CONSENSYS

Via Email
2 June, 2023

Fintech-Innovation Hub
Autorité de Contrôle Prudentiel et de Résolution
Banque de France

Re: “Decentralised” or “disintermediated” finance: what regulatory response?

ConsenSys Software Inc. respectfully submits this letter in response to your discussion paper concerning decentralised finance (“DeFi”) published in April 2023. We are encouraged that the ACPR and the Banque de France are consulting with the public, and the crypto ecosystem in particular, on these novel and complex issues. We generally agree with your “disintermediation” framing of the programmable blockchain space and welcome the opportunity to discuss with you and policymakers across government about the innovation in the programmable blockchain ecosystem.

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 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 the email addresses set forth below at your convenience.

Background on ConsenSys

ConsenSys was founded in 2016 after the launch of the Ethereum protocol with the goal of facilitating decentralisation through the development of global, blockchain-based computing platforms. We believe that decentralised networks like Ethereum will allow people to collaborate in ways never before possible and change not only finance but also commerce and culture. We have dedicated our personnel, product offerings, and resources to help drive this evolution.

ConsenSys is a 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. Ethereum is the largest programmable blockchain in the world, leading in developer community, user activity, and business adoption. On this open-source foundation, people around the world are starting to build the digital economies and online communities of tomorrow. Our software suite, which includes MetaMask, Infura, Diligence, Besu, Teku, and QBS, is used by millions and supports billions of blockchain calls.

MetaMask specifically is one of the most broadly used unhosted wallets in the world by both Web3 developers and users. It is open-source software[1] 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.

Few recognize that MetaMask 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 a MetaMask application that allows developers to create new features that can be tested and refined before offering to the public more broadly.[2] 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.[3]

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. Nations around the globe are rightfully curious and excited about the opportunity to attract talent by leading in this space.

Consultation questions

Q1: Do you have any comments on the definition of DeFi used in the paper? Does the document correctly reflect the real level of decentralisation of services?

We agree with the notion that the essence of DeFi is replacing the trust between players with the transparency and immutability of computer code, and that this code serves to disintermediate transactions that have traditionally required an intermediary.

We also agree that many projects currently remain reliant on project founders, with some intent to eventually decentralise. It is important that ambitions to decentralise be sincere and that such processes are transparent. Deceptive actions and misleading marketing about decentralisation efforts are a serious concern and may even violate the law in many jurisdictions. With legitimate efforts to decentralise, it is critical that regulatory regimes do not construct barriers that explicitly require or practically result in centralization.

We disagree that protocol staking, which is the mechanism for ensuring the data integrity of a chain, should be considered a part of DeFi. This type of activity, including on-chain services that

[1] *See* https://github.com/MetaMask (accessed June 2, 2023).
[2] *See* https://metamask.io/flask/ (accessed April 29, 2023).
[3] *See* https://docs.metamask.io/guide/snaps.html#what-is-snaps (accessed April 29, 2023).

make proof of stake validating more accessible, is not financial in nature but instead represent technical services that users perform and for which they receive compensation.

In fact, we urge the ACPR and the Banque de France to lead in differentiating between staking as a way of securing proof-of-stake networks, including differentiating between the many ways in which users can stake[4], and crypto asset lending, which has an entirely different risk profile.

As DeFi matures, and more institutions participate, there will likely be applications that are designed to cater to their regulatory requirements.

Q2: In your opinion, which use cases of DeFi are likely to develop in the future? Can they serve the real economy?

Any real world transactions, including those that are financial in nature, which can be executed through code deployed on a programmable blockchain can theoretically be developed. These include tokenizing real world assets such as real estate, invoices or royalties, and use cases enabling remittances and cross-border payments. The development of oracles, which introduce off-chain data to blockchain transactions, will be an essential element as to what types of transactions will be possible.

Q3: What do you think about the concentration phenomena described in section 1-5 of this document?

It is not surprising that Ethereum has a considerable proportion of DeFi activity given that it was the first programmable blockchain and is the ecosystem with the broadest and most diverse application development. As newer programmable blockchains establish track records of performance and offer developers different trade offs relating to speed, cost, and security, we would not be surprised if developers used different chains for different purposes. The barriers to entry are low and concentration is likely a time-limited phenomenon which might become less meaningful as the industry grows. That said, even if the concentration of activity on Ethereum increased, then that would be no cause for concern as long as the security and reliability of the network continues to improve, as it is expected to do.
With respect to the concentration of activity in specific DeFi applications, it demonstrates that certain projects have experienced meaningful adoption despite being relatively new. That the number of highly-used applications is very small compared with the overall number of applications is, in our view, no different than the dynamic between the total number of start up companies in the tech economy and the very small percentage which become highly-successful. Said differently, most ideas will ultimately not work out, but those that do work may usher in a new paradigm from which further innovation can spring. We are early in that process with respect to DeFi and Web3.

[4] For more details on staking and the important differences between solo staking, custodial staking, self-custodial staking-as-a-service offerings and smart contract-facilitated liquid staking, please see https://consensys.net/blog/news/staking-is-data-validation-not-investment/ (accessed June 2, 2023).

Q5: Do you have any comments on the description as regards risks related to decentralised governance?

We generally agree with the particular risks the discussion paper identifies with respect to token-based governance. Of particular concern are instances in which a project's governance is publicly understood to rely solely on a token holder vote but, in practice, works differently. Whether public policy should seek to mitigate any governance risks should depend on the activity of the application that is being governed. For instance, relatively small projects and ones that have no meaningful financial function likely do not present risks serious enough to warrant any regulatory oversight, let alone from financial supervisory agencies.

We also note that the Markets in Crypto-assets Regulation ("MiCA") will address some of the identified risks. In particular, the requirement to obtain authorisation for the activity of "placing crypto-assets" is expected to address the instances of misleading marketing or lack of disclosure around the launch of new tokens.

Q6: Do you think that layer 1 solutions can exacerbate the security issues of the blockchain infrastructure? What about layer 2 solutions? In your opinion, are there significant differences in this respect between the layer 2 solutions considered?

We take this opportunity to highlight that ConsenSys has recently introduced a developer-friendly zk-Rollup solution called Linea, which was developed in large part by a team of French developers.[5] Linea will enable the creation of a new wave of applications that rely on the security model of the Ethereum blockchain. By harnessing the power of zero-knowledge proofs and maintaining full Ethereum Virtual Machine ("EVM") compatibility, Linea offers developers the ability to build scalable decentralised applications (or "dapps") or migrate existing ones seamlessly from Ethereum mainnet, without the need for extensive code modifications or smart contract rewrites. Linea's innovative prover[6] software design offers faster transaction speeds and reduced gas costs while maintaining security.

The discussion paper correctly notes that the prover part of ZK-Rollups is not yet decentralised. As an initial matter, running a prover is computationally intensive, which means that this service is currently provided by a limited number of players. However, developers are working on addressing this by reducing the cost of running a prover and allowing multiple provers to run in parallel in a sustainable way.

Many zk-Rollups, including Linea, have expressed the intention to eventually decentralise. The estimated timeline for such a transition cannot be stated with certainty, but it is essential that regulatory authorities do not implement constraints that hamper the transition from centralised to decentralised provers. And there is reason to believe that there will be market forces that

[5] *See* https://linea.build/ (accessed June 2, 2023).

[6] A prover is anyone that can run the software/hardware needed to produce a proof of the correct execution of EVM instructions.

encourage decentralisation. For instance, provers are rewarded for their work through Layer 2 ("L2") fees. The economic incentives to perform this work are comparable to validation activities on proof of stake blockchains like Ethereum or mining on proof of work chains like Bitcoin. In each of those cases, a diverse and decentralised group of validators and miners has emerged in response to economic incentives, as the rewards they receive for their services outweigh the operational costs.[7] We expect the same will happen on ZK-Rollups.

Working towards decentralisation of L2 transaction sequencers ("sequencers") is also important. A centralised sequencer presents a risk that it can rewrite the history of the L2 chain, changing transfer histories until the rollup is validated on L1. Decentralisation avoids this risk. With permissionless participation in sequencing, the possibility to rewrite the history or revert a transaction is much lower because it would require the sequencers to collude with each other. Thus, decentralisation will give L2s more reliable transaction finality.

We additionally recognize that how a L2 protocol handles its data impacts its risk profile. Every rollup must, by definition, post L2 transactions on the L1 to let anyone recalculate the state of the data themselves, independently from the L2 operator. L2 chains that prefer off-chain data availability, which have been referred to as "Validiums",[8] raise concerns about auditability of transactions, as it may not be possible to have the state of the chain verified freely by anyone. Linea, by way of example, was designed to avoid this risk by posting its L2 transactions on L1 as calldata. This allows anyone to verify the state of the blockchain, thereby increasing transparency and security.[9]

The main concern related to the maturity of ZK-Rollups that is not expressed in the discussion paper relates to the risk of technical bugs on the constraint that is used to generate the zero-knowledge proof. This risk is minimised by (i) robust stress-testing of the network on a realistic type of usage, simulating a large number of users interacting with a diverse range of real world dapps, and (ii) a full stack auditing and peer review of the arithmetical constraints that will be used by the proving system to prove the execution of every functional specification of the EVM. With respect to Linea, it allows for peer review by releasing the full stack open source code for public scrutiny and working closely with the broader zero-knowledge community to crowd-source potential improvements.

We do not agree that L2 chains present any meaningful risks to interoperability. L2 chains are part of a shift away from purely monolithic blockchains such as Ethereum towards a modular

[7] In the case of Ethereum validation, opening a new validator requires depositing 32 ETH; Bitcoin mining requires investment in equipment and ongoing operational costs.

[8] *See* https://ethereum.org/en/developers/docs/scaling/validium/ (accessed June 2, 2023).

[9] In the future, the industry could envision L3 or adjacent L2s that will rely on restaking data availability providers or consortium data availability approaches for use cases that put greater emphasis on performance or privacy requirements.

approach by decoupling the execution layer from consensus, settlement and data availability layer. This modular approach will not impact the interoperability of L2 chains, as there are multiple ways to implement a trustless bridge across two different L2 chains. If the source L2 is a zkEVM, then its L1 can act as a trustless bridge. In the case of an Optimistic Rollup, solutions like shared sequencers can achieve the same benefits. Moreover, L2 to L2 interoperability can also be achieved using a Hashed Timelock Contract or zkBridges. The latter facilitates interactions between different L2 chains through cross-chain liquidity pools.

Currently, the main drawback of multiple L2 chains is the absence of composability, which is one of the most interesting features of EVM chains and that propelled the early growth of the DeFi ecosystem. There are novel approaches to improving composability, including atomicity or async composability, but these will take multiple years before they will be fully explored and potentially adopted by developers.

Q7: Do you think that the use of rollups or similar solutions will result in less transparency of information for an observer?

In the case of a rollup, the same information will be simultaneously present on the L1 (as calldata) and the L2 (as the global state, blocks and transactions). There is no loss of transparency for an observer.[10]

Q8: Do you have any comments on the description (provided in section 2-3) of the risks related to the application layer of DeFi?

We generally agree with the description of the major risks attendant to blockchain applications. We particularly agree that open source smart contract code, which allows all nefarious actors the opportunity to expose and take advantage of vulnerabilities, ultimately results in more secure applications over time.

We further agree that composability is a trade-off, namely that smart contracts calling other smart contracts can greatly increase what transactions are possible but also can proliferate buggy or malicious code if precautions are not taken.

Lastly, we recognize the importance that data availability plays in DeFi and the crucial role of oracles in that process. Despite their infancy, oracles have proven remarkably efficient and reliable to date, while risks certainly remain. General understanding of oracles and their risks should improve throughout the crypto ecosystem and among policymakers if the proper policies

[10] However, it is true that any scalability solution can provide a way to implement new use cases that are not possible on L1 today (giving the prohibitive cost of gas fees), including account abstraction and client-side zkDapps. These use cases can, and most probably will, introduce greater privacy by limiting the transparency of information for an observer (or even for the operator of the L2). But thanks to zero-knowledge proofs, the L2 will nevertheless be able to ensure that the execution is correct and fair and network rules are being complied with.

are to be fashioned. Oracle manipulation, which is not a meaningful concern currently in our view, is nonetheless a serious issue and one that may warrant a public policy approach.

Q9: Do you have any comments on the identification of DeFi risks for retail customers (section 2-4-1)?

Everyday users of DeFi applications would be best served by reliable, coherent, and informative disclosures about how a particular protocol works and risks attendant to its use. These would be more easily implemented and policed, and far more effective, than explicit restrictions on the type of transactions in which specific users are permitted to engage. Individuals who knowingly misrepresent risks or the benefits of particular applications in order to profit off of the misunderstanding of others should properly be the subject of regulatory or law enforcement scrutiny.

Q12: Do you have any comments on the description of the potential AML/CFT risks of DeFi (section 2-4-4)?

We agree that pseudonymous blockchains do not provide anonymity, as is widely believed. We recognize that illicit activity on-chain, while not remotely comparable in volume or frequency to illicit activity in traditional finance, is a serious matter that requires both public policy and technical solutions to address. We note that the traceability of blockchain transactions has been a boon to law enforcement in their efforts to identify illicit behaviour on-chain. Out of our many interactions with law enforcement around the globe, not once has any agency expressed to us that digital assets are a space where their effectiveness is meaningfully undermined. Indeed, our greater concern is ensuring that, as more people and commerce moves on-chain, current norms around privacy are not seriously eroded both in the law and society more broadly. Blockchain analytics represent a useful way to reduce AML/CFT risks in DeFi and its use by law enforcement should be encouraged, but we must do so in a way that does not unduly sacrifice the privacy of lawful users, who represent the overwhelming majority of DeFi participants.

Q13: In your opinion, are there any other risks that should be taken into account which are not mentioned (or not given sufficient attention) in the document?

Our view is that this discussion paper presented as comprehensive a list of risks as we have ever seen, and where we may disagree, it is in all likelihood a question of degree or emphasis. We truly welcome the open-minded approach of how public policy may be used to minimise risk and where technology and market-based approaches are more appropriate.

Q14: Should public blockchains be governed by a framework or by minimum security standards?

Given the composability of blockchain applications, the security of the base layer component (*i.e.* L1 blockchains) is clearly important. However, regulating public blockchains by way of implementing certain minimum standards would not achieve the desired security outcomes and would come at the cost of greatly restricting innovation. Additionally, the practical difficulties of imposing jurisdictionally-determined standards on otherwise global ecosystems should not be ignored and would render any such framework either ineffective or, worse, counterproductive.

Public blockchains are purpose agnostic. It is a technology that can be used for both purely non-financial, non-commercial purposes, and also for financial applications. Like the approach taken with the broader internet, and communication channels more generally, regulation should not focus on the underlying blockchain technology infrastructure, but on commercial applications built on blockchains. Those applications are what users actually interact with and, depending on use case, where more acute risk of consumer harm is likely found.

The discussion paper proposes that the underlying code of a public blockchain should be certified *a priori*. Putting aside whether such a measure is even feasible, it is already happening in practice. A new blockchain that has not passed multiple audits or has demonstrated its robustness over time has minimal chances of any meaningful adoption. The success of a blockchain is ultimately determined by an active developer community building applications on the blockchain, and developers are unlikely to do so if the blockchain was not successfully audited and has a good track record of reliable performance. Further, regulation of core protocol development in a particular jurisdiction would likely ensure that the impacted developer cohort finds more friendly locations from which to continue their work.

The discussion paper also proposes rules on the minimum number of validators required on a public blockchain. In our view, this would be unworkable. First, any pre-defined number would most certainly be arbitrary, as the number that is required to ensure security is different for each proof of stake blockchain and depends on different variables such as the number of native tokens required to become a validator and their value in fiat currency. Moreover, requiring a minimum number of validators would also create a meaningful barrier to entry for new projects, which would limit competition.

Q15: Should public authorities supervise the concentration level of validation capacities on public blockchains? If so, through what kind of measures?

No. Problems similar to those set forth above would arise if public authorities tried to prescribe the maximum degree of concentration of validation activities on public blockchains. A rules-based approach at this stage of technology development will very likely result in ill-intended actors gaming the system and well-intended actors being dissuaded by its rigidness.

A better solution to concentration risks is self-regulation prompted by the inherent incentive of users and developers to keep the blockchain safe. The Ethereum community has repeatedly shown its ability to address issues through social intervention and new technological solutions, as discussed below. This approach is more effective, nimble, and ultimately more beneficial for users than prescribing a concentration limit through regulation.

In 2022, before the Merge, the Ethereum community had an active discussion about the proportion of validators running for Lido, the most widely used liquid staking protocol.[11] The Ethereum community's answer to Lido's market position has been more competition and more user choice, as demonstrated by the diversifying landscape of staking providers.[12] Developers are exploring new technological solutions aimed at further bolstering the decentralisation of the Ethereum staking ecosystem.[13] The community is also focused on increasing the awareness of network control among users to nudge them towards a diverse range of staking providers.[14]

Nevertheless, some players will inevitably attract a greater proportion of staked ETH than others, at least for a period of time, due to a variety of factors that users value. These factors include product features and a long operational track record. Some level of concentration is to be expected and, as long as users continue to have a wide range of staking providers to choose from, should be acceptable.[15]

It is also worth briefly mentioning another aspect of Ethereum's architecture which supports network resilience through a self-imposed limit on concentration of control over the network. The Ethereum community maintains a number of "clients," each of which is a software program that implements the Ethereum programming specifications and that verifies data against the protocol rules, keeping the network secure and orderly. These clients happen to have been developed in different locations across the world and run by different teams.[16]

This client diversity makes the network stronger by reducing any single points of failure.[17] This was demonstrated during a recent event when Ethereum experienced a temporary delay in block finalisation for a short period of time. This was due to a technical issue with two of the

[11] *See* https://notes.ethereum.org/@djrtwo/risks-of-lsd (accessed June 2, 2023).

[12] *See* https://dune.com/hildobby/eth2-staking (accessed June 2, 2023).

[13] For example, distributed validator technology allows for distributing the job of an Ethereum validator among a set of distributed nodes in order to improve resilience (safety, liveness, or both) as compared to running a validator client on a single machine. *See https://github.com/ethereum/distributed-validator-specs* (accessed June 2, 2023).

[14] For example, MetaMask users can stake with different staking providers through the MetaMask Portfolio interface and are able to sort the providers by network control. This gives users information on the estimated percentage of staking validators associated with each provider (with the lower amount of network ownership suggesting greater decentralisation benefits), allowing them to make an informed choice.

[15] With respect to Lido, it is important to note that the node operators providing services to Lido are not controlled by a single entity. In fact, there are 29 different, independent node operators that have been selected by holders of Lido governance tokens (LDO), including ConsenSys's staking service. Therefore, while LDO holders are the only ones able to add or remove node operators, from a network security standpoint, the ETH staked through Lido is spread across a diverse range of validators. See https://operatorportal.lido.fi/node-operator-onboarding-history (accessed June 2, 2023).

[16] See https://ethereum.org/en/developers/docs/nodes-and-clients/#what-are-nodes-and-clients (accessed June 2, 2023).

[17] For more information please refer to https://clientdiversity.org/#why (accessed June 2, 2023).

consensus clients, which was soon identified and fixed. The three remaining clients were still able to propose blocks and create attestations, which helped ensure that there was no “outage” of Ethereum, only a temporary delay in block finalisation.[18]

In sum, the best approach to ensure reliable, secure, and resilient blockchains is to encourage software development, diversity of software offerings, and organic incentive structures.

Q16: Do you agree with the analysis provided in the paper on the merits and limitations of private blockchains (section 3-1, regulatory scenario B)? Should private blockchains operated by private operators be regulated through a supervisory framework, if at all?

Private blockchains can be useful for certain solutions, namely those in which the costs of running the infrastructure is outweighed by the value the system creates for its permissioned participants. But it is in the public interest to have an active ecosystem of both public and private blockchains, each with their own distinct benefits and disadvantages. The suggestion to switch purely financial functions to private blockchains would be an undue market intervention on the part of public authorities.

As an initial matter, such financial functions—or some subset of them—may not turn out to be economically viable on private blockchains, and thus such restriction would prove over time to be a *de facto* ban. Second, as a normative matter, regulation should not “pick winners” in technology or restrict use of permissionless public networks to only certain functions. Doing so would harm innovation and would ultimately be bad for users as, in our view, only public, permissionless blockchains fully realise the key benefits of blockchain technology, such as immutability, resilience and transparency. For example, the benefits of Ethereum client diversity discussed above are not present in private blockchains, which are run by a single entity or a group of entities controlling the network in a centralised manner.

Simply said, you can use and develop on top of a public blockchain without the high cost of having to build out all of the data integrity infrastructure that the chain and its nodes and validators provide. You cannot use and develop on top of a private blockchain without providing that expensive infrastructure yourself. The economics of the two models are meaningfully different, with recent results indicating that public blockchains have a bright future while private blockchains have challenges. As stated above, requiring certain applications to reside only on private blockchains may precipitate their inevitable failure, which is not practically different than simply banning those applications outright. To the extent some applications could effectively exist on either type of network, the market should be the arbiter of which they exist on (perhaps both), not regulation.

[18] For more details please refer to https://offchain.medium.com/post-mortem-report-ethereum-mainnet-finality-05-11-2023-95e271dfd8b2 (accessed June 2, 2023).

Q17: Should public players directly manage the blockchains that provide the infrastructure for DeFi operations?

Having a centrally managed blockchain defeats the purpose of a distributed ledger and the data integrity, accessibility, and ownership that comes from distributing the data updating and maintenance function and placing ownership in the hands of users, nor providers. Such a framework would completely undermine a blockchain's central purpose, resulting in a more complex system that can be much less efficient than a hub-and-spoke model while not providing any real benefit.

Further, a government-supervised blockchain network would not be able to compete with any alternative that operates under and evolves according to market forces. As a result, developers would flock to better ecosystems, assuming they were not explicitly prohibited by regulation from doing so. One could foresee the inevitable result being analogous to the dramatic differences between open and closed economies in the latter half of the 20th century..

Before reaching a conclusion regarding this question, policymakers could, of course, create and manage a blockchain and assess for themselves how successful they might be if they put this strategy into action on a grander scale. Alternatively, policymakers could begin participating in public blockchains like Ethereum now, and test whether participating in such a system rather than attempting to run an independent one is a better approach. We would wholeheartedly favor the latter approach.

Q19: Is a certification mechanism an effective solution to determine the scope of "safe" smart contracts (for a given state of knowledge)? Would alternative solutions achieve the same result?

At ConsenSys, we believe in the value of auditing smart contracts and have built a successful line of business around that belief. We have seen first hand the positive impact that proofing and auditing can have on end users of applications. We also recognize that auditing is a finite supply service and can be beyond the reach of some projects, at least initially, or simply be out of reach due to very high demand.

In our view, requiring for-profit enterprises like companies that offer financial services which rely in pertinent part on maintaining a smart contract to seek and obtain some kind of certification, which could include satisfactory completion of an audit, is worthy of serious consideration. We are not, however, in favour of requiring all smart contracts, regardless of use case, being subject to such certification requirements, nor are we supportive that all developers should be required to get one. Limiting certain regulated users, such as traditional financial services providers, to using only certified contracts for purposes of their offerings might also be a reasonable approach. Any certification program for smart contracts would only get more complicated as it got better tailored to the different types of users and smart contracts being deployed, and that trade-off would need to be carefully assessed.

What we would never be able to support is a regime that purports to limit the deployment and use of free, open source contracts that are akin to free, open source software that is liberally licensed and accessible on a public code repository. Such code has historically been more or less a public good, and its development and use is an unquestionably productive activity for not only developers but also users. The modern economy simply would not exist today without it. Any regulation that would have the effect of, let alone seek to, chill the development and deployment of freely usable software tools would be very negatively received by the public and particularly the software developer ecosystem, and rightly so.

We disagree with the notion that formal methods of auditing present greater potential because those methods can be automated. In our experience, formal methods can be less scalable than manual security reviews. That is both because the coding talent required to write formal specifications is rare, and because formal methods can be hard to implement. That said, we do agree that formal proofing and human auditing methods, while not serving as a silver bullet, can complement each other in the effort of reducing risks.

With respect to the life cycle of such certifications, having an arbitrary time period after which the certification would lapse would not be an efficient practice. Today, new audits are often warranted when a material change has been made to the contract code. Given that service providers are incentivized to improve their services, including by updating software that supports those services, new certifications would happen in the ordinary course.   Further, it is reasonable to expect developers to stay abreast of best coding practices with respect to smart contracts and respond proactively to new information about bugs and vulnerabilities, including information gleaned from bug bounties and other proactive measures that are standard practices.

It is not reasonable, however, to legally impute to developers constructive knowledge of the latest information from across the entire blockchain ecosystem so that they may be liable for upgrades that they were not actually aware were called for. Liability for such smart contract use should remain defined by the relevant terms of service offered by these providers. Expanding liability by legally imputing unreasonably broad knowledge would precipitate a new cottage industry of software developer liability litigation that would hamper growth and increase costs.

Q23: Should smart contracts embed a number of regulatory requirements in their code in the future?

No. Such a requirement would be contradictory to the “same outcome” approach because it would dictate the means as well as the ends. There are a number of ways that a blockchain-based service can institute controls or other regulatory requirements, and in many cases, instituting such controls on-chain is neither efficient nor effective when compared with other mechanisms. A better approach is to allow a service provider the freedom to institute sensible controls in the manner which makes the most sense for that product and its applicable market.

Q24: Who should set the security standards for smart contracts (refer to section 3-2-2, item b) and why?

While regulators and policymakers can play an important role as collaborator in any process, the best result would be achieved if the ecosystem itself established any and all technical standards that would come to form one or more ecosystem-wide benchmarks. The participants in the space have the highest technical expertise and the most practical experience with the subject matter and are thus in a far greater position to set standards. The best role for regulators in such a scenario is to collaborate on a road map and to facilitate ecosystem participation and cooperation in such an effort.

One example of industry-led initiatives concerning smart contract auditing is the Enterprise Ethereum Alliance's (EEA[19]) EthTrust Working Group. The EEA EthTrust Working Group works on a technical standard for security review of smart contracts, with a first version published in August 2022.[20] No fewer than 7 ConsenSys employees contributed to this effort. The group is currently working on an updated version. Support from policymakers of efforts such as this would only enhance the adoption of such standards by the larger ecosystem.

The working group has also developed the EEA EthTrust Certification, which serves to confirm that a smart contract has been reviewed and found not to have a defined set of security vulnerabilities. To grant the EEA EthTrust Certification, an auditor provides a conformance claim that the tested code meets the requirements of the specified security level for which it is certified. The Certification is available at three security levels, with each providing successively stronger assurance that a smart contract does not have specific security vulnerabilities. The optional Recommended Good Practices, if correctly implemented, further enhance the security of smart contracts.

In addition, the EEA DeFi Risk Assessment, Management and Accounting ("DRAMA") Working Group was formed with the goal to develop and promote the use of common assessment criteria for risks involved in the use of DeFi protocols, to encourage mainstream acceptance and enterprise adoption.[21] The group has carried out an industry survey on this topic and is currently developing a discussion paper on the risks associated with DeFi that is intended to describe best practices for both risk assessment and mitigation. The paper is currently in an internal drafting phase and will be made available for public comment in the coming months.

Q25: Should interaction with uncertified smart contracts be discouraged or prohibited (refer to section 3-2-2, item c)?

Our position is that freedom of choice and access on-chain should be optimised because that is what benefits everyday people. Given that perspective, users are best served by a framework that permits users to make their own choices while reducing information asymmetries, so users can be well informed if they so choose to be. No user should be prohibited from using non-certified smart contracts, particularly those that pose no meaningful risks to markets or the

[19] The EEA brings together representatives from leading technological companies, smart contract auditors, financial institutions, consultancies, academic researchers and others. It also welcomes the participation of governments and public authorities.

[20] *See* EEA EthTrust Security Levels Specification v1 (available at https://entethalliance.org/specs/ethtrust-sl/) (accessed June 2, 2023).

[21] *See* https://entethalliance.org/groups/DRAMA/ (accessed June 2, 2023).

public generally. There should be no pervasive, systemic discouragement of such use either. Instead, the proper approach is to allow market mechanisms to give users what they want and need in this regard, while bolstering mechanisms to ensure they can be better informed.

And that is happening now, with our MetaMask wallet being a good example. That software has been updated to warn users about risky approvals they are asked to make when linking their wallet to a particular application.[22] This feature was added based on user feedback and our own experience with navigating Web3. We are confident that, as the ecosystem evolves, the tools and applications in the blockchain space will naturally seek to protect users in ways that are well-tailored for those particular users, much like today's Web2 tools such as browsers have developed various measures over time to safeguard their users as they browse the internet.

Q26: Who should bear the certification costs of smart contracts (refer to section 3-2-2, item b) and why?

If contract certification is limited to for-profit entities that are using a smart contract in the course of their business, then it makes sense for those entities to generally cover the costs of certification themselves. As for other developers, such as private persons and not-for-profit organisations, the burdens of a broad certification requirement become clear. Requiring those types of developers to seek certifications, particularly for any type of contract and not just financial ones, would serve as a meaningful barrier to entry that undoubtedly hurts competition.

The suggestion of funding certification by means of a tax paid on transactions carried out by smart contracts is an interesting one, and one that has to some extent been under consideration by the developer community. Those public debates concerned whether there should be a block reward imbued into the protocol that goes towards public goods funding, such as smart contract auditing. Those discussions concluded that such an approach was not advisable because it risked causing governance issues and organisational burden in a system that is neither formally governed nor organised.

Q27: Do you have any comments on the description made of the risks inherent in the decentralised oracle model? Can these risks be mitigated using a certification mechanism tailored to the specifics of these applications (refer to section 3-2-3)? Do you have any comments or alternative proposals for a framework governing the activities of oracles?

We note at the outset that the risks outlined in the discussion paper regarding decentralised oracles, namely the risk of collusion, incentive to tamper, and risks of a highly automated system, are also risks that a centralised oracle presents, and even perhaps to a more troubling degree.

Setting that aside, the problem with obligating oracle providers to comply with a certification system, at least at the current moment, is that oracle technology is still in its infancy. This is true

[22] *See* https://support.metamask.io/hc/en-us/articles/4428045875483--Deceptive-site-ahead-when-trying-to-connect-to-a-site (accessed June 2, 2023).

about how oracles are constructed, how they operate, and what they are intended to do.[23] Setting a regulatory benchmark for such technology at the current stage would be to prematurely define the scope of the technology and inhibit any further organic growth. We wholeheartedly encourage further study of these services before any conclusions are reached.

With that said, oracles can be seen in some sense as an intermediary, ones that connect real-world information with blockchain data structures. Their reliability, accuracy, and transparency are crucial. Policymakers should become very familiar with these protocols, and expect that, if regulation of these information providers is indeed necessary, the path to implementing regulation should be incremental and involve considerable collaboration with the space.

Q29: Do you think that in some cases it may be necessary to "recentralise" specific sensitive activities (section 3-3-1)?

We are not supportive of any proposals purporting to “recentralise” blockchain software. It should first be noted that, given how easy it is for third parties to copy (or “fork”) a protocol and redeploy it, any effort to recentralize a protocol in one jurisdiction would in all likelihood result in the same protocol persisting (or perhaps even re-decentralizing) in other jurisdictions if there is market demand for a decentralised version. That, of course, raises the pervasive question of whether persons in one jurisdiction could be convinced not to access, or reliably prevented from accessing, protocols that are easily accessible in foreign jurisdictions.

That issue aside, if an application was actually too “sensitive” or dangerous for the public to use, which has to be an extremely high bar, then the appropriate remedy is to use existing authorities to ban its use rather than determine after the fact that the developer is responsible for other’s use of that publicly-accessible code. It should be noted that, in many situations, the developer of the code does not have the ability to modify it or remove it, thus any regulatory penalties imposed on that developer would not improve the particular situation but instead would serve the purposes of general deterrence. Of particular concern is the notion that a developer could be strong-armed into doing a regulator’s bidding simply by having “the power to influence the community.” Such an approach could not avoid being used arbitrarily and capriciously.

On the other hand, it is not unreasonable to question the responsibilities of a DAO member or development team that has sufficient control over a protocol already. But such circumstances really do not neatly fit into a category where “recentralisation” is an appropriate concept. Further, they are themselves complicated, given that “sufficient control” is not likely to have a clear meaning that allows for a bright line rule.

[23] This point was correctly echoed by Professor Tarik Roukny in his June 2022 paper for the EU Commission titled “Decentralized Finance: information frictions and public policies.” We further agree with his observation that “[u]ltimately, the nature of the information that needs to be transmitted to the contract should determine the optimal design of oracle service and its related market structure.” (*Id*. at 34.)

Q32: What requirements should apply to intermediaries facilitating access to DeFi?

Any regulatory requirements should be limited to those services that do more than serve as purpose-agnostic tools that allow users to safeguard their own data and conduct transactions on their own. Just as it would be entirely inappropriate and overly burdensome to require web browsers like Chrome and Safari to screen, monitor, advise, and warn their users for all manner of dangers as they browsed the web, it would be unreasonable to place requirements on open source software tools to do the same in the context of a blockchain network. Further, it is practically impossible for open source tools to be designed in a manner that could effectively serve these purposes. For instance, it is simply not possible for ConsenSys to foresee let alone inform and advise about all the potential uses that a MetaMask user might make of his or her wallet. Placing requirements on a developer in such a manner would ensure they avoid your jurisdiction at all costs.

Q33: Should the same rules apply to all intermediaries in DeFi (including, where appropriate, decentralised web interfaces)?

Web interfaces, such as unhosted wallets, are not intermediaries in DeFi. They are software tools that the users of DeFi (those actually moving their own funds and interacting with the on-chain smart contracts) use on their own to compose their transactions, read the data structure, and send signed transaction messages to the blockchain.

As the discussion paper itself recognizes, DeFi can be thought of as disintermediated finance, where the traditional counterparty or middle man is replaced by a system which offers you access to code that you can use on your own to execute transactions for yourself. That purpose-agnostic software makes this system more accessible to people who are not comfortable using a command line interface does not render that software package an intermediary in any sense.

To the extent that some interfaces offer other services, including information aggregation or curation, or access to off-chain computer programs that facilitate on-chain transactions, a one-sized fits all approach to rules makes very little sense, given the variability in what the services are and how they impact the user.

Q34: Should access to financial products be conditional on customers' financial literacy level and risk appetite?

Our view is that one of the core promises of permissionless blockchain networks is that, when on chain, no other person or entity can make a judgement about how sophisticated you are or what types of activity are too risky for you or act on that judgement by excluding you from certain activities that are free for others to participate in. The impulse to protect people from threats is one thing, but that impulse becomes less comprehensible when those threats are defined to include the user him or herself.

Rather than excluding certain people from accessing applications on blockchain networks, risk disclosures could be an appropriate mechanism to help users make informed choices, as discussed in our response to question 9. This would arguably be more effective than assessments of users' financial literacy that would furthermore require users to disclose their personal information or necessitate the injection of otherwise superfluous market intermediaries. Additionally, ConsenSys and other industry players are dedicating resources to educating users about responsible use of Web3 technology. For example, MetaMask Learn is an educational platform available in 10 languages where users can learn through easily accessible content and interactive simulations.[24]

The bargain that blockchain protocols present is more freedom and safety at the price of more responsibility. For those who are not interested in that bargain, then the traditional financial system will presumably still serve them well. But denying people the choice when that choice is now possible, thanks to blockchain, would be the wrong path.

Respectfully submitted,

CONSENSYS SOFTWARE INC.

by/

Bill Hughes
(william.hughes@consensys.net)
Natalie Linhart
(natalie.linhart@consensys.net

[24] *See* https://learn.metamask.io/ (accessed June 2, 2023).