Via Electronic Mail: innovation@amf-france.org

Autorité de Marchés Financiers
17, place de la Bourse
75082 Paris Cedex 02

Re: Decentralised Finance (DeFi), Trading Protocols and Governance Issues: Overview, Observed Trends, and Regulatory Discussion Points

To Whom It May Concern:

The DeFi Education Fund (DEF) thanks the Autorité des Marchés Financiers (AMF) for the opportunity to respond to the request for comments on the Discussion Paper (Paper) on Decentralised Finance (DeFi).[1] We appreciate your openness to public discourse on this new and promising technology.

By way of background, DEF is a non-partisan research and advocacy group. Our mission is to educate lawmakers about the technical workings and benefits of DeFi, achieve regulatory clarity for the future of the global digital economy, and advocate for individual users and developers in the DeFi space. DeFi has immense potential to advance innovation in the world economy, and we believe that potential can best be realized in conjunction with smart policy. DEF is not a trade association and does not represent the interests of any specific parties.

Discussion Points

1. Permissionless versus Permissioned Blockchain Protocols

[1] Autorité des Marchés Financiers, "Discussion Paper on Decentralised Finance" (June 2023), *available at* https://www.amf-france.org/en/news-publications/public-consultations/amf-discussion-paper-decentralised-finance-defi.

We agree with the Paper's sentiment that if a blockchain protocol is permissioned then it is not decentralized. Decentralization requires the distribution of authority and storage over data to a network of two or more nodes. By distributing authority, no single entity dictates who can or cannot participate in the network — i.e., the network is permissionless. A permissioned network implies that there is a central entity with the authority to be the gatekeeper.

The Paper suggests an evaluation of how many entities, individuals, users, or nodes can control the activity on the network — e.g., for onboarding users or for validating transactions. However, the Paper does not exactly specify how AMF intends to do so. The industry would benefit from having clear guidelines in this regard. We suggest that AMF follow up with a comprehensive proposal, open for public comment, so we may further assess the matter.

2. Smart Contracts

a. Determine a legal basis for the enforceability of a smart contract

The Paper addresses the challenge of determining a legal basis for the enforceability of a smart contract. However, a legal framework is only required when trust in human discretion is required for a financial relationship to function properly; on the contrary, DeFi aims to develop a financial infrastructure in which trust is established through software such as smart contracts — i.e., autonomous code that functions without intermediation. Unlike a traditional contract, which legally binds two parties to fulfill their obligations of an agreement, a smart contract skips the legal requirement for someone to fulfill their obligations and simply executes the terms of an agreement. Additionally, to maintain an honest relationship between parties, the code is open-source[2] for anyone to audit in real-time and ensure there are no back-doors that would enable dishonest activity.

b. Legal liability of parties involved in development and deployment of smart contracts

Legal liability of smart contract developers is not a logical proposal since their code is open-source for anyone to audit at any time, granting users the ability to make an informed decision as to whether or not to use them — i.e., users choose to accept the terms of the contract willingly. Users must exercise due diligence to make informed financial decisions.

[2] Software that is free to view, use, modify, and distribute.

Furthermore, open-source code contains "creative and scientific expression" that brings about significant political and social changes in an era dominated by internet communication.[3] Therefore, developers who simply write code are engaging in free speech and should not be held liable for the outcomes of a smart contract. Both France's Declaration of the Rights of Man and of the Citizen[4] and the European Union's (EU) Charter of Fundamental Rights[5] emphasize the importance of freely expressing and publishing ideas, and we believe this extends to open-source code.

c. Stop / start mechanism

The Paper proposes the idea of legislation that could require smart contracts to be designed to include a "stop / start type mechanism." This mechanism is technically possible; however, the mechanism would be left to the discretion of the authorizing entity, requiring trust in a third-party which is counterintuitive to the utility of smart contracts — i.e., a trustless, p2p approach to contractual agreements. Therefore, an emergency stop mechanism cannot be granted to a central authority as it would avail the opportunity for its misuse and potential financial discrimination. If employed, authority over the emergency stop mechanism would need to be decentralized and subject to an on-chain voting mechanism or a multi-sig wallet.[6] Furthermore, already deployed smart contracts cannot implement a stop / start mechanism because once they are deployed on a blockchain, they are immutable.

d. Smart contract certification

The Paper also proposes a form of compliance certification of smart contracts' code with applicable regulatory requirements; however, the deployment of a smart contract is done in a decentralized manner. Essentially, anyone can take open-source code and deploy it on a blockchain, and the nodes will accept the code so long as the deployment transaction is a valid transaction—this process cannot be prevented since blockchain protocols are decentralized and permissionless. Here is how it works:

---

[3] *See* Coin Center, "Electronic Cash, Decentralized Exchange, and the Constitution" (March 2019), *available at* https://www.coincenter.org/app/uploads/2020/05/e-cash-dex-constitution.pdf.
[4] "The Declaration of the Rights of Man and of the Citizen," Article 11 (1789), *available at* https://www.elysee.fr/en/french-presidency/the-declaration-of-the-rights-of-man-and-of-the-citizen.
[5] European Union, "Charter of Fundamental Rights," Article 11 (2000), *available at* https://www.europarl.europa.eu/charter/pdf/text_en.pdf.
[6] *See* Corwin Smith, "Smart Contract Security" (June 2023), *available at* https://ethereum.org/developers/docs/smart-contracts/security/.

1) Developer writes the code;
2) The developer, or another user wishing to deploy the code, creates a *deployment transaction* that includes the bytecode of the smart contract and its initialization parameters, and signs the transaction with their private key to authenticate and authorize it—the sender does not specify the recipient;
3) The deployment transaction is then sent to the sender's connected nodes within the blockchain network;
4) These nodes then relay the transaction to their own connected nodes and the transaction continues to propagate across the network;
5) Each receiving node verifies and validates the transaction's digital signature and sufficient gas, and ensures that it complies with the network's rules—they do not audit the smart contract's code;
6) Once the deployment transaction has reached consensus, miners or validators include it in their new block, which finalized the deployment;
7) Once it is added to the blockchain, the smart contract is activated and is assigned a unique address on the blockchain—its bytecode and initialization parameters are stored in the contract's storage.
8) Once it is deployed, the smart contract is autonomous and immutable.

Furthermore, because a blockchain is decentralized, there is no central entity to identify someone who wants to deploy a smart contract on the network, making it difficult for authorities to determine who is held liable for the outcomes of a smart contract.

Technicalities aside, a certification process for smart contracts would require a central authority and designating a central authority would undermine technological neutrality. Decentralization prevents any one person or group from imposing their bias or objectives into a network — designating oversight of the smart contract certification process to a central authority is counterintuitive to the objectives of decentralized networks. Additionally, should such a certification exist, there would need to be a set of standards to abide by. The two possible candidates for setting such standards would either be public authorities or market participants. However, each candidate comes with its own set of challenges. Granting authority over standard setting to public authorities would not mitigate risks as the code is complex and public authorities have limited expertise. On the other hand, granting authority to market participants would enable a conflict of interest — e.g., chosen market participants could set standards that are high and increase the barrier of entry, monopolizing the market for large, existing actors.

3. Open-Source Code for Protocols

a. Benefits of open-source

The Paper asks for the consideration of the use of open-source code in DeFi protocols, and we believe that code that can be viewed, modified, copied, and distributed without any obligations to those who developed it is what is best for accountability, decentralization, and the future of innovation.

Open-source code is fundamental to the DeFi ecosystem for a variety of reasons. First, developers can build off each others' work, making it cheaper and easier to innovate.[7] Second, it empowers diversity in the space since the code is available for anyone in the world to use, modify, and distribute — all one needs is a computer and an internet connection.[8] Third, the code is auditable for anyone to ensure there are no bugs or backdoors, and contribute fixes — this is especially important since trust is conducted through code.[9] Lastly, it "enables rapid proliferation of ideas."[10]

Furthermore, open-source code and decentralized protocols work in tandem: by making code open-source, decentralized protocols promote transparency and community involvement. If protocol developers made their code proprietary, a single entity or group would have excessive influence and control over the code.

b. Permissive license

Permissive license allows code to be viewed, modified, copied, and distributed without any obligations to those who initially developed the code[11] — the most compatible with the DeFi ecosystem.

c. Business source license

---

[7] *See* Nadia Eghbal, "Roads and Bridges: The Unseen Labor Behind Our Digital Infrastructure," pg. 23 (2016), *available at* https://www.fordfoundation.org/media/2976/roads-and-bridges-the-unseen-labor-behind-our-digital-infrastructure.pdf.

[8] Ibid., pg. 26-28.

[9] Ibid., pg. 36.

[10] Ibid., pg. 35.

[11] *See* Fossa, "All About Permissive Licenses" (June 2021), *available at* https://fossa.com/blog/all-about-permissive-licenses/.

There has been an increase in business source licenses (BSL)[12] that allow software to be available and modifiable but restrict commercial usage until a certain number of years until it then transitions to an open-source license. In those restrictive years, purchasing a commercial license is required to use the software in a commercial way but developers can still use the code as long as it is kept open-source.

In these cases, we must acknowledge that under a BSL, the code is still auditable which holds those distributing the code accountable to the public. Furthermore, a decentralized governance model can still exist with a BSL, meaning that the protocol's token holders still have authority over its changes — the BSL would only prevent external parties from using and modifying the code for their own commercial benefit.

Ultimately, the question of whether it improves or harms innovation is left to perspective. One could argue that intellectual property rights incentivizes innovation or that freeing code for use, modification, and distribution without restrictions does. However, in the context of DeFi protocols, any license that allows code to be auditable and maintains decentralized governance is acceptable for accountability and decentralization — the two most important factors in maintaining the integrity of DeFi.

d. Proprietary license

A proprietary license means that the publisher has exclusive control over the software and any changes to its "design or implementation have to originate from the company itself."[13] This code is least compatible with DeFi for this reason.

4. Risks Posed by DeFi Activities

We believe that "ad hoc" type regulation is most suitable for DeFi as it is not comparable to traditional finance and should therefore be regulated based on its own set of risks and attributes. We'll need the AMF to elaborate on how they intend to take an "ad hoc" approach to provide further guidance.

5. DeFi Trading Protocol Market Rules

a. Approval process

[12] *See* "Business Source License 1.1," *available at* https://mariadb.com/bsl11/.
[13] Eghbal, pg. 30.

The Paper suggests that an approval process of smart contracts' code could be a potential regulatory approach to DeFi trading protocols. However, an approval process would prove difficult to enforce since authorities cannot prevent a decentralized network of users around the world from deploying a smart contract and once it is deployed, it is immutable.

Furthermore, the concept can be compared to requiring an approval process for every piece of software ever created — a suppressive approach that would harm innovation and prosperity. Experimentation of new technologies is essential for innovators to learn and refine them so they may improve the quality of life. A permissionless ecosystem, such as DeFi's, allows just that.

The freedom to innovate has its risks but DeFi's open-source infrastructure grants anyone the ability to audit code for bugs, backdoors, etc. and decide which smart contracts are safe and efficient for use. This coincides with the ethos of decentralization found across the ecosystem — there is no small, aligned group of gatekeepers, instead authority over what prevails in the ecosystem is distributed among a diverse and unaffiliated network of individuals.

Additionally, and as alluded to with smart contract certification, there would need to be a set of standards for this approval process that would cultivate its own set of challenges and risks.

b. Non-technical language

Whitepapers for the initial deployment of DeFi protocols is an already established industry standard; however, this would be an administrative burden to require a whitepaper for every smart contract deployed thereafter, since protocols are governed by decentralized governance models. If AMF were to administer the same white paper requirements as the EU does in its Markets in Crypto Assets (MiCA) legislation,[14] it would face the same

[14] The European Parliament and Council, "REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on markets in crypto-assets, and amending Regulations (EU) No 1093/2010 and (EU) No 1095/2010 and Directives 2013/36/EU and (EU) 2019/1937" (May 2023), pg. 20 clause 24 ("When making an offer to the public of crypto-assets other than asset-referenced tokens or e-money tokens or when seeking admission to trading for such crypto-assets, in the Union offerors or persons seeking admission to trading should draw up, notify to their competent authority and publish an information document containing mandatory disclosures ('a crypto-asset white paper')."; pg. 26, clause 34 ("competent authorities should be

challenges as alluded to in the certification and approval processes: smart contract deployment is done in a decentralized manner, there is no centralized entity to enforce these requirements.

6. Definitions of DEX and AMM

Concerning the incorporation of off-chain elements in crypto-asset trading platforms, what distinguishes a DeFi protocol from a CeFi trading platform in this regard is the degree of decentralization of off-chain elements. Both oracles and off-chain order books can be developed in a decentralized manner for DeFi protocols — meanwhile, CeFi platforms don't use oracles and their order books are controlled by the centralized entity controlling the platform as well.

a. Oracles

An oracle provides off-chain, or "external," data to smart contracts on a blockchain. Oracles are not used in CeFi platforms, instead CeFi platforms may develop their own oracles to communicate data with DeFi protocols. However, because oracles are off-chain, the AMF raises reasonable concerns about the integrity of decentralization in DeFi protocols. Therefore, oracles' degree of decentralization must be examined themselves; otherwise, they could introduce a single point of failure — e.g., system failures, where the oracle goes offline, or hacks that manipulate the data.[15]

Centralized oracles are controlled by a single entity and rely on said entity for their data. Meanwhile, decentralized oracles require consensus of multiple nodes in a peer-to-peer network before sending data to a smart contract. Decentralized oracles do come in various degrees of decentralization — e.g., there are "semi-decentralized oracle networks where anyone can participate, but with an 'owner' that approves and removes nodes based on historical performance."[16]

---

able to suspend or prohibit an offer to the public of crypto-assets… where such an offer to the public or admission to trading does not comply with the applicable requirements of the Regulation, including where the crypto asset white paper is not fair, not clear, or misleading."), *available at* https://data.consilium.europa.eu/doc/document/PE-54-2022-INIT/en/pdf.

[15] *See* Chainlink, "What Is a Blockchain Oracle?" (May 2023), *available at* https://chain.link/education/blockchain-oracles.

[16] *See* Ken Carv, "Oracles" (June 2023), *available at* https://ethereum.org/en/developers/docs/oracles/#types-of-oracles.

Fully decentralized oracle networks usually incorporate their own standalone blockchain with consensus mechanisms for coordinating nodes and punishing misbehavior — much like in other blockchain networks. One way to validate information is the voting/staking on accuracy of data — users stake their tokens (much like in a PoS network) with the information they've provided and are penalized if they deviate from the majority of answers, as it assumes the majority is full of rational economic actors that are reflecting the most accurate information.[17]

b. Order books

Off-chain order book protocols maintain a degree of decentralization by making themselves accessible to any developers to create their own relayer order books. To understand the process, here's how an order book works on the 0x protocol:[18]

1) Maker — a user who places a limit order to buy or sell an asset at a specific price, waiting for a taker to fulfill the order — approves the decentralized exchange (DEX) contract to access their balance of Token A.
2) Maker creates an order to exchange Token A for Token B, specifying a desired exchange rate, expiration time (beyond which the order cannot be filled), and signs the order with their private key.
3) Maker broadcasts the order over any arbitrary communication medium.
4) Taker — a user who accepts a maker's existing order from the order book, completing the trade immediately at the specified price — intercepts the order and decides that they would like to fill it.
5) Taker approves the DEX contract to access their balance of Token B.
6) Taker submits the maker's signed order to the DEX contract.
7) The DEX contract authenticates the maker's signature, verifies that the order has not expired, verifies that the order has not already been filled, then transfers tokens between the two parties at the specified exchange rate.

Order books on 0x are hosted and maintained by what are known as "relayers" in exchange for transaction fees. As explained above, a maker broadcasts their order with the fee for them to pay to the relayer and the fee for a taker to pay to the relayer should they fill the order, as well as their address in which to charge the transaction fee. The maker signs

[17] Ibid.
[18] *See* Will Warren, Amir Bandeali, "0x: An open protocol for decentralized exchange on the Ethereum blockchain," pg. 5 (February 2017), *available at* https://github.com/0xProject/whitepaper/blob/master/0x_white_paper.pdf.

the order with their private key and broadcasts it for any relayer to intercept the broadcast. When a relayer intercepts the broadcast, they check its validity — as in its format, if it contains the required fee values, and if it meets the relayer's specific requirements — then the relayer posts it to their specific order book for a taker to fill the order.[19]

By allowing anyone to become a relayer and participate in hosting and maintaining order books, protocols foster an open and decentralized ecosystem where multiple independent actors can contribute to trading activity. These protocols still use smart contracts to execute transactions without an intermediary. The relayers simply broadcast the makers' limit order to buy or sell for takers to fulfill them — they do not execute the trade.

c. DEX versus AMM

It is worth noting that automated market makers (AMM) are a type of DEX, the two are not separate concepts. And the AMF is correct that in determining different models of DEXs, the main aspect to consider is their pricing mechanism — where on-chain order books determine price based on what is set between buyers and sellers, AMMs determine their price based on a ratio formula.[20]

7. Decentralization and Degree of Control

a. Pseudonymity risks

AMF's concern that pseudonymity prevents anyone from understanding who may exert control over a DAO is a valid concern; however, evaluating the degree of decentralization over a DAOs governance would require an identification mechanism, which is an evolving space within DeFi that requires trade-offs.

Lifting pseudonymity to identify the state of concentration of a DAO would harm users' autonomy. Privacy enables individuals to live and make choices authentic to what they believe. By removing privacy protection, an individual could be pressured to act in

[19] Ibid., pg 7-8.

[20] An AMM uses the ratio of two assets in a special-purpose smart contract — called a liquidity pool — to determine the relative price of two assets. In this formula, x and y represent the assets and k represents the constant product value. The AMM calculates the prices of each asset based on their supply and demand: as x increases in supply, its price decreases to maintain a constant product value of k. As the exchanges are validated by the underlying blockchain, new prices are calculated in real-time. One benefit of this is that an exchange cannot manipulate asset pricing as it is mathematically formulated.

conformity with the group — and against their beliefs — or targeted and coerced by a malicious actor.[21]

Reasonably, the trade-off between decentralized governance and privacy proves to be a complex and contentious issue. In order to solve the concentration of governance in DeFi, the ecosystem must instill a way in which to identify users. However, there are no centralized entities to gather and maintain this information, and such an approach would violate critical privacy protections and interfere with DeFi's fundamental infrastructure. For this reason, we believe public authorities should give the industry time to develop its own solutions — there are a variety of developers in the ecosystem already attempting to solve the problem of governance concentration without violating the privacy of users.

b. Considerations

There are a few considerations to take into account when evaluating decentralization and the degree of control over a protocol's governance. First, the initial token distribution — it may be communicated in governance documents how many tokens are allocated to the developers of the protocol.

Second, quorum and participation requirements. Quorum refers to the minimum number or percentage of eligible voters or tokens that must participate in a governance vote for the vote to be considered valid and binding. Participation requirements refer to the conditions that token holders must meet to be eligible to vote — e.g., requiring tokens to be locked or staked. While these have their utility, they may also serve as barriers that could concentrate voting.

Third, "authority over the functioning of the code," which requires an evaluation of whether there is an "administrative key that allows control over the protocol" and if there is a "central decision-making authority that can control the protocol through governance votes or otherwise."[22]

---

[21] *See* Dorota Mokrosinska, "Privacy and Autonomy: On some misconceptions concerning the political dimensions of privacy" (May 2017), *available at* https://link.springer.com/content/pdf/10.1007/s10982-017-9307-3.pdf.

[22] Polygon Labs, "Response to ACPR's Discussion Paper, ''Decentralised' or 'Disintermediated' finance: what regulatory response." (May 2023), *available at* https://webflow-user-file-uploads-production.s3.amazonaws.com/637359c81e22b715cec245ad/602cebee-2ec6-4696-afe3-d79d2187b332.pdf?X-Amz-Algorithm=AWS4-HMAC-SHA256&X-Amz-Credential=AKIAQLLHWD6MEJGETLST%2F20230914%2Fus-east-1%2Fs3%2Faws4_request&

* * *

Thank you again for the opportunity to provide input on this consultation. The DeFi Education Fund is sincerely grateful for AMF's engagement on these issues.

Sincerely,

Lizandro Pieper
Policy Associate

X-Amz-Date=20230914T201210Z&X-Amz-Expires=300&X-Amz-Signature=aa8aadb63dded2c9d52e42ed09a9b73ddf4292b509af2af487927ebe955d9f97&X-Amz-SignedHeaders=host.