September 2023

“Decentralised” or “disintermediated” finance (DeFi): what regulatory response?

Summary of responses to the public consultation

Authors: Olivier Fliche, Julien Uri, Mathieu Vileyn
Fintech-Innovation Hub

ACPR
BANQUE DE FRANCE

Executive summary

The ACPR's discussion paper submitted for consultation provided a description of the specific risks associated with decentralised or disintermediated finance (DeFi), distinguishing schematically between the **three main strata** that make it up: **blockchain infrastructure, the application layer of "services"**, and the **devices by which users can access** these services. It also noted the **high level of concentration** that characterizes the DeFi ecosystem, as well as the **sometimes highly centralised governance** of its applications.

Since some of DeFi risks are closely linked to the characteristics of the technologies that make it attractive, the approach of the discussion paper was to propose regulatory options tailored to the specific characteristics of DeFi, without merely replicating the arrangements currently governing traditional finance.

The interest generated by the discussion paper and the responses received during the consultation broadly validate these choices. The consultation also helped to clarify or deepen some of the issues under consideration.

Thus, as regards the **concentration phenomena** described in the discussion paper, the consultation provides two new points for reflection. First, **the concentration of ecosystem players does not necessarily reflect the immaturity of the DeFi ecosystem**; on the contrary, it could well be due - as more generally in the digital world - to the existence of **increasing returns**, leading to situations of **monopoly** or **oligopoly**. This situation, already apparent at the level of the blockchain infrastructures themselves, could also be observed at the level of certain services provided. To be relevant, any future regulation of DeFi will naturally have to consider this trend, if it is confirmed. Second, some respondents highlighted **another aspect of DeFi concentration**: the **physical infrastructure hosting the blockchain nodes** and the central role played by cloud providers in this regard. This point, which is in line with the operational resilience concerns recently addressed by the DORA Regulation for traditional finance, does indeed merit consideration.

The main areas for regulation mentioned in the discussion paper call for the following comments.

The overwhelming majority of respondents supported the idea that **public blockchains** can host DeFi activities, and there are strong reservations about the possibility of a transition to private blockchains (usually in the name of the ability to innovate). At the same time, many participants recognized the need to strengthen the resilience of public blockchains and agree on the need to audit their functioning on a regular basis, in line with the discussion paper's idea of **setting security standards**. However, there were major differences of opinion on how this should be achieved. In this regard, it is important to include in the regulatory debate the "**layer 2" solutions** used for the large-scale management of blockchain transactions. The consultation thus highlighted a wide variety of views on the risks linked to these solutions, to be compared with the wide variety of technical solutions themselves, which is a sign of a **technological landscape that is still immature and rapidly changing**.

The idea that public authorities manage **archive nodes** of certain public blockchains, in particular to help restore the registry after an attack, was rather consensual among the participants.

The principle of **certifying smart contracts** received a broad support. The scope of such certification and its practical modalities are more controversial; several respondents nevertheless put forward interesting avenues in this area (proportionality, smart contracts 'user manual', escalation of incidents to a central authority, etc.). Mention should also be made here of the concept – yet to be explored - **of "governance minimization"**, developed by some respondents as a means of limiting the risks that too much concentration of voting rights could pose to the “decentralised” protocols and services they provide.

Finally, **there was broad agreement on the idea of a regulatory framework for intermediaries or user interfaces**: however, contrary to some comments received, this approach does not seem to exempt the authorities from thinking about a framework for the other two layers of DeFi. A point of attention lies in the way decentralised (and rapidly developing) interfaces will have to be regulated in practice, with numerous feedback from the consultation indicating that they cannot be regulated in the “same way” as centralised intermediaries.

Follow-up work planned by the ACPR

As announced when the discussion paper was published, **the lessons learned** from this consultation **will feed into the ACPR**'s **contributions to the discussions under way at European level on the follow-up to the MiCA Regulation**. In particular, it seems possible and advisable to lay down measures relating to the reliability of the blockchain infrastructures on which DeFi – or other forms of tokenized finance – may develop, to draw up rules – e.g. certification – suited to the nature and operation of smart contracts, and to define governance and conduct of business rules that would ensure adequate protection of DeFi customers.

In addition, the consultation showed the value of **further examining** the many issues raised by **the certification of smart contracts**: this examination and additional analyses could be carried out in the coming months, drawing on the expertise of the sector and relevant authorities.

Finally, beyond the necessary technological watch on still evolving topics, **certain topics**, such as the security of certain infrastructure bricks (layer 2), or ways of limiting concentration phenomena and the associated risks, could probably be explored more effectively **by the research community**. Strengthening the links that already exist between the ACPR and research would be one possible way to shed light on these issues, also with a view to promoting appropriate regulation at European level. Studies of a more legal nature, notably on the representation of *decentralised autonomous organizations* (DAOs), could usefully complement this work.

Table of contents

Background

“Decentralised” or “disintermediated” finance (DeFi) refers to a set of crypto-asset services that are comparable to financial services and executed without the intervention of an intermediary.

Despite its modest size and the currently limited number of its use cases, DeFi is attracting interest because of the **technological innovations** on which it is based and because of its fundamental promise: to replace trust between players with **computer code as a common rule**. The interest in **DeFi also stems from the fact that it could foreshadow future transformations in finance.** The interest of the financial supervisor in DeFi obviously also stems from the **risks** it poses, which raise the question of a **regulatory framework**.

Following a series of interviews with ecosystem participants, the ACPR published a **discussion paper** on the framework for DeFi in April 2023. This document did not express a definitive position of the ACPR, but rather aimed to develop an initial analysis of regulatory avenues, with a view to discussing them with stakeholders in a public consultation.

This **public consultation**, which was held in April-May 2023, allowed to verify the ACPR's understanding of the main DeFi mechanisms and to seek the views of participants on the regulatory avenues outlined in the discussion paper.

As a reminder, these regulatory avenues covered the **three main layers of the DeFi system,** and were essentially aimed at:

- Ensure the resilience of blockchain infrastructure that support DeFi, for example by imposing security standards and limiting the risks of concentrating transaction validation capabilities in the hands of a few players;
- Strengthen the security of smart contracts, in particular through a certification mechanism covering security of the IT code, the nature of the service provided and governance;
- Better regulate the provision of services and users’ access to these services, for example by introducing a framework for enhanced control of intermediaries providing users with access to DeFi services in practice.

Through all of this work, the ACPR intends to **contribute to ongoing discussions, particularly at European level**, in the wake of the MiCA regulation, which provides for a report to be drawn up, within 18 months of its entry into force, on whether DeFi should be subject to European regulations.

Participation in the consultation

Open for two months (April-May 2023), the public consultation on the ACPR’s discussion paper **received a wide response, in France and Europe but also in the rest of the world,** resulting in **39 responses**. A **wide range of players** took part: traditional financial institutions, consulting and audit firms, but also representatives of the crypto and DeFi ecosystems, including some world leaders in the sector (see table).

Looking beyond the sheer number of replies received, the ACPR would like to praise the **high quality of the replies received**, which make a valuable contribution to the many debates on DeFi.

Table: Respondents to the public consultation

Category	Total	FR	EU	Rest of the world
Individuals	6	5		1
Banks, payment institutions	2	1		1
Consulting, audit	3	2		1
TradFi - professional associations	5	3	1	1
DeFi / crypto / DLT - Professional associations	5	1	3	1
CASP	6	3	1	2
DeFi / crypto / DLT ecosystem	11	2		9
Venture capital	1			1
Total	**39**	**17**	**5**	**17**

Source: ACPR

Responses to the consultation

Generally speaking, the discussion paper was **well received**. Even if the analyses and proposals made were not all unanimously shared, many respondents praised the initiative taken by the ACPR and the precision of its work.

At the technical level, the consultation provided useful additions to the elements set out in the discussion paper (notably on certain technical aspects of blockchain attacks): these are set out in this summary. However, the responses received **do not fundamentally call into question the ACPR's understanding of the subject, which has therefore been strengthened overall**.

Several of the **avenues for regulation** outlined in the discussion paper were also the subject of **considerable interest by respondents**. While a few of them reject the very idea of regulating DeFi activities, most - including players in the digital asset sector - recognize the need for mechanisms to control or limit a number of risks.

This document presents the responses received during the public consultation. It has sometimes been deemed useful to include a brief discussion of these responses. **These statements represent only the views of the authors and do not express an official position of the ACPR**.

This summary follows the structure of the initial discussion paper, which covered (i) the description of DeFi (definition, use case, structure), (ii) risks (relating to governance, infrastructure, application layer and uses) and (iii) regulatory options.

I. Description and operation of DeFi

1-1. Definition and scope of DeFi

Summary of responses

Several respondents praised the ACPR's definition of decentralised or disintermediated finance ("DeFi"), which emphasises its imprecise nature and characterises this activity using a range of criteria. Other respondents criticised the choice made and felt that any plan to regulate DeFi would require a precise definition.

Indeed, rather than participating in the numerous debates aimed at defining the 'real' DeFi, the discussion paper presented an **ecosystem in its actual functioning**, i.e. also in its interactions with **centralised elements** (stablecoins, conversion between official currency and crypto-assets etc.). Some participants in the consultation also stressed that, beyond the various building blocks that make up the ecosystem, **certain elements of centralisation remain at the heart of how DeFi protocols work today**: oracles, "multi-sig" devices, updating mechanisms etc. This shows that the boundary between a theoretically centralised finance ("CeFi") and a theoretically decentralised finance ("DeFi") is difficult to draw.

As for **the diagram presenting the DeFi application architecture** (end of Part I of the discussion paper), some respondents observed that it did not show all the IT layers that make up the blockchain.

Discussion

Despite the practical difficulty of doing so, is it true that it will become necessary to define the contours of "DeFi"? Actually, it depends on how one views the regulation of digital assets. **Defining precisely the contours of "DeFi" is only necessary if we want to develop regulations specific to this way of providing services on digital assets**. By contrast, one can imagine **homogeneous** regulation - which does not necessarily mean uniform regulation - covering the entire range of digital asset services, whatever their mode of delivery. Such regulation could take the form of a "MiCA 2" regulation, for example. From this perspective, the need for a "DeFi" object is less obvious.

1-2. The question of concentration in the DeFi universe

Summary of responses

The discussion paper noted the paradoxical concentration of the DeFi ecosystem at several levels (section 1-5). Two distinct phenomena were highlighted: the **economic concentration** on the DeFi market on the one hand, and **the concentration of blockchain and application governance** on the other (on this second aspect, see Section 2 of this summary).

On **economic concentration**, one respondent first remarked that, in the case of lending protocols, the market shares of decentralised applications could be put into perspective, bearing in mind that they also faced competition from centralised applications. Nevertheless, the observation made in the discussion paper was widely acknowledged by respondents to the consultation**:** a few blockchains and a relatively small number of applications concentrate most of the assets in terms of value. Some respondents also noted that **a third dimension should be added** to this to this observation of a concentrated ecosystem: **the physical infrastructure hosting the blockchain nodes**. Some surveys indicate that cloud providers host a majority of Ethereum nodes, with a significant proportion hosted by Amazon Web Services (AWS). This point is all the more interesting as it constitutes a **risk factor, should one of these service providers fail**. In addition, with the rise of blockchains, the "full nodes"[1] of the network may need to store more information in the future; this risk is therefore likely to persist, if not increase.

Discussion

First, it is worth pointing out that concentration is not necessarily a problem in itself, particularly in the area of infrastructure, where **network effects**[2] are important. In addition, while some respondents tried to explain the concentration in DeFi by the relative youth of the ecosystem, the opposite hypothesis can be formulated: that **the DeFi universe, like perhaps more generally that of digital activities, is a space of increasing returns**. According to economic theory, production with increasing returns leads to a situation of **natural monopoly**, or at least **oligopoly**.

Thus, a decentralised lending protocol cannot function without a critical mass of liquidity, provided by users. In return, abundant liquidity and a large number of users allow the protocol to achieve **economies of scale** and, in particular, to charge less for certain services, which makes the service **more competitive** and attracts new users, hence even more liquidity. Moreover, all else being equal, more users and more liquidity generate more **trust**, which again contributes to the attractiveness of the service. Unlike in the production of most real-world goods and services, **modest investments** generally prevent the increase in the number of users from leading to service **congestion** (this point may be different for blockchains, see the discussion on scaling below, but it then affects all the protocols located on the same blockchain). On the other hand, more users, and hence more assets traded, can whet the appetites of malicious actors, and consequently lead to an increase in computer attacks against the protocol, and therefore to a drop in user confidence if the service is not robust enough.

In the end, the economic concentration observed in the DeFi universe is perhaps neither **a surprise nor a sign of the ecosystem's immaturity**. Beyond the classic competition issues, this situation makes the **issue of the resilience of blockchain infrastructure particularly critical** in any event, whether in terms of the risk of failure or the risk of a takeover by attackers (see below).

[1] Typically, full nodes each store a full copy of blockchain history (unlike light nodes, which retain only a small part of the history). However, there are exceptions: for example, on the Ethereum blockchain, for reasons of size, a full node only stores the last 128 blocks (archive nodes storing older data). In all cases, a large amount of memory is required for the operation of a full node.

[2] The phenomenon whereby the use of a good or service by new users increases its value for existing users. This positive externality applies in particular to communication networks.

II. The risks associated with DeFi

2-1. Risks related to decentralised governance

2-1-1. The persistence of centralised elements in decentralised governance

Summary of responses

Whether through the concentration of the majority of governance tokens in the hands of a few players, the retention of administrator keys, or the existence of other privileges that relativise voting mechanisms, the discussion paper showed that the **governance** of many protocols appeared to be **falsely decentralised** ("decentralised in name only" or DINO, see section 2-1 of the discussion paper).

In this regard, some respondents to the consultation put forward an interesting idea: it is perhaps less the *de facto* centralisation of governance that is problematic than its **possible concealment** from the users of a blockchain or DeFi application. For example, the possession of administrator keys by a few individuals with privileges would appear to be less of a problem if it were known to everyone, and if the conditions for using these keys were set in advance (computer attack, need to update the protocol, etc.).

Beyond transparency efforts, the fact that elements of centralisation remain at the heart of the operation of DeFi protocols (see Section 1-1 of this summary) is a risk that led some respondents to advocate for "**governance minimisation**". This principle consists in limiting to the maximum the scope of actions that governance bodies can take to amend the protocol[3]. With governance reduced to its strict minimum, a protocol is **virtually immutable**: governance bodies cannot change how it works in depth, but can only vary some of the parameters, such as the level of charges levied for each use of the service[4].

Discussion

First, **transparency** about governance mechanisms can indeed be accepted as an important principle. In fact, one of the ways in which DeFi protocols promote transparency is through the frequent, or even real time, publication of data enabling the public to find out who holds the governance tokens.

While welcome, efforts to improve transparency are not a definitive answer to all risks arising from falsely decentralised governance. Firstly, **because transparency is generally not complete on blockchains**: this is the problem of pseudonymity (on this subject, see also point 2-4 of this summary, dealing with the fight against money laundering and the financing of terrorism). For example, the publication of data on the holders of blockchain or protocol governance tokens does not necessarily allow for a picture of the actual concentration of validation or decision-making capabilities, since the holders are only identified by their address on the blockchain; but the same individual may have several addresses, while entities linked to each other in the real world (a parent company and a subsidiary, for example) may have apparently unrelated blockchain addresses.

Secondly, it seems clear that the persistence of **elements of centralisation** in theoretically decentralised protocols poses a constant **risk of arbitrariness in governance**, even when these

[3] Uniswap or Liquity are often cited examples of the implementation of this principle.

[4] Moreover, that variation may itself be constrained within a "hard" fixed range, in order to prohibit in advance any attempt to set fees at a confiscatory level.

elements are circumscribed or specified in advance. For example, who will judge the reality of the danger hanging over a protocol, a danger that could be invoked by a group of individuals to use their administrator keys? Even if the user community disavows the intervention afterwards, it will probably be difficult to reverse decisions that have already generated economic events. **Risks stemming from the persistence of elements of centralisation can therefore be mitigated, but not eliminated**.

Against these risks, the principle of **"governance minimisation"** is an interesting idea: it is of particular relevance in terms of security and could therefore be **included among the criteria used to certify smart contracts** (see below). However, it should be noted that other challenges might arise from the limited power left to the governance bodies: for example, how can security updates be made to a quasi-immutable protocol, or how to react in the event of a cyber-attack?

2-1-2. Flash loan attacks on protocol governance

Summary of responses

The discussion paper mentioned (in section 2-1) the risk **of attacks on governance through** "flash loans", aimed at borrowing large amounts of governance tokens in order to vote on a decision that is harmful to other users, before immediately repaying the sum, once the misdeed has been completed. Some respondents to the consultation indicated that **such attacks had become rare in practice**, due to the **protective mechanisms** deployed in many protocols. For example, it is typically required that votes are first sent within a first transaction block, before the vote itself takes place in a separate transaction block (whereas the flash loan mechanism requires borrowing and repayment to take place within the same block). Respondents also indicated that the most common governance systems allow for a **significant delay** between the vote on a proposal and its implementation (three days for the Uniswap protocol, for example). As the submission of a proposal and its voting are transparent processes, stakeholders can know who voted for it. The implementation deadline thus gives users time to leave a blockchain or application if a proposal they consider malicious has been approved.

2-2. Infrastructure risks: debates on "layer 2" solutions

Summary of responses

The public consultation confirmed that, apart from governance issues (see above), the risks associated with blockchain infrastructure essentially relate to **scalability** issues. On this subject, respondents confirmed that **"layer 2" solutions**[5] are currently the main route used by the ecosystem to overcome network congestion. Respondents also indicated that the ACPR had clearly identified the main risks of the various layer 2 solutions: security of bridges connecting blockchains, when layer 2 solutions are other blockchains (e.g. sidechains); importance of the delay (7 days in general) to make transactions final in the case of optimistic rollups; critical role for centralised operators, which could lead to fraudulent behaviour, in calculating zero-knowledge proof (ZK), for the case of ZK-rollups.

The responses received during the consultation also highlighted the **great diversity** of layer 2 solutions currently implemented in a highly evolving technological environment. This diversity is also a reflection of the **great technological heterogeneity** of layer 1 blockchains, whose characteristics are more or less

[5] A type solution for scaling blockchains, the principle of which is to process part of the transactions off-chain, recording only the minimum information in the main chain (layer 1).

adapted to each layer 2 solution. In addition, certain technical questions widely divided respondents to the consultation, such as whether ZK-rollups reduce the transparency of information for users who are not party to transactions, or whether transactions taking place on rollups[6] should be considered as "on-chain" or "off-chain"[7]. Even more crucially, the responses to the consultation also revealed a **wide variety of views on the risks** induced by layer 2 solutions, as well as on the difficulties related to the interoperability of blockchains between them.

Discussion

The dispersion of the technical solutions adopted and the diversity of assessment by players as to the risks presented by these solutions **raise the question of the maturity of the ecosystem as regards the question of scalability**. It is therefore important to continue exploring this issue in future studies.

2-3. Computer attacks on blockchains and protocols

Summary of responses

The public consultation provided useful technical advice on the risks of cyberattacks on blockchains and DeFi protocols. For example, some respondents to the consultation noted that the discussion paper did not mention as such "**sandwich attacks"** on the blockchain "mempool", despite the significant risks involved.

The mempool is the temporary storage location where transactions are put on hold on the blockchain, until a block of transactions is created that will incorporate them. The mempool is usually public: all blockchain users can see what transactions are pending, and what fees users have agreed to pay for their validation. As a result, a malicious user - typically a robot specialized in this task - can look for high-value transactions in the queue. Consider the example of a user X who sent a transaction to acquire a certain quantity of a crypto-asset A. The malicious bot that spotted this transaction will then seek to interpose a second purchase order for the same asset A *before* the transaction sent by X ("front run"). It typically does this by paying a higher transaction fee than the initial transaction, as most blockchains validate transactions in descending order of fees ("gas" on Ethereum). The purchase of crypto-asset A by the malicious robot increases its price, and therefore leads X, when her transaction is validated, to buy asset A at a price higher than the price initially set, which represents a loss for her. Finally, the final phase of the attack consists in the robot selling its stock of asset A, but this time at a price higher than the purchase price (since the price of A was pushed up by the previous two transactions). Again, by setting the transaction fee appropriately, the robot can get this transaction validated just after the transaction of user X ("back run"): the initial transaction is eventually framed by two new malicious transactions, one positioned just before and the other just after (hence the name "sandwich" attack). The robot thus makes a profit at the expense of user X, thanks to the ability to observe the mempool[8].

[6] Rollups are the most widespread layer 2 solution today, consisting of "rolling up" a group of transactions in a single operation (hence the name), and compressing the information by sending only the data strictly necessary for the definitive recording of these transactions on the blockchain.

[7] This debate could raise questions in terms of regulatory scope, as crypto-assets are defined in particular as assets whose value is transferred using blockchain technology.

[8] This type of attack also relies on the tolerance mechanisms for the variation in the price of the crypto-assets to be exchanged between the sending of the transaction and its validation ("slippage"): users set in advance the

Several respondents showed that the risk of a "sandwich" attack **fundamentally raises the question of the type of mempool to use** on layer 1 blockchains, but also in layer 2 solutions (where transactions are also validated). Today, most rollups use a "single sequencer" model, meaning that a single entity receives pending transactions, orders them, and makes blocks out of them. However, while the public mempool entails the risk of "sandwich" attacks (which are widespread), the private or permissioned mempool model is not without its problems either, since third parties cannot see pending transactions or check compliance with sequencing rules. This allows the sequencer to order transactions according to an arbitrary process, including inserting its own transactions in order to make a profit.

2-4. AML/CFT risks: pseudonymity

Summary of responses

The discussion paper referred to the debates surrounding the **pseudonymity** in use on most blockchains. Admittedly, pseudonymity is not the same as anonymity: it allows a certain traceability of transactions, which leads to forms of self-regulation on blockchains. However, **the absence of user identification[9] is likely to weaken the fight against money laundering and terrorist financing (AML/CFT)**. Conversely, the inclusion in a public blockchain of the identity of participants in each transaction would risk breaching **privacy protection** requirements (section 2-4-4 of the discussion paper).

Several respondents to the consultation felt that recent technological innovations could provide a solution to this difficult problem. **Digital identity solutions** have been developed in recent years. Based on advances in cryptographic proof techniques (in particular zero-knowledge proof), they theoretically make it possible to provide an identification that is verifiable, scalable, usable by everyone, interoperable between different systems, and guaranteeing individuals that only the minimum amount of personal information needed is shared. These digital identity solutions could facilitate the implementation of "Know your customer" (KYC) obligations directly on the blockchain[10]. They would thus make it possible to reconcile **the identification of individuals involved in blockchain transactions, for AML/CFT purposes, with privacy protection requirements**.

Discussion

The use of digital identity solutions is an interesting technological avenue. However, in order to effectively combat money laundering and terrorist financing, this type of mechanism requires that the data used to identify the protagonists is first **collected with certainty**, then **duly verified**, and finally that it is **accessible to all entities needing to identify the beneficial owners of transactions**. Indeed, the implementation of digital identity solutions with unreliable content could paradoxically facilitate the execution of illicit transactions.

maximum slippage they are willing to accept. The risk of "sandwich" attacks can thus be mitigated by setting a lower slippage, at the risk, however, that some of the transactions sent by a user for validation are ultimately cancelled in the event of excessive price slippage, which can pose other difficulties.

[9] This is all the more true given that most DeFi applications operate without any access control: user participation requires only a connection to a wallet, and some of these wallets can be opened without identity checks or verifying the origin of deposited funds.

[10] For example, one respondent mentioned the possibility of issuing a personal (non-transferable) token, which could serve as the user's "KYC certificate", after enrolling a user and carrying out the verification procedures.

III. Avenues for a regulatory framework

3-1. Ensuring minimum resilience of the blockchain infrastructure

Summary of responses

The idea of using **private blockchains** (scenario B in section 3-1 of the discussion paper) was widely criticised by respondents to the consultation. Private blockchains are indeed considered less secure than public blockchains in that, like all centralised elements, they present a risk of single point of failure. Most importantly, respondents felt that they do not generate the same network effects as public blockchains, and are therefore less efficient.

A large majority of consultation respondents therefore advocated the use of **public blockchains** (scenario A in the discussion paper), while generally acknowledging the need to **strengthen their resilience**. **However,** some respondents were **opposed to the very principle of regulating the infrastructure**, generally using the example of the internet[11]. Another frequently cited argument against the principle of regulation is that the current level of DeFi knowledge is not sufficient to regulate properly blockchains, or even the entire ecosystem. One respondent suggested the creation of a DeFi observatory to gather knowledge on blockchains and protocols and thus help to stimulate discussions on the forms of supervision to be implemented.

In terms of **ways** to strengthen resilience, many respondents agreed on the need **to audit regularly the functioning of blockchains**. From this point of view, standardisation of practices was widely mentioned (on this issue, see section 3-2-1 of this summary). This is in line with the idea of setting **security standards** for blockchains, which has been widely approved. However, respondents differed on how to develop these standards. The idea most frequently mentioned was that market participants and public authorities should develop them jointly (a suggestion also made in the discussion paper).

The introduction of minimum standards for the security of blockchains could however constitute an **obstacle to the entry of new players** into this market, as they often have limited resources to apply the regulations. Some respondents therefore suggested that security standards should be voluntary rather than mandatory. The underlying idea is an incentive mechanism: the biggest players would wish to comply with the security standards in order to increase the confidence of their customers and attract new ones; new entrants would have time to reach a certain size before deciding to comply with the standards. To provide additional incentive, some respondents proposed that financial supervisors should be able to decide whether the institutions they supervise are entitled to interact with a particular blockchain, depending on their assessment of the latter's level of security.

The discussion paper also indicated that public supervisors could monitor the **concentration of validation capabilities** on public blockchains in real time, and communicate when certain thresholds are exceeded. These proposals have been widely debated among respondents to the consultation. Some pointed to initiatives by certain blockchains to limit the risk of concertation between validators (or even of takeover), for example via **random selection mechanisms** for validators of a new block. Others, in the other hand, were in favour of the principle of oversight, and suggested using the regulations **applicable to the capital of listed companies** - for example as regards the crossing of certain thresholds – as a model for regulating the concentration of validation capacities.

[11] Website-based regulation, as the communication infrastructure itself is largely unregulated.

Finally, there was broad agreement among participants on the idea that public authorities should be able to operate **archive nodes** of certain public blockchains, in order to help restore the ledger after an attack, or possibly transfer information to another blockchain in the event of definitive corruption.

Discussion

The two main arguments against the use of **private blockchains** seem likely to be put into perspective. On **security** matters, first, the failure of a centralised brick that has become systemic - and therefore subject to regular computer attacks - represents a significant risk. It should be noted, however, that many public blockchains have also experienced failures, particularly because of attacks on them. Most importantly, this risk must be weighed against all the risks associated with the functioning of public blockchains (see section 2-2 of the discussion paper on this point). Second, the **network effects** argument probably makes sense when it comes to comparing public blockchains and private blockchains in their current forms. However, if a pan-European (or even global) private blockchain, housing the bulk of digital asset activities, were ever to be created - for example for regulatory reasons - its network effects would certainly be considerable.

As regards **public blockchains**, and the very principle of their regulation, the comparison made by some respondents with the way the Internet works has one major limitation: **unlike blockchains, the Internet network does not of itself make it possible to exchange, store and directly prove ownership of financial assets**. The risks for users - in particular individuals - and ultimately for financial stability, are therefore not comparable.

On the resilience of public blockchains, it is clear that the potential **competition** problem that would result from the introduction of security standards calls for **proportionality measures** to be considered in the implementation of this type of obligation. In any case, the various proposals made by the respondents call for clarification of one point: **it would be difficult for the financial supervisor to regulate the operation of blockchains itself**. **Its action would therefore necessarily be limited to the institutions it supervises**, even if it is not excluded that other public players could contribute to the supervision - or even direct operation - of blockchains.

With regard to the supervision of validation capacities by public authorities, it should be stressed in any case that **effective supervision requires that two conditions are met**: on the one hand, that addresses on the blockchain can be effectively linked to the identity of users (at least for the supervisory authority), in order to identify the multiple addresses of the same person; on the other hand, in the real world, that supervisory authorities have enough information to link together individuals or companies (parent and subsidiary companies, for example) that may collude on the blockchain.

It seems clear, in any case, that for the public authorities to be able to exercise **effective supervision** of activities linked to digital assets, they need to have a good level of information at their disposal. From this perspective, the creation of **databases** that are fed regularly - or even in real time - and make it possible to monitor activity on blockchains, **is an essential step** . For the same purpose, the **financial supervisor could operate a** "**supervisory node"** with specific privileges.

3-2. Propose a framework adapted to the algorithmic nature of the services

3-2-1. Certification of smart contracts

Summary of responses

The vast majority of respondents to the consultation recognised that smart contracts too often present dangers for users, particularly unsophisticated individuals. For this reason, they generally **supported the principle of certification**.

Respondents also stressed the existence of **market initiatives** to ensure or strengthen the security of smart contracts. First, the practice of "bug bounties"[12] is often deemed effective. Tools for automatically exploring the smart contracts code are also available on the market. Regarding audit techniques, respondents indicated that **formal methods** are not widely used at present, due to their high cost, despite their significant potential. Finally, a number of respondents pointed to the promises of the **development of artificial intelligence (AI)** in IT auditing.

However, the majority of respondents agreed that **existing audit mechanisms are often not sufficient**, for two main reasons. On the one hand, the audit of smart contracts generally focuses solely on IT security aspects, which are certainly essential, but does little to address economic functionalities, governance or regulatory compliance. On the other hand, audit techniques that focus on examining computer code have difficulty in taking into account the systemic aspects of IT security, especially vulnerabilities linked to the use of another smart contract's functionalities.

Respondents also emphasised the **wide variety of practices for auditing smart contracts**, and **called for some standardisation in this area**. This idea is very close to one of the main proposals in the discussion paper: a smart contract certification mechanism.

While the principle of certification was widely accepted, its **modalities** were the subject of debate among respondents and, in the first place, on **the scope of smart contracts to be certified**. For example, as a proportionality measure, one respondent suggested that **certification should only be required for the largest projects,** and that only a lighter security audit should be required below a certain size. To this end, it proposed establishing a typology of smart contracts that are risky or complex to certify (experimental, interactive, complex, evolving, etc.) Another respondent noted that the exclusive use of audited components could require the audit of all blockchain software or tokens compatible with the Ethereum virtual machine, which seemed out of reach.

As regards interaction with **uncertified smart contracts**, many respondents argued that this should only be discouraged[13]. One respondent suggested that supervised financial institutions should not be able to interact with such a smart contract, but that other entities should be able to do so. The underlying idea is that the resulting reduced liquidity would provide an incentive for certification.

Other **practical difficulties** are also mentioned. Examples include the difficulty of defining a significant change to the code in practice, or the risk that a renewed certification requirement after such a change could discourage developers from updating smart contracts. Another respondent observed that a

[12] Also called "bounty reward". Mechanism aimed at having a computer programme tested by a community of developers and informed users, by offering rewards to those who manage to reveal design flaws or vulnerabilities.

[13] It should be pointed out that the proposal concerns only interactions with uncertified smart contracts, not the production of these objects or their existence.

smart contract could be used in a way that the creators had not anticipated, unless restrictions had been included in the computer code.

Lastly, some responses to the consultation contained suggestions for implementing or monitoring the certification of smart contracts. Mention should be made of the idea of requiring a **renewal of certification when a new general vulnerability** has been detected[14] and of **referring the vulnerabilities detected during audits and certifications to a central authority**, which would also have the role of certifying certifiers or auditors, recognising their experience in the field.

Discussion

As regards interactions with uncertified smart contracts, disincentives rather than prohibition mechanisms could actually go in the direction of greater proportionality. However, they would raise a problem in principle: if the security, governance or very principle of a smart contract were not sufficiently compliant with commonly accepted standards - preventing its certification - it would seem strange to prohibit interactions only from certain categories of players (especially if the participants thus protected are professionals, leaving private individuals unprotected). On the contrary, the dangers of such a smart contract would justify a **ban on interactions for all users**.

The fact that a smart contract may be used in a way not intended by its creators deserves consideration. This could lead, in the event of regulation, to asking smart contracts developers to provide **a user manual for their tool, which would determine in particular the scope of uses considered legitimate**. The possible adverse effects of such a measure on innovation would naturally have to be carefully studied if such a regulatory approach were adopted.

More generally, the interest aroused by the certification of smart contracts, the diversity of situations to be considered and the wealth of comments received show that the topic is far from being exhausted and **deserves further analysis, in partnership with professionals and experts in the sector**.

3-2-2. The case of oracles

Summary of responses

The respondents widely acknowledged the critical nature of data provision in the blockchain, and thus the **crucial role played by oracles** in the smooth functioning of the system. From this perspective, one respondent considered that high-quality data was an important element in mitigating financial risks, which in his view justified **reserving its provision to centralised entities specialising in the data business**. Other respondents argued for **more decentralised models**, which they felt were the only way of ensuring that the data provided was free from conflicts of interest.

Some participants in the consultation also questioned the classification of oracles implicitly established in the discussion paper. In particular, they believed that the **decentralised oracle** model described[15] therein should be classified as a centralised oracle. These models, such as Chainlink's, are only decentralised to the extent that several entities (often under pseudonyms) participate in the submission of values. According to those respondents, true decentralised oracles would be those

[14] This idea is close to - but distinct from - the idea developed in the discussion paper of certification for a limited period (point a in section 3-2-2).

[15] Typically, several parties or nodes submit an updated value for the bitcoin price, and the median of the submitted values is published on the blockchain and then used by smart contracts.

based entirely on publicly available data, and therefore independently verifiable, such as Uniswap's Time Weighted Average Price (TWAP) oracle.

In any case, respondents acknowledged that **all oracles**, regardless of their degree of (de)centralisation, **could be manipulated** (at a variable cost depending on the tool's specifications). Faced with this problem, some respondents mentioned attempts, on some lending protocols, to operate **without recourse to oracles**, in order to limit risks. For the time being, however, this type of model appears to be rather limited. Other respondents raised the idea of creating **public service oracles**, which is an interesting avenue. As DeFi currently stands, however, a majority of respondents felt that the principle of **certifying decentralised oracles**, on the one hand, and **monitoring the operation of all oracles**, on the other, would be appropriate[16].

3-2-3. The case of stablecoins

Summary of responses

Among other things, the discussion paper proposed **extending the MiCA framework applicable to electronic money tokens (EMT) to all crypto-assets whose purpose is to replicate the value of an official currency**. Thus, a token referring to an official currency, even issued by a decentralised protocol, would have to apply MiCA requirements on EMT, and in particular: the right to reimbursement at face value, and the management of a reserve consisting of liquid assets denominated in the same currency. This proposal has received **many reactions**.

It was welcomed by a number of respondents, who stressed that this approach would **limit the risks** identified in the discussion paper (potential to destabilise many DeFi applications and potential vector for transmission of shocks from the DeFi ecosystem to traditional finance) and would **provide legal clarity**. One respondent pointed out that the decentralised protocol behind the issuance of a stablecoin could include in its code the information allowing its identification as an EMT.

Other respondents, on the contrary, felt that it would be inappropriate to extend the EMT framework to all stablecoins, as those issued by decentralised applications operate in a **fundamentally different way**: in the absence of a centralised issuer, the reserve is generally based on a collateral deposit mechanism, possibly accompanied by algorithmic adjustment mechanisms. However, some respondents felt that decentralised issuance of stablecoin could, at the very least, require a **duty of advice** towards users, allowing the latter to make informed choices between EMT and other crypto-assets that refer to an official currency.

Some respondents made another proposal: to subject stablecoins issued by decentralised protocols to the regime for "**other crypto-assets"** in Title II of MiCA. This would result in particular in an obligation to make a white paper available to users; this obligation would fall on the issuer or, failing that, on the intermediary allowing the acquisition of such stablecoin.

Discussion

These alternative proposals **do not address the promise of stability and security made to users** by issuers of a stablecoin, even if it is decentralised. Furthermore, they could make it difficult for users to **distinguish true MiCA-regulated e-money tokens from other, less secure crypto-assets**.

[16] For example on the model of the European Benchmark Regulation, as proposed in the discussion paper.

3-3. Regulating the provision of and access to services

3-3-1. Potential recentralisation of certain activities

Summary of responses

Some respondents supported the idea of compulsory recentralisation of activities in certain cases: for instance, it was proposed to recentralise DeFi protocols whenever they engage in regulated traditional finance activities, in order to ensure a level playing field. However, the vast majority of respondents had reservations about the possibility of recentralising certain activities, in the name of respecting the decentralised governance of DeFi protocols. Many felt that greater security required **more decentralisation** rather than centralisation, in line with their risk assessment (see above).

Discussion

At least two situations in which the current forms taken by a number of DeFi protocols pose excessive difficulties: civil or criminal **liability**, particularly with regard to users; and the **need for occasional or regular interactions with public authorities**, such as financial supervisors. Both situations require, depending on the case, **an established organisation or designated representatives**.

Without prejudice to the proposals that the Legal High Committee for the Paris Financial Centre (HCJP) may make in this area[17], it seems theoretically possible to find a **middle way**, since the requirements of organisation or representation do not necessarily contradict the desire for a largely decentralised operation. For example, decisions on the administration of a protocol may be taken by community vote (without undue dominance or influence by an individual or group of individuals), but the protocol may have statuses or representatives at the same time. Depending on the territories concerned, the statutes to be applied may already exist or may be created for the occasion.

3-3-2. Regulation of access points

Summary of responses

The **principle of regulating access points**, in particular with a view to protecting users, **was the subject of a very clear consensus** among the participants in the consultation. However, there were differing views regarding the role of this measure within the overall framework: for some respondents, regulating access points is certainly a necessary but also a sufficient element, which should lead to refraining from any other form of regulation of DeFi.

While the principle of regulation was widely accepted**,** the idea of a regulatory regime applying to **all intermediaries**, possibly by extending the obligations of the MiCA Regulation (section 3-3-2 of the discussion paper), was rejected by the majority of respondents. However, the details of the replies showed that the proposal put forward in the discussion paper was probably not clear (see below).

The discussion paper also suggested **making the distribution of certain products conditional** on customers demonstrating their **financial aptitude**. This proposal was subject to some criticism. The key

[17] In 2022, the HCJP considered the questions posed by DeFi in French law. This will concern in particular the legal status of the DAOs.

point, according to some respondents, would be to provide transparent information in order to give users complete freedom of choice. This opinion was sometimes coupled with criticism of existing European arrangements in traditional finance: there would be no good way of testing customers' understanding, and the regulation would lead to the *de facto* exclusion of the least well-off savers.

Discussion

Firstly, on a common regime for all intermediaries, the idea put forward in the discussion paper was not to introduce exactly the same obligations for all the contact points allowing users to interact with DeFi protocols. Instead, it was proposed to establish a **minimum user protection regime based on the nature of the service provided and not on the type of entity providing it** (centralised entities, simple front-ends of decentralised applications etc.). Certain consumer protection mechanisms applicable to centralised intermediaries could thus be extended to decentralised access points, with certain technical adaptations if necessary.

Secondly, with regard to making the selling of products conditional on the demonstration of customers' financial aptitude, the discussion paper referred to the principles of customer protection generally applied in the financial sector in Europe. From this point of view, the responses received during the consultation **do not seem to demonstrate in what way, for services comparable to those of traditional finance, DeFi would present a specificity justifying the development of entirely different protection principles**.