EU DeFi Policy Roundtable Summary

polygon Labs | coinbase

Introduction

On July 8, 2024, Polygon Labs and Coinbase co-hosted a policy roundtable in the European Union ("EU") as part of a series of roundtables that have been held globally with regulators, policymakers, academics and industry to educate on and address key policy questions related to decentralized finance ("DeFi").

DeFi continues to grow in importance in policy discussions, especially in the EU where the Markets in Crypto Assets ("MiCA") regulatory framework has entered the final stages of implementation. Although MiCA excludes services conducted in a "fully decentralised manner without any intermediary," it left open how to define and identify such services, leaving national regulators to contend with the difficult task of understanding decentralization. For example, the Danish Financial Supervisory Authority recently released preliminary guidance for market participants and called on the private sector to provide feedback on the definition of decentralization. To solve this regulatory fragmentation and inform next policy steps, MiCA includes a provision requiring the European Commission (the "Commission") to write a report on DeFi by 2025.

This EU roundtable brought together industry participants to discuss a framework for activity involving DeFi software systems, as the Commission and national regulations seek to achieve positive policy outcomes for these markets.

Executive Summary

A group of public and private sector participants came together in Brussels to discuss the benefits of DeFi, the regulatory challenges of this novel financial system, and a potential regulatory framework. The discussion first focused on creating a common understanding of how a DeFi transaction works — as well as whether it was possible to identify any actors within these systems that are engaged in activities that require regulation — before discussing issues related to policy questions around user protection, market integrity, and financial integrity. Experts presented on each of these issues, with a robust discussion on each, under Chatham House rules to ensure all participants could speak freely.

On each of the three topics, participants debated underlying policy goals and policy "solutions," but ultimately agreed that DeFi remains nascent and thus, is not yet ready for comprehensive regulation. Instead, leveraging technology advancements to address emerging risks and issues within DeFi may offer a more effective and adaptive approach, which could help achieve policy goals while allowing for continued innovation.

Generally, participants concluded that in constructing policy frameworks, policymakers can be guided by the following: (i) do not aim for "zero tolerance" on each issue but focus on minimizing and mitigating risks to ensure safe engagement on DeFi activities, (ii) clearly define the problem and/or goal, enabling a more targeted and thus, effective regulatory framework, and (iii) acknowledge that there are no solutions, only tradeoffs to each regulatory approach, which must be carefully considered.

Analysis of Discussion

I. Mechanics of a DeFi Transaction

The roundtable began with a demonstration of a transaction through the Uniswap protocol — a type of DeFi application known as a decentralized exchange ("DEX") — demonstrating how a user can exchange one cryptoasset for another in a self-directed manner, without any intermediary. This session ensured that all participants had a common understanding of "DeFi" and the disparate parts of the software that comprises and/or is involved in a true DeFi transaction.

The demonstration started by downloading a new software wallet — software that allows a user to communicate desired transactions and interactions to a blockchain network. One participant sent cryptoassets to the demonstrator to show the speed with which peer-to-peer transfers of value can occur.

The demonstrator then connected the wallet to a user interface (also referred to as a "front end" or UI), found at app.uniswap.org. A front end is a website that refers to the visual interface of a software system with which a user interacts. This front end provides information by allowing users to view blockchain data in an easy-to-read way, including which tokens are available to exchange, and other information such as network costs (also called "gas fees"). Such front ends do not initiate, "facilitate", or carry out any transactions on behalf of the user.

The user then determined which cryptoasset to exchange for another, provided the relevant inputs on the website and then communicated those inputs via the self-hosted wallet to the Uniswap protocol (i.e., a set of smart contracts — autonomous, self-executing code that function in a conditional manner) through a remote procedure call ("RPC") node that then communicates with the underlying blockchain network for settlement.

The blockchain network – also referred to as the "base" or "infrastructure" layer – is, at its core, used for accounting. Its central function is to time stamp and publicly store data for anyone to access and see, which gives the network its integrity and security. Participants generally agreed that preserving the neutrality of the base layer is necessary for ensuring the continued development of permissionless blockchain networks.

II. Identifying Intermediaries in Decentralized Systems

The first session provided context for whether and when a person or entity is engaged in activity involving the use of DeFi software systems that could or should require regulation, if at all. Two

approaches for identifying potential intermediaries were considered: define "decentralized" to determine if a DeFi system is or is not decentralized or look for "centralizing vectors" within the entire DeFi system – or technology stack – that may signal points of control but that do not necessarily make a determination on the state of decentralization.

The *first approach* of legally defining "decentralized" poses some challenges and may produce unintended consequences. The primary difficulty in constructing such a definition is that it would need to be specific enough to delineate decentralization as it stands today from both a technological and governance perspectives, broad enough to remain evergreen as decentralized technology evolves and matures (i.e., decentralization today may look different than decentralization five or ten years from now), and favorable enough to reach a consensus among industry and policymakers on one definition of decentralization. Most likely this definition would not meet one of those criteria, and instead of serving as a tool, the definition would lead to a number of unintended consequences such as producing prescriptive regulation and cooling innovation.

The *second approach* may solve for the challenges in the first approach by instead identifying "centralizing vectors" in blockchain-based systems that signal points of control without determining if the system in itself is "sufficiently" / "fully" decentralized or centralized. Such an approach is consistent with the way that traditional regulations are structured, in that they identify and target natural person(s) and activities. Although this approach avoids having to define "decentralized", it does require a definition of "control" with the red line of control being an ability to do something with user assets against the user's will and/or without the user's consent.

Centralizing vectors present different types and levels of control. For example, a user interface run by a company – the centralizing vector – may be used to view information about a DeFi protocol in a more easy-to-read way, but it would not make the entire DeFi protocol centralized or even rise to the level of regulated activity. In another example, a decentralized DeFi protocol deployed on a permissioned chain – the centralizing vector – may be decentralized at the protocol layer but not at the base layer, suggesting that the focus of potential obligations would fall not on the protocol but on the entity controlling the permissioned chain. In addition to identifying these vectors, their intent should also be considered (e.g., these vectors may be added on purpose to increase security or for other purposes that would benefit users).

The presence of centralizing vectors does not necessarily mean the entire system is centralized; instead, they point to areas where there may be an intermediary or a vulnerability present. Once identified, these vectors can be assessed based on their individual facts and circumstances to determine what, if

any, regulations may be needed. Focusing on identifying centralizing vectors could offer a more productive policy alternative to legally defining "decentralization".

III. Policy Considerations for DeFi

The following sessions debated a variety of possible legal and regulatory solutions that will address the three policy goals – protecting users, preserving market integrity, and ensuring financial integrity – for activities with DeFi software systems in which no intermediary is involved.

A. User Protection

Protecting users generally entails preventing loss of user funds and reducing information asymmetries. In addition, another important consideration includes providing users an ability to evaluate all their options in making decisions. The discussion focused on two areas for achieving user protection in DeFi: disclosures and marketing practices, with potential implications for front ends.

[Light approach] ***Disclosures.*** Generally, disclosures may be useful in some contexts. As is true for disclosures in traditional systems, these disclosures should not maximize the amount of information available to users, but instead, should focus on providing accurate, complete, and necessary information for users to make informed decisions. For DeFi protocols, such information likely should include underlying code of the DeFi protocol, descriptions of the technology, governance mechanisms, any potential risks and/or centralization vectors, to name a few. The industry already engages in a variety of best practices such as making the code for the DeFi protocol they developed either open source – or, at least, source available – as well as publishing public documentation on the protocol itself and its accompanying governance mechanism.

[Medium approach] ***Marketing guardrails through front ends.*** Marketing plays a key role in DeFi protocol adoption – just as it does with traditional products and services – by bringing awareness and driving engagement with a protocol, ecosystem, community, etc.; however, marketing practices must be consistent with the technology and level of risk involved. There needs to be heightened awareness around marketing approaches and practices, especially – and most importantly – to avoid pushing cryptoassets associated with DeFi protocols as investments. Ultimately, questions around marketing relate to the differences between retail and institutional users that may have different levels of knowledge about DeFi. Some proposals were discussed for addressing these information gaps through front end regulation, such as geoblocking retail users and/or implementing certain "gated access" touchpoints through know your customer ("KYC") checks, wallet addresses screening to determine experience levels, and/or "adequacy" questionnaires, all of which would limit retail access to these protocols. All approaches discussed raised implementation concerns.

Targeting front ends as potential regulatory touchpoints is consistent with the centralizing vectors approach outlined above and would preserve base layer neutrality. However, any approach that exclusively targets front ends has limited effectiveness in that blocking or restricting users on front ends doesn't prevent these same users from accessing the DeFi protocols and underlying technology in other ways.

B. Market Integrity

In DeFi, "efficiency" is different than in traditional markets given the inherent features of DeFi (e.g., transparency, liquidity, user-directed transactions, etc.) and thus, may emanate from different sources (i.e., not from centralized actors) than in traditional finance; moreover, "efficiency" can refer to a number of factors, such as efficiency in spreads, liquidity, and routing. In aiming to achieve fair and efficient markets in DeFi, efficiency must first be defined and a specific problem identified. During this session, two policy frameworks were discussed that broadly address how to approach solving for issues or inefficiencies present in DeFi systems: allowing the technology to function as a solution or regulating directly on-chain.

[Light approach] ***Technology as the solution.*** Given the rapidly evolving technology, any policy prescriptions may quickly become obsolete or produce unintended consequences; therefore, technology and free markets may address regulatory concerns more effectively and efficiently than any policy framework. For example, Maximal Extractable Value ("MEV") – i.e., maximum value that can be realized from a block of transactions through the selection and prioritization of transactions for and within a block – can produce both positive outcomes for DeFi markets (e.g.., arbitrage to support market efficiency) as well as negative ones (e.g., front running user transactions with MEV bots). Previously, the International Organization of Securities Commissions ("IOSCO") suggested making "providers" of DeFi protocols and/or validators responsible for preventing the negative MEV risk to users, which as discussed previously, would be unimplementable (i.e., there are no "providers" of DeFi protocols) and/or would take a non-neutral approach to the base layer. Meanwhile, the industry – through the development of new technologies – has taken on addressing these risks, such as through certain base layer networks that prevent the front running of user transactions.

[Heavy approach] ***Regulate directly on-chain.*** An alternative approach could be to directly regulate DeFi on-chain through means such as embedded supervision in smart contracts. This approach would be the most effective in preventing abuses, but would produce a number of unintended consequences such as compromising base layer neutrality, creating regulatory fragmentation, cooling innovation, discouraging software development, among others. Given such potential consequences, the industry is widely disapproving of such an approach. An alternative approach to directing how the technology is

developed could be policymakers and regulators participating in Improvement Proposals (e.g., EIPs for the Ethereum blockchain), where they can submit their concerns and technology guidance to a public forum where such approaches can be discussed, improved on, and implemented, given the consensus of governance token holders. Such an approach requires a high degree of technical knowledge, which may be challenging for policymakers and regulators but does offer a public-private solution to directing the development of technology, while remaining technologically neutral.

C. Financial Integrity

Financial integrity seeks to preserve the use of a market system for good and mitigate/deter the use of that system by illicit actors. Given the national security implications, financial integrity in DeFi should be the top priority in policy discussions. Several solutions were discussed, such as front end regulation (e.g., implementing wallet screening) and risk-based decision-making for regulated entities with on-chain tools (e.g., smart contract and wallet screening).

[Medium approach] ***Wallet screening.*** Many believe that front end wallet screening is an industry best practice, especially to identify risk, by restricting users associated with high-risk activities such as sanctions or terrorist financing. In addition, entities interacting with DeFi protocols directly could use other measures such as screening smart contracts (e.g., pools in DeFi protocols) to identify other potential sources of risks and vulnerabilities before deciding where to send funds; this is typically thought of for traditional financial institutions engaging with DeFi, which was not a topic discussed during the day.

One of the most effective solutions to combating illicit finance in DeFi is to regulate on and off ramps. DeFi, and blockchain technology more widely, is a closed system, meaning to enter and exit the system, a user must at one point interact with a traditional financial institution – a centralizing vector. These centralized financial institutions are already highly regulated but not all of them follow strict guidance for identifying, tracing, and blocking illicit transactions and actors; primarily an issue for offshore institutions. Targeting these access points could serve as a deterrent for illicit finance.

Conclusion

The evolving landscape of decentralized finance presents both significant opportunities and complex regulatory challenges. The participants agreed that as DeFi continues to grow, the focus should be on leveraging technological advancements to address risks and vulnerabilities within the DeFi ecosystem, ensuring that solutions remain flexible and adaptive to ongoing developments. A premature regulatory framework could hinder innovation and fail to address policy goals.

Ultimately, the future of DeFi regulation will require ongoing collaboration between industry and policymakers. By collaborating on thoughtful, technology-driven solutions, it is possible to create a regulatory environment that not only protects users but also encourages the continued evolution and success of decentralized finance.