coinbase

To:

Autorité de Contrôle Prudentiel
et de Résolution

Banque de France

4 Place de Budapest
CS 92459
75436 PARIS CEDEX 09

Date:

19 May 2023

Re: “Decentralized” or “disintermediated” finance: what regulatory response?

Coinbase welcomes the opportunity to respond to the discussion paper published by the Autorité de Contrôle Prudentiel et de Résolution (**ACPR**) on: *Disintermediated and Decentralized Finance* (**Discussion Paper**).

Coinbase started in 2012 with the idea that anyone, anywhere, should be able to send and receive Bitcoin easily and securely. Today, Coinbase is a publicly listed company in the United States that provides a trusted, easy-to-use platform that millions of users in over 100 countries rely upon to access the broader digital economy.

Coinbase is active in Europe through our crypto license in Germany, our e-money license in Ireland and a number of registrations across key national markets in the EU. Looking forward, the Markets in Crypto Assets (**MiCA**) regulation is a landmark achievement in delivering a well-designed regulatory framework that supports responsible innovation. It will raise standards across the industry and deliver important legal and regulatory certainty to the market, which gives firms like Coinbase the confidence to invest and grow across the region.

We note that the approach taken under MiCA to monitor and assess the evolution and impact of DeFi is sensible and reflects the fact that this is a nascent and non-systemic part of the digital asset ecosystem. DeFi holds incredible promise and it is critical not to restrict this innovative technology at such an early stage of development. Coinbase looks forward to supporting the ACPR in this exploratory phase of its work on DeFi.

Sincerely,

Tom Duff Gordon
Vice President, International Policy
Coinbase

Introduction

The total value locked across DeFi globally was approximately $50bn at the end of April 2023,[1] and this figure is projected to increase over the coming decade.[2] Decentralized Finance (**DeFi**) offers enormous promise: "interest in DeFi lies as much in what it is today as in what it could foreshadow for the future," as the Discussion Paper recognizes. Through openness, interoperability, and transparency, DeFi can increase competition, promote innovation, and facilitate inclusion in new forms of financial services. For jurisdictions seeking to assert digital asset leadership and promote the next generation of financial market applications and practices, it is critically important not to restrict innovative technologies at this early stage of development.

DeFi currently does not pose systemic risk to the financial system. Even as it grows there is no evidence that it will become systemically important, given that by design decentralization does not engender the concentration of risks that make some of today's large financial institutions systemically important. The Discussion Paper states that supervisors should anticipate the risks before they become "vectors of contagion to traditional finance." The Discussion Paper does not, however, acknowledge the resiliency and robustness that the DeFi ecosystem demonstrated during recent market turbulence and volatility. One important metric of the overall size of the DeFi ecosystem, total value locked (**TVL**) in DeFi protocols, fell by 75% in 2022.[3] Despite these precipitous declines, DeFi protocols performed well and continued operating as designed, with trades successfully completing, loans being serviced, and collateral managed, and there was no wider impact on the financial system.

We also agree with the Discussion Paper that "regulation of disintermediated finance cannot simply replicate the systems that currently govern traditional finance," and that instead any regulatory approach should accommodate the promising features of DeFi. Most notably, the approach must recognize the fundamental difference between offerings by centralized intermediaries and direct access to software protocols.

Key principles

We appreciate the ACPR's thoughtful engagement with DeFi and strongly share many of the same objectives, including assurance that users have access to reliable, efficient financial services, and to prevent illicit financial transactions. Nonetheless, in our view, the Discussion Paper's approach of evaluating DeFi by comparison to the traditional financial system reflects a misconception about the nature of DeFi.

The primary objective of DeFi is not to offer decision making tools and advice that underpin traditional financial services. Instead, DeFi smart contracts are designed to

[1] See DeFiLlama, DeFi Overview, accessed 25 April 2023.

[2] For example, Grand View Research estimates that the DeFi market will expand at a compound annual growth rate of 46% from 2023 to 2030. See Grand View Research, Report Overview.

[3] See DeFiLlama, DeFi Overview, *supra* note 1.

perform specific functions based on well-defined and publicly verifiable code. Closed source, centralized versions of most of these tools already exist in today's financial systems. DeFi is a technological innovation that creates an open marketplace for these tools, not a replacement for the financial services industry. This important distinction may result in a different, more appropriate approach to regulating DeFi.

More broadly, the blockchains that enable DeFi protocols are a recordkeeping technology, and the development and operation of blockchain networks is not a financial service. The Discussion Paper identifies as one of its goals to "strengthen the security of blockchain infrastructures." Blockchains are not inherently financial in nature, and the development and operation of blockchain networks is not a financial service. By analogy, banks today create apps to enable their customers to use banking services online, and these apps may be within the scope of banking supervisors' authority. But that authority does not apply by extension to other apps, the programming languages in which they are developed, or the smartphones on which they run. The same reasoning holds true for blockchains and smart contracts.

The Discussion Paper assumes there is an available "right" approach to regulating DeFi or blockchain technology, such as what it means to be sufficiently secure or decentralized. Although we do agree with the ACPR that these answers will emerge over time, we ask the ACPR to recognize that DeFi is still new, and thus needs space for continued experimentation in order for it to mature and grow, and for these standards to develop. We urge policymakers to proceed with care, in order to consciously understand and preserve the potential benefits of the developing DeFi ecosystem.

We recommend that such an approach should reflect the following five principles:

1. **To protect consumers, regulation of crypto assets should focus on centralized platforms, not DeFi protocols, apps or smart contracts.** This will preserve the freedom for developers and engineers to advance the cutting edge innovations that provide direct access to the base layer of the blockchain, while focusing regulatory resources on the players who should have both the ability and the responsibility to provide a positive experience for consumers who would otherwise lack the technical expertise to interact with blockchains directly.

2. **Do not assume that regulatory tools designed for centralized crypto asset intermediaries will work for DeFi.** We caution against applying MiCA requirements designed for centralized intermediaries in a DeFi context. The ACPR should take the necessary time to explore different options in order to ensure a risk-based and innovation-friendly approach.

3. **Lawful operation of protocols, smart contracts or applications should not require accreditation.** Instead, regulators should initially allow protocols to voluntarily develop responsible disclosure systems. This may yield more effective and immediate benefits by empowering users with information about a protocol,

while leaving a path open to what future accreditation or certification of systems could entail as DeFi matures.

4. **Legal liability should attach only to financial services, not to the pure development of code or use of governance tokens in a DAO.** Extending supervisory and regulatory requirements beyond the remit of financial services will chill innovation without commensurate benefits for consumer protection or other regulatory objectives.

5. **Allow market forces and innovation, not regulatory intervention, to guide the evolution of DeFi.** The Discussion Paper identifies issues – e.g., public vs private blockchains, concerns around security and sufficient decentralization, and other aspects of DeFi – for which the DeFi ecosystem is already actively developing solutions.

We address each of these principles in more detail in the sections below.

Challenges in regulating DeFi

We recognise that DeFi introduces novel challenges for regulation and supervision. Historically, regulators have overseen financial markets by imposing and enforcing rules on market intermediaries. DeFi applications are automated protocols that use code to explicitly define how parties can interact to accomplish a goal, such as exchanging assets. The code is not a centralized intermediary, making it impossible to regulate DeFi using existing regulatory frameworks. As recognized by Professor Tarik Roukny in a paper for the European Commission:

> *"The combination of permissionless access to the consumption and provision of financial services by (legally) unidentified agents through automated protocols constitute an unprecedented setting where standard intervention tools may simply not be appropriate nor implementable."*[4]

We also note specific challenges with concepts set out in the Discussion Paper.

The first relates to regulatory hooks. Extending legal liability beyond financial services, to software itself or to the development of code, raises extraordinarily important – and difficult – questions. Whereas individuals and entities can change their behavior in response to legal mandates, the same cannot be said of code or protocols themselves. Some important jurisdictions, like the United States, provide Constitutional and other legal protection for the freedom of speech, including the writing of software code. Many more jurisdictions follow the legal principle that liability should be assigned only to those who actually engage in wrongdoing. The Discussion Paper's proposed constraints on DeFi raises questions akin to the imposition of penalties on an email service, as opposed to a

[4] European Commission, Information frictions and public policies: approaching the regulation and supervision of decentralized finance (June 2022).

spamming scammer, because the email service was used to send messages communicating fraudulent promises.

Further, an overbroad assignment of liability may discourage innovation and participation on the market without commensurate benefits, particularly at this early stage of development. Parts of the value chain may not be practical or even possible to regulate, for example the underlying protocol, if that has become truly open sourced and decentralized over time.

The second relates to private versus public blockchains. We disagree with the view that private blockchains are viable alternatives to public blockchains. Private blockchains (where activity is permissioned through a central authority) and public blockchains (that permit activity without permission of a central authority), have coexisted for almost a decade, and the DeFi ecosystem has overwhelmingly chosen to build on public blockchains. This is because private blockchains are not a viable alternative as they do not have the features of decentralization, credible neutrality, and permissionless innovation of public blockchains. Much like why the internet succeeded, and the intranet did not, these features bring freedom to entrepreneurs and enable them to serve customers in innovative ways. While we believe that private blockchains have their place and can support many kinds of worthwhile innovation, they are alternatives to traditional databases, not public blockchains.

The third relates to minimum standards. We do not believe that public blockchains should be subject to prescriptive requirements in a wide range of areas including the minimum number of validators, caps on concentration of validation capacity, communication in advance of various alert thresholds, and the like. In our view, there is insufficient data for policymakers to reach meaningful conclusions that these requirements are needed or effective. Some networks have run securely for years with less than two dozen validators, while Ethereum has run securely with over 500,000 validators; neither has been successfully attacked so it is impossible to say one is objectively more secure than the other. A more efficient and effective solution is to allow blockchain developers to build protocols and introduce innovations that rely on market forces to guide their efforts to improve public blockchains' security and efficiency.

More generally, DeFi is like the internet: global, permissionless and borderless by nature. Therefore it is inherently problematic for policymakers in any one jurisdiction to apply regulation in isolation. In particular, countries should not introduce inconsistent and overlapping regulatory approaches, as this will result in lack of legal clarity and regulatory certainty around which rules apply, and in turn make compliance challenging. The work of the global standard-setting bodies and international coordination more broadly are critical in this regard.

Regulatory approach

Given the evolving nature of crypto assets and blockchain technology, a fit-for-purpose regulatory regime should focus on outcomes[5] and should be technology neutral. In developing a regulatory approach, different tools will be required for DeFi compared to traditional finance, in order to preserve DeFi's unique characteristics. We caution against applying MiCA requirements that have been developed for centralized exchanges in a DeFi context. Even seemingly straightforward ideas like "requir[ing] each intermediary to publish a white paper setting out the characteristics of all the crypto-assets on which a service is provided" quickly runs into issues. Many DeFi protocols are created by loose collections of pseudonymous individuals scattered around the globe with no legal or economic ties between them. This is often the case with the development of open source code. There is not always a clear answer for who is responsible for publishing the whitepaper if there is no clear intermediary or issuer. The ACPR should take the necessary time to explore different options in order to ensure a risk-based and innovation-friendly approach.

The focus of regulation should be on centralized entities that are providing actual services to users, such as "on and off ramps" for the crypto asset ecosystem. Further exploration is needed on whether, in the future, entities traditionally outside the regulatory perimeter could or should be regulated in some way. For example, DeFi interfaces do not provide a direct service to users; they surface information from the blockchain and create an interface for users to craft and sign their own transactions. It is important to explore whether DeFi interfaces could reinforce specific safeguards, such as wallet screening or a "blacklist" that denies services for sanctions enforcement or other illicit activity. However, this screening is easy to circumvent, which is why it is critical to focus regulation on centralized entities (especially on and off ramps) through which any ill-gotten gains held by malicious actors would need to be funneled. Centralized entities have the resources, skills, and responsibility to fulfill regulatory requirements.

We note that there are a number of proposals in the paper which effectively apply a traditional financial regulatory approach in a DeFi context, or that seek changes to DeFi in order to make it operate more like CeFi. For example, the Discussion Paper suggests the "partial 'recentralisation' of services deemed sensitive" by requiring the holders of governance tokens or administrative keys to a protocol to incorporate. Without knowing what services may be sensitive, we believe such requirements for recentralization are unnecessary regulatory interventions that would stifle innovation without commensurate benefits. An interesting comparison is to consider what the economy may look like today if, in the 1990s, policymakers had required anyone seeking to create a website to first obtain a license. It is likely that the result would have been far less spam and scams on the internet at that time, but also far less innovation and dynamism over the longer term.

[5] As noted above, IOSCO Secretary General has advocated for a similar approach. See Regulatory Insights Session - Interview with Martin Moloney, IOSCO Secretary General (13 June 2022).

We also wish to emphasize crucial differences between DeFi and CeFi with respect to self-hosted wallets. A self-hosted wallet enables a user to retain control and possession of crypto assets held in the wallet, without entrusting the assets to any other person or entity. In this respect, a self-hosted wallet is therefore not like a bank or brokerage account, it is the digital equivalent of a physical wallet that a person may use to hold paper currency in their pocket. A self-hosted wallet application is a software product, not a financial service.

Possible forward looking options

We believe that it would be a mistake to regulate DeFi at this early stage of development, while it remains a nascent and quickly evolving ecosystem. However, we note that there are a number of possible approaches to DeFi, which would allow it to develop in a way that advances innovations that benefit society, much like the development of the internet. While further exploration is necessary, these might include:

- **Focus on on-ramps and off-ramps like exchanges.** This approach would focus on the regulation of legal entities engaged in certain identifiable activities, such as operating a centralized exchange for crypto assets. In broad terms, this approach has the virtue of clarity but is likely to be both under- and over-inclusive in certain respects, and so should be supplemented with elements of other approaches.

- **Voluntary accreditation or certification system.** Regulators could oversee an accreditation system for smart contracts and applications that satisfy relevant operational, implementation and design standards. Accreditation would not be required for lawful operation nor be a guarantee from the regulator. It would, however, provide consumers and market participants some assurance that they are interacting with well-tested smart contracts and applications that have been subject to a degree of scrutiny and validation. It would also leave room for developers to continue to improve smart contracts and applications, including those that have not yet received accreditation.

- **Self Regulatory Organization (SRO).** The ACPR may also consider supporting the establishment of one or more SROs with the ability to create and enforce industry best practices standards and procedures pursuant to delegated regulatory authority. This approach may strengthen oversight and ensure standards remain fit for purpose and adaptable as the market evolves, while allocating a greater proportion of administrative costs to the industry and maintaining supervisors' authority to determine applicable requirements. Such an approach is also fitting and commensurate given the size and early-stage nature of the technology.

The ACPR should explore each of these options in more depth, including whether to pursue one or more of the approaches in isolation or in tandem.

Security in DeFi

We agree that security is of utmost importance in blockchains and DeFi, and also that security across the industry needs to be stronger to reduce the frequency of hacks and bugs. However, there are important considerations when deciding on the best approach.

First, decentralized public blockchains like the Bitcoin and Ethereum networks have already proved to be secure and resilient. The resilience of blockchains is based ultimately on cryptography: changes to things like user balances cannot be made except using cryptographic keys, which cannot be counterfeited, guessed or hacked – barring human error – thanks, fundamentally, to human ingenuity in devising maths problems that are functionally impossible for computers to solve in any reasonable time frame. Although 51% attacks on networks are possible, and have occurred with small proof-of-work blockchain networks in the past, the impact of these attacks is limited and temporary, and takes the form of a double spend — tokens that appear to be spent twice, but are actually only spent once, thereby deceiving the recipient of the fake spend. Importantly, these kinds of attacks are incredibly rare, do not corrupt the blockchain, and have never occurred on any network with meaningful user or DeFi activity, such as Ethereum.

Second, a public blockchain is the harshest environment in which code can ever be deployed. They are open source (meaning attacker can read the code), open state (attacker can choose an opportune moment), open entry (attacker cannot be censored), and open exit (attack's consequences are immutable). For these reasons, security is already the single most important property for which DeFi protocols are optimized, and innovative solutions are regularly developed and implemented to increase security – including audit competitions, transaction simulation, mempool monitoring, and much more. Just as the internet has created https, ssl, password managers, spam filters, and many other security mechanisms – in other words, the architecture for open communication, as well as the tools to mitigate its downsides – DeFi is doing the same.

Secure DeFi protocols become the most powerful and utilized tools. Uniswap, a decentralized exchange, has deployed three versions over five years, has never been hacked, and today facilitates $250bn in annualized trading volume on only $4bn of TVL. Whereas policymakers may see the concentration of trading on this and other DEXes as a drawback, we see it as a signal of vigorous, global competition in which the most secure protocols gain the most traction. This dynamic is the reason why attempting to approve DeFi applications, rather than enabling the free market to work, will only weaken DeFi's security, instead of strengthening it.

Measures of decentralization

The Discussion Paper recognizes that decentralization is not a binary state, but "variable over time" – and, indeed, that decentralization is a process that takes time and effort to achieve. For this reason, we strongly recommend that the ACPR refrain from regulatory interventions that impede the process of developing protocols and decentralizing governance.

The most important feature in assessing the degree of decentralization of a particular project or protocol is dispersion of control – the extent to which an individual person or entity is able to make changes to core functions or underlying code of a protocol, and to what extent these changes impact other users of the protocol. In a more decentralized protocol, agreement must be reached across a large number of disparate stakeholders for updates to be made; in a less decentralized protocol, updates could potentially be made unilaterally, or by a small number of persons or entities. These stakeholders are often referred to as a "community," and often include hundreds or thousands of widely dispersed individuals who each participate for their own reasons.

In practice, a protocol is likely to proceed through phases of increasing decentralization, at each phase enabling greater levels of participation from stakeholders beyond its initial development team. Two key variables in this respect are the mechanisms for authorizing updates, and the time given for proposed updates to be reviewed. Early in a protocol's development, the necessary changes may be frequent and straightforwardly technical in nature. The best method for authorizing such changes has generally been a multi-sig, i.e., a mechanism requiring cryptographic signatures from a small number of well-informed experts, with immediate effect or with only a short window for review. Over time, as a protocol matures, governance tokens can be distributed based on the extent of individuals' use of the protocol, and the best method of authorizing updates to the protocol would be a vote by the holders of governance tokens. Governance token holders can be given a period of time — e.g. seven days, 30 days or even longer — to review the proposed updates and decide how they want to vote, and optionally "exit" from the protocol if they don't agree with the changes.

For example, the Ethereum network is highly decentralized, as demonstrated in its September 2022 shift from a proof-of-work to a proof-of-stake consensus mechanism. This feat took years to achieve, not only because of the technical complexity of the engineering, but because the wide dispersion of control across the Ethereum network necessitated a great deal of work to achieve alignment across many stakeholders.

Retail investors and DeFi

The ability to interact directly with blockchains – without intermediaries – is an important aspect of the potential benefit of this technology. However, as the Discussion Paper recognises, most people lack technical knowledge of blockchains and how they work.

We therefore believe broad-based market participation will be facilitated through centralized platforms, especially in the early stages of development of blockchain technology. Regulation should focus on centralized platforms to provide consumer protection, while preserving the freedom for developers and engineers to advance the cutting edge innovations that provide direct access to the base layer of the blockchain.

Through MiCA, for example, the majority of retail investors' exposure to crypto assets will be regulated, as they engage in the ecosystem through centralized exchanges.

We do not agree that intermediaries should be responsible for preventing every user from "interacting with fraudulent or dangerous protocols (duty of care), or from engaging in excessive risk-taking (duty of advice)." As a matter of principle, we believe that users should generally be free to interact with protocols as they see fit – such activity is not inherently financial in nature, and the application of investment suitability-like requirements in this context is inappropriate. Moreover, the intermediaries that should bear greater responsibilities in respect of consumer outcomes are those which MiCA has already addressed – e.g. centralized intermediaries that hold crypto assets in safekeeping for customers. We do not believe that MiCA's requirements should be imposed indiscriminately on anything with a touchpoint to DeFi. In many cases, these so-called "intermediaries" may only provide an interface for users to interact directly with DeFi protocols – they are not providing financial services, and the users are not clients or customers of the intermediary.