validators, etc. Traditional financial services which require screening of customers or licensing of service providers.

- Transparent and deterministic rules: Contracts and infrastructures supporting DeFi solutions are coded in public and autonomous scripts (i.e. smart contracts). This feature contrasts with traditional finance where contracts can be private and rules subject to arbitrary decisions.

- Non-custodial services: Holders of crypto-assets in a DeFi process have full control over the treatment of their assets once they are associated with holders' public addresses. This feature contrasts with the traditional use of custodial services by financial intermediaries to manage their clients' portfolios.

- Interoperable and composable protocols: DeFi protocols can be combined and interfaced at will to generate new solutions. The capacity to freely interoperate digital services and seamlessly interface protocols is intrinsic to the open and public nature of DeFi protocols. This feature is inherited from the legacy of open source systems in computer science. As such, there is no direct mirror of such a dynamic in the traditional financial system."

These differences mean that the risks present in traditional finance and CeFi may not be present in DeFi, which may make rules that would be appropriate for the former unsuitable for DeFi. On the

[1] Prof. Tarik Roukny, *Decentralized Finance: Information Frictions and Public Policies* (2022), accessed 13 December 2022, https://finance.ec.europa.eu/system/files/2022-10/finance-events-221021-report_en.pdf.

other hand, DeFi poses distinct risks that rules modelled on traditional financial regulation may not adequately address. We discuss below some of FSB's recommendations that may need to be adapted.

Same activity, same risk, same regulation (recommendation 2)

The "same activity, same risk, same regulation" approach must be applied carefully. We caution against applying the same rules to CeFi and DeFi activities that are, at first sight, similar, but function differently and pose different risks to markets, consumers and financial stability. For example, trading through an account with a centralised exchange is very different from connecting a self-custodial wallet to and exchanging assets through an Automated Market Maker (AMM). The former involves risks relating to human error, mismanagement or wrongdoing by representatives of the centralised exchange (such as fraud, theft, loss of assets, conflicts of interest). These risks are less relevant, if at all, to trading through an AMM. This is partly thanks to decentralised governance, as discussed below.

Governance framework (recommendation 4)

In respect of recommendation 4, we caution against advising authorities to "require compliance with rules and regulations for effective governance irrespective of the structures of activities and technology used to conduct the crypto-asset activities". The emergence of new structures means that regulations should be expanded to cover them, rather than restricting them through regulation that is not adapted to such structures.

Having "clear and direct lines of responsibility and accountability, clear definition of the roles and responsibilities of the management body and the decision-making process" is a step in the right direction, however it needs to be understood that the traditional 'one position-one person' or the "leadership body" do not exist in decentralised projects. While we acknowledge that some projects are 'decentralised in name only', we disagree with the suggestion that decentralisation is only 'useful' as a way to frustrate the identification of a responsible entity or for regulatory arbitrage. If done properly, decentralised projects have greater transparency and more dynamic adaptation to poorly performing members compared to centralised entities. As a matter of fact, the nature of governance has been evolving for much longer, due to the pressure of globalisation, digital environments, and technological specialisation moving to systems much more distributed, horizontal, and ultimately - decentralised.

Indeed, when the concept of decentralised autonomous organisations emerged in 2014, the main idea was to run organisations in a fully automated, human-independent manner. It was a response to the failures of the centralised systems, the lack of trust in very powerful leaders and corporations, and the disappointment in the existing governance mechanisms. While, initially, the proponents of DAOs and distributed ledgers were very libertarian, advocating for no governance, today

organisations are realising the need for a level of reliability and structure that is inspired by what some would consider "traditional". The governance mechanisms currently used in the biggest DeFi protocols try to marry the openness and lack of centralisation with frameworks that make participants accountable. To achieve this, protocols introduce guilds or subDAOs that are responsible for management of different areas - marketing, treasury, community growth, grants, etc. To become part of those groups, members of a DAO need to present their expertise by participating in the general community activities before being approved for the guilds. The more sensitive the topics the more walled the access to the guilds.

One of the biggest benefits of decentralised governance, from a regulatory perspective, is the transparency of decision making. Each protocol has a defined proposal process which has to be followed by anyone who wants to suggest an improvement. The discussion is kept public, through forums and mailing lists, so that at any point in time the reasons for making the decision are retractable. For lower impact votes, tools like snapshot.org are utilised. Members of the organisation have to connect their self-custodial wallet to prove they have voting rights, and votes are recorded on the platform. For high impact votes, usually there are a few stages of making a decision - first "temperature checks" using a snapshot, then (provided there is a clear agreement in phase 1) using on-chain voting tools. These record every vote on the distributed ledger, making that entry immutable, transparent and visible to everyone. This process has the potential to provide better auditability than traditional organisational structure with boards of directors making decisions behind closed doors.

The decisions are rarely immediately executed for two main reasons. One, it gives an opportunity to people who disagree with the decision to leave the protocol (sell their governance tokens and leave the community). Two, it prevents attacks whereby a malicious actor manipulates the community to make a bad decision and uses the time pressure to implement that decision. Decentralised governance is characterised by a great degree of caution and planning for the worst case scenario.

Next, decentralised governance is not a binary state. Most often we talk about a progressive decentralisation. To quote a paper by one of the leading researchers in the industry "[it is] a process in which founding teams relinquish control by degrees, over time. Doing so step-by-step allows teams to focus and creates a path toward regulatory compliance, including issuing tokens that hopefully will not run afoul of securities regulations".[2] The reason behind progressive decentralisation is to enable the community to learn how to do governance, slowly opening more sensitive topics to a public vote. Any potential regulation should be flexible enough to allow for a governance framework that changes over the course of the project.

---

[2] Jesse Walden, *Progressive Decentralization: A Playbook for Building Crypto Applications* (2020), accessed 15 December 2022, https://a16z.com/2020/01/09/progressive-decentralization-crypto-product-management/.

Moreover, decentralised governance may encourage longevity and successful continuance of a project. The evolution of a protocol is driven by many people, so it is not reliant on a single founder or a small leadership group, and allows for a flow of contributors in and out. This also brings greater diversity of voices and gives an opportunity for newcomers to spot bad behaviour or poor governance design. From a regulatory perspective, this brings challenges in terms of identifying who is "in the community", but long term it brings better outcomes for participants and introduces an extra level of control.

Finally, as FSB points out and as evident from recent events, there have been projects that claimed to have decentralised, autonomous governance, but in practice were run by a small group of publicly known "leaders" that had a disproportionate influence over the project. Insufficient decentralisation made wrongdoing easier to conduct and cover up; in contrast, a properly auditable track of votes, decisions and a community driven model could have prevented malicious actions.

The industry is still grappling with the question of what constitutes "sufficient" decentralisation. The insufficient decentralisation that we observe today comes from numbers - there are not enough members in decentralised projects who actively participate in the governance. A project is not decentralised when it has a 10 or 20 people committee that participates in each vote. It is only when we reach numbers in the 100's that the promise of decentralisation is delivered. One of the reasons for lack of participation is lack of clarity as to the potential legal liability of people participating in governance votes.

In this respect, we would like to note the approach taken by the European Union (EU) in the Markets in Crypto-Assets Regulation (MiCA). According to Recital 12(a), MiCA "applies to natural, legal persons and other undertakings and the activities and services performed, provided or controlled, directly or indirectly, by them, including when part of such activity or services is performed in a decentralised way." Based on our interpretation, MiCA will apply if there is a clearly identifiable party, which could be the case for projects that are "decentralised in name only", but will not apply to projects that are in fact decentralised. The implementation and enforcement of MiCA will be key to providing guidance on the scope of its application. National competent authorities should assess the level of decentralisation on a case by case basis and take a proportionate approach to enforcement, so as not to discourage people from participating in governance voting.

Effective risk management framework (recommendation 5)

The above discussion is also relevant to recommendation 5. An effective risk management framework enhances user confidence, and many DeFi protocols already have some form of risk management in place. However, we caution against overly prescriptive rules requiring a specific form of framework modelled on risks pertinent to centralised entities. These risks typically relate

to the existence of insider actors, potential abuse of power, and information asymmetries, all of which are less present (if at all) in DeFi.

On the other hand, given the non-custodial nature of DeFi projects, users have fewer avenues to recover lost funds in case of a technical failure of the protocol compared to claiming losses against a centralised entity. A risk management framework for DeFi should therefore focus on reducing risks of hacks and bugs. Best practices with respect to software development, already applied by responsible actors in the space, include having a third party code audit conducted before the software is released. ConsenSys specialises in this type of service through its Diligence offering. Diligence maintains a suite of blockchain security analysis tools and pairs up that service with in-person review of smart contract code by a qualified code auditor. This service has been increasingly popular among smart contract developers who wish to avoid vulnerabilities, employ mitigation best practices, model possible threats, and test their software before it is published. The Diligence team has worked on projects for many of the most notable names in the blockchain developer community, such as Uniswap and Aave. Industry-led solutions like software auditing will play an important role in keeping blockchain network users safe from hacks and bugs.

DeFi projects should also analyse their interdependencies with third party actors, such as oracles. In this respect, we encourage FSB to consider Prof. Roukny's suggestions for supporting a stable and efficient development of oracle services.[3]

Data and disclosures (recommendations 6 and 7)

As explained above, one of the advantages of open source programmable software is transparency - the ability to see what is happening in real time on the blockchain network. However, we acknowledge that only technically proficient parties are able to analyse on-chain data in a way that would be useful for auditing and monitoring purposes. We would encourage the FSB and the relevant national authorities to not only look at top-down regulatory initiatives, but also cooperate with the industry to find ways to leverage the potential of blockchain data in a way that would enhance transparency of activities conducted on blockchain networks.

Similarly, while open source code that underpins DeFi protocols or other blockchain applications can in theory be read and verified by anyone, in practice few users have the technical capabilities to do so. FSB's proposal to make available information about the functionality and risks of software "in an understandable manner for the intended audiences" would enhance user confidence and enable users to make informed decisions.

(II) Differentiation based on the magnitude/severity of risks posed

[3] Prof. Tarik Roukny, *Decentralized Finance: Information Frictions and Public Policies* (2022), p. 42-46, accessed 13 December 2022, https://finance.ec.europa.eu/system/files/2022-10/finance-events-221021-report_en.pdf.

We support FSB's emphasis on applying the recommendations proportionately to the risk, size, complexity and systemic importance of the given service provider. To adhere to this principle, we encourage a more granular differentiation between the different types of service providers both during the legislative process and during implementation.

The programmable blockchain ecosystem is characterised by a large number of individual developers, or small groups of developers, innovating and spinning out new projects quickly. Programmable blockchains like Ethereum allow anyone to write and publish code that is accessible to anyone else in so long as they have access to the blockchain network and the ability to compose and transmit on-chain transactions. In recent years, the increase in blockchain software development, as reflected in the number of developers committed on platforms such as Github to solve particular programming problems, has been notable. According to one analysis published at year end 2021, over 18,000 monthly active developers were working on blockchain programming projects, with over 34,000 new developers migrating to the blockchain ecosystem in 2021.

This trend is also something that ConsenSys is working hard to bolster by offering software platforms that permit developers to innovate new tools that can be shared with an increasingly broad user base. While the ConsenSys offering MetaMask is recognized as the world's most popular Ethereum self-hosted wallet, few recognize that it is as much a developer platform as it is a client-side key management solution. The clearest expression of this is the release of MetaMask Flask, which is an experimental MetaMask application that allows developers to create new features that can be tested and refined before offering to the public more broadly. The first feature offered through Flask is the Snaps system, which allows developers to create their own programs that expand the functionality of the wallet. ConsenSys is not alone in working to bolster developer engagement and productivity. Examples abound of a thriving developer ecosystem where brilliant minds from all over the globe are tackling the novel problems presented by a nascent technology.

Products and services that result from this innovative process must not be constrained by burdensome compliance requirements that smaller projects might not have the resources to comply with. This could lead to crowding out smaller players and strengthening the position of established centralised entities, at the expense of innovation.

The crypto industry as a whole has suffered intense market stress over the past six months. The collapse of numerous centralised players has fleshed out the risks associated with lack of supervision over centralised issuers and providers of crypto asset services. These risks are already well understood and defined in FSB's Consultative Document. Further, authorities already have experience with regulating centralised players and financial intermediaries in traditional finance.

In contrast, as demonstrated in our response, risks relating to programmable blockchain and DeFi are novel, less understood, and cannot be addressed by a 'one size fits all' regulatory approach. In our view, the most effective way to safeguard financial stability and protect users would be to focus, as the first step, on the risks posed by centralised issuers and providers of crypto asset

services (including players that are 'decentralised in name only'). The EU has rightly included a carve out for decentralised projects in MiCA, and has rightly recognised the need to examine the programmable blockchain ecosystem in more detail before consulting on potential regulation affecting it. We encourage FSB and national authorities to follow the same approach.

Finally, we note DeFi is currently a fraction of CeFi in terms of its size and interconnectedness to the traditional financial system. These two factors alone suggest that authorities should prioritise addressing financial stability risks posed by CeFi.

Have the regulatory, supervisory and oversight issues and challenges as relate to financial stability been identified accurately? Are there other issues that warrant consideration at the international level? (Question 8)

We would like to focus on section 3.4 (*Risk management related to wallets and custody services*). MetaMask specifically is one of the most broadly used self-custodial wallets in the world by both Web3 developers and users. It is open source software[4] that can be downloaded from the Apple or Google app stores and run locally as either a mobile application or a browser extension. The software is maintained by a development team at ConsenSys and also supported by a global community of developers and designers who wish to democratise access to the decentralised web.

As FSB points out, the risks relating to use of self-custodial wallets are two fold. First, as FSB notes, "only the users themselves can access or recover their private keys. In general, users are responsible for maintaining their own wallets." This responsibility carries with it a risk of loss or theft of private keys due to actions on the part of the user. Despite our ongoing commitment to the security of MetaMask users, scammers and other online criminals continue to target users through a variety of schemes. The MetaMask team has extensive educational materials and FAQs drafted to guide MetaMask users through smart and safe use of the wallet.[5] ConsenSys has also partnered with Phishfort, a third party anti-phishing solution, so that phishing threats against MetaMask users are identified and taken down.[6]

MetaMask developers and Ethereum developers more broadly recognize these threats and believe it is important to mitigate them not only through vigorous law enforcement but also through technology. For example, Ethereum community developers have since 2016[7] considered ways to separate the account from the private key, whereby having the latter stolen did not necessarily

[4] *See* https://github.com/MetaMask (accessed 15 December 2022).
[5] *See*, *e.g.*, https://metamask.zendesk.com/hc/en-us/articles/360015489591-Basic-Safety-and-Security-Tips-for-MetaMask (accessed 15 December 2022).
[6] *See* https://metamask.zendesk.com/hc/en-us/articles/5168786362779-How-to-report-a-scam (accessed 15 December 2022).
[7] *See* https://github.com/ethereum/EIPs/issues/86 (accessed 15 November 2022).

mean that the former would be also. This concept has been referred to as account abstraction. ConsenSys remains at FSB's disposal to provide further details on this technology.

It is widely recognized that the current system, which is entirely dependent on public-private key pairs and is thus highly vulnerable to user predation, faces a real challenge to achieving its aim of scaling to billions of people with ease. The innate incentive for the Ethereum community to improve security should give pause to any well meaning regulator who might otherwise think the sole solution lies with new statutes, regulations, or administrative guidance.

Scams and phishing attacks can be devastating for affected individuals. However, as each user stores their private keys on their own device and no centralised entity has access to those keys, the effects of scams and phishing schemes tend to be isolated and are unlikely to pose broader financial stability risks.

Second, FSB points out the risk of the wallet software being disrupted by a cyber incident. Security is critical for MetaMask to be a powerful and reliable tool for both developers and users. Its code has been audited by security experts and independent researchers, and the audit reports are publicly available.[8] The MetaMask team at ConsenSys sponsors a bug bounty program that rewards volunteers who report vulnerabilities so they may be patched.[9] We are also investing in novel research and development into new security technologies with applications far beyond our ecosystem, such as LavaMoat.[10] Technical risks relating to the quality of software or a technical product currently are not, and should not be, addressed through regulation. Any potential losses resulting from cyber incidents affecting unhosted wallet software should be resolved between the parties according to the Terms and Conditions of the software provider.

Does the report accurately characterise the functions and activities within the cryptoecosystem that pose or may pose financial stability risk? What, if any, functions, or activities are missing or should be assessed differently? Do you agree with the analysis of activity patterns and the associated potential risks? (Questions 6 and 7)

The list of activities is generally complete and accurate. However, we would like to comment on the following aspects of Annex 1 (*Essential functions, risks and relevant international standards*).

Software developers

We respectfully object to referring to software developers as "service providers" in the Consultative Document. Further, referring to software development as one of the crypto activities that might need to be regulated alongside activities such as custody or provision of a centralised

[8] *See* https://metamask.io/security/ (accessed 15 November 2022).
[9] *Id.*
[10] *See* https://medium.com/metamask/how-metamasks-latest-security-tool-could-protect-smart-contract-developers-from-theft- e12da346aa53 (accessed 15 November 2022).

trading platform is inappropriate. A clear distinction must be drawn between the development of the underlying technology that supports a product or service, and the actual product or service that is offered to the public. The former is typically not regulated in any sector at the moment, as it does not represent inherent risks (subject to limited exceptions, mainly for technologies that have the potential to cause non-financial harm, such as certain weapons). Only when the underlying technology is used to build a product or service that is offered to the public do we need to consider any potential risks relating to such offering.

For example, the internet infrastructure that powers https websites is not constrained by legal or regulatory rules, while an online marketplace leveraging that infrastructure might be. Similarly, publishing a piece of open source code that may be used to create blockchain-powered products or services must be distinguished from what is actually offered to and used by the public. A contrary proposition might give rise to concerns among software developers that, by developing and publishing code, they will breach some inconspicuous regulatory rules and be exposed to legal liability. Such concerns would have a chilling effect on developers' willingness to innovate and develop the blockchain ecosystem.

Unhosted wallets

In respect of the provision of self-custodial wallets, FSB correctly notes that "there is no corollary in traditional finance". However, we respectfully disagree with FSB's qualification that self-custodial wallets "have some resemblance to broker dealer, money transmission, [or] depository". MetaMask is essentially a piece of software that encrypts the private keys leading to the part of the Ethereum blockchain where the owner's funds are held (an "externally owned account" on the Ethereum blockchain), and temporarily decrypts the private keys when the owner signs a transaction. In other terms, it is a user interface that permits users to access and execute transactions using their account.

The direct interaction with the blockchain makes use of self-custodial wallet software fundamentally different from a broker, which executes transactions on behalf of a client, or a money transmitter, which takes customers' funds and sends them on their behalf. A depository institution takes control of and safeguards clients' funds, and may also be authorised to use clients' funds for internal purposes such as lending to other clients. A self-custodial wallet is fundamentally different in that only the holder of the private key may access the funds; the software wallet provider has no access to users' funds.

Staking

In respect of providers of Staking as a Service and Delegated Proof of Stake, we agree with FSB's assessment that there is "no direct corollary in traditional finance", but respectfully disagree that these providers "can resemble issuers (e.g., of interests in a pooled vehicle or other investment opportunity)". In our view, the key difference lies in the way revenue is generated through staking.

Staking as a Service or Delegated Staking providers do not issue the tokens constituting staking rewards. The tokens are generated by the protocol during the validation process. Validation entails running code that verifies new transactions do not violate rules of the blockchain protocol and are consistent with its transaction history.

Custody

The description of "provision of custodial (hosted) wallet and custody services" includes DeFi protocols among "custody service providers" on the basis that they "manage users' cryptoassets or information about their interests in crypto-assets using smart-contracts that pool users' crypto-assets, typically as part of DeFi protocol offering exchange or lending activities." Depositing tokens into a smart contract (e.g. a liquidity pool in an AMM) should not necessarily be treated as custody. This would be an undue extension of the concept and against the parties' expectations. The governance of the protocol would need to be examined on a case by case basis to determine whether there is an individual or entity that retains an "administrative key" to that smart contract, and the potential level of control over users' assets while they are deposited in the smart contract.

Respectfully Submitted,

CONSENSYS SOFTWARE INC.

by:

Natalie Linhart, William C. Hughes