October 2023

Response to Discussion Paper from the Autorité des Marchés Financiers entitled, "Decentralised Finance (DeFi), Trading Protocols and Governance Issues: Overview, Observed Trends, and Regulatory Discussion Points"

Introduction

As a follow up to our meeting in June 2023 on this topic, Polygon Labs respectfully submits this response (the "Response") to the Discussion Paper from the Autorité des Marchés Financiers ("AMF") entitled "Decentralised Finance (DeFi), Trading Protocols and Governance Issues: Overview, Observed Trends, and Regulatory Discussion Points" (referred to as the "Discussion 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 and transact.

We appreciate the opportunity to respond to the Discussion Paper and believe the questions posed by the AMF are useful in "encourag[ing] discussions with ecosystem stakeholders" which will ultimately "foster the development of a balanced regulatory approach" for DeFi and the identifiable actors engaged in regulated conduct (or reasonably regulated conduct).[1]

Creating a regulatory regime for decentralized finance ("DeFi") that both "offer[s] opportunities for technological innovation"[2] 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 the blockchain industry while protecting DeFi ecosystem users and builders, and *second*, it will further establish France as a hub for responsible innovation in the EU.

We are broadly supportive of the AMF's view of legislation needing to be approached "in a progressive and proportionate manner" that recognizes "the benefits to innovation" while "considering the risks they pose".[3] However, we challenge the concept of "same activities, same risks, same regulation" and instead encourage regulators and policymakers to view regulating DeFi from the lens of "*different* risk, same regulatory *outcome*" in order to account for "the novel aspects" of DeFi and the different *sources* of risk (*e.g.*, cyber and technological). With this in mind, the AMF and other French regulators can create robust, evergreen laws that will evolve as blockchain technology continues to evolve.

[1] Discussion Paper at 3.
[2] Discussion Paper at 3.
[3] Discussion Paper at 24.

We recognize that in addition to the AMF, the Autorité de Contrôle Prudentiel et de Résolution ("ACPR") has already made proposals around regulation of DeFi as part of its Discussion Paper entitled "'Decentralised' or 'Disintermediated' finance: what regulatory response". Just like the AMF, we support a "coordinated approach towards regulation", so we offered our perspective on ACPR's approach to regulating DeFi,[4] and discuss a number of those same ideas throughout our Response.

Response to Definition of Decentralized Finance

The Discussion Paper recognizes, similar to many international regulatory bodies, that "there is no single definition of DeFi" but attempts to provide certain distinguishing characteristics of DeFi: "fully decentralised, automated and disintermediated", "without the need for human intervention, and solely relying on the use of decentralised blockchain protocols".[5] We agree that these are critical "distinguishing feature[s] of DeFi" as are the use of "smart contracts" comprising the "DApps".[6] ("DApp" has been used in varying ways throughout the industry; we use that abbreviated term herein to refer to the decentralized protocols that comprise DeFi, for the purpose of this Response only.)

Hallmarks of DeFi

As discussed further below, there are additional "hallmarks" of DeFi that should be used to distinguish whether a protocol or application should be considered part of this novel financial infrastructure:

- that the protocol/application is non-custodial (*i.e.*, there is no identifiable entity or person who holds cryptoassets on behalf of others at any point in the transaction flow);
- that the code for the protocol is open source or source available (as addressed below in response to *Discussion Point 3*): this allows users, developers and other third parties to verify how the protocol functions and/or is intended to function and that there is no "point of centralization"; and
- that all transactions are user-directed and user-controlled (*i.e.*, there is no identifiable entity or person necessary to effect any transaction; this is akin to the "without the need for human intervention" feature identified in the Discussion Paper).

Where the use of a protocol or application is "permissioned" (as discussed below in response to *Discussion Point 1*), we argue that it is not classified as "DeFi" even if it allows for economic transactions through a protocol comprised of smart contracts deployed to a blockchain network.

Assessment of Decentralization

We agree with the AMF that, in practice, there are "varying degrees of decentralisation", but we caution against using an overly-prescriptive definition of "decentralisation" because

[4] For Polygon Labs's full response, *see* https://polygon.technology/blog/response-to-acprs-discussion-paper-decentralised-or-disintermediated-finance-what-regulatory-response

[5] Discussion Paper at 4.

[6] Discussion Paper at 6-7.

decentralized blockchain-based applications, including in DeFi, continue to evolve from a number of perspectives.

Determinations on decentralization should be made with the fundamental characteristics of DeFi in mind: to enhance transparency in the system and to ensure that individuals or institutions do not have to trust or rely upon an external, third party for their own financial transactions or economic well-being, including for information about those transactions. This means emphasising (i) a lack of a single point of failure or control in the protocol, including any accompanying governance system and (ii) control – not custody – to determine whether there is a "regulatable" individual or entity. Thus, any test must be based on these tenets surrounding decentralization.

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 "decentralized". As the AMF suggests, decentralization has two layers: the protocol (*i.e.*, "no single party deciding on the processing of transactions, or as to whom can participate") and the infrastructure (*i.e.*, "distributed nature of the nodes"). The three-prong test can be applied to either of these layers.

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 decentralized or (ii) certain services that seek to call themselves "DeFi" without having the hallmarks of decentralization. The following factors provide a solid foundation in determining "decentralization": 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 protocol 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 centralization 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 centralized 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 centralized entity is creating the yield).

- To ensure decentralization at the infrastructure level, one must also assess whether the network to which the protocol has been deployed is itself permissionless and decentralized. 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 is not be "decentralized".

Governance and administration relates to the authority over who is able to upgrade or make changes to the protocol, 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 decentralized – there still may be points of centralization 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 "decentralization" must be flexible and account for the "regulatory outcome" looking to be achieved rather than something definitive.

Additional Points on Defining DeFi

One point of correction relates to Figure 2 – The DeFi "stack" – and the layers it sets forth. The Layer 1 and Layer 2 "levels" are correct and appropriate. The "protocol layer" should be removed because it is redundant in that a "protocol" is simply a piece of software or code. Protocols make up the software for all the other layers in "the DeFi stack", and, therefore, should be distinguished from Layer 1 and Layer 2 blockchains as well as dApps.

Thereafter, a DeFi application – a dApp, as it is referred to in the Discussion Paper – is deployed to a Layer 1 or Layer 2 protocol (or a number of them – for example, the Uniswap Protocol is deployed to Ethereum as well as additional networks such as the Polygon proof-of-stake network). For that reason, we encourage the removal and/or collapsing of the "protocol layer" and the "smart control layer" into one. The "smart contract layer" is the dApps layer. Smart contracts are - as the AMF notes - "composable" and deployed on top of Layer 1 and/or Layer 2 blockchains and form the back-end of decentralized applications. In addition, dApps refer to the DeFi protocols themselves – not the user interfaces or "front ends" that provide information to users about specific DeFi protocols so we encourage the removal of "(DApp)" from the top level of Figure 2 and adding the same parenthetical to the layer between "Layer 2" and "Application Layer".

Critically, DeFi protocols do not "display[ ] activities;"[7] rather, DeFi protocols allow *users* to themselves engage in economic activities; the users make transactions occur by broadcasting the information to the network through their self-hosted wallets. Without users initiating the transactions, nothing would happen. To this end, we advocate for an approach that only

[7] Discussion Paper at 13.

regulates identifiable persons or entities engaging in regulated financial activities (*e.g.*, TradFi, CeFi) and not software that allows third parties to do so (*i.e.*, a DeFi protocol itself).

We believe the points above are many of the same hallmarks that European regulators should use when determining whether cryptoasset activities are occurring in a "fully decentralised manner without any intermediary"[8] such that they would fall outside the scope of the Markets in Cryptoasset Regulation ("MiCA") and other EU-based regulations.

Response to Discussion Points

Discussion Point 1 - Permissionless versus Permissioned blockchain protocols

We agree with the AMF's position that determining whether activities (or, in our view, a software protocol) constitutes "DeFi" requires "an assessment of whether a blockchain is permissionless or not, including an assessment as to the degree of permissibility of the blockchain".[9] We believe the same assessment must be made at the dApp layer as well: *is the dApp permissioned or permissionless?*

Put simply and as stated above, a "permissioned" network or a "permissioned" DeFi protocol or application does not constitute DeFi.

A permissioned system – whether a blockchain network or an application protocol – does not and cannot meet the definition of "decentralization" set forth above, or any honest definition of "decentraliztion". "Decentralization" means "the dispersion or distribution of functions and powers."[10] Where there is a centralized actor – or even identifiable groups of actors – it does not meet the test for "the dispersion or distribution of functions". One may argue that if there are, for example, multiple unrelated parties engaged in the "permissioning" of only a single part of a system for a DeFi protocol, then it still can meet the traditional definition of decentralization. But DeFi protocols must be analyzed holistically – as a complete system from the base layer (Layer 1 or 2) to the "application layer". Where there is a centralized point of admission for use of or participation in activities or transactions that occur through a smart contract-based software protocol, there is a single point of "control," where an actor has responsibility for, at a minimum, certain functions in the protocol and thus, it cannot be considered DeFi.

Further, we discourage the use of permissioning in pure DeFi protocols or systems – or from seeking to switch all DeFi protocols to a permissioned system. As an initial matter, this would create significant fragmentation of liquidity for DeFi protocols across various blockchains. 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. 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.

[8] Markets in Cryptoassets Regulation, Recital 22.
[9] Discussion Paper at 6.
[10] See https://www.merriam-webster.com/dictionary/decentralization.

Furthermore, permissioned or "private" blockchains operated by private parties arguably do not need a new 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.

Discussion Point 2 - Smart contracts

Although we agree that smart contracts are a type of "automated software" "to execute software logic",[11] we do not agree that the "aim" of smart contracts is "to mirror the functionality of a 'real world' contract between parties".[12] A "smart contract" is not an actual contract between parties; the term itself is an unfortunate misnomer. Put simply, smart contracts are pieces of software (i.e., code) and "do not on their own constitute a legally binding agreement". Rather, they are called "smart" because they are "self-executing", and they are called "contracts" because they "carry out a transaction" when "a number of predetermined conditions have been met" "without the need for human intervention". Indeed, smart contracts function conditionally like many contracts – *e.g., the code recognizes the condition that if X occurs under certain circumstances, then Y will automatically follow.*

This correction is a necessary precursor to understanding what we view as the four questions posed by the AMF in regards to smart contracts (with our responses inline below):[13]

1. Is there or should there be a "legal basis for the enforceability of a smart contract"?

Code comprised of smart contracts does not have any "legal basis for enforceability" without the traditional hallmarks of a contract – and the legal enforceability thereof – as set forth in common law. The common law of contracts has existed for hundreds of years, and should not be modified or otherwise forced to fit novel software that uses the term "contract" but otherwise does not carry the same functions or features of a contract.

2. Is there or should there be "legal liability of parties that participate in the creation, development, or use of a smart contract," including the software developers who wrote or created the code?

As set forth in the Polygon Labs Policy Principles, we do not believe that there is – or should be – liability for software developers who create DeFi protocols, absent some other "special relationship" that creates such liability (namely, one borne out of a contractual relationship).

Specifically, the Policy Principles state, "Developing software is not a regulated activity today. Only those who offer the developed software to customers [in a centralized or intermediated way] are subject to consumer protection and other relevant laws. This framework should apply

[11] Discussion Paper at 3, 6.
[12] Discussion Paper at 6.
[13] Discussion Paper at 7.

equally to the development of blockchain and blockchain-based software. As has been recognized in the historical approach to regulating technology development, imposing laws directed at software development will chill innovation and ignore the opportunities of an Internet that users, rather than Big Tech, control."[14]

Further, financial laws regulate *activities undertaken by identifiable actors* – e.g., custodians who hold assets on behalf of third parties, brokers who facilitate transactions on behalf of third parties, etc. These laws arose in order to allow consumers to "trust" these intermediaries and to ensure that their assets and data were handled safely and with integrity. The same approach should guide any approach to regulating cryptoassets – that is, intermediated activities involving cryptoassets can and should be regulated, not the cryptoassets or the decentralized systems in which they may operate in a non-intermediated way. That is, "where technology replaces functions typically performed by persons in traditional systems, lawmakers should not import or otherwise force the existence of intermediaries [in order] to apply traditional regulation."[15]

Some 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, for which anyone – not just the original software developer of the protocol – 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 self-regulatory organization in which industry participants, stakeholders and regulators work collaboratively to set industry standards. We favour 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.

3. Should legislation impose "rules" that require DeFi protocols to "meet legal or regulatory requirements"?

Although, creating a "legal basis for the enforceability of a smart contract" (*i.e.*, "embedded supervision" such as "'stop / start' type mechanism[s]" or "compliance certification of their code") may produce some benefits (*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 decentralized smart contract-based systems are permissionless and thus, not tied to a single jurisdiction.

Further, this may also indirectly regulate software development – something that is not otherwise done for other technologies and create points of centralization that remove many of the benefits of blockchain-based technology. Therefore, any potential benefit of "rules" for DeFi protocols must be appropriately weighed against the costs to chilling innovation or otherwise making compliance impracticable to the point where DeFi ultimately "disappears" into a permissioned or impracticable set of software.

Instead of regulating code and software, we propose an alternative, risk-based approach. In fully decentralized systems, risk to users and to market integrity is borne primarily from technology

[14] https://polygon.technology/blog/polygon-labs-core-policy-principles.
[15] https://polygon.technology/blog/polygon-labs-core-policy-principles.

risk and cyber risk[16], or from integration with centralized systems (*e.g.*, centrally issued cryptoassets or centralized 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 subjective judgement. "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.

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 decentralized technology.

Despite the benefits of auditing, there are a number of helpful improvements in auditing practices that can be made: *first*, a standardization of the approach to auditing smart contracts for DeFi protocols, potentially codified in law; *second*, a standardization of when and how third party audits are used (*e.g.*, prior to launch, at the time of an upgrade to the code, etc); and *third*, standardizing transparency around protocol audits, which will enhance accountability both for auditors and development teams, and will allow for even greater examination of the safety of code.

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 decentralization 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.

[16] The AMF refers to technology and cyber risk as "unregulated market risk" in the Table on p.18.

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. In addition, the longer protocols exist and have time to mature, the more time they have had for users and developers to notice and fix vulnerabilities in the code. Therefore, with each phase of "software maturing", risk becomes isolated to incremental components, rather than the full project. However, two measures – "opt in" standards system and auditing approvals – could help ensure that consumers are protected while the technology develops and addresses technology and cyber vulnerabilities.

4. How can already-developed or -deployed smart contracts meet any newly-imposed legislation for DeFi protocols?

This question highlights precisely why laws should not regulate code. Although code is dynamic, it is inanimate – it cannot itself take actions, including those to ensure it complies with the law. This principle should counsel in favour of an approach that regulates activities (but not software development) rather than technology itself.

Discussion Point 3 - Use of open source software

"Open source code or software" is one of the hallmarks of permissionless networks, as discussed above. On the other hand, "code which is closed-source in nature" is that of permissioned systems, which are closed, centralized networks that function under relationships - like those of trustees, even if they don't hold custody in the traditional sense - that are regulated in traditional systems.

We agree that open source code in truly decentralized systems provide a number of benefits, including transparency, auditability and composability, among others.[17]

Discussion Point 5 - DeFi trading protocol market rules

As mentioned in our response to Discussion Point 1, permissionless networks and applications are open-source, meaning the code underlying them is open and accessible for anyone with an Internet connection to see. In addition, there are a number of tools (*e.g.*, AI technology) and industry best practices (*e.g.*, developers releasing documentation[18] about the protocol or other practices, like audits, mentioned in our response to Discussion Point 2) that make the underlying code of permissionless blockchain networks and applications more accessible and easier to understand for those unfamiliar with the technology. Lawyers and regulators can use these tools to enhance the effectiveness of "ensur[ing] proper disclosures".

[17] Discussion Paper at 8.
[18] All truly permissionless applications have this accessible. See Uniswap as an example, https://docs.uniswap.org/

Discussion Point 7 - Decentralization and degree of control

The Discussion Paper highlights that "the effective degree of decentralization is a key component that should be evaluated when determining the effective degree of control that is exerted over a DAO's governance, and thus over the underlying blockchain protocol that it governs". Please see our response to Discussion Point 1 for a framework around decentralization, which includes a section around governance and the "degree of control".

A key issue in assessing governance in DAOs – even in the face of certain actors purportedly having outsized "effective degree of control" (whether "de facto" or "de jure") in voting – 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 protocol – for a reason such as "identifying and resolving software bugs or errors that could affect [the DAO's] security or operation" – 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.

In addition, governance tokens – and concentration around holders and voters – also require a more nuanced discussion. For example, measuring holders of governance tokens on Etherscan (the block explorer for the Ethereum ecosystem) 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 (*i.e.*, "de facto" control), the appropriate measure for decentralization 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).

Conclusion

We greatly value the AMF's thoughtfulness in engaging on questions relating to DeFi through the Discussion Paper and look forward to continued collaboration on these matters.

To the extent discussion or clarification of the points described above would be helpful, we would be happy to provide additional written materials or engage further with the AMF.