April 2023

“Decentralised” or “disintermediated” finance: what regulatory response?

Discussion paper

AUTHORS
Olivier Fliche, Julien Uri, Mathieu Vileyn
Fintech-Innovation Hub

ACPR
BANQUE DE FRANCE

Summary

So-called “decentralised finance” or DeFi refers to a set of crypto-asset services, which are similar to financial services and carried out without the intervention of an intermediary. Based on the decentralisation principle popularised by blockchain technologies, it has developed in the wake of innovations related to crypto-assets, in particular the widespread use of automated clause execution tools (also known as smart contracts). **As the transparency and immutability of the computer code should replace the trust between players, decentralised finance is also, and perhaps above all, a disintermediated finance**. DeFi has garnered significant interest both in the public debate and from supervisors, as much for its current state as for what it could become in the future: “tokenization” of finance, benefits of blockchain technologies for the activities of many economic sectors.

This discussion paper provides a brief description of the DeFi ecosystem, its main use cases, its promises, but also its limitations. Among these limitations, this paper highlights **the high level of concentration that characterises the DeFi ecosystem**, **as well as the fact that governance of its applications is sometimes highly centralised**, which constitutes the first risk factor to be considered. In this respect, it seems that the term "decentralised finance" misrepresents the reality of DeFi and that it is more appropriate to speak of “disintermediated finance”.

On a broader level, this paper offers a description of the risks that are specific to this disintermediated finance, schematically distinguishing the three main layers that make it up: blockchain infrastructure, “services” application layer, and mechanisms allowing users to access these services. **Some of the risks associated with disintermediated finance are closely linked to the specific -and indeed attractive- features of the technologies used.** Thus, the solutions sought to improve the performance of blockchains -their "scaling up"- are the same ones that can weaken consensus mechanisms (layer 1 solutions) or create new security problems (layer 2 solutions). Similarly, at the level of the application layer, the transparency of computer code, the composability of smart contracts, their reliance on blockchain oracles: all these advantages of disintermediated finance are also factors of its vulnerability. **User access to these services raises more traditional issues for a financial sector supervisor:** the high volatility and complexity of products, and their non- or little regulated access expose users to high risks of capital loss and may threaten the internal stability of the ecosystem - although for the time being they do not pose a threat to the stability of the financial system.

In view of these risks, this discussion paper puts forward a number of regulatory options, some of which are complementary, others alternative. The main idea developed in this paper is that **the regulation of disintermediated finance cannot simply replicate the systems that currently govern traditional finance.** On the contrary, regulations must take into account the specific features of DeFi. Moreover, such regulation should not be conceived as a monolithic block, but rather as a combination between traditional financial regulations and regulations inspired by other economic sectors.

Among the proposals made, a first set aims to **strengthen the security of blockchain infrastructures**. To this end, this paper explores two main potential organisational arrangements: in the first one, the infrastructure would continue to rely on public blockchains but, before being cleared for use, these blockchains would need to be "certified" according to minimum security standards (certification of computer code, minimum number of validators, cap on validation capacity concentration). In the second arrangement, financial functions would be transferred to private blockchains, in order to guarantee appropriate governance and security levels; these functions would then be managed by trusted private or public players, although this could limit the innovation capabilities of disintermediated finance.

With regard to the application layer, this paper proposes to **strengthen the security of smart contracts using a certification mechanism**, covering security of the computer code, nature of the provided service and governance. This would either be encouraged or made mandatory should interaction with a non-certified smart contract be prohibited. Certification would be obtained following an auditing process performed by a human expert, or using formal methods or a combination of these methods. Such certification would include a software composition analysis component: certification of a smart contract would thus require the prior certification of all the called components. **Certification would also follow three fundamental rules**: it should **be withdrawable at any time**; it would only be granted for a **limited period of time**, in order to take into account developments in IT security knowledge and techniques; it should **be renewed after any significant change to the computer code**. Lastly, in the event that, in the future, smart contracts were to have a certain number of regulatory requirements embedded directly in their code, certification could include checks to ensure that the legal provisions concerned are properly translated into computer language.

Finally, this paper proposes an **improved framework for the provision of services and user access to these services**. On the provision of services, this paper explores the possibility of creating statutes for some service providers, by operating a recentralisation: **players exercising effective control over sensitive services could be required to incorporate**, becoming subject to supervision. As an alternative, players exercising effective control over services could directly fall in the scope of supervision. Assigning a **legal statute to "decentralised autonomous organisations"** (DAO), which would, as necessary, allow supervision, also appears to be a promising avenue: in this regard, this discussion paper refers to the ongoing work carried out by the Legal High Committee for the Paris Financial Centre (HCJP).

On user access, this paper envisages a **strengthened control framework for the supervision of intermediaries facilitating users' access to DeFi services**. Indeed, only a few users have the skills needed to interact directly with DeFi applications; while it would prove difficult to regulate the access of these expert users, it is essential to regulate that of the majority of users. In this respect, **intermediaries can play an essential role in risk prevention**, by preventing investors -especially retail ones- from interacting with fraudulent or dangerous protocols (duty of care), or from taking excessive risks (duty of advice). In return, the risk-taking of intermediaries must itself be regulated by the supervisory authorities in order to limit failures and contagion effects. To this end, this paper proposes as a first step to explicitly extend the provisions of the European MiCA Regulation to decentralised financial intermediaries. In order to prevent the regulation from giving rise to unequal treatment, this extension of its scope would apply to all players that facilitate users' access to DeFi services; the potential "decentralised" interfaces should also be included in such a framework. Secondly, it is proposed that **access to financial products be made contingent on the level of financial literacy and risk appetite of the customer**, both of which should be objectively assessed.

This discussion paper is intended to **contribute to ongoing discussions**, **especially 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, assessing, among other things, the value of and procedures attached to a European regulation on disintermediated finance.

Table of contents

Keywords: blockchain, crypto-assets, DAO, DeFi, finance, oracle, regulation, smart contracts.

JEL No. G15, G23, G28, O33, O38

Introduction

“Decentralised” or “disintermediated” finance -generally referred to as "DeFi"- came to the forefront of the public debate as it developed rapidly in the years 2020-2021. Despite the sharp decline recorded for DeFi from May 2022 onwards, which affected the entire crypto-asset ecosystem in the wake of the crash of Terra-Luna system and its cascading effects, DeFi continues to be a key topic on the agenda of international organisations and working groups. Indeed, beyond its size -which remains relatively modest, even at its peak valuation- DeFi is attracting interest because of the technological innovations it is built on (public blockchain, smart contracts) and because of its fundamental promise: replacing trust between players -such as financial institutions- with computer code as a common rule. **Interest in DeFi thus lies as much in what it is today as in what it could foreshadow for the future**: “tokenization” of finance, benefits of blockchain technologies for numerous activities across economic sectors.

Obviously, financial supervisors’ interest in DeFi also stems from the risks it poses: beyond its innovative nature, it is then a matter of identifying the specific, and potentially systemic, risks borne by this ecosystem. In terms of **financial stability**, DeFi does not currently appear to have the ability to destabilise the financial system as a whole, due to its small size and limited interconnections with traditional finance. However, supervisory authorities must anticipate risks and include into their reasoning elements that could, in the future, become vectors of contagion to traditional finance.

At present, though, the most significant shortcomings of DeFi relate to **customer protection**. Beyond the assets on which the services it offers are based (crypto-assets), which are highly volatile, the risks that are specific to DeFi stem from its innovative technological infrastructure, its governance methods, certain aspects of its financial logic and its terms of access. A thorough analysis of these risks therefore requires an assessment of the entire technical framework of DeFi.

In order to manage these risks, this discussion paper proposes **regulatory avenues**, reasoning on the **three main layers that make up DeFi**: blockchain infrastructure, “services” application layer, and systems allowing users to access these services. The guiding idea behind this discussion paper is that regulating DeFi **should not be conceived as a monolithic block**, but rather as a combination of traditional financial regulations and regulations inspired by other economic sectors.

This discussion paper was written by the Fintech-Innovation Hub of the Autorité de contrôle prudentiel et de résolution (ACPR), following a series of interviews with players in the French ecosystem supplemented by a review of the literature and exchanges with the academic world. The drafting process also benefited from discussions led by numerous bodies at international level, such as the European Systemic Risk Board, the Financial Stability Board, the Organisation for Economic Cooperation and Development (OECD) and the Bank for International Settlements (BIS).

This paper is not intended to provide an exhaustive view of all issues related to DeFi or all positions taken by all stakeholders involved, nor does it intend to reflect any official ACPR position on the matter. It aims to develop an initial analysis of the potential avenues for regulating DeFi, with a view to discussing them with stakeholders, especially professionals, during a public consultation.

In this way, the ACPR intends to **contribute to ongoing discussions, notably those held at European level**, in the wake of the MiCA regulation, which provides for a report to be drawn on the appropriate EU regulatory treatment of DeFi within 18 months of its entry into force.

I. "Decentralised" or "disintermediated" finance: definition, use cases and schematic structure

1-1. "Decentralised" or "disintermediated" finance: an imprecisely delineated concept

"Decentralised finance" or DeFi refers to a set of crypto-asset services, which are similar to financial services and carried out without the intervention of an intermediary.

It generalises the principle of **technical decentralisation** popularised by blockchain[1] technologies and, in fact, it has developed in the wake of innovations linked to **crypto-assets**, in particular the generalisation of **smart contracts** and the emergence of crypto-assets deemed stable, known as "**stablecoins**".

A **set of criteria** can therefore be used to characterise DeFi, even though none of them is sufficient to qualify a use case and, conversely, many DeFi services do not meet all these criteria:

- an **architecture based on public blockchains**: the public nature of the blockchain is a first indication of decentralisation, thereby avoiding the intervention of an authority or a trusted third party; in a private blockchain, however, an authority decides on the principle behind and terms of participation;
- **protocols based on smart contracts**, i.e. computer programs that are automatically executed upon the occurrence of triggers;
- **decentralised governance**, which means it relies on a community-based form of governance - sometimes organised around a "**decentralised autonomous organisation**" (**DAO**[2])- with no central authority or party holding administrator rights, and no user or group of users having effective control over the protocol; in practice, this criterion isn't usually fulfilled (see below);
- **the absence of a custodian** (non-custodial): in a decentralised framework, users are expected to hold their crypto-asset funds themselves, meaning hold the private keys required to access them on the blockchain rather than holding them through intermediaries.

Many such projects are of a mixed character. In addition, decentralisation can be **variable over time** throughout the protocol development cycle. The early stages of a project are usually highly centralised: in the software development phase, the core team of developers, which is often funded by venture capitalists (who get protocol governance tokens in return), holds the administrator keys of the protocol. It is this team that usually develops the main operating rules of the protocol (fees, voting rules, etc.), which are embedded in the program code. The protocol is then deployed on the market, and begins to operate on the basis of the encoded rules. In some cases, the developers keep administrator keys during the early stages of the roll-out (test phase), so that any malfunctions can be corrected as quickly as possible (with the possibility of shutting down the system). Often, the development team forms a foundation or an association.

According to a decentralised approach governance is subsequently transferred to a community, often organised around a DAO (e.g.: MakerDAO, Compound, Uniswap). However, it sometimes happens that

[1] Refer to the glossary in the appendix for a definition of technical terms.

[2] A DAO is a common (yet not systematically used) component of DeFi protocols, designed to organise governance over them; it is usually determined by a community of governance token holders, and by smart contracts that govern its operating rules and the assets it holds control over (protocol treasury).

the developers or founders of a project keep administrator keys even after the test phase, which exposes protocols to manipulation risks, especially when such information is not communicated to the users (refer to section 2-1 on risks related to governance).

Box 1: The semantic difficulties of DeFi: when the usual terms badly describe the realities

- ***DeFi***: ***decentralised or disintermediated finance?*** The usual term emphasizes the notion of decentralisation, which may refer to the governance of applications, but also to the property of the blockchain infrastructure: a shared registry in which each node of the network holds all or part of the information. With regard to governance, the promise of decentralisation is not always kept (see section 2-1); therefore, the emphasis could more legitimately be placed on the disintermediated nature of these financial activities and the use of the term "disintermediated finance" encouraged. Without claiming to settle this debate, this document uses more often than not the English contraction "DeFi", which has become widely accepted in the literature on the subject.

- ***Smart contract*** **or automated clause execution tool**: the term "smart contract" does not appear to be very appropriate to designate these computer programs, which are not "smart" in the sense that they do not modify their behavior over time, but instead simply execute a code when predefined conditions are met. Smart contracts are not necessarily contracts in the legal sense either. Despite this, the term has become widely used in the literature, and is therefore used in this report.

- ***Stablecoin***: crypto-asset whose objective is to maintain a stable value by reference to an official currency (or a basket of such currencies), to other real-world rights or assets, or by reference to other crypto-assets. The term can therefore appear misleading, since stability is an objective and not a guarantee; many stablecoins have thus experienced temporary or permanent "depegging" from their reference value.

1-2. The development of DeFi

The first significant DeFi service combining stablecoin, decentralised governance and lending protocols appeared in 2017 (MakerDAO), with limited subsequent developments until 2020 (Bancor, Uniswap v1, Synthetix, Compound, REN, Kyber, 0x). The year 2020 marks a breakthrough, with the "summer of DeFi" and the gaining momentum of reward programs as well as governance tokens (Compound, Yearn Finance, SushiSwap, Uniswap v2).

Between the summer of 2020 and the beginning of 2022, DeFi experienced **sustained growth**. Thus, notwithstanding the fact that this metric is not entirely satisfactory[3], the total amount of crypto-assets deposited in protocols (total value locked or TVL) reaches $170 billion at the end of 2021[4], compared to $2 billion in June 2020, a year and a half earlier (see chart 1). At the same time, the market capitalisation of the main DeFi tokens reached around $150 billion[5] (compared with $6 billion at the

[3] While it is the best estimate available to date, TVL is a biased unit of measurement, notably due to tokens reinvestment phenomena through collateralised lending protocols: a user holding crypto-assets A may decide to deposit them as collateral to obtain a loan in crypto-assets B, part of which may in turn be deposited as collateral to obtain crypto-assets C. Aggregating TVLs calculated for the various protocols involved would, in this scenario, lead to adding up holdings in A, B and C, whereas assets B and C are only the result of the leverage exerted by the user through his holdings in A. For this reason, the accounting used here ("net" TVL) notably excludes tokens borrowed or deposited using staking or liquid staking mechanisms (read more on these concepts below).

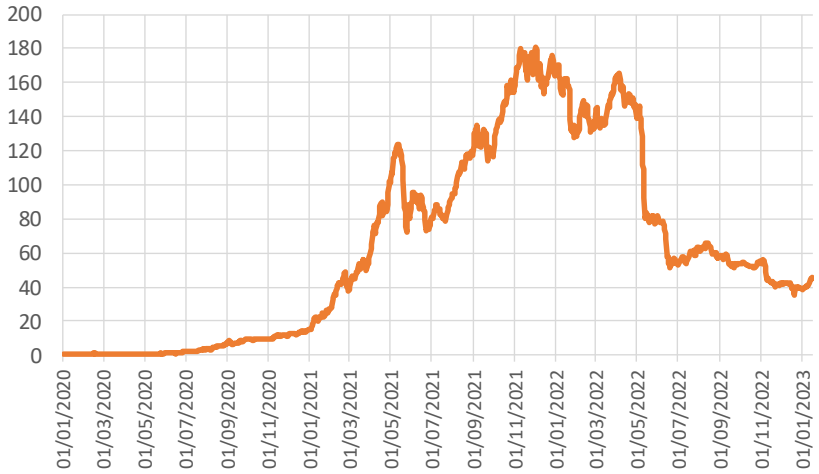
[4] Source DefiLlama - DeFi Dashboard

[5] Source: Coingecko

end of June 2020), totalling nearly 5 million digital wallets in use[6] (compared with around 200,000 at the end of June 2020).

In the course of 2022, however, the market value of the DeFi ecosystem recorded a **sharp drop**, especially from May onwards (crash of Terra-Luna, see below). By the end of 2022, the size of DeFi had been divided by more than 4 compared to its peak at end-2021, with TVL shrinking to around $40 billion (see chart 1).

Chart 1: Total value of assets locked (TVL) in DeFi protocols, expressed in USD billion



Source: DeFi Llama

The growth dynamic of DeFi in the 2020-2021 period can be explained in part by the recycling of profits linked to the development of crypto-assets, especially with the price increase of Bitcoin[7]. This striking development was also supported by the macroeconomic environment, and more particularly low interest rates, which guaranteed easy access to liquidity and drove risk-taking. The increased availability of developers during the Covid-19 lockdowns and afterwards with the emergence of new work organisation arrangements also contributed to this trend.

In contrast, from 2022 onwards, investors reacted to the global monetary tightening and increasingly uncertain economic and geopolitical environment by reducing their exposure to riskier assets. The collapse of the Terra-Luna ecosystem and the bankruptcy of several players[8] (Celsius Network, Three Arrows Capital, Voyager Digital, BlockFi, FTX), which led to increasing doubt about the crypto-asset ecosystem, also added to the momentum of this downward trend. Thus, after benefiting from the buoyant growth of crypto-assets in 2020-2021, DeFi was affected by their downturn in 2022.

It should also be noted that, even at its highest capitalisation level (towards the end of 2021), the size of the DeFi ecosystem **remained relatively small** compared to that of the crypto-asset market ($2,500bn[9] at end-2021: DeFi therefore accounted for less than 10% of this total), and even more so compared to traditional finance.

[6] Source: DeFi users over time (dune.com)
[7] OECD, *Why DeFi matters and the policy implications*, January 2022.
[8] It may be noted that they are all "centralised" players.
[9] Source: Crypto Market Cap Charts | CoinGecko

1-3. The use cases for DeFi

In practice, use cases are now focused on a limited number of restricted activities. Speculative activities are widely prevalent, as well as uses serving the real economy, such as corporate finance, remain underdeveloped. The main use cases are the following:

- **Collateralised lending** is the main activity, in terms of "net" TVL[10], in the DeFi sector. It allows one to bet on the future upward or downward evolution of the value of crypto-assets. This system is very similar to the repurchase agreement (repo) activity in traditional finance, since the loan is guaranteed by a collateral deposit, which allows the lender (another user or more often a "liquidity pool", see below) to hedge against the volatility inherent in crypto-assets and against the risk of borrower default. This collateral is immediately liquidated as soon as its value falls below a pre-defined threshold (on automated liquidation, see section 2-4-2).

- **Token swaps**: the swap takes place on decentralised exchanges[11] (DEX). Originally, the system operated through the use of an order book system, similar to the one used in traditional finance. In many protocols, order book models have gradually been replaced by Automated Market Makers (AMMs), another major innovation of DeFi: trading is no longer carried out directly on a peer-to-peer basis, but rather against a "liquidity pool". This pool is composed of all the tokens contributed (deposited) by users, which makes it possible to buy or sell without necessarily requiring a reciprocal order. The provision of "liquidity" in the pool is incentivised by remunerating token providers with application governance tokens[12].

- **Staking protocols and liquid staking protocols**: staking, or “token locking”, is linked to the validation of transactions on "proof of stake" (PoS) blockchains: in this system, the validation of a block requires that blockchain governance tokens be sequestered[13], as a guarantee of the validation process, by "staking" on the network (hence the name "proof of stake"[14]). Initially, staking was only carried out by validators, and required a significant financial commitment on their part. Some blockchains quickly resorted to a "delegated proof-of-stake" system[15], in which validators entrust their tokens to delegators, who are responsible for securing the blockchain. As block validation is remunerated through the granting of new governance tokens, users who lock their tokens in staking receive a share of the earnings (minus the delegator's commission).
  The system has gradually developed towards liquid staking: users wishing to stake deposit their tokens in a liquidity pool, and receive in exchange a kind of certificate of deposit (in the form of a wrapped token), which can itself be swapped, deposited as collateral, etc. In turn, the protocol uses the deposited crypto-assets for staking, paying a commission to the delegators effectively in charge of the validation of transactions[16].

[10] According to the OECD, in June 2021, it accounted for 53% of the total value of the DeFi ecosystem.
[11] Examples of swap protocols include: Uniswap v3, Curve.
[12] Examples of lending protocols: Aave, Compound.
[13] These tokens are sometimes referred to as "protocol tokens", to distinguish them from governance tokens in DeFi applications.
[14] The main competing system, "proof of work" (PoW), on which Bitcoin, for example, operates, consists of miners performing extremely sophisticated cryptographic calculations that require sophisticated hardware and significant energy use.
[15] Delegated Proof of Stake is used for instance by Tezos, Lisk, or EOS.
[16] The staking-as-a-service market is currently largely dominated by the Lido protocol.

- **Yield farming (or liquidity mining) protocols**: these protocols allow users to lock their crypto-assets in a smart contract -which can then use them- in exchange for a given yield. As counterpart to the borrowing facilities, they contribute to the proper functioning of decentralised services. Yield farming can be compared to staking, although the latter only involves blockchain governance tokens.

- **Flash loans (uncollateralized loans):** users can borrow crypto assets without collateral, provided they repay the loan within the same blockchain transaction. This mechanism is based on IT developments that allow transactions to be bundled within a single transaction that aggregates them all. This way, users can make profits by taking advantage of arbitrage opportunities between various crypto-assets, and of these assets' price differentials between different decentralised exchange platforms. Flash loans are also used to liquidate positions: through this technique, liquidators can sell the collateral in order to repay the relevant debt before it ceases to be covered by the collateral.

- **Derivatives on traditional financial assets**: a crypto-asset is issued to virtually represent the value of a real financial asset held as collateral, the price of which it follows. This way, a crypto-asset can replicate the value of the stock a large company. This systems is similar to that of stablecoins, which are indexed to the value of a currency or to that of other assets (such as gold).

- **Derivatives on crypto-assets**: the DeFi ecosystem offers the whole range of traditional derivatives (futures, options) with a crypto-asset as the underlying asset. There crypto-asset derivatives are traded on centralised or decentralised platforms. One type of product is specific to the crypto-asset world: perpetual futures[17], which are an equivalent to contracts for difference (CFDs)[18] in traditional finance (see in particular sections 2-4-2 and 3-3-2 on this topic).

- **Decentralised insurance protocols**: some of these protocols aim to cover risks specific to DeFi activities[19], while others consist of parametric insurance services on real goods and services[20].

- **Crowdfunding protocols**: many crowdfunding projects opt for a decentralised form of governance and are hosted on a blockchain, with the added promise of greater transparency.

- **Prediction markets**: a platform connects two bettors with opposing predictions.

- **No-loss lotteries**: these are based on the pooling of crypto-assets, positioned on various staking protocols. The user buys tickets that give him or her the opportunity to win the interest earned on a daily basis. That user can redeem his tickets to recover his initial stake at any

[17] A futures contract is a commitment to deliver an underlying asset at a future date under predefined conditions. Perpetual futures contracts have no expiry date, so they allow positions to be held open for as long as desired, without the need to change the relevant contract.

[18] CFDs are speculative financial instruments that bet on the rise or fall of the value of an underlying asset (indices, stocks, etc.) without actually holding the asset. The transaction between the buyer and the seller is based on the difference between the current value of the underlying asset and its value at the time of sale. CFDs are usually offered with leverage, meaning a multiplier of gains and losses.

[19] For example: Unslashed Finance.

[20] For example: Etherisc.

time[21]. This means that the user sacrifices a small amount of interest in exchange for the possibility of a significant profit.

Box 2: Access to DeFi for investors

Investments in DeFi protocols are made exclusively in crypto-assets. Investors must therefore first hold crypto-assets, or acquire them in exchange for official currency[22] from **centralised intermediaries** ("crypto on-ramp"): **crypto-asset exchange platforms**. Once crypto-assets are acquired, **they can be invested in DeFi in three ways.**

The **first way**, which is completely disintermediated, involves interacting directly with DeFi applications and therefore requires computer programming skills. For users without programming skills, meaning the majority of them, **a second way** to invest consists in using **web-based interfaces** that allow "click-button" access to decentralised platforms. These interfaces can be designed by the developers of the decentralised applications to which they offer access, or by independent actors.

A **third mode of access** is through **centralised intermediaries**, who make investments in the DeFi ecosystem on behalf of their clients. This last method of investment is sometimes referred to as "CeDeFi" (decentralised intermediated finance). These platforms, of which Binance and Coinhouse[23] are examples in France, thus play a key intermediary role in facilitating access to DeFi services.

1-4. The growing involvement of institutional stakeholders

The returns offered and the possibility of engaging in highly leveraged transactions on crypto-assets have attracted a number of institutional investors (investment funds in particular) to DeFi in 2020-2021. This has led to the creation of **applications tailored to the needs of institutional investors**[24], the main distinctive feature of which is the inclusion of procedures for verifying the identity of participants ("Know your customer" or KYC). These applications are thus **permissioned**, meaning that their access is restricted to authorised participants. In return for these checks, and after assessing their solvency, these applications offer authorised participants the ability to borrow without collateral, in the same way as in traditional finance.

The evolution of the price of "gas" on the Ethereum blockchain, meaning that of the fees to be paid[25] to register transactions on the blockchain (gas fees), is another indication of the growing involvement of institutional players. The price of gas evolves according to the status of supply (validators available to register transactions) and demand (transactions to be validated). Moreover, the more complex a transaction is (size of the smart contract to be executed, potential calls to other smart contracts, nature of the calculations, need for data etc.) and the faster it has to be validated, the more expensive it is.

As interest for DeFi has grown, transaction fees have increased significantly on Ethereum over the course of 2021, during which they almost continuously exceeded USD 10 per transaction in the first

[21] This is how the PoolTogether protocol works.
[22] A currency issued by and guaranteed by governments (sometimes also referred to as fiat currency).
[23] Binance France and Coinhouse are registered as digital asset service providers (DASPs) with the Autorité des marches financiers (AMF, the French financial markets supervisor), with the approval of the ACPR.
[24] For instance, Aave Arc (the version of the Aave protocol dedicated to institutional investors) or Atlendis.
[25] Fees are settled in ether (ETH), the native crypto-asset of the Ethereum blockchain (which also serves as its governance token).

half-year -and sometimes reached USD 70 during speculative episodes- before falling back to around USD 5 in the second half of the year. Such prices clearly discourage small-amount transactions, and only remain affordable for higher value transactions, which are usually carried out by institutional players.

1-5. An ecosystem characterised by high concentration at every level

Paradoxically, one of the notable characteristics of the DeFi market is its high degree of concentration. This is true, first of all, at the level of **blockchains** that support DeFi applications: at end-2022, the Ethereum blockchain alone concentrated 60% of net TVL for DeFi -a share that is almost identical to that recorded for end-2021[26]-, while more than 80% of the net TVL of the ecosystem is concentrated on 3 blockchains at the end of 2022[27]. In addition, the validation capacity of blockchain transactions may themselves be highly concentrated[28].

Concentration is also present in DeFi **applications**. Although thousands of protocols have been developed, in practice only a few dozen concentrate the bulk of funds and uses. Thus, by the end of 2021, the top 3 DeFi applications put together accounted for 33% of total net TVL[29], the top 7 accounted for 50% of the total, and the top 36 for 80% of the total. This concentration trend has also been increasing in the course of 2022, as the value of the ecosystem decreased: 16 protocols thus concentrate 70% of net TVL at end-2022, compared to 21 protocols at end-2021[30] (see Table 1). Finally, the ownership of **application governance tokens** can itself be highly concentrated (see in particular section 2-1 on this subject).

Table 1. Measuring concentration in DeFi applications at end-2021 and end-2022

Share of total net TVL	Number of protocols	
	At end-2021	At end-2022
33%	3	3
50%	7	6
60%	11	9
70%	21	16
80%	36	34
90%	65	83

Source: DeFi Llama
Reading aid: At end-2021, the combined net TVL of the top 7 protocols represented at least 50% of the total; as at end-2022, the top 6 protocols put together accounted for at least 50% of the market.

[26] The Terra blockchain gained momentum in the first months of 2022, accounting for up to 15% of TVL, before its crash in May 2022.
[27] In addition to Ethereum, the Tron and Binance Smart Chain blockchains accounted for 11% and 10% of net TVL respectively, at that date.
[28] Before the shift to proof-of-stake validation, five entities accounted for 65% of Ethereum's mining capacity (*Les Echos*, 30 August 2022). In proof of the stake validation, there are more validators, but the concentration risk does not disappear, especially if the former are brought together by centralised platforms in validator pools (such as Coinbase).
[29] It should be borne in mind that activities leading to double counting (see above) are not included here.
[30] However, the 90% threshold is reached with 83 protocols at end-2022, compared to 65 at end-2021, which reflects a measure of diversification in the middle of the distribution.

1-6. Diagrammatic overview of the players and "components" of DeFi

In terms of architecture, DeFi is composed of various layers (see diagram below). **Blockchain infrastructure** forms the basis of it, comprising a distributed ledger over a set of nodes, which agree on its content via consensus algorithms. Blockchain allows for the execution of smart contracts. Infrastructure forms the "settlement layer" of DeFi. In order to address the performance issues of blockchains, so-called "layer 2" solutions can process part of the off-chain transactions (see section 2-2), recording only the result in the main chain (layer 1). **Bridges** are used to connect blockchains to each other.

Decentralised applications (dApps) or DeFi protocols are, strictly speaking, stacks of software -smart contracts- built on the blockchain infrastructure, each corresponding to specific use cases. The fact that the layers build on each other, added to the generally open source nature of the applications' code, makes it possible to create an open architecture that encourages **composability**[31]: one smart contract can easily call other smart contracts to use their properties; existing applications can be combined to create new ones. **The ability to easily form and combine modular elements is very conducive to the creation of innovative activities and products; it is one of the major innovations of DeFi, the network effects of which it amplifies**[32]. At the same time, the recycling of software elements adds to the complexity of an already dense ecosystem and increases operational risks (see section 2).

In addition to decentralised applications, **centralised applications**[33] can connect to the blockchain infrastructure, via APIs[34], in order to offer services: centralised exchange platforms[35] (CEX), data analysis, oracles, etc. In practice, CEXs are often an entry point to DeFi for users (see box 2), in particular by offering them custodian wallets.

Lastly, the top layer of DeFi is made up of **interfaces** that allow users to interact more easily with centralised or decentralised applications. These interfaces can also play an **aggregator** role: by providing a simultaneous connection to multiple applications and protocols, they allow users to perform tasks that would otherwise be more complex without their presence (for instance, comparing returns on a loan across several competing applications).

Most users also use a crypto-asset **wallet** to interact with DeFi applications. This wallet is an interface containing a public key to receive crypto-assets, and a private key to access them. Crypto-assets are not stored in the wallet (they always remain on the blockchain); contrary to what its name suggests, a wallet is therefore closer to a key ring. Wallets can be hosted (custodial), meaning that a third party

[31] It should also be noted that the level of concentration of DeFi services on a single settlement layer (with the Ethereum network being predominant) is mainly due to the fact that a common infrastructure makes it possible to take full advantage of composability properties (by relying on elements that are already built on the infrastructure).

[32] An externality mechanism, in this case positive, whereby the value of services increases as participation in the network increases.

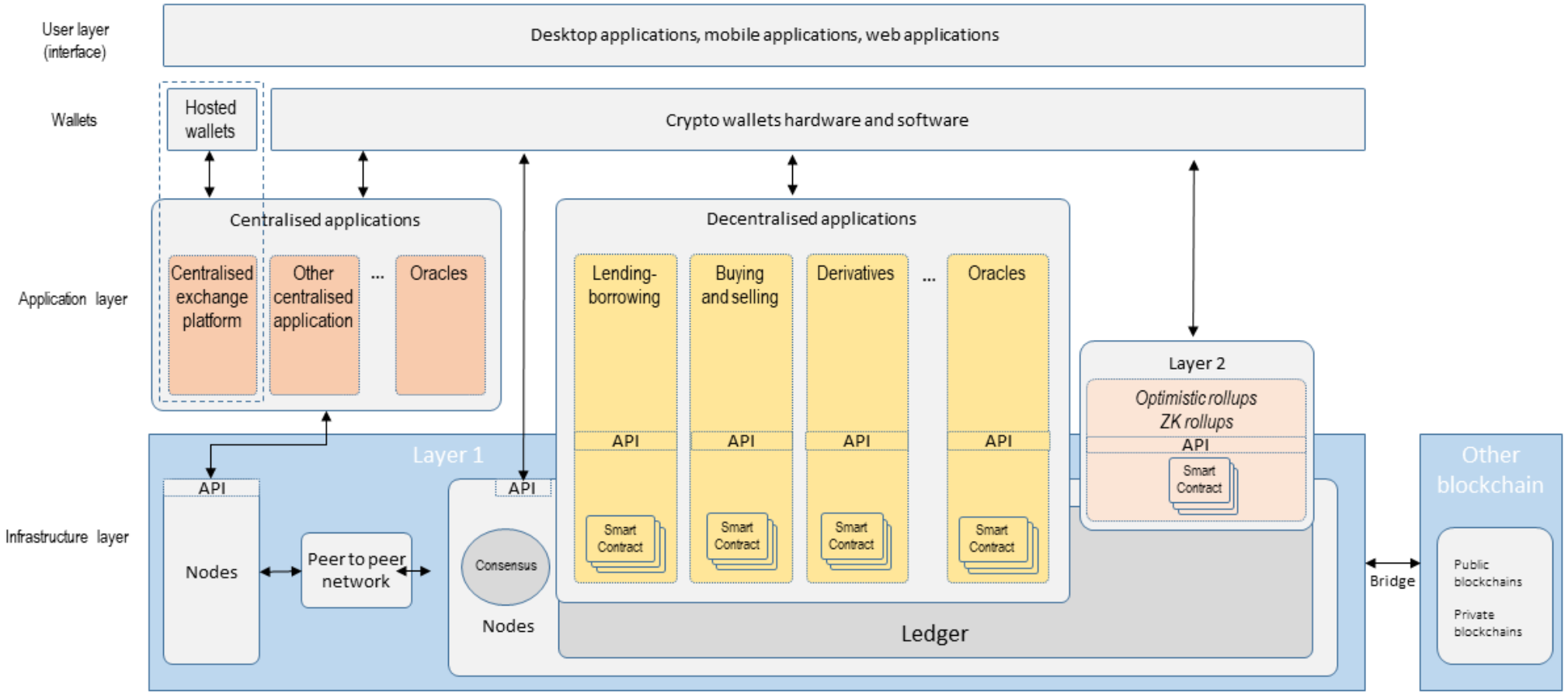
[33] As their name suggests, strictly speaking centralised applications are not DeFi. However, they play a key role in this ecosystem, being its primary source of funding and its main entry point for users. The OECD thus considers that centralised applications are the "lifeline" of DeFi (OECD, *Lessons from the crypto-winter*, December 2022).

[34] Application programming interface, i.e. a software interface allowing to "connect" a software or a service to another software or service, in order to exchange data and functionalities.

[35] Such as: Binance, Coinbase.

holds the private key and thus ultimately has control over the relevant crypto-assets. With non-hosted (non-custodial) wallets, on the other hand, the user has direct control over his or her funds. Finally, some wallets are software-based and connected to the internet (*hot wallets*), which makes them easier to use, while other are hardware wallets, i.e. physical offline devices (*cold wallets*), which is supposed to reduce the possibilities of attack.

Diagram: The application architecture of "DeFi"



II. The risks associated with DeFi

2-1. The risks associated with decentralised governance

Whether in terms of blockchains or applications built on top of these infrastructures, **decentralised governance** carries significant risks: users effectively holding governance power over a protocol can make decisions that are detrimental to minority owners. This issue is all the more salient in the world of DeFi as many protocols provide **pseudo-decentralised governance**.

Firstly, **governance tokens are sometimes concentrated in the hands of a few players**. This may be related to the fact that governance tokens can be traded like other crypto-assets, allowing significant users ("whales") to accumulate substantial shares of the tokens. In fact, flash loans can even be used to carry out attacks against a protocol, by borrowing significant amounts of governance tokens for a short period of time, but one that is sufficient to vote a decision that is harmful to other users.

Token concentration can also stem from the fact that the **founders, developers or funders of a protocol have kept a majority of the governance tokens for themselves**: in February 2020, for instance, when the Compound protocol launched its governance token (COMP), close to 50% of the tokens were allocated to the project's developers and funders[36]; several years later, the protocol's governance is still in the hands of a small number of players[37]. This is all the more true as many governance token holders do not usually take part in the various votes, either because they are unfamiliar with the procedures or are not informed that a vote is being held, or because they anticipate that they will have difficulties influencing the decision in front of the "whales"[38]. It should also be noted that the logic of pseudonymity that reigns in the DeFi ecosystem prevents transparency on the concentration of governance tokens, since a single user can have several addresses (see also section 2-4-4 on the issue of pseudonymity).

Secondly, it should be noted that many blockchain protocols or DeFi applications **do not rely entirely -and sometimes, not primarily- on the votes** of governance token holders. The adoption of a measure to change protocols is thus often subject to the prior approval of certain parties, while some entities may have veto rights[39]. Similarly, the founders or developers may have retained the **administrator keys** of a DeFi protocol, and thus have the ability to change its operating rules without the agreement of the decentralised governance bodies. While this practice may seem legitimate at the launch of a protocol, in order to be able to quickly address malfunctions, such continued practice contradicts the promises of decentralised governance, especially when other users are not informed of this situation.

A classic example of the risks associated with poor governance is the so-called "**rug pull**" manoeuvre, a situation in which the issuer of a crypto-asset absconds with investors' funds. In fact, a new token can be issued on a blockchain for a small fee; with an injection of liquidity, the token can then be introduced on decentralised exchange platforms (DEX); events such as marketing campaigns on social

[36] Out of the 10 million tokens issued, 4.9 million were distributed internally: 2.3 million to Compound Labs shareholders, 2.2 million to founders and development team members, and 0.4 million to future team members.
[37] As at 20 January 2023, 50% of the voting rights were shared between 9 players (source: protocol website).
[38] For more information on this topic, refer to OECD, *Why Decentralised Finance (DeFi) Matters and the Policy Implications*, January 2022, p. 35
[39] For example, the adoption of a change in the functioning of Ethereum is subject to the approval of the protocol's developers, and also requires the agreement of many stakeholders (see: Ethereum Governance | ethereum.org)

networks, sometimes using popular influencers, as well as free token distributions (*airdrops*), can then be organised to drive up the price; when the price reaches suitably high levels and liquidity is high, the founders or developers of the project sell their retained tokens *en masse* and disappear with the funds and reserves[40]; other investors are then left with vast quantities of zero-valued tokens.

2-2. The risks associated with infrastructure

2-2-1. The challenges of scaling up and their consequences for infrastructure

Some blockchains face episodes of **network congestion** due to a substantial number of transactions that require high computing power. This congestion issue causes some transactions to fail, impacts withdrawals in crypto-asset or prevents the update of a number of quotes. Congestion is the consequence of the challenges blockchains face around **scalability**, which refers to the ability to process a more significant number of transactions per second without losing efficiency[41]. The decentralised nature of transaction validation on blockchains implies energy and storage constraints - and therefore costs- for each validator node. The balancing decisions required between decentralisation, security and scalability have been termed the "blockchain trilemma"[42]. This issue could become critical if DeFi transactions were to play a significant role, either in addition to or instead of traditional finance, as the number of transactions would then become substantial.

a. Layer 1 solutions increase blockchain corruption risk

The first solutions to emerge as a response to the issue of network congestion were **internal to the blockchain**, also referred to as **layer 1** solutions. They may first involve increasing validation power. Yet, due to the limited number of machines available and the cost of validation, this tends to simultaneously reduce the number of validator nodes, therefore decreasing the level of security of the network and its decentralisation (see below). Another solution, called *sharding*, consists in breaking a blockchain into several smaller and more flexible blockchains, called shards. The validation nodes then store only part of the information, while such information can still be shared, which increases their operating speed.

The common disadvantage of these solutions is that they make blockchains more easily corruptible, especially through "51% attacks" (see below). The scalability obtained with layer 1 solutions is therefore **achieved at the expense of security and decentralisation**.

[40] As a way to tackle this issue, most of the administration keys for protocols that offer funds deposit are secured by timelocks (locking the funds for a given period of time) or, more frequently, using multi-signature mechanisms (*multisig*) according to which the protocol's funds can only be released after several people have signed off on it (often around ten people). This multisig system is not without risk, however, since the people in question may know each other (for instance, the team of developers behind the protocol), and therefore may collude with malicious intent.

[41] Ethereum can currently only process between 10 and 15 transactions per second (around 7 for Bitcoin), while a network like Visa processes up to 24,000 transactions per second.

[42] However, the development of new generations of blockchains and layer 2 solutions could help overcome this trilemma (see below).

b. Layer 2 solutions may exacerbate the lack of interoperability between blockchains and present security issues

Another way to improve scalability is to use **layer 2 solutions**, **located off the main blockchain** (considered as layer 1) to increase its efficiency. Their underlying principle is to allow for transactions to be carried out off the main blockchain, with only their results being written on-chain, thus limiting the need to record new blocks. It can be implemented using a variety of techniques (state channels[43], nested blockchains[44], sidechains[45], etc.); the most commonly used at present being "**rollup**" systems. Rollups execute the transactions carried out on their network, "roll up" these transactions in a single transaction (hence their name), and compress the relevant information, sending only the data that is strictly necessary for the verification of transactions on the blockchain.

At present, there are two main types of rollups available that vary according to the way the validation of transactions posted on the main blockchain is handled. The first type, **optimistic rollups**[46], operate on the assumption that transactions are valid until proven otherwise (hence their name). In practical terms, batches of transactions are sent by an operator to the blockchain; this triggers a 7-day time window during which any node in the blockchain network can challenge the validity of the transaction; if a fraudulent transaction is detected, a rollback is performed; the node that challenged the validity is then rewarded, while the operator that submitted the batch of transactions receives a penalty (forfeits part of the crypto-assets previously deposited as collateral). Once the 7-day dispute period has elapsed, the batch of transactions is permanently posted on the main blockchain. Optimistic rollups therefore require the presence of at least one reliable validator on the network, otherwise the rollup operator[47] can create fraudulent blocks to steal crypto-assets. In addition, the time it takes for transactions to be final leads to significant latency for users.

The second kind of rollup is referred to as **Zero-knowledge rollups** (or ZK-rollups)[48]. In this model, each time an operator places a batch of transactions on the blockchain, that operator also deposits a cryptographic proof of their validity, known as "zero-knowledge proof" because it proves the veracity of a proposition without delivering any other information, which notably generates significant information savings[49]. This model also allows any player to post transactions to the main blockchain. However, it is still under development and has yet to reach widespread adoption. Most importantly, the calculation of proofs requires considerable computing power; in practice, these proofs are therefore only produced by a few players today, which generates a risk.

The **fast-paced development**[50] of layer 2 solutions tends to turn layer 1 blockchains into mere "bookkeeping" layers, with transactions increasingly being carried out on layer 2. However, it also

[43] They make peer-to-peer transactions between users known to each other possible without the intervention of a third-party validator (examples include Lightning Network on Bitcoin or Raiden Network on Ethereum).

[44] A system of nesting dolls of different blockchains with transactions being subcontracted from one more fundamental blockchain to the next (such as Plasma on Ethereum).

[45] Adjacent blockchains operating on infrastructure and consensus mechanisms that are entirely independent from those of the main chain. However, they communicate directly with the main blockchain: therefore, and unlike with state channels, transactions are not private, but instead are publicly displayed on the blockchain (e.g.: Polygon for Ethereum).

[46] Examples on Ethereum: Arbitrum, Optimism.

[47] Optimistic rollups are currently operated by centralised entities.

[48] Examples on Ethereum: Starkware, zkSync.

[49] The size of the proof being logarithmic to the size of the operations.

[50] It should be noted that these solutions themselves can also be affected by network congestion problems, due to their success. The more general-purpose layer 2 solutions seem particularly strongly affected by this

tends to **exacerbate the lack of connectivity or interoperability**[51] **between blockchains**, which is a major concern: indeed, each blockchain currently operates in isolation[52]. Furthermore, none of these solutions offer the same level of security as the main blockchains, as the result is not guaranteed until transactions are recorded on layer 1. Lastly, it may be argued that some of the layer 2 solutions hinder the transparency of information on the main blockchain.

The development of solutions either internal to blockchains or using layer 2 solutions may therefore lead to limitations in terms of security of the infrastructure, or to increase some of its vulnerabilities, which should draw the attention of regulators.

2-2-2. These developments could result in increased vulnerabilities in the blockchain infrastructure[53]

The resilience of a DeFi protocol is measured by its ability to avoid being either hacked or diverted from its primary use. Because of its relative newness and early stage of maturity, DeFi is particularly prone to so-called zero-day vulnerabilities: cases of protocol misuse that are unprecedented. These vulnerabilities include:

- **Attacks on the network layer of the blockchain**: when a node connects to the blockchain, it is connected to other nodes through a peer-to-peer network to share information about changes made in the blockchain. Creating new nodes is relatively easy. A malicious user can create fake nodes, which are then linked to a targeted legitimate node, which is then isolated from the rest of the "real" network. The targeted node can then be obscured: the blocks it validates are never added to the blockchain, while the crypto-assets it receives can be double-spent.

- **Attacks on the consensus layer or governance layer**: these attacks take advantage of the vulnerability that a governance layer concentrated in the hands of a few actors can create. This may occur, among other ways, when governance is only pseudo-decentralised -for instance, when the founders have kept a majority of the governance tokens for themselves- or under stressed conditions[54]. Blockchains are especially vulnerable to so-called "51% attacks" which occur when a group of malicious users holds more than 50% of validation capabilities. This

phenomenon, while restricted layer 2 solutions, such as Bitcoin's Lightning Network, that only offers peer-to-peer transactions, do not appear affected to the same extent.

[51] The challenge concerning interoperability also extends to the data format provided by oracles and used by blockchains, which is not standardised yet.

[52] Although a number of recent projects point to potential developments in this regard: Polkadot, Cosmos or Avalanche for instance.

[53] It may be noted that, to a broader extent, in order to guarantee the security of the transactions that are carried out on them, blockchain infrastructures rely heavily on public key cryptographic techniques, which could eventually be threatened by the development of quantum computing. For more information on this topic, refer to the experimentation report published by the Banque de France in November 2022.

[54] For instance, when the Luna token lost 98% of its value in May 2022, a small group of malicious players had the opportunity to buy a majority of the Terra blockchain's governance tokens and to take control of the infrastructure by delegating their decision-making power to a complicit validator. To prevent this scenario from occurring, the blockchain had to be paused by its administrators (the main validators having agreed to temporarily stop the validation of new blocks).

majority allows the group to tamper with the blockchain by validating falsified blocks[55] or by blocking the addresses of selected users. The smallest blockchains are the most vulnerable to this type of attack, as having the majority of the validation capabilities (computing power or validation tokens) on the largest blockchains is exceedingly expensive[56].

- **Attacks on bridges between blockchains**: these bridges are the focal point of a fair number of recent significant attacks[57]. In the case of centralised bridges, these attacks most often aim to take control of the signatures required for validation, especially when these signatures are relatively concentrated in the hands of a single player. For decentralised bridges, they are often focused on exploiting vulnerabilities in smart contracts. The vulnerability of bridge structures, regardless of their form, has led many players to favour layer 2 solutions rather than multi-chain systems.

2-3. The risks related to the application layer

A significant share of the risks associated with DeFi services stems from the **computer code behind smart contracts**, whether this code has intentional flaws (fraudulent program) or unintentional vulnerabilities (program written without malicious intent, but with flaws that can be used by attackers). The main risks in this area include "reetrancy" attacks[58], which make it possible to drain the available funds, integer overflow or "underflow" attacks[59], and potential tampering by validators[60]. In this respect, the fact that the code behind smart contracts is public makes them an open target exposed to all: the attack surface is therefore increased, although it can be argued that this characteristic makes them, in use, more resistant than private algorithms.

It should be noted that the vulnerabilities of the application layer of DeFi are exacerbated by one of its most attractive features, the **composability** of its components: a flawed smart contract can be called by other smart contracts; its vulnerabilities can therefore spread to a significant number of applications without the users being aware of it.

The issue of **data reliability**, which has received relatively limited attention, also contributes to the risks for the user. The successful relaying of information is indeed a fundamental prerequisite for the efficient functioning of markets, in DeFi as in traditional finance. However, one of the specific features

[55] The main risk lies in the potential for "double-spending", which makes it possible to recover crypto-assets that have already been spent by putting a first block before the one that permanently validates the transaction.
[56] It is worth noting that the Ethereum Classic blockchain has been repeatedly targeted using this particular type of attack in 2019 and 2020.
[57] Such as Wormhole (Solana) in February 2022, or Ronin Network in March 2022.
[58] The ability to use certain smart contract functions recursively, meaning several times at a very fast rate; typically, this operation allows for many withdrawals of funds to be made from an account before the account balance update function can run.
[59] An integer overflow occurs when a mathematical operation generates a numerical value that is greater than that which can be represented in the storage space available (for example, in 32-bit architectures, the maximum representable value is 2^{32}-1). Similarly, integer underflow occurs when a non-null result is obtained that is lower than the lowest representable non-null value. These computer errors can be exploited by attackers to override verification procedures, such as the ones that ensure that an account holds a minimum amount before a withdrawal is validated.
[60] For example, by exploiting the ordering dependence transaction, that is to say by altering the order in which transactions are executed. This gives a validator the ability to change the price of a transaction while it is being processed, by previously validating another transaction at a different (possibly manipulated) price.

of DeFi is that a number of transactions are automatically executed when specific conditions are met. Yet, this is a highly complex task, as data entry has to be carried out in near-real time for a wide variety of data (reflecting the wide variety of underlying investments that smart contracts can relate to: crypto-asset or traditional asset prices of course, but also weather, logistics flows etc.).

This level of complexity underlines the critical role of data providers -**oracles**- who import exogenous data flows into blockchains (it should be reminded that blockchains cannot access external databases). These oracles can be conventionally centralised entities, but they also can be decentralised applications, both from a governance perspective and in the way they collect information: volunteers are called upon to send data; the oracle synthesises the information provided into an average (that is usually weighted); the information providers are then remunerated according to how close they are to this average, which is deemed correct.

The crucial role of oracles highlights the risks that can arise from errors or fraud on their part: erroneous execution or non-execution of smart contracts, or even market prices manipulation. These errors are all the more problematic as transactions on a blockchain are almost always irreversible.

2-4. The risks related to services and uses

2-4-1. DeFi poses specific risks to retail customers

The DeFi ecosystem has attracted a significant number of retail investors in 2020-2021, seduced by the hype and "fear of missing out" (FOMO), as well as by the promise of high returns. For instance, in February 2021, the provision of liquidity in Tether within the Compound lending protocol was associated with an interest rate at 11%[61]. Furthermore, capital gains in DeFi appear to be correlated with the number of participants: this may reflect a change in the fundamental value of the ecosystem, benefiting from increased liquidity and market depth, but it may also be an indication of a Ponzi scheme.

In fact, individuals who entered this market were confronted with **high risks** of capital loss, due to the volatility of crypto-asset prices, to risks related to protocol governance (see section 2-1), to the complexity of the products offered and the proliferation of scams, theft and hacking. Yet, these users were not always fully aware of the level of risk involved in the investments they had subscribed to. The web interfaces designed to facilitate access to DeFi protocols can indeed contribute to giving users a **false impression of understanding** of complex financial mechanisms. Similarly, the transparency of the code can give a false impression of control to users who have no programming skills, or even to computer programmers with no financial skills.

The problem is exacerbated by the ease with which **highly complex products** can be coded, thanks in part to the composability of smart contracts on the blockchain. The DeFi ecosystem is characterised by the growing popularity of derivatives on crypto-assets, in various forms, which notably make it possible to take on debt with a substantial leverage effect (see below). This enables individuals to participate in high-risk contracts that are usually restricted to seasoned professionals in the world of traditional finance without any prior assessment of their financial knowledge.

[61] Annual percentage rate of charge. Source: European Central Bank (ECB), Decentralised finance – a new unregulated non-bank system?

2-4-2. The DeFi ecosystem suffers from systemic weaknesses compounded by mechanisms such as automated liquidation

a. The systemic weaknesses of DeFi

The systemic weakness inherent in DeFi stems first and foremost from the **price volatility of the crypto-assets** that are traded therein. This phenomenon can also affect assets presented as safe and stable by their developers, as illustrated by the collapse of the Terra-Luna system in May 2022. Moreover, the **DeFi ecosystem has a feedback effect on the crypto-asset market, which tends to increase its volatility**: firstly by contributing to the creation of numerous tokens (often in return for operating DeFi protocols), the fundamental value of which is difficult to estimate, often giving rise to large-scale speculative movements; and secondly, by increasing the leverage effect of players, which exacerbates the magnitude of price shocks, and therefore the risks in the event of a downcycle (see below).

Its vulnerabilities also stem from **the endogeneity of many investments**, especially given the scale of lending and borrowing activities, and the level of **concentration of the DeFi market** in the hands of a few players: a small number of protocols thus concentrate most of the value of the ecosystem (refer to section 1), while several holders of massive amounts of governance tokens (whales) have effective governance power over many protocols (refer to section 2-2-1).

Lastly, another source of vulnerability is linked to the **significant leverage effect** of many borrowers. Admittedly, loans in the DeFi ecosystem are usually "over-collateralised", meaning the collateral deposited with the lender (often a "liquidity pool") is worth more than the amount borrowed[62]. **Over-collateralisation** is a consequence of the **lack of trust** between parties to the exchange, on the one hand, and of the price **volatility** of crypto-assets on the other. A borrower who wishes to avoid the risk of his position being liquidated must constantly check the value of the collateral he has deposited and, when its value decreases, that borrower must block more tokens. This system is equivalent to "margin calls" issued by clearing houses in the traditional repo or swap markets. It has the benefit of limiting the leverage of borrowers, all other factors being equal.

Yet, **several mechanisms challenge this pattern** and explain why debt levels are often high in the world of DeFi. Firstly, the correlation observed between the value of crypto-assets and the strength of the DeFi market (see above) can lead to increased leverage (expressed in relation to the starting value of positions): the increase in the value of tokens increases the value of the relevant collateral, which in turn makes it possible to borrow more. In addition, the growth of **decentralised derivatives trading** - including in perpetual futures[63], which do not require the effective borrowing of the underlying crypto-assets[64]- allows users to achieve considerable leverage, in the order of x25[65] in early 2023 on the dYdX platform, or of x50 on the GMX platform[66].

---

[62] The level of over-collateralisation usually depends on the nature of the collateral deposited. For example, in January 2023, on Aave, over-collateralisation stood at 133% for "stablecoins" such as USDC or DAI, between 166% and 250% for other crypto-assets, and reached 600% for crypto-assets deemed low-quality.

[63] Also refer to Section 1-3 dedicated to these contracts.

[64] Other similar techniques are also used, such as the purchase of leveraged tokens, which encapsulate the desired exposure.

[65] Leverage is expressed as multiples of the assets actually held by the borrower. This way, a leverage effect by x25 means that a borrower holding the equivalent of EUR 100 in crypto-assets takes on debt for EUR 2,500. The higher the leverage, the higher the gain if successful, but the greater the loss otherwise.

[66] The levels shown here change over time; they have reached x100 in 2021.

Even in traditional finance-based borrowing scenarios, it should be noted that **over-collateralisation is far from being a fixed rule**, especially as it is **not very capital efficient**: as a result of competition, lending applications may in future offer collateralisation rates below 100%, which would then probably be associated with creditworthiness assessment mechanisms that could be decentralised themselves. In any event, **collateralisation is not a foolproof line of defence, especially when the value of all crypto-assets decreases simultaneously**. This vulnerability even tends to be exacerbated by the automated position liquidation mechanisms that are now the norm in the DeFi ecosystem.

b. Automated liquidation mechanisms in contracts can paradoxically increase the vulnerabilities of the system

In all the existing lending applications of DeFi (traditional lending of crypto-assets, lending through derivative swaps such as perpetual futures etc.), the borrower's position is liquidated when the value of that borrower's collateral falls below a given threshold. The liquidation process is then carried out with the help of a third party called a "liquidator" -usually a robot-, which reimburses the lender for the lent crypto-assets and proceeds to liquidate the collateral by charging a commission: the borrower therefore suffers a capital loss as a result of the operation (and bears the entirety of the loss alone). **This liquidation process is almost completely automated**, that is to say it is encoded in the loan's smart contract: as soon as the value of the collateral falls below a pre-determined threshold, the position is liquidated[67].

At first glance, the liquidation of positions is a protection system for the lender and the borrower. Indeed, it ensures that the lender does not suffer any capital loss, only an opportunity cost if the loan has not generated any return due to liquidation. For the borrower, it guarantees that losses remain limited: by design, maximum loss cannot exceed the value of the pledged collateral. Thus, taking out a highly leveraged loan does not increase the maximum amount of capital that can be lost by the user, but it increases the probability of losing that capital and the rate at which it can be lost.

The automated liquidation system, however, **carries the risk of a global collapse of the system**. The decrease in value of a token can trigger the liquidation of a number of positions secured by it; the automated liquidation of positions in turn leads to a significant sell-off of the token concerned, which further depreciates it[68]. This tends to lead to further liquidations and then, through a contagion effect, to decreasing the value of other crypto-assets, which may ultimately bring about a global collapse leading to major losses (including for lenders).

This risk is all the more serious as instances of **aggressive liquidation** behaviour are frequent: since they pocket a commission for each liquidation, liquidators may be tempted to provoke them, notably by speculating on the value of given crypto-assets. When they are of a sufficient size, these players thus have the ability to manipulate the market to trigger liquidations. This is all the more true when the value of a crypto-asset decreases very quickly, as users do not always have enough time (or resources) to re-collateralise their positions.

[67] More specifically, the position is "open for liquidation" by the smart contract; liquidation only occurs if a liquidator intervenes. That said, in practice, many liquidators are robots, which makes the mechanism highly automated.

[68] Similarly, in traditional finance, the repo business incurs fire sales risks.

2-4-3. The particular role played by “stablecoins” and the related risks have already prompted an initial regulatory response

“Stablecoins”[69] are now essential to the functioning of DeFi on account of the two roles they play in this ecosystem. **First, they are the settlement assets used for transactions**: stablecoins are notably widely used as collateral for crypto asset loans. In fact, given their price volatility, other crypto-assets could not readily fulfil this role. **Secondly, they are DeFi’s main point of contact with the real world.** Therefore, many users retain their holdings in stablecoins as a hedging strategy against the volatility of crypto-asset prices without having to convert them back into official currency (yet retaining the ability to do so at any time). The other way around, the leading issuers of stablecoins, who have invested some of their reserves in commercial paper and other short-term assets in the United States, became major players in this market in 2021[70]. For both of these reasons, stablecoins are a critical part of the DeFi ecosystem: within the ecosystem, the loss of parity (*depeg*) of a stablecoin (against the currency it is supposedly pegged to) has the potential to undermine the stability of many applications, as the chain effects of the Terra-Luna collapse have shown. Outside the ecosystem, stablecoins are the primary potential vector through which shocks can be transmitted from DeFi to the more traditional areas of finance.

The most significant stablecoins are currently issued by **centralised entities** (Tether for USDT, Circle for USDC, Binance for BUSD), in return for collateral deposits made in official currency. Yet, some **DeFi applications** also issue assets aimed at replicating the value of an official currency. There are two main models: firstly, **decentralised collateralised stablecoins** are issued in exchange for collateral in crypto-currency deposited by users (whereas centralised stablecoins are issued against collateral in official currency); the best-known example of this model is MakerDAO's DAI. **Decentralised "algorithmic" stablecoins**, however, are intended to meet their stability goal by dynamically adjusting the supply of tokens: depending on the level of demand, the protocol issues new tokens to increase the supply or, conversely, redeems tokens to destroy them. Each of these actions is governed by rules previously written into the protocol's algorithms. The best known example of decentralised "algorithmic" stablecoin was Terra's UST.

The **European regulation on markets in crypto-assets, also referred to as MiCA**[71]**,** is a first regulatory response to the issue of stablecoins. The regulation defines three categories of crypto-assets; among them, electronic money tokens (EMTs) refers to crypto-assets the aim of which is to maintain a stable value by reference to an official currency, while asset-referenced tokens (ARTs) seek to reach the same goal, only by reference to a basket of currencies or other types of rights or assets (such as gold, for instance)[72]. In particular, the MiCA Regulation provides that EMTs are (i) convertible at par, at any time, against their reference currency and (ii) issued by entities the reserve of which shall only contain safe

[69] They can also be referred to as "low volatility units of account". See also box 1 on semantic difficulties with the term “stablecoin”.

[70] Tether (the issuer of USDT) was able to hold up to USD 30 billion in commercial paper in the US in the course of 2021, making it the world's 7th largest investor in this market, according to JP Morgan. In 2022, Tether announced that it had switched some of its reserves to US treasury bonds, a deeper market that is therefore less prone to liquidity stress. On this topic, reference can be made to Barthélémy, Gardin and Nguyen, *Stablecoins and the Financing of the Real Economy* (Banque de France, Working paper, February 2023).

[71] The Markets in Crypto-Assets Regulation (MiCA) will come into force in 2023, and will apply in the second half of 2024.

[72] MiCA identifies, in addition to EMTs and ARTs, a third category comprising "other crypto-assets".

and liquid real-world assets. This second criterion is the only possible guarantee that the issuer will be able to reimburse its clients at any time, even in the event of a run.

However, the MiCA Regulation does not apply to services provided in a fully decentralised manner without any intermediary[73], and in particular it does not cover protocols issuing a so-called stable crypto-asset or services that use EMTs for their operation. **This gap should presumably be bridged** by establishing the following rule: **if a decentralised service claims to create or use a crypto-asset with an official currency as a reference, this crypto-asset must be an EMT** (or an equivalent asset) **within the meaning of MiCA**. The name stablecoin is a pledge of stability and security for users. As such, its use must be strictly regulated, in order to protect customers and to limit the potential contagion effects to the real world.

2-4-4. Money laundering and terrorist financing risks in the DeFi ecosystem

The lack of user identification procedures (Know Your Customer or KYC) and the lack of control mechanisms to check the origin of funds quite logically generate money laundering and terrorist financing (ML/FT) risks in the DeFi ecosystem. Indeed, on the public blockchains that serve as infrastructure for DeFi, **pseudonymity** is the rule: users are identified by way of their address on the blockchain (and/or a pseudonym), rather than by their name. Moreover, most DeFi applications operate without access control: the only requirement to participate is connecting to a wallet (refer to Section 1-6), and some of these wallets can be opened by customers without identity verification or control framework assessing the origin of deposited funds.

It should be noted, however, that **pseudonymity dos not equate to anonymity**: the operations carried out from each address are recorded in the blockchain and, insofar as public blockchains[74] are used, these actions are publicly traceable, which is usually not the case in the world of traditional finance. This means addresses can be identified as malicious or suspicious by the user community. In fact, a form of self-regulation is already at work in the DeFi ecosystem, that is essentially exercised through the practice of sharing lists of addresses of malicious users and services (black lists), which are mainly exchanged via social networks. On the basis of this information, as well as the links that can be traced between addresses on the blockchain, specialised companies[75] offer risk analysis services for blockchain addresses or DeFi protocols. Traceability is nevertheless limited given how easy the address creation process. Furthermore, it can be hindered by the use of various techniques (mixers[76], chain-hopping[77], assets with enhanced anonymity). According to the Financial Action Task Force (FATF), digital assets have fostered the considerable growth of certain areas of crime, especially ransomware[78] (ransoms being almost systematically paid in digital assets).

[73] However, the regulation provides for a report to be drawn on the compliance of DeFi with European Union law within 18 months of its entry into force.
[74] In contrast, the development of layer 2 solutions (see above) tends to reduce transparency of information.
[75] Examples include ScoreChain, Chainalysis.
[76] Mixer platforms pool the assets of various users into a single "pool", which then redistributes the amount deposited to each member, making the funds more difficult to trace.
[77] The act of switching from one infrastructure to another, or from one digital asset to another, often in quick succession, in order to evade tracking attempts.
[78] FATF, *Countering Ransomware Financing*, March 2023.

III. Avenues for a regulatory framework

When a financial activity based on technological innovations emerges, regulators first try to determine to what extent that activity should be considered a novelty, and whether it presents specific risks. Indeed, being technologically neutral, financial regulation should essentially be risk-based, as summarised by the phrase "same activity, same risks, same rules".

DeFi, based on blockchain infrastructures, has characteristics that make it **difficult to assimilate with "traditional" finance**. More specifically, traditional finance is critically reliant on a number of **intermediaries** (banks, insurance companies, clearing houses, etc.), which carry out key operations and manage the associated risks, and on which the bulk of the regulatory burden logically falls. However, the very concept of DeFi consists essentially in building an area of finance without intermediaries or trusted third parties (although it has been shown in sections 1 and 2 that this promise is not always kept), which in turn generates specific risks. When tackling this development, two pitfalls must be avoided.

The **first pitfall lies in trying to replicate the existing regulatory framework only and exhaustively**, without taking into account the specific characteristics (and therefore the potential benefits) of DeFi. This tempting approach leads to **restricting the focus of analysis to the identification of intermediaries** to whom requirements should be applied –and there are in fact intermediaries in DeFi, although not necessarily at all levels. This approach may therefore have its limits: this report therefore proposes **to explore other types of solutions as well**, drawing in particular on **non-financial regulations**, such as those governing product safety in the European Union (EU). In these particular regulations, a number of requirements are placed directly on **products**, thus building a chain of obligations for all players involved in their manufacture and distribution, which may notably lead to substitution mechanisms when one of these players is located outside the European Union. Thus, this paper proposes a certification system for smart contracts, which would apply to the product itself, without the need to define a person that would be directly responsible for compliance with this obligation. If no one wants to have a product certified, that product will simply not be distributed. This makes it possible to define a set of products deemed "safe", which will be the only ones that can be offered by the intermediaries ensuring access to DeFi services for the greatest number of people.

The opposite pitfall lies in thinking that, faced with the decentralised nature of DeFi and the lack of territorial embedding[79] of its protocols, **regulation is necessarily powerless**. Firstly, this would mean taking all the promises of DeFi at face value; in reality, **decentralisation is far from being a given** in the DeFi ecosystem, while some centralised actors play key roles. Secondly, it would also equate to **underestimating the regulatory capacity of public authorities**: the fact that a few individuals with specialised skills can gain access to DeFi services is not the main issue at stake (in the same way that regulation of the internet is not rendered useless by the existence of the dark web). The main concern is access to DeFi for the general public, on the one hand, and for institutional players, on the other. To return to the example of mandatory certification of smart contracts: if the vast majority of individual

[79] This paper does not intend to underestimate the problems linked to the extraterritoriality of DeFi services, which raise the question of the capacity to regulate the players effectively. As regards intermediaries, the problems of extraterritoriality arise in the same way in DeFi as in traditional finance. It may be noted that intermediaries providing services do not always seek to establish themselves in the least favourable territories from a regulatory point of view, because they need to gain the trust of their clients. But these issues may also concern the nodes of the blockchain infrastructure (in particular the nodes that validate transactions, see section 3-1), or even the application managers. Nevertheless, the avenues proposed in this document seem likely to reduce the problems posed by the possible extraterritoriality of the various actors.

users are in practice prevented from accessing unlabelled protocols, and if companies know that they incur fines and reputational damage in the event of infringement, such a measure is indeed likely to have tangible effects.

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

Further developments in DeFi in the future would require strengthening the security and resilience of the blockchain infrastructure. This can be addressed through two main types of regulatory scenarios, depending on the degree of criticality of the infrastructure and the degree of commitment of public authorities.

Regulatory scenario A: an infrastructure based on public blockchains, but subject to regulation or even oversight

In a system based on public blockchains, trust between players is not the element that guarantees the soundness of the infrastructure, that role being performed by the automated rules of the game. The main advantage of this form of organisation is that it is open and accessible to all: anyone can decide to participate in the network, or even to become a validator node. Moreover, service providers can build their project on an existing infrastructure, which they do not need to manage or maintain.

However, public blockchains should be regulated by way of a number of **minimum standards**[80], 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). With regard to the **risk of failure**, the security standards could provide for the underlying code to be certified *a priori*, either by way of human audits or using formal methods (refer to section 3-2 on the certification of computer code for DeFi applications, which may be broadly applicable to blockchain infrastructure).

Since the risk of a group of attackers taking control of a network (a "51% attack") is all the higher when the number of nodes is low, a logical response could be to set rules on the **minimum number of validators** required in a public blockchain. However, this may cause **issues in terms of competition**: if transactions -or transactions exceeding a given volume- were to be prohibited on blockchains that are too small, it would be difficult for them to grow to reach the minimum size required. More to the point, it should be noted that this competition issue already exists, as it does in any industry generating network effects, therefore setting rules would merely accentuate it.

In any case, public authorities should pay close attention to the **degree of concentration of validation capacities** on public blockchains, as soon as the infrastructure concerned reaches a certain level of criticality -this applies indifferently to all infrastructures: layer 1 blockchains, but also rollups, sidechains, nested chains, shards etc. The state of concentration of validation capacities (protocol token holders and delegated validators) should be monitored at all times, and **caps should be set** on concentration in order to guarantee the security of blockchains. It should be noted that in order to avoid indirect control phenomena, such a measure would require the lifting of pseudonymity, in order to be able to group together the various addresses of the same individual or company; it would also require exhaustive knowledge of the capital holders of each company with governance tokens.

[80] In order to avoid overly constraining emerging projects, this regulatory framework could be proportionate to the size (number of nodes, value handled, etc.) of each blockchain.

However, in the event that alert thresholds were exceeded on a public blockchain, various intervention mechanisms would have to be devised to prevent fraudulent use of the infrastructure. The first step could be **advanced communication**, especially to application managers and users. A warning indicator could also be included on the interfaces of each of the services relying on this infrastructure. These warnings would allow users of the targeted blockchain to withdraw their assets and move them to other blockchains. Be that as it may, **a shutdown of the infrastructure cannot always be implemented**: as it is a public blockchain, it requires widespread agreement across the validator nodes. For crypto-assets locked in contracts, however, it could be envisaged that, beyond a given alert level, the authorities concerned would order a resolution mechanism (immediate termination of current contracts, reimbursement of funds). It would then be necessary for the regulation of smart contracts to provide for such mechanisms (refer to section 3-2). Lastly, public authorities could operate an **archive node** on public blockchains: this node would not participate in validation processes, it would only contribute to the recovery of information if the chain ceased to function following attack or failure of the system.

Regulatory scenario B: an infrastructure based on private blockchains

Another way to address the security and efficiency challenge posed by public blockchains would be to switch purely financial functions to **private blockchains**[81].

Unlike in public blockchains, the functioning of private blockchains relies on **trusted players**, each of them being clearly identified and approved by the governance of the infrastructure, which has two main benefits. Firstly, in terms of efficiency: with fewer nodes and simpler consensus mechanisms, these infrastructures can process transactions more quickly. They also update their operating rules (security, consensus algorithm, technical upgrades, etc.) more quickly because the decision-making process is faster and less extensive than that of public blockchains.

Private blockchains also have an **edge in terms of security**: by filtering the members authorised to participate in the network, they limit the presence of malicious users. The risk of a hostile takeover is therefore almost eliminated, whereas corruption of a public blockchain by way of a 51% attack is always possible.

The drawback of an architecture based on private blockchains is that it **limits** composability and therefore **the capacity for innovation**. However, it should be noted that the efficient coexistence of private and public blockchains is not an unreachable goal, as long as the issue of securing the points of connection is resolved.

Private blockchains could be **operated by various types of trusted players**. First of all, they could be **private players** either recognised or accredited by public authorities. Banks or banking consortia could, for example, operate such blockchains, but it is also possible that innovative start-ups (Fintechs) make blockchain administration their core business. Non-financial players could also operate blockchain infrastructures. For instance, telecommunication operators, digital service companies (DSCs), or

[81] In this context, private blockchains should be understood as referring to blockchains to which access is only open to authorised users. Thus, each new member must be co-opted by the already existing members, and has differentiated access rights to shared data. In addition, only certain members of the network may fulfil the role of validator. On public blockchains, some applications can be "permissioned", meaning its use is restricted to specific preselected users; however, the validation of blocks remains tasked to validators across the entire network.

industrial players[82] could develop expertise in this technology due to specific business needs (logistics, etc.).

Private blockchains operated by private players could fall under a specific **supervisory framework**, similar to the one that currently exists in the euro area for retail payment systems (refer to box 3). Compliance with a number of rules would be monitored on an ongoing basis, and reporting requirements would be imposed on blockchain administrators, giving rise to recommendations and public warnings[83]. It should be noted that, in such a supervisory framework, blockchain administrators must be located on national or European territory.

Box 3: The PISA framework (Payment instruments, schemes and arrangements)

At the end of 2021, the Eurosystem published a framework for the oversight of electronic payments, known as "PISA", which will enter into force at the end of 2023. Indeed, the smooth operation of payment systems is one of the missions entrusted to the Eurosystem.
This framework establishes a set of oversight principles, based on international standards, to assess the safety and efficiency of electronic payment instruments, systems and arrangements:

- The notion of electronic payment instruments is understood in a broad sense and includes credit transfers, direct debit, payment cards, electronic money transfers and electronic payment tokens (such as the crypto-assets used in a stablecoin system).
- A scheme is a set of formal, standardised and common rules for the transfer of value between end-users through electronic payment instruments. It is managed by a governance body.
- An arrangement is a set of operational features that support the end-users of several payment service providers in their use of electronic payment instruments. Arrangements are managed by a governance body which, *inter alia*, decides on the relevant rules or terms and conditions.

The PISA framework is aimed at the governance bodies responsible for such schemes that have reached a significant degree of significance for the euro area. It is based on a methodology for assessing compliance with the supervisory principles defined by the Eurosystem. All supervised undertakings will therefore be invited to submit self-assessments and benchmark documents, which will form the basis for an ongoing dialogue between them and the supervisor.

Another possibility would be for **public institutions to operate the blockchain infrastructure directly**. This could be justified, for instance, if a significant share of finance were to become tokenised. These public institutions would logically be European rather than national; they could be European entities created specifically for this purpose, or partnerships between public players in a scenario involving a European sovereign blockchain[84] the use of which would go beyond financial matters alone; the central banks of the Eurosystem could also play that role. In traditional finance, the Eurosystem currently operates Target 2 (interbank payments) and Target 2 Securities (securities settlement) systems. Such a scheme could be all the more relevant as wholesale central bank digital currencies (CBDCs) could

[82] In France, industrial players are already providing the technical infrastructure used to host the nodes of certain blockchain networks. The operation of a blockchain at an industrial level requires physical infrastructure with minimum quality standards, in order to be able to ensure a given level of service on a continuous basis.
[83] The European Commission has initially proposed that decentralised financial actors should comply with such a supervisory framework on a voluntary basis (European Commission, June 2022, *Decentralized finance: Information frictions and public policies*).
[84] On this topic, refer for instance to the European EBSI project

also emerge in the future: central banks could then be managers of integrated systems providing liquidity to financial players and digital wallet custody services.

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

3-2-1. The limitations of existing certification solutions

Firstly, the fact that the **code[85] behind smart contract is public** is sometimes considered to be an effective way of avoiding hacking risks (principle of security through transparency). It allows communities of developers to identify and report fraudulent or vulnerable programs. However, these exchanges take place on specialised forums and do not necessarily reach less sophisticated users. Furthermore, the public nature of the code does not always allow vulnerabilities in a computer program to be spotted in time, as the major *Log4Shell* security breach in open source software has shown. Publication of the code can even have the effect of allowing attackers to find vulnerabilities. Lastly, it should be noted that the ability to review that computer code is not a guarantee that the financial mechanisms at work in a smart contract are understood.

A common way for developers to address these vulnerabilities **is to have their protocols tested by the community** of developers and knowledgeable users in order to detect vulnerabilities. This is done through the bounty reward system (also referred to as bug bounty system), which rewards people for finding design flaws.

A more regulated version of this practice consists in conducting **an audit of the code** behind smart contracts[86]. This audit is carried out by players specialising in IT security, such as consulting firms. But the demand for certification is very high, which may lead to a shortage of skilled personnel in this field[87]. Furthermore, code auditing is not an easy task: a recent Cornell University study[88] found that only 15 to 55% of developers (depending on their level of experience) were able to identify vulnerabilities in a smart contract after conducting a thorough audit.

As an alternative solution, the code of smart contracts could be tested with a **formal proof** mechanism. These methods analyse the semantics of programs, meaning the formal mathematical description of the purpose of a given program, which is provided in its source code. The main idea is to check that the program under review performs the tasks for which it was designed, and that it does not allow a number of actions identified as dangerous.

The potential of formal methods lies in the fact that **they can be automated**, which theoretically allows for almost infinite scaling, whereas human auditing does not. However, their use is not yet

[85] It should be noted that the code of some smart contracts is only partially public.
[86] The OECD has made a similar proposal (*Why DeFi (DeFi) Matters and the Policy Implications*, January 2022*)*
[87] This may lead to new players, who are not necessarily experienced, to offer audit services.
[88] Tanusree Sharma, Zhixuan Zhou, Andrew Miller, Yang Wang (University of Illinois), Exploring Security Practices of Smart Contract Developers, April 2022.

widespread[89], partially owing to their high cost[90]. In addition to the issue of the limited number of dedicated experts, formal methods generally assume that smart contracts have been written in a **compatible programming language**, which is currently far from being the norm. These methods have also been the topic of a more fundamental criticism: while they make it possible to check that a program complies with a set of specifications, it would still also required to be able to check the validity of these specifications[91].

If they is no silver bullet, **formal proofing and human auditing methods present, as we can see, complementary strengths**; their combined use offers a promising avenue. Furthermore, it should be noted that code verification and the practice of improving code is of interest to smart contract developers, users, and blockchain administrators alike; this alignment of interests is likely to lead to the emergence of communities working together to detect vulnerabilities.

3-2-2. Certifying the computer code used in DeFi applications

Given the numerous attacks recorded against smart contracts, and in order to decrease the technological and counterparty risks, a logical avenue for regulation would be to define the **scope of protocols deemed "safe"** (at least for a given state of technical knowledge). This set of protocols would establish the list of smart contracts whose computer code has been **certified**. It should be immediately noted that the system described below would only apply to smart contracts that do not present an issue in terms of underlying principles; it should not be possible to certify a smart contract that provides services deemed dangerous.

a. What would having the code certified entail?

Certifying computer code consists in going through the source code of a program to check that it really performs the tasks for which it was designed, and that it does so in compliance with a given number of security standards (refer to section b below concerning the setting of standards). Certification is not necessarily binary, and it may include several levels of security[92], like the security visa created by ANSSI (the French information system security agency). In any case, it is carried out by **specialised assessors**, who would perform a human auditing process, use formal methods, or a combination of both. In its broadest acceptation, **certification includes three key dimensions**: **static analysis** makes it possible to detect formal errors in programming or design; **dynamic analysis** focuses on monitoring the execution of the program; finally, **software composition analysis** (SCA) makes it possible to draw up an inventory of the external dependencies of the program under review to third-party libraries or open source components.

[89] Among the use cases, Nomadic Labs (developer of the Tezos blockchain), for instance, has created Mi-Cho-Coq, a formal verification framework for smart contracts.

[90] So far, formal methods have mainly been used in the development of algorithms in fields especially concerned with human safety, such as in transportation.

[91] This issue was brought to light by a security breach on the Dexter exchange platform (Tezos blockchain). Nomadic Labs had announced the successful completion of its formal verification process, but the specifications tested themselves contained vulnerabilities.

[92] The idea of a security scale is also mentioned in the French cyberscore Act (also referred to as “loi Lafon”) of 3 March 2022, which establishes a "cyberscore" enabling Internet users to find out how secure their data is on the websites and social networks they use.

In the DeFi ecosystem, the software composition analysis component takes on particular significance. Indeed, it is very frequent for a smart contract to call a number of others so as to use their functionalities. This modular form of architecture, in which smart contracts are "stacked" on top of one other, is a characteristic feature of the DeFi ecosystem, and calls for a simple rule to be set: **the certification of a smart contract requires the prior certification of all the called components**[93].

Like any other authorisation mechanism, certification has a **life cycle**, a fact that prompts the statement of **three general rules**. Firstly, it must be possible to **withdraw certification at any time**, for instance if a new security breach is discovered. Secondly, certification must be granted for a **limited period of time**, in order to accommodate developments in computer security techniques. Thirdly, if certification reflects a given state of computer knowledge, it also reflects a **given state of the program under review**. Smart contracts are supposed to be immutable in the blockchain. In reality, however, it is possible to modify them -to fix vulnerabilities, for instance- without necessarily creating a new program: this can be done using call mechanisms (through proxies), or using configurable smart contracts. This is not an issue that is specific to DeFi: any audited code base may contain configuration parameters and tends to undergo regular updates, potentially making certification obsolete. One possible solution to this typical problem lies in defining what constitutes a **significant change to code**, and in **making it compulsory to go through the certification process again** whenever an update meets these criteria.

It should be noted that, if DeFi were to become more regulated in the future, smart contracts could directly embed a number of regulatory requirements in their code[94]. This would be an effective way to ensure compliance on an on-going basis[95]. Code certification could then include verification of the correct translation of legal provisions into computer language.

b. Who would be charged with setting the security standards?

In a first scenario, security standards would be **set by the market participants themselves**. In this kind of setup, the standards adopted tend to be close to market realities, which guarantees their acceptability and facilitates their implementation. However, this presupposes that the private players, who are usually competitors, agree on common standards. For their part, public authorities can promote the adoption of these standards.

In a second scenario, **public authorities set the standards themselves**[96]. This usually has the advantage of ensuring that the standards chosen meet public interest objectives, and allows for the resolution of disagreements between market players or segments. In practice, standards set by public authorities are generally discussed jointly with market players in order to ensure their practicability.

It should be noted that such a scenario does not necessarily give public authorities the duty to certify compliance with these standards themselves: the method consisting of entrusting product certification

[93] This criterion is necessary but not sufficient in and of itself: the assembly of certified smart contracts does not guarantee the proper functioning of the whole set. For further information on this topic, refer to the case of Chainlink during the Luna shutdown, which is discussed in section 3-2-3.

[94] Rafael Auer (2022), *Embedded Supervision: How to Build Regulation into DeFi*, CESifo Working Paper Series 9771.

[95] The Monetary Authority of Singapore (MAS) put forward the idea of "institutional grade DeFi protocols", which would embed regulatory safeguards into their code (press release published in May 2022: *MAS Partners the Industry to Pilot Use Cases in Digital Assets*).

[96] In addition, these standards may go beyond technical aspects, for instance by integrating good governance considerations.

to a group of private sector laboratories carrying out their tasks under the oversight by a public supervisory authority[97] is broadly used in the field of product safety (refer to box 4 on the AI Regulation).

c. Which consequences would a lack of certification bring?

Once again, in this case, there are two main options to consider. In the first case, **lack of certification would only be discouraged**. In order to provide their clients with reassurance regarding the potential risks of theft or fraud, some intermediaries (DASPs) would choose to work exclusively with certified protocols; as a guarantee of professionalism, certification would therefore become a selling point. In order to make it visible, certification could be referenced on each protocol or on each blockchain; more sophisticated techniques could also make it possible to integrate certification-related information directly in the smart contract itself. For their part, public authorities would highlight the usefulness of certification as a mechanism for preventing risks to customers in their communication, especially when addressing the general public. If the practices upheld by the most virtuous players are gradually adopted by the entire market, certification may become almost effectively mandatory. In this incentive-based regulation scheme, however, there is a possibility that virtuous practices will not spread due to the associated costs.

According to another option, **interactions with uncertified smart contracts could be prohibited**, whether because certification has not been requested or because it cannot be obtained. Such a ban would apply to both individuals and firms, whether they are trading platforms, DASPs, institutional investors, banks or non-financial companies. For regulated entities, certification would be monitored by financial supervisors. Any proven interaction would give rise to a sanction (fines, bans from future involvement...).

It should be noted that in this scenario involving bans, the law would impose **specific obligations on the "smart contract" object, as a product** -in the model of the AI regulation (see box 4)-, even though the criminal or civil liability of the developer (individual, legal unit, etc.) could not be engaged, either because such developer could not be identified or because sanctions could not be imposed on that developer (territoriality issue).

[97] The French national information systems security agency (ANSSI) already certifies IT security professionals based on the same principle.

Box 4: The draft European regulation on artificial intelligence (AI)

In April 2021, the European Commission proposed a draft regulation aiming at ensuring that the AI systems used in the EU are safe, transparent, ethical, unbiased and remain under human control. In line with the GDPR, this regulation focuses on the potential effects on individuals and the infringement of their fundamental rights.

The draft regulation is partially inspired by European regulations on product safety (which apply for instance to toys, motor vehicles etc.). Thus, while some of the requirements introduced by the regulation concern market participants (suppliers, users, importers, etc.), others relate directly to the developed or marketed products themselves (in this case, AI systems). This kind of structure may constitute a source of inspiration for DeFi, in which some of the products are not provided by an individual or by an identified legal entity.

In addition, to certify the compliance of AI systems with the requirements set by the regulation, the draft text provides for the use, in certain sectors, of third-party assessors, approved by the public authorities for sectoral supervision. This is yet another organisational aspect that is typical of product safety, which makes it possible to increase oversight capabilities while creating an industry dedicated to such assessment. While this method of oversight is seldom used in financial activities, it already exists in the field of IT security (security certification by ANSSI), and could inspire the supervisory architecture of DeFi.

d. Who should pay for certification?

Having computer code certified by specialised bodies entails specific costs, which inevitably raises the question of which actors should bear them. Two main models can be envisaged in this case, each with their own set of benefits and drawbacks. Firstly, the costs of certifying a smart contract could be **borne by the developer or manager of the relevant program,** that is to say the provider of IT services. There would be a clear economic incentive to pay this cost: it would allow for the product to be more widely used, which can be profitable both directly and indirectly. However, when developers are natural persons, the cost of certification may seem excessive[98]. It should be noted that smart contract providers will frequently be able to re-invoice all or part of the cost of certification to users, by charging a fee for each use of the service.

Another possible approach would involve **having the users of smart contracts**, that is to say, for the most part, the platforms acting as intermediaries, **pay certification costs directly** (refer to section 3-3-2). This solution would also follow an economic rationale: the service would be paid by the agents who need it. Moreover, this solution would also be more parsimonious, since it would only lead to the certification of the smart contracts whose use is attractive for at least one player. Lastly, since the intermediaries concerned are commercial companies, this means they can afford to pay for certification costs. Yet, such a system suffers **two shortcomings**: firstly, it may lead to a tendency to favour "older" smart contracts that have already been certified rather than opting for new ones, which may deter innovation and could lead to the use of less secure programs (under the assumption that "new" smart contracts are more secure than older ones, even if the latter are certified). Secondly, this system tends to generate free-riding phenomena, creating either a risk that certification will be

[98] The issue seems less significant when, as is often the case, the development of smart contracts is mostly driven by a foundation or a commercial entity, such as the company Aave Limited for the smart contracts used in the Aave protocol.

blocked (if each intermediary waits for the others to pay for certification in order to use the products free of charge), or a risk of unfairness in the distribution of costs between intermediaries[99].

Another way of getting users to contribute while avoiding the abovementioned shortcomings would be to **fund certification by means of a tax paid on transactions** carried out by smart contracts (meaning a levy paid in crypto assets for each order placed). This tax would be paid into a joint fund set up for the ecosystem, which would prevent developers of new projects from being constrained by the cost of certification (creators would always bear part of the cost, in order to discourage misuse).

3-2-3. Data provision in the DeFi ecosystem

As a first step, it seems necessary to **assess the risks associated with the decentralised oracle model**. Theoretically, the most accurate data does not always correspond to the weighted average of the information provided; the provision of data requires expertise. Above all, decentralised oracles presents a risk of collusion on the part of the associated information providers, whenever a data item is only provided by a limited number of nodes in the oracle. The same applies when the weight given to an information provider depends on its past "reliability": any player with a high weighting vector due to the first n pieces of information provided may have an incentive to tamper with the relevant information the $(n+1)^{th}$ time. Moreover, due to their highly automated nature, decentralised oracles present significant operational risks. Chainlink, for instance, which provided the price of LUNA, stopped working when the Terra ecosystem was shut down[100], sending a quote at USD 0.10 (hardcoded), even as the actual quote plummeted to 0.01 and then to 0. Users who noticed the discrepancy between the actual price and the price sent by Chainlink in some platforms, such as Blizz Finance, took advantage of this to buy significant amounts of LUNA at USD 0.01 and use it as collateral, then valued at USD 0.10, in the borrowing of other crypto assets.

A solution to this problem could be devised based on a decentralised oracle **certification system**, similar to the one described in the previous section, but with a **particular focus on the consensus mechanism** leading to the final result (weighting of various sources for example). **Introducing a circuit breaker** on the data supply is also an interesting feature, but it would then have to be combined with a mechanism designed to shut down applications that use the oracle.

Another way of injecting data into the DeFi ecosystem is through **centralised entities**. However, the latter are not immune to operational risks, nor to market manipulation risks. In traditional finance, regulation essentially relies on "**market discipline**": errors or failures are reflected in reduced customer trust, leading to financial losses or even bankruptcy. However, this model relies on the existence of well-established data providers with expertise and significant resources dedicated to quality control. Furthermore, this form of regulation is associated with deficiencies such as that fact that it leads to sanctions delivered *ex post facto*, which does not necessarily prevent failure from occurring and potentially leading to serious consequences. This concern is especially salient for the DeFi ecosystem: the provision of information automatically triggers the execution of contracts, the outcome of which is final on the blockchain.

[99] This is not an altogether new concern: for instance, the MiCA Regulation provides that a platform wishing to market a crypto-asset issued outside of the EU must write the white paper itself; other platforms can then in turn use the same white paper to market that crypto-asset; platforms can agree on contractual arrangements with each other to deal with this free-riding issue.

[100] Due to a circuit breaker embedded in its code in the event of severe price turbulence.

It could therefore be argued that the regulatory model of traditional finance is not suited to the specific risks faced by DeFi. This would support the establishment of a **framework dedicated to the supervision of (centralised or decentralised) data providers** by public authorities[101]. This framework could be incremental, and regulate the production of financial data based on thresholds set on their use by smart contracts, following the same lines as the model provided in the 2016 European Union Benchmark Regulation[102], which was established to address documented instances of market manipulation using benchmarks such as Libor. According to the Regulation, entities responsible for the provision of financial benchmarks must be authorised or registered by public authorities in charge of market supervision, according to the level of criticality of the provided benchmarks (assessed in terms of the value of the contracts that refer to them), and fall under such authorities' supervisory remit. This regulation introduces rules on governance arrangements, internal control arrangements and the prevention of conflicts of interest, which could be extended to the data supply market in the DeFi ecosystem.

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

3-3-1. The creation of statutes for selected service providers

The mechanism for certifying or prohibiting smart contracts may have limitations. Indeed, **in the case of sensitive services** -be that in terms of customer or systemic risks-, **it may be necessary to impose restrictions** or require *ex-post* corrective measures, **which cannot be anticipated when the algorithms are designed**. In such case, an alternative or complementary approach to the certification of smart contracts would be to **identify the players who are responsible** for providing these DeFi services and **capable of exercising the minimum level of control** required for their correction or termination[103].

This **partial "recentralisation" of services deemed sensitive** could be achieved in a number of ways. Firstly, consideration could be given to **requiring players that exercise effective control** over sensitive services, for instance the holders of a significant amount of governance tokens for a given DeFi application, or the holders of the administrator keys of a protocol, **that they incorporate**, becoming subject to oversight, or to facilitate recognition by judges of "*de facto* corporations"[104], at the request

[101] The European Commission puts forward a proposal for the introduction of a specific legal framework governing the operation of oracles with a view to improving their efficiency as well as user confidence (Decentralized Finance: information frictions and public policies, June 2022).

[102] European Regulation 2016/1011 on indices used as benchmarks in financial instruments and financial contracts or to measure the performance of investment funds

[103] In some cases, it could be a founder who does not hold a significant amount of governance tokens but has the power to influence the community.

[104] In French law, a "*de facto* corporation" (*société créée de fait*) refers to a situation in which two or more persons have acted as partners in practice, without having expressed willingness to establish a partnership (this type of venture should not be confused with a "*société de fait*", which is a company that had actually been registered but the incorporation of which has subsequently been annulled by way of a court decision). Article 1873 of the French Civil Code specifies that its legal regime is that of joint ventures. Therefore, the "*de facto* corporation" established this way has no legal personality, but this characterisation, which is established by a judge, confers rights and duties to the individuals considered as partners in the corporation, who are notably held personally and jointly and severally liable vis-à-vis third parties.

of the relevant authorities. **An alternative option would be to subject players exercising effective control[105] over the service[106] to direct supervision**.

The requirement to set up an entity responsible for DeFi services could also be an opportunity to **establish a legal status for DAOs** that would allow them to be subject to supervision, among other things. On this particular point, we would refer to the ongoing work carried out by the HCJP (see box 5).

Thus, without calling into question the decentralised operation of DeFi, the participants in its decentralised governance would be subject to regulations inspired by traditional finance.

Box 5: Research carried out by the HCJP on DeFi

The Legal High Committee for Financial Markets of Paris (HCJP) is composed of lawyers, academics and other qualified individuals. It includes representatives from the Autorité des marchés financiers (the French Financial Markets Authority), the Banque de France and the ACPR. It conducts and releases legal analyses. In 2022, it has been called upon to consider issues raised by DeFi from the standpoint of French law. This analysis will focus primarily on the legal status of DAOs. The HCJP is expected to deliver its conclusions at the beginning of the third quarter of 2023. Its report will, jointly with this discussion paper, provide input for the ongoing debate on DeFi at the European level.

3-3-2. Controlling access to DeFi to protect customers

It is technically difficult for a user who is not a programmer to interact directly with a smart contract. As a result, the bulk of the general public's interactions with DeFi protocols currently take place[107] - and will probably continue to do so in the future- through intermediaries. These intermediaries are currently organised into two main categories: **the (centralised) providers of crypto-asset services, and the (front-end) web interfaces of decentralised protocols**. In France, centralised service providers include players that are currently registered as **digital asset service providers (DASPs)** under the framework laid down in the 2019 PACTE Act. Web interfaces, however, which provide a means of interaction with decentralised protocols without communicating through computer code, are not currently subject to any particular regulation[108].

Therefore, stricter regulation of access to decentralised financial services in order to reduce the many risks they entail, especially for individual investors, would logically require a **strengthened supervisory**

[105] A similar line of reasoning was applied by the FATF in 2021: a DeFi application is not as such a virtual asset service provider (VASP), since the FATF standards do not apply to the underlying software or technology. However, the creators, owners and operators of a DeFi mechanism, as well as all persons exercising control of or significant influence over that DeFi mechanism may constitute VASPs for the purposes of the FATF, even where these mechanisms appear to be decentralised. This remains true even in cases where other parties play a role in that service, or if parts of the process are automated.

[106] Several institutions have made similar proposals: the OECD in January 2022 (*Why DeFi (DeFi) Matters and the Policy Implications),* the ECB in April 222 (*DeFi – a new unregulated non-bank system?)* and the IMF in September 2022 (*Regulating the Crypto Ecosystem - The Case of Unbacked Crypto-Assets*).

[107] It has been found that only an estimated 2% of the addresses on Ethereum interact directly with DeFi protocols.

[108] In the specific case of decentralised web interfaces, it would appear necessary to apply the reasoning described in section 3-3-1 to the persons who are *de facto* responsible for the interface.

framework for intermediaries providing access[109]. In order to be effective, this framework should include two key elements. Firstly, intermediaries must prevent investors (especially individuals) from interacting with fraudulent or dangerous protocols (**duty of care**) or from engaging in excessive risk-taking (**duty of advice**). Secondly, the risk-taking of intermediaries must itself be monitored by the supervisory authority, in order to limit bankruptcies and contagion effects such as those that were observed in 2022 (refer in particular to box 6 on the risks associated with "intermediated DeFi"). In this context, the **links and interdependencies** between the various (centralised) providers of crypto-asset services should be better identified, especially when they are controlled by the same persons or groups of persons (on the subject of "crypto conglomerates", see box 6). This would prevent conflicts of interest between these players, but also reduce systemic risk[110].

Box 6: Specific risks associated with decentralised intermediated finance (CeDeFi) and "crypto-conglomerates"

The recent failure of several intermediaries providing lending and trading services in crypto-assets (Celsius Network, FTX and Alameda Research) have highlighted vulnerabilities stemming from excessive risk-taking (especially through excessive leverage), excessive maturity transformation, or simply fraud. In the case of FTX, excessive risk-taking was primarily linked to the platform's fraudulent interdependencies with its sister company Alameda Research: crypto-assets deposited by third parties with FTX were then lent to Alameda Research so that it could remunerate its own investors and managers.

In order to offer high returns and attract deposits, players like FTX did not just hold crypto-assets, but also engaged in risky investment strategies. While these players are ultimately engaged in activities akin to traditional finance, they are not currently bound by prudential, internal control or risk management requirements. As a result, in the event of a crisis, these players can suddenly interrupt their services and freeze clients' funds.

On a broader level, beyond the matters of fraud and governance, the "crypto conglomerate" model seems to present financial vulnerabilities: the vertical integration of various functions, in particular, make it easier for leverage and liquidity imbalances to accumulate (with little transparency), generating systemic risk.

The **European MiCA Regulation** is expected to strengthen the supervisory framework applicable for intermediaries (see box 7), now referred to as "**crypto asset service providers" (CASPs)**. However, as the regulation excludes fully decentralised services from its scope, it is currently unclear whether it will apply to service providers that would exclusively provide services on crypto-assets originating from DeFi. **It would therefore appear appropriate, as a first step, to explicitly extend the scope of the provisions of the MiCA Regulation concerning CASPs to DeFi intermediaries**[111].

[109] A balance should be found between the approaches mentioned in sections 3-3-1 (regulation of sensitive service providers) and 3-3-2 (regulation of intermediaries providing access), one that takes account of the balance of power and the effective capacities of the various players involved. As things currently stand, the regulation of access providers appears to be a high priority. There may, however, be some proportionality issues for smaller intermediaries.

[110] In this respect, the collapse of FTX has led the Financial Stability Board to add to their research agenda for 2023 work on crypto-conglomerates (referred to as : "multifunction crypto-asset intermediaries").

[111] The OECD has made a similar proposal (*Why DeFi (DeFi) Matters and the Policy Implications,* January 2022*).*

At the very least, the regulation could require each intermediary to publish a white paper setting out the characteristics of all the crypto-assets on which a service is provided[112], and to implement a KYC mechanism. In any event, in order to prevent the regulation from giving rise to unequal treatment, **this extension should apply to all players** that facilitate users' access to DeFi services: they should all be governed by a common regime, depending only on the nature of the services provided (and possibly their volume), and not on the technical system used for their provision. Among other things, this would mean that **web interfaces would also be required to carry out standard customer identification procedures (KYC)** before providing access to decentralised services. In more general terms, all providers of access to DeFi would be subject to rules of good conduct -for instances, rules prohibiting the manipulation of customers' crypto-assets without their knowledge- and would be required to meet prudential requirements, with a view to reducing the risk of bankruptcy.

Secondly, while it would not be achievable -and perhaps not advisable- to provide for a guarantee that DeFi services users would not suffer any financial losses, regulation should nevertheless aim to **limit the risk-taking of users**, and especially the least informed among them. From this point of view, and in addition to the requirements laid down by MiCA, **it seems essential that access to financial products should depend on the financial skills of customers and their risk appetite**. Furthermore, financial literacy should not be assessed subjectively by the users themselves, but objectively through questionnaires, along the lines of the ones provided for in MiFID2[113] for investor profiling purposes. For example, intermediaries should restrict the ability to invest in complex products -such as highly leveraged loans through contracts on perpetual futures- to very experienced users, or even to professionals. Lastly, and even for the latter categories of users, regulation should set a maximum leverage effect, along the lines of the rules issued in 2018 by the European Securities and Markets Authority (ESMA), which sets maximum leverage at x30 in CFD trading.

[112] The requirements included in the white paper as provided for by MiCA could be adapted to take into account the specific characteristics of DeFi.

[113] Directive 2014/65/EU of the European Parliament and of the Council of 15 May 2014 on markets in financial instruments.

Box 7: The obligations of crypto-asset service providers under the MiCA Regulation

The MiCA Regulation sets that the provision of crypto-asset services should be subject to requirements to make access to these services more secure and transparent for users. The services concerned are the following:

- the custody and administration of crypto-assets on behalf of third parties;
- the management of trading platforms;
- the exchange of crypto-assets against legal tender or other crypto-assets;
- the execution of orders in crypto-assets on behalf of third parties;
- investment in crypto-assets;
- the provision of crypto-asset transfer services on behalf of third parties;
- the receipt and transmission of orders in crypto-assets;
- the provision of advice on crypto-assets;
- the management of a crypto-asset wallet.

Authorisation as a crypto-asset service provider (CASP) will be compulsory (whereas it is optional under French law, in the regime introduced by the PACTE Act) in order to provide these services in France (and within EU territory). These service providers will be bound by rules of good conduct, and will in particular be required to act honestly, fairly, professionally and in the interests of their customers. In addition, the information provided to customers will have to be clear and not misleading, including as regards the risks associated with crypto-asset transactions, as well as the costs associated with the various services provided.

Lastly, in addition to specific requirements applicable to certain activities, the authorisation of CASPs will be contingent on compliance with a common framework namely providing for:

- prudential requirements;
- governance requirements (fitness and propriety assessments for directors and shareholders);
- rules relating to the custody of customers' crypto-assets and funds;
- rules on the handling of customer complaints;
- rules on conflicts of interest;
- rules covering the outsourcing of services;
- rules providing for orderly winding up proceedings;
- rules on the disclosure of information on the environmental impact of crypto-assets;
- rules on the fight against anti-money laundering and terrorist financing.

Glossary

API (application programming interface): a software interface that allows one software or service to be "connected" to another software or service in order to exchange data and features.

Application: program or software package directly used to perform a task.

Blockchain or distributed ledger technology (DLT): is defined in French financial regulations as a shared electronic recording device. It is an electronic registry that stores transaction data and is shared and synchronised between a set of user network nodes operating through a consensus mechanism. The conditions of access to the network and use of the registry determine whether this blockchain is public, in other words open to all, or private, that is to say restricted to selected users.

> Consensus mechanism: the set of rules and procedures by which agreement is reach among the nodes of the blockchain network to validate a transaction.
>
> Network node: computer that is part of a peer-to-peer network (refer to the corresponding glossary entry), which contains a full or partial copy of records for all transactions carried out on a distributed ledger.
>
> Block validation protocols: the validation of new blocks relies on a consensus algorithm (refer to the glossary entry above). The historical method used to achieve this type of consensus is called "*proof of work*". This method uses a mathematical problem the solution to which verifies that the "miner" has performed a task; solving the proof requires a substantial amount of computing power, which in turn requires sophisticated (and energy-intensive) hardware. In contrast, "proof of stake" requires the user to prove possession of a certain amount of crypto-assets in order to validate additional blocks.

Bridge: protocols connecting two blockchains, allowing them to interact with each other. By default, most blockchains exist in isolated environments, with their own rules, governance mechanisms, native assets and data, which are incompatible with other blockchains. These bridges can be centralised (operated by a third party, who must then be trusted by users) or decentralised, meaning based on a smart contract.

Crypto-asset: A digital representation of a value or right that can be transferred and stored electronically using a blockchain. Some crypto-assets are referred to as "tokens".

> Stablecoin: a crypto-asset the purpose of which is to maintain a stable value by reference to an official currency (or a basket of such currencies), other real-world rights or assets, or by reference to other crypto-assets. Stablecoins can be issued and managed by centralised entities -the most significant of them are currently managed by such entities. They can also be issued by DeFi applications, in which case the rules governing their issuance are written into smart contracts and their management is carried out by these smart contracts. At present, two decentralised stablecoin models are available: collateralised stablecoins, that are issued in exchange for deposits (as with centralised stablecoins); and "algorithmic" stablecoins, that are based on the dynamic adaptation of the supply of tokens.
>
> *Depeg*: loss of parity of a stablecoin with the asset the value of which it aims to replicate (official currency, crypto-asset etc.).

Cryptography: A field of study concerned with protecting messages, ensuring their confidentiality, authenticity and integrity, often using keys. It aims to make information unintelligible to anyone other than the intended recipient.

Decentralised autonomous organisation (DAO): usual (yet not systematically used) component of DeFi protocols, aiming at organising its governance; it is usually defined by the community of governance token holders, the smart contracts that govern its operating rules and the assets it controls (protocol treasury).

Key: parameter used as input to a cryptographic operation (encryption, decryption, sealing, digital signature, signature verification). An encryption key can be symmetrical (the same key is used to encrypt and decrypt) or asymmetrical: it is this latter type that is used on blockchains. It uses two different keys: the public key is used for encryption, while the private key, which allows decryption, is kept secret.

KYC (Know your customer): the name given to the processes by which the identity of a company's customers is verified. This term is also used to refer to the banking regulations that govern these activities. KYC processes are used to ensure the identity and integrity of customers, and are intended to prevent identity theft, tax fraud, corruption, money laundering and terrorist financing.

Layer 1 solutions: scaling solutions for blockchains, consisting in increasing the validation power (at the expense of the network's security and/or its decentralised character), or fragmenting a blockchain into several smaller and more flexible blockchains, called shards. With this partitioning (*sharding*), the validation nodes only store part of the information, while such information can still be shared; this increases their operating speed.

Layer 2 solutions: scaling solutions for blockchains (alternatively to layer 1 solutions), relying on a model in which parts of the transactions are processed off-chain, recording only the minimum amount of information in the main chain (considered as layer 1). These solutions include rollups (refer to the glossary entry for this term).

Oracle: an entity that transfers information from the physical world to smart contracts. It provides a link between the physical world and a blockchain, and allows smart contracts not to be limited to information internally available on the blockchain.

Peer to peer network: An exchange model where each entity in the network is both client and server, as opposed to the client-server model. The terms "peer", "node" and "user" are generally used to designate the entities making up such a system. A peer-to-peer system can be partially centralised (part of the exchange goes through a central intermediary server) or fully decentralised (connections are made between participants without any particular infrastructure).

Rollup: the most widespread layer 2 solution today, consisting of executing off-chain transactions, "rolling up" these transactions in a single operation (hence its name), and compressing the information, sending only the data that is strictly necessary for the definitive recording of the transactions on the blockchain. Two main rollup models exist today, which vary according to the way in which the validity of transactions reported on the blockchain is ensured: optimistic rollups consider transactions to be valid until proven otherwise, and are therefore based on a 7-day latency period allowing the network nodes to detect any fraudulent transactions; while zero-knowledge rollups deposit cryptographic proof of the validity of transactions, referred to as "zero-knowledge proof", on the blockchain.

Smart contract: a computer protocol that facilitates, verifies and executes transactions. These computer programs are not "smart" in the sense that they do not change their behaviour over time,

but instead simply execute code when predefined conditions are met. Smart contracts are also not necessarily contracts in the legal sense. The term “automated clause execution tool” could thus better describe their nature.

Wallet: an interface containing a public key to receive crypto-assets, and a private key to access them. Crypto-assets are not stored in the wallet (they always remain on the blockchain); contrary to what its name suggests, a wallet is therefore more of a key ring than a wallet. Wallets can be hosted (custodial), meaning that a third party holds the private key and thus ultimately has control over the relevant crypto-assets. With non-hosted (non-custodial) wallets, on the other hand, the user has direct control over his or her funds. Finally, some wallets are software-based and connected to the internet (*hot wallets*), which makes them easier to use, while other are hardware wallets, i.e. physical offline devices (*cold wallets*), which is supposed to reduce the possibilities of attack.

Selected bibliography

Rafael Auer, *Embedded Supervision: How to Build Regulation into DeFi*, CESifo Working Paper Series 9771, 2022.

Bank for International Settlements (BRI/BIS): *DeFi risks and the decentralisation illusion*, BIS Quarterly Review, December 2021.

Banque de France, Experimental report, *Solution de sécurisation post-quantique des échanges de données*, Le Lab, October 2022.

Jean Barthélémy, Paul Gardin and Benoît Nguyen, *Stablecoins and the Financing of the Real Economy*, Working papers by the Banque de France, February 2023.

Ethereum.org, *Introduction to Ethereum governance*, accessed in January 2023.

European Central Bank (ECB), *DeFi – a new unregulated non-bank system?*, Macroprudential Bulletin, April 2022.

European Commission, *Proposal for a European regulation on markets in crypto-assets* (MiCA), 2020.

European Commission, *Decentralized finance: Information frictions and public policies*, 2022

Financial Stability Board, *The Financial Stability Risks of DeFi*, February 2023.

Financial Action Task Force (FATF), *Updated Guidance for a risk-based approach - Virtual assets and virtual asset service providers,* October 2021.

FATF, *Countering Ransomware Financing*, March 2023.

International Monetary Fund (IMF), *Regulating the Crypto Ecosystem - The Case of Unbacked Crypto-Assets*, September 2022.

Monetary Authority of Singapore (MAS), *MAS partners the Industry to Pilot Use Cases in Digital Assets*, May 2022.

Organisation for Economic Co-operation and Development (OECD), *Regulatory Approaches to the Tokenisation of Assets*, OECD Blockchain Policy Series, January 2021.

OECD, *Why DeFi (DeFi) Matters and the Policy Implications*, January 2022.

OECD, *Lessons from the crypto winter: DeFi versus CeFi*, OECD Business and Finance Policy Papers, December 2022.

Tanusree Sharma, Zhixuan Zhou, Andrew Miller, Yang Wang (University of Illinois), *Exploring Security Practices of Smart Contract Developers*, April 2022.

Consultation questionnaire

Responses should be sent to fintech-innovation@acpr.banque-france.fr by **19 May 2023**.

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

Q1: Do you have any comments on the definition of DeFi used in the paper? Does the document correctly reflect the real level of decentralisation of services?

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

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

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

Part 2: The risks associated with DeFi

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

Q6: Do you think that layer 1 solutions can exacerbate the security issues of the blockchain infrastructure? What about layer 2 solutions? In your opinion, are there significant differences in this respect between the layer 2 solutions considered?

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

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

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

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

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

☐Yes

☐No

Why?

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

Q13: In your opinion, are there any other risks that should be taken into account which are not mentioned (or not given sufficient attention) in the document?

Part 3: Avenues for a regulatory framework

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

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

☐Yes

☐No

If so, how? If not, why?

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

☐Supervising concentration in real time

☐Setting caps on concentration

☐Publicly disclosing when specific concentration thresholds are exceeded

☐Taking further action (specify how)

Q16: Do you agree with the analysis provided in the paper on the merits and limitations of private blockchains (section 3-1, regulatory scenario B)? Should private blockchains operated by private operators be regulated through a supervisory framework, if at all?

☐Yes

☐No

Why?

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

☐Yes

☐No

Why?

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

☐Yes

☐No

If so, what are they?

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

Q19: Is a certification mechanism an effective solution to determine the scope of "safe" smart contracts (for a given state of knowledge)? Would alternative solutions achieve the same result?

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

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

☐Yes

☐No

If so, which ones?

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

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

☐Yes

☐No

Why?

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

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

☐Discouraged

☐Prohibited

☐Neither discouraged nor prohibited

Why?

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

Q27: Do you have any comments on the description made of the risks inherent in the decentralised oracle model? Can these risks be mitigated using a certification mechanism tailored to the specifics of these applications (refer to section 3-2-3)? Do you have any comments or alternative proposals for a framework governing the activities of oracles?

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

☐Yes

☐No

If so, what are they?

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

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

☐Yes

☐No

If so, which ones? If not, why?

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

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

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

☐Information requirements

☐Duty of care and duty of advice

☐White paper publication requirement

☐KYC requirements

☐A comprehensive framework inspired by MiCA

☐Other

Why?

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

☐Yes

☐No

Why?

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

☐Yes

☐No

Why?

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

☐Yes

☐No

If so, which ones?

Avenues for a regulatory framework: cross-cutting aspects

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

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

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