June 2, 2023

**Via email:** fintech-innovation@acpr.banque-france.fr

Autorité de Contrôle Prudentiel et de Résolution
Banque de France

**Re: Response to ACPR's Discussion Paper: "'Decentralised' or 'Disintermediated' Finance: What Regulatory Response?**

To whom it may concern:

The DeFi Education Fund[1] ("DEF") appreciates the opportunity to provide comments to the Banque of France ("Banque") on the Autorité de Contrôle Prudentiel et de Résolution ("ACPR") discussion paper titled, "'Decentralised' or 'Disintermediated' Finance: What Regulatory Response?" ("Paper" or "Discussion Paper").[2] This letter addresses the key proposals raised in the paper.

The DEF thanks ACPR for soliciting public feedback on this Paper and sincerely appreciates the rigorous knowledge of DeFi that the Paper evidences. While we share the policy objectives the Paper's proposals seek to accomplish, some of the proposals require further consideration. At core, the promise of DeFi protocols stems from their decentralized and permissionless characteristics, and regulatory proposals should seek to maintain those characteristics.

## Discussion of Key Proposals

### I. Public Blockchain Minimum Standards

[1] DEF is a nonpartisan advocacy group based in the United States with a mission to educate policymakers about the benefits of decentralized finance and to achieve regulatory clarity for the DeFi ecosystem.

[2] Autorité de Contrôle Prudentiel et de Résolution, "'Decentralised' or 'Disintermediated' Finance: What Regulatory Response?" Banque de France (April 2023), *available at*: https://acpr.banque-france.fr/en/decentralised-or-disintermediated-finance-what-regulatory-response

The Discussion paper proposes regulating "public blockchains… by way of a number of minimum standards, concerning the infrastructure's computer code design (risk of failure), governance rules (refer to section 2-1 on this topic), effective number of validators and concentration (see below)."[3] We do not support this proposal because it would directly regulate technology (violating the principle of technological neutrality), apply financial regulatory obligations to non-financial activities, and be prohibitively impractical to implement.

Applying financial regulatory standards to public blockchains or smart contracts would run contrary to the principles of technological neutrality and "same activities, same risks, same rules." By definition, applying standards to public blockchains is not technologically neutral, a principle the Discussion Paper seeks to protect. In practice, applying minimum standards for a technology—public blockchains—would mean imposing financial regulatory obligations on persons engaged in the validation of public blockchains (either mining or staking), an activity that is not appropriately subject to financial regulation. As the Discussion Paper explains, financial regulatory obligations generally follow the principle of "same ***activities***, same risks, same rules." Validators and miners secure public blockchains by checking and agreeing to the validity of data to be newly incorporated into the blockchain via its consensus mechanism. This non-financial activity should not be subject to financial regulation. The individual and uncoordinated efforts of miners and validators collectively provides permissionless public infrastructure that can be used for a variety of purposes, both financial and non-financial.

The implementation of this policy may also, paradoxically, undermine its intended goal. For example, validators must retain the ability to remain pseudonymous to maintain the integrity of a blockchain network's consensus mechanism (bolstering the security of the entire blockchain[4]) for the same reason many free societies protect the "secret ballot." Privacy is essential for individuals to validate transactions freely, which is foundational to a public blockchains security. An easily coerced network is neither secure nor effective in maintaining a valid record of information.

Moreover, requiring a minimum number of validators before launching a blockchain inhibits growth and competition in the space by elevating the barrier of entry to deploy a blockchain—an issue the ACPR acknowledges in the paper[5]—and inhibit competition in the space. Competition provides users with a variety of choices and incentivizes developer communities to

---

[3] Discussion Paper, at p. 28.

[4] *See* Dorota Mokrosinska, "Privacy and Autonomy: On Some Misconceptions Concerning The Political Dimensions of Privacy" *available at:* https://link.springer.com/content/pdf/10.1007/s10982-017-9307-3.pdf.

[5] Discussion Paper, at p. 28.

create blockchains with users in mind[6]—essentially a means for protecting users. For example, prior to the deployment of Zcash, a group of computer scientists recognized that while Bitcoin transactions are pseudonymous, there are analytical tools that help identify which addresses are associated with whom. Recognizing this flaw and the importance of financial privacy, the Electronic Coin Company forked Bitcoin's code to develop a blockchain with privacy-oriented infrastructure.[7] Zcash users now have the ability to decide who can and cannot see their transactions—a necessary feature for those who live under regimes with limited political freedom.

Finally, because mining and validating public blockchains is a permissionless activity, adopting minimum standards for public blockchains would be a policy highly unlikely to accomplish its objectives. Because anyone anywhere in the world can engage in mining and validating and access public blockchains, subjecting mining and validating to financial regulatory obligations in any one country is unlikely to have its intended effect.

## II. Private Blockchains

We do not believe that prohibiting the use of public blockchains is a proportional policy response to the risks posed by DeFi. Transferring "financial functions" to private blockchains composed of "trusted players" would undermine the essential innovation of blockchains—their permissionless and decentralized characteristics. Moreover, we do not believe that private blockchains raise novel regulatory or policy questions because the "consensus" and "trust" of such networks is developed using traditional means, e.g. inter party agreements, contracts, etc.

## III. Smart Contract Certification

A certification process for smart contracts would require a central authority—in this case, "specialized assessors"[8]—to audit smart contracts before their use. We do not support the Discussion Paper's proposal for *a priori* certification of smart contracts for similar reasons to those discussed in Section I. Such a policy would directly regulate technology (violating the principle of technological neutrality), apply financial regulatory obligations to non-financial activities, be prohibitively impractical to implement, and undermine free speech rights.

Applying regulatory obligations to a technology itself, in this context smart contracts, is necessarily violative of the principle of technological neutrality. Instead, financial regulatory obligations should apply to persons engaged in financial activities, in accordance with the principles of "same activities, same risks, same rules." Because persons engaged in the writing and

---

[6] Once a blockchain is deployed, it is decentralized—competition in this sense is a competition of ideas and applications. Ethereum was developed with the idea of a blockchain that developers could build applications on as a Layer 2, and Zcash for privacy, as mentioned above.

[7] *See* Founding Zcash Scientists, *available at*: https://z.cash/founding-scientists/.

[8] Discussion Paper, at p. 32.

publishing of open-source software are not engaged in a financial activity, it would be inappropriate to extend financial regulatory obligations to those persons.

Additionally, granting discretion to set security standards to public authorities or market participants each comes with its own set of issues. Public authorities may find it challenging to mitigate smart contract risks with their limited expertise in complex code. Alternatively, market participants would be able to provide their expertise but—as ACPR expressed in the paper[9]—this would present conflicts of interest between competitors and make it challenging to agree on common standards. Also, should standard setting be granted to market participants, it could not include every voice in the ecosystem, which would avail the opportunity for big players in the space to set high compliance costs that could monopolize the market.

## IV. Governance

While concern of concentrated voting power in DeFi governance is warranted, we do not support "forced centralization," a policy that would likewise violate the principles of technological neutrality and undermine the core benefits of DeFi.

Governance structures in DeFi are extraordinarily varied. For example, some smart contracts can be designed such that governance powers can change everything about a smart contracts, while others can have no governance mechanisms whatsoever. For example, though token holders may be able to vote on proposals, they may not have direct control over a DeFi protocol's core functions. Moreover, iIncorporation would necessarily imply that governance token holders are working together as a single, centralized entity and that they directly control the protocol. Yet participation in many governance arrangements is more akin to participation in elections: yes, voters reach some threshold of consensus for a candidate but that does not imply that they are working together or even know each other and, more importantly, it does not imply that they have direct control over the subsequent "output" of elections. Establishing a legal status for DAOs must only be done in a manner that maintains the integrity of a DAO—e.g., decentralization, autonomy, and pseudonymity. Legal frameworks should be adapted to recognize and accommodate the decentralized nature of DAOs rather than trying to fit them into existing structures that are based on centralized control.

The DeFi community recognizes that governance is a major problem to be solved. Many in the DeFi ecosystem are already committed to making governance more efficient and secure and are actively proposing solutions to do so—e.g., multifactorial consensus model.[10] Public authorities should work with industry participants and experts to instead develop a regulatory "sandbox" for DeFi that would still allow for experimentation and innovation within defined boundaries, and

---

[9] Discussion Paper, at p. 33.

[10] *See* Vitalik Buterin, "Notes on Blockchain Governance" *available at:* https://vitalik.ca/general/2017/12/17/voting.html.

provide regulators with a better understanding of policies that can effectively accomplish their regulatory objectives in DeFi.

## V. "DeFi Intermediaries"

Web interfaces serve as a communication bridge between users and DeFi protocols and do not hold users' assets to intermediate transactions. For clarification, a web interface acts more as a "translator" from human to blockchain similar to the way email works. When sending an email, a person writes the email using the Roman alphabet to coherently write words and sentences. When that email is sent, the email provider "translates" the message into a form that can be transmitted to the recipient which are essentially data packets that can be sent over the internet. Likewise, DeFi frontends "translate" human-understandable activities into a form that blockchains can understand.

The discussion paper proposes that "DeFi intermediaries" fall under the provisions of MiCA; however, doing so here would not be responsive to the risks identified. Even if regulating some of these "DeFi intermediaries" may be deemed appropriate, such systems are incompatible with MiCA's requirements for crypto asset service providers (CASPs). Among MiCA's requirements, CASPs must implement internal controls that detect and prevent the misuse of data pertaining to standing orders; must adhere to capital requirements; must implement measures for preventing conflicts of interest; and must keep records of all transactions for authorities to access.[11]

Many of these requirements are unnecessary and unresponsive to certain risks in the context of DeFi. With regards to internal controls, DeFi does not have privileged access to users' standing orders and other sensitive information the way CASPs do. All such information is also publicly available on public blockchains. Additionally, DeFi protocols do not custody users' assets and would not need to reserve capital; and, since DeFi protocols do not have control of assets, there is no need to control for risks like the inappropriate use or theft of customers funds.

Lastly, MiCA would follow the Fifth Money Laundering Directive (MLD5) for anti-money laundering and the combating of financing of terrorism (AML/CFT) requirements on financial institutions. Under the Fourth Money Laundering Directive (MLD4), financial institutions must apply customer due diligence (CDD) measures—such as identifying customers and monitoring transactions—when there is a business relationship.[12] MLD5 amends MLD4 to include crypto exchange services and custodial wallets.[13] However, while this may be applicable to centralized

---

[11] *See* Watson Law, "MiCA - Regulation of Crypto-asset Service Providers" *available at* https://watsonlaw.nl/en/mica-regulation-of-crypto-asset-service-providers/.

[12] *See* Fourth Money Laundering Directive, Article 3(13).

[13] *See* Fifth Money Laundering Directive, Amendment 8.

exchanges, DeFi protocols cannot comply with such requirements as there is no business relationship between users and open-source software.[14] DeFi protocols are not subject to central control. Even when DeFi protocols originate from a single software developer or small group of developers, they are generally designed to involve governance arrangements that ensure dispersal of control among a decentralized and disaggregated group of unrelated users. Furthermore, DeFi protocols are more like traditional information-service providers than they are like financial intermediaries, entities not traditionally subject to financial surveillance requirements.

## VI. Access Restrictions

The discussion paper ends with the proposal for "[DeFi] intermediaries" to restrict access to "DeFi services" depending on the financial literacy of a user. This requirement would inhibit DeFi's efforts for financial inclusion and make it a permissioned ecosystem much like the traditional financial system, which has proven to raise financial inclusion concerns—according to the European Savings and Retail Banking Group's (ESBG) assessment of the World Bank's Global Findex Database, 13 million Europeans were unbanked as of 2021.[15] Should the ACPR's proposal become law, millions of unbanked Europeans would not have the opportunity to experiment with an alternative financial system and gain access to the global economy.

* * *

Thank you again for the opportunity to comment on the ACPR's discussion paper. Please do not hesitate to contact me if you have any questions at lizandro@defieducationfund.org.

Sincerely,

Lizandro Peiper

---

[14] *See* Peter Valkenburgh, "Electronic Cash, Decentralized Exchange, and the Constitution," *available at* https://www.coincenter.org/app/uploads/2020/05/e-cash-dex-constitution.pdf.

[15] *See* ESBG, "Number of Unbanked adult EU more than halved in the last four years," *available at* https://www.wsbi-esbg.org/number-of-unbanked-adult-eu-citizens-more-than-halved-in-the-last-four-years/#:~:text=According%20to%20the%20World%20Bank,to%2031%20million%20in%202017.

## ADDENDUM: DEFI PRINCIPLES

### Outline



---

### 1. Introduction

Traditional financial regulation largely is based on pursuing policy objectives via the regulation of financial intermediaries that typically custody assets or clear transactions. Because the decentralized finance ecosystem establishes trust via rules-based, encoded protocols maintained by numerous independent parties around the world instead of intermediating financial institutions, this traditional regulatory approach does not transpose onto, or account for the features of, the DeFi ecosystem.

Thus, achieving long-standing policy objectives in the DeFi ecosystem necessitates updating current regulatory frameworks and methodologies—a critical and challenging task. Reaching mutual appreciation of core policy objectives and the functionality of this new technology and successfully modernizing existing regulatory approaches will require the cooperation and coordination of policymakers, market participants, and other stakeholders inside and outside the DeFi ecosystem.

DeFi ecosystem participants' pro-active adherence to principles that vindicate long-standing policy objectives could meaningfully contribute to this critical endeavor. The principles listed in this document are intended to start a conversation to that end, not only among DeFi users, developers, and investors, but also between the ecosystem and policymakers.

These principles, put together by a group of DeFi proponents, are a "first shot" at this effort. Advice and thoughts on this discussion draft—and the premise more broadly—are welcome from all parties.

## 2. Illicit Activity Prevention

DeFi market participants should commit to adopting a risk-based approach to preventing illicit financial activity that leverages and supports the distinctive innovations of distributed ledgers and decentralized finance. A risk-based approach should include the development and implementation of advanced technological solutions that effectively deter, detect, and disrupt illicit activity, such as money laundering, terrorist financing, and other national security threats, while preserving individuals' privacy and enabling greater access to financial products. Market participants' commitment to a risk-based approach to mitigating the illicit use of DeFi protocols should recognize that privacy is essential to security and the minimization of vulnerabilities, including the potential for identity theft and exploitation.

## 3. Development & Launch

### a. Code Review, Audits, and Testing

Before deploying a DeFi protocol on the mainnet of a blockchain network, development teams should ensure the protocol's code has undergone testing according to current best practices and consistent with the level of risk involved in an application's use.

Currently, development teams may wish to consider ensuring:

i. *the code is reviewed internally;*

ii. *a full peer code review is performed, recommended changes to the code are made, and steps 1-2 are completed on any changes;*

iii. *if an independent security review is performed, the changes reviewers mark as severe are made, other recommended changes are considered, and steps 1-3 are completed on any changes;*

iv. *both individual smart contracts and the interactions between smart contracts are thoroughly tested; and*

v. *the on-chain state of contracts are validated following each phase of deployment.*

**b. Blockchain Standards**

A DeFi protocol should be deployed on a permissionless blockchain network, the consensus rules of which are not modifiable by a single person, entity, or coordinated group of persons or entities known to one another that do not act independently.

**c. Governance Decentralization**

A DeFi protocol's governance structure (if any) should ensure that no single person, entity, or coordinated group of persons or entities that do not act independently can unilaterally control governance or block or approve transactions on the protocol.

**d. "Guarded" Launch**

A DeFi protocol should consider initially launching with controls in place appropriate for the nature of the protocol, such as liquidity caps, to allow for use of the protocol without significant risk of capital loss to users. If any bugs or potential attack vectors are discovered during the "guarded" launch, then the development team should address such bugs and attack vectors.

**4. <u>Transparency and Disclosures</u>**

The information set forth in this section, and any material changes to the information set forth in this section, should be made available on a freely accessible public website as soon as practicable. Conspicuous hyperlinks to the information will satisfy these requirements. "Verifiability" means the ability to independently ascertain the truth of the information disclosed. To the extent that information regarding trades executed through a protocol is made available, it should be provided on a non-discriminatory basis. Avoid making inaccurate or misleading statements regarding trade volumes or available liquidity, and if such volumes or liquidity is disclosed, the methodology for calculating the same.

**a. Open Source Code and Transaction Verifiability**

Before deploying a DeFi protocol's audited source code on a blockchain network, a text listing of commands to be compiled or assembled into an executable computer program used by participants to access the protocol, amend the code, and confirm transactions, as applicable, should be published pursuant to an open source license. All transactions on the protocol should be

publicly verifiable, and a narrative description of the steps necessary to independently access, search, and verify the transaction history of the protocol, as applicable.

**b. Token Economics**

The economics of a DeFi protocol's associated token, if any, should be disclosed and independently verifiable. This information should include the token's launch process, generation process, supply cap, release schedule, initial allocation, total outstanding amount, and how changes can be made to the protocol's token economics, if applicable.

**c. Earnings**

Disclosures should include an explanation of the potential earnings of a user, including through mining, staking, liquidity provision, liquidations, funding rates, or any other way in which a user may produce earnings using the protocol. This information should include an explanation specifying the common circumstances that could result in a user not receiving those earnings.

**d. Fees**

Disclosures should include an explanation of the potential fees a user may incur, including through mining, staking, borrowing, liquidity provision, effecting liquidations, being liquidated, or any other way in which taking an action on the protocol may result in a user receiving less value than a typical user would otherwise expect to receive should be disclosed, including the common circumstances that could result in such user incurring those fees.

**e. Equity Financings, Prior Token Sales, and Related Commitments**

Prior token allocations, sales, or commitments—and any limitations or restrictions (e.g. vesting schedules) associated with them—should be disclosed and, to the extent possible, independently verifiable.

Any restrictions or commitments (e.g. development limitations, prior equity holder approval right before launch, protections tied to protocol activity, etc.) associated with equity financings that affect the development or operation of a protocol should be disclosed and, to the extent possible, independently verifiable.

**f. Governance Rights and Process**

Information related to the following should be disclosed:

*i. whether and the extent to which a DeFi protocol is governable;*

*ii. what powers governance can exercise over the protocol;*

*iii. how the terms and the scope of governance powers can be modified;*

iv. *how any single person, entity, or coordinated group of persons or entities can unilaterally control may modify the protocol, including the effect of those changes on users, any required time delays when making those changes, and the manner in which those changes may be made;*

v. *how governance rights are distributed and exercised;*

vi. *how the governance process works;*

vii. *how a person can participate in governance;*

viii. *how a person can exit a protocol and governance; and*

ix. *the identity of any person or entity, or group of persons or entities under common control, holding more than 1 percent of the voting power of the governance mechanism, a description of any limitations or restrictions on the transferability of tokens held by such persons to participate in governance, and a description of any rights held by such persons to obtain tokens in the future in a manner that is distinct from how any third party could obtain tokens.*

**g. Negative Events**

Any event or situation that materially affects in any way the normal and expected functionality of a DeFi protocol should be promptly disclosed and information to independently verify such an event or situation should be made available. Developers of DeFi protocols should develop and test predefined procedures for responding to such an event or situation.

**h. Deployment of New Code**

Before any changes to a DeFi protocol's deployed code are implemented, the new code should follow the same procedures set forth in Section 3 above.

**i. Third-Party Networks, Protocols, and Oracles**

A list of all third-party blockchain networks, protocols, or oracles on which the DeFi protocol relies to function as disclosed to users and a link, if available, to information regarding that third-party blockchain network, protocol, or oracle.

**j. Risks**

Inform users of the DeFi protocol that a high degree of risk exists when using the protocol, which may result in a loss of funds. Conduct periodic reviews of risk, including reviews of underlying risk assumptions.

### k. Communications

The information hub should include information about any official communication channels, including for discussion of technical matters related to the protocol.

## 5. Market Integrity

### a. Manipulation and Fraud Prevention

DeFi market participants should not:

*i. engage, or attempt to engage, in any manipulative conduct or scheme to defraud;*

*ii. make, or attempt to make, any untrue or misleading statement with respect to material information or omit to state any material information in order to make information made available not untrue or misleading;*

*iii. engage, or attempt to engage, in any act, practice, or course of business to, or to attempt to, defraud or deceive any person; or*

*iv. deliver, cause to be delivered, or attempt to deliver or cause to be delivered false, misleading or inaccurate information that affect or tend to affect the price of any asset, knowing or acting in reckless disregard of the fact that such information is false, misleading or inaccurate.*

### b. "White Hat" Incentivization

Developers of DeFi protocols should incentivize benign testing and auditing of the code they write, such as by implementing a "bug bounty" program.