FedFin Client Report

Tuesday, March 29, 2022

Global Securities Regulators Diss DeFi

Client Report: DEFI

Executive Summary

As promised, this report provides an in-depth analysis of IOSCO's new paper on decentralized finance, one sure to advance the FSB's efforts to bring DeFi systems under greater regulatory scrutiny due to the findings we here detail. In the U.S., President Biden's crypto-focused executive order (see FSM Report **CRYPTO26**) highlights DeFi's risk with regard to illicit finance. IOSCO's work on this report was headed by the SEC, suggesting rapid U.S. action not only on this concern, but also on many other risks by the Commission, as well as the FSOC and other U.S. agencies. IOSCO concerns go well beyond those specific to investors and trading platforms, noting, for example, significant risk posed to retail customers in DeFi lending and payment, settlement, and clearing products. As with the FSB, IOSCO disputes assertions that DeFi is fully decentralized, noting that most of the services delivered via any DLT purporting to be DeFi are analogous to traditional financial products and services (TradFi) other than regulation. The report also details the off-chain activities that result in significant inter-connectedness with TradFi without appropriate controls over possible contagion or even systemic risk. Product-by-product analyses also detail concerns regarding governance, conflicts of interest, and resilience, largely rejecting industry arguments that DeFi advances financial inclusion. Despite these concerns and a detailed discussion of risks that may quickly become systemic, the report makes no recommendations for industry reform or policy action. IOSCO invites comments on this paper without setting a submission deadline.

Analysis

In addition to describing DeFi and policy actions to date, the IOSCO report concludes that:

- Much of the decentralization attributed to DeFi does not exist because cross-chain and off-chain interfaces such as highly leveraged trading, custody accounts, graphical user interfaces principally used by retail clients, and advisory features atop smart-contract transactions have numerous nodes of accountability and control. Protocols are moving some of these off-chain activities into DeFi, but many remain and are likely to do so for a considerable period of time.

Federal Financial Analytics, Inc.
2101 L Street, NW – Suite 300, Washington, D.C. 20037
Phone (202) 589-0880
E-mail: info@fedfin.com www.fedfin.com

- Governance methods -- e.g., tokens authorizing a say over smart contracts -- may centralize protocols even if they are principally on-chain in crypto-trading platforms (here called CeFi). Stablecoins are inherently CeFi and thus pose an array of governance considerations separate from on-chain DeFi.
- Lending, borrowing, trading (i.e., bots), asset-management, clearance/settlement, custody, derivatives, NFT, and numerous other protocols are detailed along with risks to various parties in each protocol (e.g., front- or back-running, theft or asset disappearance, miner extractable value, payment fails). IOSCO also compares -- generally unfavorably -- these various protocols and user implications with TradFi. Stablecoin reserve assets are described and discounted, citing much in the FSB's stablecoin report (see *Client Report* **CRYPTO20**).
- Insurance and risk-protecting measures are only now coming into use and are more akin to shared-risk pools than robust risk mitigation.
- Many DeFi products have embedded self-reinforcing incentives (e.g., building investors to increase advisory fees, creating the appearance of a "virtuous circle" that is actually an echo chamber reinforcing insider interests, settlement "block rewards").

With specific regard to regulation, IOSCO notes that:

- DeFi's disintermediation impact eliminates gate-keeper intermediation and exacerbates information asymmetry, structural and investor risk, and lax AML/sanctions monitoring. TradFi buffers such as capital, liquidity, and deposit insurance also provide critical protections against asset loss, fraud, and other harm.
- Retail investors are at particular risk in DeFi products in which initial investors liquidate their holdings as new ones enter the system, eliminating any initial capital at risk and other protections for customers who may be enticed by influencers or others to invest. Fraud risk via "rug pulls" and other schemes is also a hazard.
- DeFi products often lack essential ex ante disclosures.
- Technical complexity may make some DeFi products unsuitable for retail investors due to their inability to assess material risk.
- DeFi poses significant risk of front-running, flash-loan loss, market dependencies (e.g., on a single crypto asset), leverage (e.g., via collateral rehypothecation across different flash loans), and heightened risk of illicit finance (a particular concern where anonymity-enhancing software is deployed). IOSCO also details numerous risks specific to smart contracts e.g., lack of code auditing, "daisy-chaining").
- DeFi is subject to significant operational and technology-based risk (e.g., DLT failure, validation incentives and/or concentration that does not deter risk, centralized but unregulated sources of control, congestion and lack of scalability), risks posed by off-chain tech such as cloud-service providers and "oracles".
- Cyber-security is another acute concern as is the governance risk that may make this even more hazardous (e.g., ransomware) for systems with poor internal controls.

Federal Financial Analytics, Inc.
2101 L Street, NW – Suite 300, Washington, D.C. 20037
Phone (202) 589-0880
E-mail: info@fedfin.com www.fedfin.com