January 29, 2024

Genuine DeFi as Critical Infrastructure: A Conceptual Framework for Combating Illicit Finance Activity in Decentralized Finance

Rebecca Rettig, Michael Mosier & Katja Gilman[1]

Issue: Traditional finance integrity laws and regulations attach to intermediaries, including — with respect to anti-money laundering obligations — those intermediaries the Bank Secrecy Act ("BSA") defines as "financial institutions." These current laws are not amenable to intermediary-less, blockchain-based software systems like decentralized finance ("DeFi").

Background: Global regulators and policymakers have long been focused on ways to regulate cryptocurrencies and the blockchain-based technological systems in which they operate, including in DeFi. As the International Monetary Fund and Financial Stability Board recognized, "In the case of DeFi . . . , the lack of intermediaries means that the traditional approach to AML/CFT regulation, in which AML/CFT requirements are imposed on a private sector entity and compliance is monitored by supervisors, *cannot be applied*."[2] The U.S. Department of the Treasury recognized the same in its Illicit Finance Risk Assessment of Decentralized Finance: "DeFi services that lack an entity with sufficient control or influence over the service may not be explicitly subject to AML/CFT obligations."[3]

Proposed Solution: This paper *begins a conversation* around the novel ways laws and regulations can achieve financial integrity goals in DeFi and sets out a conceptual framework for doing so.

- *First*, we propose a definition of "independent control" to allow for identification of systems dependent on centralized actors ("System Control Persons" or "SCPs"), even if the system uses the term "DeFi" in a descriptive or aspirational sense. The proposed definition, tied directly to FinCEN's seminal 2019 guidance,[4] focuses on ***a person's unilateral ability to exercise operational authority over any third-party value in a blockchain-based software system***. Although SCPs are more likely subject to regulation, including — potentially, AML requirements — making such a determination requires analysis of the facts and circumstances of the system at issue and the SCP's activities within the system.

---

[1] Rebecca Rettig is the Chief Legal & Policy Officer at Polygon Labs; Michael Mosier is a co-founder of Arktouros pllc, a partner at *ex/ante*, and the former Acting Director of FinCEN, former Associate Director of OFAC, and a former Deputy Chief of the U.S. Department of Justice's Money Laundering Section; Katja Gilman is the Senior Public Policy Lead at Polygon Labs.

[2] IMF & Fin. Stability Bd., *IMF-FSB Synthesis Paper: Policies for Crypto-Assets*, (2023), https://www.fsb.org/2023/09/imf-fsb-synthesis-paper-policies-for-crypto-assets/. (emphasis supplied).

[3] *See* U.S. Dep't of the Treas., Illicit Finance Risk Assessment of Decentralized Finance, 2 (2023), https://home.treasury.gov/system/files/136/DeFi-Risk-Full-Review.pdf.

[4] Fin. Crimes Enf't Network, FIN-2019-G001, Application of FinCEN's Regulations to Certain Business Models Involving Convertible Virtual Currencies, 20 (2019), https://www.fincen.gov/sites/default/files/2019-05/FinCEN%20Guidance%20CVC%20FINAL%20508.pdf.

- *Second*, we propose classifying neutral technological ***systems*** without SCPs ("genuine DeFi") as "critical infrastructure" subject to oversight by the Treasury Department's Office of Cybersecurity and Critical Infrastructure Protection ("OCCIP"). This is consistent with the way that other critical technological infrastructure is treated in the 16 sectors overseen by the Cybersecurity and Infrastructure Security Agency, which works cross-functionally across the government, including with OCCIP on critical infrastructure that underpins aspects of financial activity. Genuine DeFi should *not* be designated as "financial institutions;" and "critical infrastructure" is wholly separate and apart from this concept and from FSOC's designation of institutions as "systemically important."

- *Third*, for certain types of ***businesses*** that interact with genuine DeFi but are not SCPs (*e.g.*, RPC-node-as-a-service providers), we propose creating a new category of "critical communications transmitters" ("CCTs") which would have regulatory obligations to aid in the protection of U.S. national and economic security but would *not* be "financial institutions" subject to the BSA. Existing AML laws and regulations do not provide authority to create risk-based programs for non-financial institutions; they do contain the foundations for such an approach, upon which new legislation and potentially additional regulation (after rulemaking with notice and comment) may be built.

The framework proposed in this paper balances government and industry interests in financial integrity in DeFi with protecting its core technological characteristics — a balance fundamentally necessary for any *effective* regulatory approach. This proposal seeks to build upon the Treasury Department's oversight over U.S. national and economic security — and the need for new legislation to build upon this for DeFi; recognize the realities of DeFi technology to identify an appropriate regulatory focal point for combating illicit activity;[5] ensure mere software providers are not subject to regulation by virtue of software development activity alone, a concept antipodal to long-standing FinCEN guidance; and — critically — maintain base layer neutrality,[6] an ideal imperative to ensuring the continued development of permissionless blockchain networks as global infrastructure.

The proposal herein overlays the policy goals underlying the financial integrity regime in the United States with the realities of the technology in an attempt to *begin* to answer questions posed by regulators and policymakers.

[5] The proportion of DeFi transactions flowing through CCTs likely will continue to grow as blockchain networks scale, meaning that large-scale CCTs will be integral to high communications throughput.

[6] For an overview of base layer neutrality and its import, *see* Rodrigo Seira, Dan Robinson & Amy Aixi Zhang, *Base Layer Neutrality*, Paradigm (2022), https://www.paradigm.xyz/2022/09/base-layer-neutrality.