May 2023

Response to ACPR's Discussion Paper, "'Decentralised' or 'Disintermediated' finance: what regulatory response"

Introduction

Polygon Labs respectfully submits this response to the Discussion paper published by the Banque de France's Autorité de contrôle prudentiel et de résolution ("ACPR") entitled "'Decentralised' or 'Disintermediated' finance: what regulatory response" (referred to herein as the "Discussion Paper" or "Paper").

Polygon Labs, an international software development company that builds blockchain infrastructure and complementary software, believes that a blockchain-based Internet will enhance the ways in which we transact and interact in society. For that reason, Polygon Labs' mission is to provide more efficient and open blockchain infrastructure on which third party developers and the global community can build.

Creating a regulatory regime for "cryptoassets" that both encourages innovation and achieves the tripartite policy goals of protecting consumers, preserving market integrity, and combating illicit finance will achieve two critical missions: *first*, it will provide clarity to industry and protection for users and consumers, and *second*, it will further establish France as a hub for responsible innovation in the EU.

Polygon Labs' responses to the Discussion Paper below and our general approach to regulation in the blockchain space is based on certain core policy principles:[1]

1. Any regulation of decentralised, permissionless blockchain-based systems must address the realities of technology. The ideal of "same risk, same regulation" – frequently cited by regulators and policymakers – must be properly tailored to decentralised, blockchain-based systems. We acknowledge that blockchains and related technology built on and around them pose various risks. However, in truly decentralised, blockchain-based systems, risks do not arise in the same way as in traditional systems (*e.g.*, risks may arise through vulnerabilities in code without human involvement). In addition, it must be recognised that we can leverage certain functions of blockchain-based systems to address regulatory goals (*e.g.*, peer-to-protocol transactions eliminate counterparty risk and increase certainty, but also raise new risks as noted above). Thus, in contemplating regulation in decentralised blockchain based systems, regulators and policymakers must first identify the risk, the source of that risk, the activities that lead to such risk (*see* Point 2 below) and then craft regulation that addresses the activities to mitigate any risk.

2. Regulate activities; be technology neutral. Today, laws regulate activities undertaken by entities or individuals. centralised actors providing particular services must abide by laws that apply to those services. Such laws are needed to allow consumers to "trust" intermediaries: the people and entities that have control over their systems and their customer's assets and data and are trusted to act with care. The same must hold true for any laws that relate to blockchain technology and the DeFi ecosystem; laws need to

[1] *See* https://polygon.technology/blog/polygon-labs-core-policy-principles.

address *activities* rather than the technology itself. Where technology replaces functions typically performed by persons in traditional systems, lawmakers should not import or otherwise force the existence of intermediaries to which to apply traditional regulation.

3. Software development in and of itself should not be directly regulated in order to ensure continued innovation.

We are broadly supportive of the ACPR's recognition that decentralised finance ("DeFi") poses *different* risks than those in the traditional financial system, which requires an understanding of and a different approach to regulation. This nuanced approach will provide additional clarity for the crypto-asset industry.

We do believe, however, that it is important to distinguish between DeFi and those involved in the creation of those software protocols versus more traditional "financial intermediaries" that may – as an entity or person – access those protocols. As stated more fully below, we do not believe that efforts to "recentralise" identifiable entities in the DeFi system is a sensible regulatory solution; the promise of DeFi rests precisely within the features of decentralisation – open systems that anyone can use, which operate more efficiently without one or more "stop gaps" or other bureaucracy. The concept that any "player[] exercis[es] effective control over sensitive services"[2] must be considered carefully so as not to import legacy concepts into a novel system; the same holds true for the concept of "decentralised financial intermediaries", which seems to be contradictory within its own definition. Any regulatory regime must clearly define and separate between "DeFi" and any "centralised intermediaries" that may use that technology.

We would be happy to discuss our positions in response to the Discussion Paper further, and thank the ACPR for its consideration.

Part 1: DeFi: definition, use cases and schematic structure

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 believe that the definition of DeFi set forth in the Discussion Paper (*i.e.*, "a set of cryptoasset services, which are similar to financial services and carried out without the intervention of an intermediary")[3] requires some revision to ensure accuracy, precision and focus. DeFi is a software system based on smart contracts, where users can engage in economic transactions in a self-directed manner, without a need for an intermediary, where no one takes custody, and where all elements of transactions occur on a permissionless blockchain network. Without acknowledging these additional features (*e.g.*, lack of custody, permissionless blockchain, etc.), regulations may capture (i) blockchain-based or blockchain-adjacent financial services that are not truly decentralised or (ii) certain services that seek to call themselves "DeFi" without having the hallmarks of decentralisation. The "set of criteria . . . used to characterise DeFi" encompasses the features set forth in the definition we have provided.

The complex nature of DeFi systems necessitates a multi-factor approach to determining "decentralisation". We caution against using an overly-prescriptive definition of "decentralisation" because decentralised blockchain-based applications – including in DeFi – continue to evolve from a number of perspectives. Thus, any test must be based on tenets surrounding decentralisation: self-reliance for and independence over one's own transactions and for information about such transactions.

[2] *See* Discussion Paper at Introduction.
[3] Discussion Paper at 1; *see also id.* at 1-1.

We propose a three-prong test with certain sub-factors that can be used, at least on a preliminary basis, to determine whether a DeFi protocol is "decentralised". The following factors provide a solid foundation in determining "decentralisation": technology, governance / administration, and user / ecosystem reliance.

Technology focuses on the code of the DeFi protocol in two ways: *is the code for the protocol open source or, at a minimum, source available?* and *is the code deployed to a permissionless, distributed blockchain network or ledger?*

- Ensuring that the entire code for a DeFi is open, transparent and available for anyone to view at any time demonstrates how the protocol works and allows individuals to independently verify that there are no points of centralisation in the protocol. If one views the code and is not able to determine how the DeFi protocol functions – or even how certain aspects of the protocol occur, then one can credibly assume that certain activities occur through a centralised individual or entity (*e.g.*, if the user cannot determine how the code of a DeFi protocol generates yield, then the user may assume that a centralised entity is creating the yield).

- To ensure decentralisation at the technical level, one must also assess whether the network to which the protocol has been deployed is itself permissionless and decentralised. If a smart-contract based application that otherwise meets the definition of DeFi is deployed to a "permissioned" blockchain – one with an intermediary or entity that determines which users can or cannot access the network – then the application may not be "decentralised".

Governance and administration relates to the authority over the functioning of the code, and by extension, over third party user assets that are supplied to or otherwise used in the protocol: *(a) is there an administrative key that allows for control of the protocol and if so, does an identifiable natural person or entity (or group of persons coordinating together) hold the key; and (b) is there a central decision-making authority that can control the protocol through governance votes or otherwise?*

Finally, user/ecosystem reliance accounts for impact, whether direct or indirect and whether real or perceived, by identifiable actors – whether the original software or an identifiable person or group of persons coordinating with each other. This concept emanates from traditional consumer protection laws and concepts: if users or others involved in the ecosystem of a protocol expect that an identifiable party or group of persons coordinating with each other are ensuring the safety and soundness of a protocol based on representations and/or actions of that actor/group, then – even if the protocol is technologically and administratively decentralised – there still may be points of centralisation that require certain types of disclosures to ensure adequate consumer protections.

Some DeFi protocols may "meet" the above-listed factors in various ways and DeFi protocols and their attendant systems may function in varied ways; accordingly, any definition of "decentralisation" must be flexible and account for the "regulatory outcome" looking to be achieved rather than something definitive.[4]

The Discussion Paper describes the "real level of decentralisation of services" in the following way, "projects are of a mixed character", "decentralisation can be variable over time throughout

[4] That being said, certain features of decentralisation set forth in Section 1-1 – public blockchains, smart contracts, decentralised governance and non-custodial – are hallmarks of DeFi and, if as the Discussion Paper submits, "many DeFi services do not meet all these criteria", we must question whether the function actually meets any definition of DeFi. "CeDeFi" (*see* Discussion Paper at Box 2) refers to centralised intermediaries who perform the role of a traditional intermediary, but automate certain functions with smart contracts and provide certain functions or assets on a permissionless blockchain network (*e.g.*, performing the role of a traditional lender, but putting the loan "on chain").

the protocol development cycle",[5] "characterised by high concentration at every level",[6] including with governance tokens[7] – suggesting that despite nomenclature, many DeFi applications are not particularly "decentralised" or have some feature of "centralisation".

We agree that decentralisation can be "variable over time" and that there is no strict "test" for decentralisation – the factors listed above require flexibility and analysis on a case-by-case basis; we further agree with some of the risks enumerated in Section 2-1 – *e.g.*, founders or developers retaining an administrative key without disclosing that fact or the powers of such administrative key; we disagree, however, that concentration of governance tokens or total value locked ("TVL") necessarily suggests that DeFi applications are not decentralised.

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

Section 1-3 addresses a number of use cases that will continue developing in the future. In addition, we would like to add the following:

- **Aid management and delivery**: DeFi provides similar benefits here as it does with the emergency aid use case. For example, UNICEF is creating its UNICEF DAO[8] – as part of its venture arm - to facilitate better communication and more efficient fund disbursements for its portfolio companies.

- **Regenerative economy**: DeFi can help facilitate two-sided markets to connect communities with sources of capital (*e.g.*, individual users and traditional lenders). This lending and borrowing – as enabled by DeFi – can help offer additional liquidity to small business owners, families, and individuals, especially in developing countries – for example, microlending for smallholder farmers in Kenya.[9]

- **Tokenisation of assets**: As entities further tokenise off-chain assets (sometimes referred to as "real world assets"), DeFi will allow for the ability to utilise those assets in new ways and with new financial primitives.

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

The Discussion Paper posits that "concentration" can happen at both the network level and the application level in DeFi. For the former, the Paper suggests that the majority of DeFi applications are "concentrated" on Ethereum – with many others concentrated on only two other blockchain networks. For the latter, the Paper states that TVL is concentrated among a small number of DeFi protocols and that control over such protocols through governance tokens "can be highly concentrated". Even if true, neither of these determines the level of "decentralisation" in the DeFi ecosystem.

Network-level concentration: Ethereum. Ethereum was the first network infrastructure layer that introduced the use of smart contract-based systems by developers, which attracted many to build atop Ethereum. Over time, Ethereum captured significant network effects, with more users and developers joining to interact with and/or build on the platform. Ethereum is decentralised and

[5] Discussion Paper at 1-1.
[6] Discussion Paper at 1-5.
[7] Discussion Paper at 2-1.
[8] https://medium.com/plena-finance/unicef-is-creating-a-dao-prototype-to-better-leverage-its-crypto-funds-b9969363b33f.
[9] https://medium.com/mercy-corps-social-venture-fund/pilot-launch-defi-enabled-salary-advances-for-smallholders-in-kenya-6c8eb821688a.

permissionless, which provides a unique value proposition to users and developers - namely, the security and reliability of the network.

Ethereum's decentralisation – and, therefore, its resilience and security – arises from a number of its core features: *first*, as of the end of March 2023, there were more than 500,000 validators on the Ethereum network, which are, as far as we know, geographically dispersed;[10] *second*, these validators are hosted on a variety of software servers; *third*, there are a multitude of clients (*i.e.*, an "implementation of Ethereum that verifies data against the protocol rules and keeps the network secure")[11]; and *fourth*, a broad variety of developers, organisations, and/or teams launch the applications on top of Ethereum. Given Ethereum's decentralisation, operational resilience, and *permissionless* design – meaning that any developer can build on top of the network without permission from some person or entity – the concentration of DeFi applications built on top of Ethereum does not undercut claims of decentralisation. Instead, the robust application ecosystem on top of Ethereum is a testament to the network's level of decentralisation. There is an added benefit to having a significant number of applications deployed to a particular blockchain network – deep liquidity – which allows for better flow of assets, better price discovery as it relates to DeFi, and added security to have additional individuals creating network effects. Fragmented liquidity – *i.e.*, small portions of liquidity across various networks – can create issues for DeFi users.

Application-level concentration: DeFi protocols. The TVL metric – concentration of total TVL among several top DeFi applications – likewise does not undercut claims of decentralisation. Some DeFi protocols may have significant users, and this has nothing to do with whether the protocols themselves meet the functional definition of "decentralisation". In fact, more users may indicate greater dispersion around users and participants in a DeFi application which further highlights decentralisation for the particular protocol, particularly as it relates to network effects (*i.e.*, more users creating more value for a protocol ecosystem).

Governance tokens – and concentration around holders and voters – also requires a more nuanced discussion. For example, measuring holders of governance tokens by Etherescan address frequently results in "false positives" - meaning that certain Ethereum addresses represent pools in other protocols rather than a single user holding a significant number of governance tokens. Even assuming that a small number of persons or entities hold a disproportionate number of governance tokens, the appropriate measure for decentralisation is whether those individuals can *control* user assets (*e.g.*, one must assess whether users are able to remove assets before a change voted on by governance takes effect).

Q4: Do you have any comments on or information to add to the schematic presentation of DeFi presented in section 1-6?

The following points should be accounted for in the schematic provided in Section 1-6:

1. Wallets, hardware, and software do not interact directly with Layer 2 scaling solutions; they only interact with APIs.

2. Building on the first point, the diagram should indicate a relationship between Layer 2s and applications. Moreover, Layer 2s are more appropriately placed in the "infrastructure layer" since they provide additional foundation for the ecosystem.

3. Typically, an application will build on top of a Layer 2, and that application will connect to the node that stores a copy of the ledger, containing the smart contract. Therefore,

[10] https://beaconscan.com/stat/validator.
[11] https://ethereum.org/en/developers/docs/nodes-and-clients/#what-are-nodes-and-clients.

decentralised applications do not "speak" to smart contracts; rather, they provide information to nodes to be able to effectuate transactions in DeFi protocols.

4. Oracles also do not "speak" to crypto hardware; crypto hardware is speaking to a node that looks up an oracle's value.

5. Finally, some applications are starting to operate under a hybrid model, where the back end is hosted off-chain with market makers and other instruments serving as network validators for execution. These completed transactions then get reported back on-chain.

Part 2: The risks associated with DeFi

Q5: Do you have any comments on the description (provided in section 2-1 of this document) as regards risks related to decentralised governance?

Our response in Q1, which provides a decentralisation framework, including on governance / administration, and our point in response Q3 on governance tokens provides useful background for Q5.

This Discussion Paper highlights "users effectively holding governance power over a protocol [who] can make decisions that are detrimental to minority owners" as one of the key risks associated with decentralised governance. Although this may pose some risks, one key issue that is frequently overlooked in assessing governance – even in the face of certain actors purportedly having outsized "voting influence" in distributed governance systems such as decentralised autonomous organisations ("DAOs") – is whether users ultimately have control over their assets regardless of governance votes. Even if a DAO makes changes or updates a DeFi protocol, are users able to (i) receive information about the changes to the protocol in a timely manner; and (ii) make decisions about removing or otherwise changing the configuration of their assets prior to such changes taking place such that any change by the DAO would not affect user assets. If users ultimately have control over their assets regardless of how a DAO - or any other form of governance - votes, then "voting power" may not be the appropriate metric for determining "control" over a DeFi protocol.

With respect to "founders or developers [who] may have retained the administrator keys of a DeFi protocol", industry best practice counsels in favor of robust disclosures regarding (i) who holds an administrative ("admin") key; (ii) the powers of such admin key; and (iii) the length of time the current holder of the admin key plans to hold the key along with any plans for the transfer of the key.

Please see responses to Q13 (discussion of risks present in decentralised systems) and Q18 (ways to mitigate these risks) for more information.

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?

"Layer 1 solutions" ("L1s") are blockchain infrastructure – networks that provide the backbone for the next iteration of the Internet. Blockchain networks are, as noted in Q3, more operationally resilient and secure than other software solutions precisely because of their decentralisation. The risks of L1s are primarily smart contract risk ("technological" and "cyber" risk, detailed in Q13) and infrastructure risk – centralisation of certain aspects of the functioning of the network.

"Layer 2 solutions" ("L2s") have the same or similar security issues as Layer 1 blockchain networks: smart contract risk and infrastructure risk. However, there are risks with an L2 that are not present with an L1 only because there is added complexity to the functioning of the system.

There are a number of assumptions for using an L2: Ethereum works properly, the L2 network itself works properly, and the sequencer and prover for the L2 works properly. Although L2s require the alignment of more systems, there are significant benefits in scalability, efficiency, privacy and the like that outweigh the operational or security risks, which can be mitigated as discussed in Q18.

An industry standard has emerged to show differences - including on risk - for different L2 solutions: L2 Beats.[12] L2 Beats is currently considered the premiere standard in evaluating L2 solutions. It provides significant information about each of the various L2 solutions that have emerged and "cuts through" much of the public discourse to give an unbiased analysis of each L2 solution.

There are significant differences between zk rollup solutions and optimistic rollup solutions. With zk rollups, the transaction or data must be proven to be true, whereas with optimistic rollups, the assumption is that the transaction or data is true unless proven otherwise. These differences are also discussed in L2 Beats evaluations.

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

Transparency in rollups may depend on the type of rollup. With regards to zkEVM, a solution built by Polygon Labs,[13] there may be less transparency than with Ethereum, but anyone can run a node for zkEVM and anyone can view the state of the rollup from the L1 (here, Ethereum). An independent observer may obtain slightly less information than in an L1, but this is an inherent part of the trust assumption for any rollup solution.

Ultimately, one can reconstruct the L2 state from the L1 state for zkEVM, which is what allows the final state transition to occur.

There is transparency with L2 but potentially not at the same level as with Ethereum.

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

Based on the definitions and explanations in the Discussion Paper, we understand "application layer" to refer to the smart contract protocols comprising the DeFi ecosystem.

Please refer to the responses to Q13 (discussion of risks present in decentralised systems) and Q18 (ways to mitigate these risks) for more information.

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

As a software development company, Polygon Labs declines to answer this question as it appears to request advice and specific disclosures for retail users of DeFi applications.[14] Polygon Labs is broadly supportive of the use of robust disclosures for software-based systems.[15]

---

[12] https://l2beat.com/scaling/tvl.
[13] https://polygon.technology/polygon-zkevm.
[14] The term "user" is more appropriate than "customer" because customer implies a contractual relationship where a person purchases something from a provider (services, goods, etc.). In DeFi, individuals or entities interact directly with software without intermediaries and typically without a contractual arrangement (frequently a hallmark of a "customer" relationship) such that "user" more accurately reflects the relationship.
[15] *See* https://polygon.technology/blog/polygon-labs-core-policy-principles.

Q10: Do you have any comments or additions to make to the description (provided in section 2-4-2) of the systemic vulnerabilities of the DeFi ecosystem (endogeneity of investments, significant leverage effects, role of automated position liquidation mechanisms)?

Section 2-4-2 item a sets forth the following "systemic weaknesses of DeFi": (a) incentivizing the creation of new tokens relating to new DeFi protocols; (b) increasing leverage in the system overall and for individual users; and (c) self-referential usage of various tokens and protocols. We generally agree that these are some of the risks in the DeFi system. We disagree, however, with the characterisation that over-collateralisation for DeFi protocols exists due to "lack of trust between parties". Rather, over-collaterisation in DeFi is a proxy for "creditworthiness" (*i.e.*, the assessment of whether an individual is a trustworthy borrower); over-collateralisation ultimately benefits the DeFi system rather than poses additional risks. As seen during certain times in the cryptoasset markets, including at the end of 2022, DeFi protocols that incorporated mandatory over-collateralisation continued to operate normally and provided the proper incentives for users within the system to either (i) repay / return open positions in a DeFi protocol (including during times of the user's own market stress – *e.g.*, centralised distressed borrowers closed positions before declaring bankruptcy); or (ii) properly collateralise open positions to ensure the overall health of the DeFi protocol.

Many of the risks outlined in Section 2-4-2 focus on financial stability risks in DeFi, which may grow as the DeFi system expands. We acknowledge concerns connected to the price volatility of crypto-assets held by users and the deployment of such assets throughout the DeFi system, which, when used as collateral or otherwise back transactions, may amplify selling behavior and cause compounded user losses in periods of market stress.

However, DeFi systems differ from traditional financial and "CeFi" systems – centralised financial platforms for crypto-assets – where intermediaries control users' assets in times of market stress. In a DeFi system, volatility may impact the assets held by users, but these users remain empowered to take control over their own holdings rather than relying on an intermediary.

A number of technological solutions may be deployed to mitigate financial stability risk in DeFi, including implementing systems and controls. For example, creating a control designed to mitigate leverage and liquidity mismatches. This could include a protocol that tracks capital within a liquidity pool to calibrate liquidity risk with utilisation, impacting interest rates and easing mismatches. These protocols could also target interest rates directly to calibrate a variety of digital assets and their respective levels of risk.

Other measures could include protocols that provide additional liquidity during times of stress or volatility, create siloed assets (*i.e.*, restriction on borrowing to isolated stablecoins), or implement caps (*i.e.*, upper bounds for reducing exposure to certain assets).

Q11: Do you agree with the proposal concerning the regulation of stablecoins issued by DeFi protocols? (refer to section 2-4-3: "if a decentralised service claims to create or use a cryptoasset with an official currency as a reference, this cryptoasset must be an EMT within the meaning of MiCA or an equivalent asset)

☐Yes

☒No

Why?

Under MiCA, an EMT is "a type of cryptoasset the main purpose of which is to be used as a means of exchange and that purports to maintain a stable value by referring to the value of a fiat currency that is legal tender" (*i.e.*, "cryptoassets that are intended primarily as a means of payment

aim at stabilising their value by referencing only one fiat currency").[16] Assuming that a DeFi protocol "creates" a decentralised stablecoin with "reference" to an "official currency",[17] such tokens would function differently than centralised fiat-backed stablecoins (*i.e.*, EMTs under MiCA).

Notably, centralised fiat-backed stablecoins have reference to a single currency because the issued cryptoasset is "backed by" the reference currency or equivalents thereof held by the stablecoin issuer. The same is not true of decentralised "stablecoins" (*i.e.*, cryptoassets created by users employing a DeFi protocol). In this case, users create cryptoassets typically through staking cryptoassets to a protocol, triggering the underlying code to issue stablecoins to the user staking other cryptoassets. Some of the collateral assets may be EMTs, but that in itself would not make the decentralised "stablecoins" EMTs.

In other words, software developers create *software* with certain parameters built into code that allows the software to create a cryptoasset that may be said to hold a stable *value* pegged to one or more fiat or other currencies; these simply "reference" the value of a national currency but they do not "hold" their value based upon the existence of a corresponding amount of national currency held by a centralised actor. Some of these assets may be collateralised by other cryptoassets and, thus, hold a stable value based on the value of the underlying collateral, while others may hold a stable value based on an underlying algorithm or other parts of the software code.

A regime relating to decentralised stablecoins (sometimes referred to as "algorithmic" stablecoins) should relate to the activity conducted by an identifiable person or entity and *not* to the cryptoassets themselves. Most of the types of assets referred to in Section 2-4-3 do not include identifiable persons or entities holding fiat backed currencies or their equivalent, who engage in decision making about reserves of such assets, due diligence on users and the like.

Accordingly, although certain parts of the EMT regulatory framework may be appropriate for decentralised cryptoassets that hold a stable value (*e.g.*, certain disclosure requirements), the overall framework is inappropriate for "decentralised stablecoins" because they function differently than EMTs.

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

Section 2-4-4 posits that pseudonymity, the "lack of user identification procedures" as well as "lack of control mechanisms to check the origin of funds quite logically generate money laundering and terrorist financing (ML/FT) risks in the DeFi ecosystem." Although reports indicate that actors have used DeFi protocols for illicit transactions, most reports on the topic state that the volume of ML/TF activities is low compared to the significant amount of illicit transactions that occur in the traditional financial system. Within the cryptoasset ecosystem, the illicit volume was around 0.24% (or USD 20.6 billion) of the total transaction volume in 2022.[18]

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?

In fully decentralised systems, risk to users and to market integrity is borne primarily from technology risk and cyber risk, or from integration with centralised systems (*e.g.*, centrally issued cryptoassets or centralised information systems such as oracles) whereas in traditional financial systems, risk is borne primarily from concentration of data or information or errors in human or

[16] See para (9) & Definitions Art. 3(4) at https://eur-lex.europa.eu/resource.html?uri=cellar:f69f89bb-fe54-11ea-b44f-01aa75ed71a1.0001.02/DOC_1&format=PDF.
[17] Discussion Paper at 1-1.
[18] https://go.chainalysis.com/rs/503-FAP-074/images/Crypto_Crime_Report_2023.pdf.

subjective judgment. "Technology risk" refers to code being inherently unsafe for use due to code errors and bugs and "cyber risk" refers to instances where the protocol is functioning and being used as intended but a "loophole" may exist (and/or may not have been detected during security audits of the code) that allows an individual to exploit the code to gain an unfair advantage.

If central actors are required to act as intermediaries in a DeFi protocol or system, additional risks from such systems (*e.g.*, errors in human judgment) would affect the functioning of the system and create opacity; these risks, however, are precisely those that DeFi was created to mitigate.

Part 3: Avenues for a regulatory framework

Section 3-1: Ensuring a minimum level of security with respect to infrastructure

Q14: Should public blockchains be governed by a framework or by minimum security standards (refer to section 3-1, regulatory scenario A)?

☐Yes

☒No

If so, how? If not, why?

We do not believe regulators should implement specific regulation or required registration and oversight mechanisms for public, permissionless blockchain networks. Such an approach regulates two activities that are not typically subject to regulation: (a) software development for open source software (and public goods); and (b) technological activity necessary for security of a blockchain network.

As to the former, there may be minimum technical standards to which software developers build as a matter of industry practice, but this is not something that is typically set by financial or other regulators. It may be possible to get industry consensus through other industry bodies or groups, but Polygon Labs does not support directly regulating software development as an activity on its own.

As to the latter, we do not believe there is merit in regulating validation activities and strongly encourage ACPR to engage in additional study before considering any regulation as it would pertain to validation activities. Validation is technical activity for implementing a consensus mechanism that verifies transactions on a proof-of-stake blockchain network. It is not the type of "activity" contemplated under the MiCA or, as we understand it, other financial regulations in France or the EU. We do believe that issuing guidance regarding safety and security of blockchain networks based upon the number of validators and risks of centralisation could be an appropriate mechanism to address the issues raised in Section 3-1.

Validators are users who operate nodes that verify data and secure blockchain networks. As many have discussed, blockchain networks are communications protocols. Thus, verifying data sent to a blockchain network requires a user through a node (*i.e.*, a computer) to employ a set of mathematical principles to check the validity of the data provided to allow it to be recorded on a blockchain network.

It is important to note that not all transactions through applications deployed to a permissionless blockchain network are *financial* transactions; indeed, some of the latest blockchain-based applications have taken the form of social networks or consumer rewards programs. Validating such transactions would not necessarily have a financial component and thus, should not be regulated as financial or economic activity.

For all of these reasons, we believe validation should not be brought into the regulatory perimeter, whether through minimum standards or oversight by financial regulators. Such regulation would have wide ranging implications and potential unintended consequences relating to technical data verification, including a breakdown of the natural processes underlying proof-of-stake blockchain networks, including the consensus mechanism, and possible censoring of the communication of data throughout the network.

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

☐Supervising concentration in real time

☐Setting caps on concentration

☐Publicly disclosing when specific concentration thresholds are exceeded

☐Taking further action (specify how)

Please see the response to Q14, which addresses why regulators should not undertake standards, formal regulation or oversight of validators.

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?

☐Yes

☒**No**

Why?

Providing or maintaining software such as a blockchain network does *not* require regulatory supervision. Private blockchain provided by private operators do not need a regulatory framework. Such operators have relationships – contractual or otherwise – with their users and/or customers that are governed by existing laws (*e.g.*, contract, negligence, tort) which obviates the need for a separate regulatory supervisory framework. Ensuring that these software service providers are *not* regulated is especially acute where other similar types of software service providers are not regulated under financial laws and rules. Imposing new regulations for private blockchain providers would not achieve the goal of "technological neutrality" in building out regulations as it would unfairly target software service providers simply for using or providing private blockchains rather than other software.

We also do not believe that all "purely financial functions" should be "switched" to private blockchains, as suggested in Section 3-1 scenario B. As an initial matter, this would create significant fragmentation of liquidity for DeFi protocols across various blockchains – a problem that we address in response to Q3. This would also eliminate a number of the benefits of the DeFi ecosystem, including but not limited to the efficiency and speed gained in eliminating intermediaries and the transparency afforded by permissionless ledgers.

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

☐Yes

☒**No**

Why?

The basis and meaning of this question is unclear. Public, permissionless blockchains are operated by validators; they are not "managed". As stated in response to Q14, we do not believe financial regulators should impose financial laws and rules on non-financial/technical activities, especially because L1 and L2 networks allow for myriad types of transactions and not only financial transactions.

Q18: Do you have any other regulatory proposals to make with a view to ensuring a minimum level of security for the blockchain infrastructure?

☒**Yes**

☐No

If so, what are they?

To mitigate both technology and cyber risk before a protocol is deployed, industry best practices include robust auditing procedures – both internal and external to the development team. After code is written, it should be shared with other members of the internal team who did not write the code to review to find "bugs" or other vulnerabilities (including economic and technical); then the code should undergo auditing by a third party auditor who likewise vets and tests the code to determine any flaws; and then the software development team should consider the results of any outside audit and determine whether alterations to the code are necessary to ensure proper functioning. It is well-recognised by industry that code audits are critical to ensuring safe and effective operation of a DeFi protocol.

Third-party auditors play an important role in the safety and soundness of DeFi protocols; there are a number of reputable, well-known third party auditors as well as smaller auditors, all of whom could play into the possibility of self-regulatory organisations ("SROs") within the context of decentralised technology.

Despite the benefits of auditing, there are at least four helpful improvements in auditing practices that can be made: first, a standardisation of the approach to auditing smart contracts for DeFi protocols; second, a standardisation of when and how third party audits are used – e.g., prior to launch, at the time of an upgrade to the code, etc; third, standardising transparency around protocol audits will enhance accountability both for auditors and development teams, and will allow for even greater examination of the safety of code; and fourth, prohibiting an auditor from exploiting vulnerabilities discovered and not disclosed during an audit.

In addition, to mitigate cyber risk for protocols not yet deployed, developers can implement "gated" or "guarded" launches, which can be done in two ways: where the developer can restrict the protocol by limiting either the liquidity that can initially be injected into the system or the level of decentralisation for a limited time so quick updates can be implemented, or by restricting individual wallets by limiting the liquidity that a single wallet can contribute to the system.

Additional best practices for ensuring the safety of the code include, but are not limited to, bug bounty programs and "audit competitions". The former refers to programs where a software developer or a DAO offers rewards to individuals who find previously-undetected vulnerabilities in the code and privately disclose those vulnerabilities to the developer for correction. The latter refers to events where software developers offer rewards during a specific time to a specified (frequently identifiable) group of individuals who compete to find vulnerabilities in the code for correction before deployment of a protocol.

Finally, while not yet codified as a "best practice" or "industry standard", meaningful progress has been made with automated, technology-based monitoring systems for cyber risks. Such monitoring allows for the identification of suspicious on-chain activity, and triggers an emergency pause on the platform.

As with all parts of the DeFi ecosystem, the risk mitigation and monitoring tools continue to improve, such that current "best practices" outlined above are not comprehensive and will evolve over time. Accordingly, any contemplated regulation should be enacted with "regulatory outcomes" in mind rather than prescriptive requirements.

Section 3-2: Providing a suitable oversight framework in view of the algorithmic nature of services

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?

Current third party auditing provides the best means for determining the scope of "safe" smart contracts. As technology develops, automated or AI-based auditing solutions may provide further security; however, the hybrid of automated and manual review will likely remain the standard. In addition to certification, internal security teams should perform additional internal audits and run automated tooling in continuous integration on the code, alongside setting up bounties and other monitoring measures.

Certification that such audits occurred may assist users in assessing the "safety" or "security" of the smart contracts. Public guidance (from a regulator, a SRO, an industry body or even third party auditors) explaining the importance of third-party security audits of smart contracts will help inform users of DeFi protocols and help them make assessments about the safety of such protocols. Requiring certification *by a software developer* prior to deployment of smart contracts is, in effect, regulating software development; we provide alternate mechanisms through which such certifications may occur in response to Q28.

Q20: Do you agree with the description (provided in section 3-2-1) of the various techniques offered to audit the computer code of smart contracts, including with their respective strengths and limitations?

The matters raised in this section are those that exist in software development generally – they are not unique to auditing or certification of blockchain networks. Manual code review (third party audits) coupled with automated tooling most likely will remain the industry standard for safety and security checks on DeFi protocols not yet deployed. In addition, auditors may begin to incorporate a suite of tools to more effectively check for errors or bugs. For post-deployment, monitoring smart contracts could offer another line of defense.

Q21: Can you identify examples of smart contracts that should not be certifiable due to the nature of the services they provide?

☐Yes

☐No

If so, which ones?

The intent of this question is unclear. A contract purporting to provide a patently illegal service should not be certifiable.

Q22: What do you think of the rules put forward in this paper (section 3-2-2, item a) on how to certify smart contracts (pre-certification of called components, certification life cycle)?

We generally agree that the certification (or audit) life cycle set forth in Section 3-2-2, item is consistent with industry standards at this time.

Similarly, static analysis of smart contracts may assist in ensuring the safety of smart contracts, but care must be taken to properly define the role of such analysis. Many of the current tools used for static analysis (those of which we are aware) may produce "false positives" such that those with exceptional skill must be employed to utilise this methodology.

Further information must be provided to assess the suggestion that dynamic analysis will be helpful in certifying or auditing smart contract-based systems.

The reference to SCA in this section may not be particularly appropriate for smart contract-based systems. With a permissionless, interoperable network, new technology can integrate with the system without a clear audit trail and thus, due to proxy patterns, the code used by a smart contract today may not be the same code used tomorrow.

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

☐Yes

☐No

Why?

"Embedded supervision" "comprises a regulatory framework that provides for compliance to be automatically monitored by reading the market's ledger" in order to "reduce the need for firms to actively collect, verify and deliver data."[19] Although there may be some benefits to embedded compliance within smart contracts (*e.g.*, reduction of administrative costs, standardisation of available data), there are costs associated with such an approach – namely, difficulty in ensuring that any smart contract can implement requirements on a global scale since truly decentralised smart contract-based systems are permissionless and thus, not tied to a single jurisdiction. Further, this may also be indirectly regulating software development, something that is not otherwise done for other technologies. It also would require creating points of centralization that remove many of the benefits of blockchain technology.

The benefits of embedded supervision must be appropriately weighed against the costs to innovation or its potential chilling effects before setting forth such requirements in regulation.

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

Combining the two scenarios – market participants and public authorities – may result in a comprehensive and effective approach to setting security standards. The SROs discussed in other parts of this Response may provide an appropriate avenue in which to set standards for security audits or certification. Market participants can provide their expertise and insights on market realities, while public authorities can ensure that the standards meet public interest objectives. This collaboration can also help resolve disagreements between market players or segments and ensure the practicability of the standards.

[19] Auer, Raphael. BIS Working Paper No. 811, "Embedded supervision: how to build regulation into decentralised finance" at 3 (Sept. 2019, revised May 2022); *see also* Discussion Paper at 3-2-2, item a.

See also the response to Q18 with regards to standard setting for audits and auditors.

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

☒**Discouraged**

☐Prohibited

☐Neither discouraged nor prohibited

Why?

ACPR could provide public guidance discouraging interactions with unaudited smart contracts – and where the audit has not been made public – to meet consumer protection goals. ACPR should not, however, prohibit interactions with unaudited or "uncertified" smart contracts by way of regulation as it will curb innovation, and have the effect of regulating software developers directly. Any regulation relating to smart contract-based systems should be based upon whether such a system or protocol is decentralised and, correspondingly, whether there are any centralised actors involved in such systems. Regulation should be based upon the activity in which an identifiable actor is engaged, not based upon the underlying technology of the system.

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

At this time, it has been industry standard for the software developers creating smart contracts to bear the costs of audits and verification for those smart contracts.

In the event regulation is enacted that requires product certifications for smart contracts, then the costs of such certification should be borne by the same actors as those who create other products that require certification from a consumer protection perspective. For example, if chemical-based products must be certified prior to those products being released publicly and the regulator bears the cost of certification, then the same should apply to smart contract certification. Since decentralised smart contract-based systems are typically public goods, then the cost of certifications should be passed on to the public.

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?

The comments on the unsuitability of centralised entities for oracles in the DeFi ecosystem are generally accurate.

Any regulation restricting who can provide data to an oracle or how an oracle can operate would likely result in a significant slowing of the speed of information into the DeFi system, allowing windows of opportunity to exploit information asymmetries by users. This is not the optimal outcome in imposing regulations on oracles – whether centralised or decentralised.

More appropriate approaches to the question of exogenous oracles for DeFi protocols can be handled through a disclosure regime and similar types of code audits applicable to Defi protocols themselves. To the extent that France regulates market data providers, the same or similar regulations could be considered to apply to *centralised* providers of oracles – along the same lines of regulating *activities* and not simply regulating software or the provision thereof.

Q28: Do you have any other regulatory suggestions that could contribute to reducing the risks associated with the application layer of DeFi?

☒**Yes**

☐No

If so, what are they?

Supervision of DeFi services should not be done through direct regulation, but rather by placing obligations on regulated, registered entities that provide access to these services. Measures such as monitoring and reporting, should be considered. This is another area in which public authorities can work with the blockchain community to establish fair and transparent governance structures that ensure validation capacities of public blockchains.

There are four main models of regulating DeFi:

- *Define a set of DeFi-specific activities – like operating a protocol - as regulated activities and then require authorisation for such activities.* This model needs to explicitly exclude software developers and only include centralised, intermediary-like activity.

- *Apply rules to persons who maintain significant control or influence over a DeFi arrangement or protocol providing cryptoasset services and activities, including but not limited to those who maintain, run and operate systems used for regulated financial activities (even if such persons include the original software developer).* This also falls under the question of whether a DeFi protocol is "truly decentralised" or not; in the instance where there are centralised, identifiable actors, then those actors fall under a separate regime, even if the "services" they provide or the business they operate relates to a smart contract-based protocol in which users can engage in self-directed economic transactions.

- *Focus regulatory responsibility for mitigating risks on centralised on and off ramps like exchanges.* We are in favor of this approach. Please see Q14 for more information.

- *Regulate interface providers and other actors facilitating consumer access to DeFi (e.g., aggregators and other consumer "front ends", by requiring them to demonstrate or check whether certain standards or rules have been met, before facilitating access to a decentralised application or service.* We do not support blanket regulatory requirements on "front end" providers. A front end is simply a website; the website simplifies, but does not affect, various types of activities – some of which may resemble regulated financial services activity. Consistent with the intent to regulate "activities", any regulation of "front end providers" should focus on the activity the host operates or controls through the front end that go beyond simple "front end hosting".

As an initial matter, if there is a point of centralisation in the operation of a "DeFi" protocol, whether it be operational, administrative or otherwise, then the individual or entity engaging in such conduct must consider whether they meet the type of financial services activities provided by identifiable intermediaries that is addressed in the Discussion Paper (*e.g.*, providing a cryptoasset exchange). They would not meet the proposed test for decentralisation set forth above (or likely any other credible test for decentralisation).

It is critical that ACPR defines "what" or "whom" it seeks to regulate when addressing certain risks that may arise from the use of DeFi protocols. Based on the approach outlined in the Discussion Paper, we understand that ACPR seeks to mitigate risk in DeFi systems (to consumers

and the market), *not* to regulate software developers who code and publish the software comprising DeFi protocols.

We suggest below various regulatory frameworks that seek creative solutions to the unique challenges proposed by decentralised, software-based systems and protect the integrity of the software development process and allow for innovation (*i.e.*, not regulating "software development"), while simultaneously ensuring consumer protection and market integrity:

Any company/business allows the company's customers access through the company's services[20] to a DeFi protocol could be required to provide certain disclosures regarding aspects of the protocol, including but not limited to (a) that the protocol had undergone auditing according to any industry standards or standards set by regulators; (b) the way in which the protocol is administrated or governed, including the existence of any administrative key and if one exists, who (not by name) or what holds it; (c) whether there are any emergency risk mitigation measures inherent in the code or otherwise (e.g., a multi-signature wallet that has emergency powers and what those powers are); and (d) discussion of any hacks or scams associated with the DeFi protocol. The concepts set forth in (a) through (d) are suggestions based on accepted "best practices" in the industry and are not intended to be exhausted.

This model is favourable because it maintains regulatory requirements with identifiable intermediaries. In addition, this model is likely to incentivise (i) better practices by software developers without directly regulating software development and (ii) more transparency about DeFi ecosystems. By requiring verifiable centralised intermediaries (not the "decentralised intermediaries" referred to in the Discussion Paper) to assume liability in undertaking investigations about DeFi protocols and providing representations about the same, software developers will be incentivised to create protocols that meet the standards intermediaries must certify (if they want intermediaries to integrate into such protocols). In addition, intermediaries likely will make representations about DeFi protocols under one of two circumstances – they receive an indemnity from the software developer for any inaccuracy (or negligence or fraud) relating to representations made if they must rely on the software developer for the information – this scenario seems unlikely for a host of reasons; or all the necessary information is publicly available and verifiable – a much more likely scenario. Imposing regulation through this framework would not change the centralised intermediaries – typically "on and off ramps" – obligation to conduct Know-Your-Customer ("KYC") due diligence, to mitigate AML concerns.

Some regulators have suggested a voluntary "opt in" standards system through which a regulator sets standards for an "approved" DeFi protocol, including but not limited to cyber-security and audit standards, governance or administrative standards, etc. and to which anyone could provide an attestation and evidence that such DeFi protocol meets such standards to receive a "stamp of approval" from the appropriate regulatory body. This type of regulatory framework could be accompanied by a SRO in which industry participants, stakeholders and regulators work collaboratively to set industry standards. We favor this significantly over a mandatory standard setting regime, which will severely restrict innovation by preferencing better capitalised and established developers or prohibiting developers or coders to publish or deploy DeFi protocols from France or those that will reach French users without undergoing a lengthy or expensive regulatory process.

Certain websites running additional backend infrastructure undertake activities that resemble or are identical to regulated financial activity, but occur entirely through algorithms or code, and may take fees for hosting and/or providing services to users. Regardless of whether any fees are

[20] This does not include software developers or others who host web interfaces that provide information relating to one or more DeFi protocols; it may, however, include individuals or entities who host web interfaces that have back ends that engage in activities much more akin to those in the traditional financial system.

collected, it is possible that, as the Discussion Paper recognises, that certain regulatory frameworks – like those for algorithmic trading – may be applicable. Such regulation would only apply to the hosts of these "front ends" that engage in additional activities from just hosting a front end and not at the protocol level.

Section 3-3: Regulating the provision of and access to services

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

☐Yes

☒**No**

If so, which ones? If not, why?

Regulations should not force centralisation. To ensure no vulnerabilities in the code once it's launched, regulations could implement a "grace period" for developers and development companies to maintain some level of control in the system – after deploying the code – in order to fix bugs or other errors; thereby, minimising technological risk. After the "grace period", the protocol should focus on decentralising, meaning getting rid of centralised points of control (*i.e.*, burning admin keys and main developers stepping away from key decision-making). The grace period could even contemplate some reasonable, enhanced requirements related to disclosures and activities associated with the control.

Q30: What do you think of the proposals on how to achieve this goal (incorporation requirements, making players with effective control liable, legal status for DAOs)? Do you have any suggestions regarding the legal status of DAOs?

Not applicable given the response to Q29.

Q31: Do you agree with the description provided of the risks associated with "CeDeFi" on the one hand and "crypto conglomerates" on the other (box 6)?

As mentioned in the paper, "CeDeFi" – including "crypto conglomerates" – includes centralised intermediaries "who make investments in the DeFi ecosystem on behalf of their clients". A centralised intermediary – even if using DeFi protocols – that takes custody of user assets and makes investments on their behalf has equivalents in the legacy financial system and, depending on the treatment of the particular cryptoassets in which those entities are dealing or advising upon, should be regulated accordingly.

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

☐Information requirements

☐Duty of care and duty of advice

☐White paper publication requirement

☐KYC requirements

☐A comprehensive framework inspired by MiCA

☐Other

Why?

We do not support blanket regulatory requirements on intermediaries "facilitating" access to DeFi. Regulation should look at what ***activities*** the intermediaries are engaging in and provide a proper definition of "facilitating" in this context. Thus, any requirements such as KYC, information provision, whitepaper publications, should be based on the activities of the intermediary rather than simply whether the intermediary somehow uses or leverages DeFi protocols as part of its activities.

Our response to Q28 provides additional background on this topic.

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

☐Yes

☒**No**

Why?

To reiterate one of the points from our response to Q28 and Q32, requirements for identifiable intermediaries should be based upon the activities undertaken by those intermediaries – not simply based on the fact that the intermediary is somehow involved in or using DeFi protocols.

"Decentralised web interfaces" should not be regulated based simply on the type of information they provide – *i.e.*, regulators should not impose rules or regulations on an entity simply for "hosting a website" that provides users information about a DeFi protocol or about multiple protocols.

Box 2 of the Discussion Paper does not accurately reflect what such interfaces actually do as it relates to DeFi protocols. It states, "For users without programming skills, meaning the majority of them, a second way to invest consists in using web-based interfaces that allow 'click button' access to decentralised platforms. These interfaces can be designed by the developers of the decentralised applications to which they offer access, or by independent actors." Web interfaces (also referred to as "websites", "user interfaces" or "front ends") do not themselves provide "access" to a DeFi protocol; websites or other user interfaces are simply software. Most interfaces providing information about DeFi protocols *only* enable users to view data from a blockchain network in a convenient, easy-to-read format. A user must open their self-hosted wallet, which may be made easy to open on the web interface, when using a web interface as it relates to a DeFi protocol and use their wallet to provide information about the transaction using a remote procedure call through a node integrated with the wallet software *directly to the blockchain*. Specifically, users then initiate transactions on a DeFi protocol through their own self-hosted wallet; in most instances, a user-initiated transaction does not "go through" or "get initiated" by a user interface. In other words, web interfaces do not "allow 'click button' access". Even assuming they did, simply hosting a user interface that provides information about a DeFi protocol deployed to a blockchain network does not seem to require regulation above and beyond ensuring full and fair disclosures. Self-hosted wallets – a web browser extension – allows individuals to communicate with blockchain networks in the manner described above.

That being said, some hosted web interfaces and some features within self-hosted wallets provide backend software that routes orders, engages in best execution or otherwise performs the same or similar activities as regulated financial intermediaries. Such activity may require regulation that is consistent with the same ***activities*** in the traditional financial system.

Consistent with the policy principle of regulating "activities" and not software, any regulation relating to user interfaces should focus on the *activity* that is undertaken by the interface that the host operates or controls.

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

☐Yes

☒**No**

Why?

Regulations should not try to limit what users have access to; instead, regulations need to ensure that users have all the information they need to make *informed* decisions, especially relating to financial products. Decentralised protocols provide information about the foundational layer of the technology. Additional disclosure standards will assist users in understanding the risks, functioning, and operations of DeFi protocols.

Q35: Do you have any other suggestions for regulating the provision of and access to services?

☐Yes

☐No

If so, which ones?

Please see our response to Q28 above.

Avenues for a regulatory framework: cross-cutting aspects

Q36: How can proportionality requirements (for small players) be taken into account in the various regulatory avenues put forward by the document (or proposed by you)?

The proposed regulatory frameworks set forth above account for variations in size, scope and growth of DeFi protocols, particularly where licensed registrants are otherwise those providing information about DeFi protocols. The proportionality question also counsels against setting standards or directly regulating software developers or DeFi protocols themselves as it will significantly stifle or chill innovation – many of today's largest and operationally resilient protocols were developed by single individuals or small teams who had little to no third party funding.

Other ways to ensure proportionality would be to impose regulation through gated or guarded launches, or to make determinations based on sustained TVL over time which could indicate the number of users involved or the total amount of capital at stake and thus, the amount of potential risk to the DeFi ecosystem.

Regulatory sandboxes could provide an additional avenue for smaller players to test solutions in a controlled environment that reduces the regulatory burden.

Q37: What regulatory avenues - whether or not they are proposed in the document - could overcome the problems related to the possible extraterritoriality of actors (from a national or European point of view)?

To provide greater legal certainty and reduce conflicting regulations and extraterritoriality issues, international regulatory standards and frameworks should be developed for DeFi. Regulatory cooperation agreements between jurisdictions could ensure consistent regulations and reduce the potential for regulatory arbitrage. Regulatory sandboxes can also be used to test new DeFi products and services across different jurisdictions.

Q38: Who should, in each case, monitor the implementation of the different regulatory tracks (whether they are put forward in this document or proposed by you)? With what means?

Responses to a number of questions above provide insight into various regulatory models and how they would be implemented.