**Commodity Futures Trading Commission**
**Market Risk Advisory Committee Meeting**
**March 8, 2023**

**Written Remarks Regarding Digital Assets Policy Frameworks –**
**Areas for MRAC Review**

Good morning, thank you for the opportunity to speak with members of the MRAC, Commission staff and leadership, and fellow panelists. My name is Mark Hays, I am a Senior Policy Analyst with Americans for Financial Reform Education Fund and Demand Progress Education Fund. There are many topics related to digital assets that would make sense for the MRAC to review, given the complexity, uncertainty, and volatility of this space. With limited time today, I wanted to name two topics for the MRAC to consider.

The first is exploring how the Commission might gain better visibility into the integrity and management of businesses seeking to acquire ownership stakes in CFTC-registered entities. CFTC Commissioner Johnson raised this issue in a speech given last January, referencing FTX's acquisition of Ledger X. The Ledger X acquisition offers lessons about both the strengths and limitations of the CFTC's ability to use its existing tools to evaluate and oversee actors in the digital asset space. But it also raises broader questions about how such acquisitions or deployment of subsidiary entities foster risk.

The Ledger X acquisition by FTX isn't unique in the crypto space. For example, FTX also acquired Farmington State Bank in what appears to be an attempt to secure access to banking services and privileges through a 'backdoor' entity. This past weekend, A WSJ investigation into Binance alleged the company may have employed a strategy to create and position its US-facing entities to draw regulators' attention towards such entities and away from other aspects of the business. And their other examples of actors in the crypto space using acquisitions or creation of subsidiary entities to achieve similar ends.

Business acquisitions of this type are typically a conventional, and often benign, means of conducting business. But given this pattern and given that many crypto firms currently operate offshore and thus provide limited information and disclosures to US authorities, we agree that the CFTC should use its existing tools and authority to effectively carry out, and if needed, deepen the due diligence it conducts during these acquisition scenarios. We also agree the CFTC should explore what additional authority or resources may be needed to enhance such due diligence when it comes to digital asset related acquisitions.

The MRAC could potentially assist in this effort in a few ways. First, the MRAC could lead a high-level review other recent acquisitions of CFTC registered entities involved with or exposed to digital assets to identify any potential anomalies, or, to identify case studies of due diligence done well. Second, the MRAC could identify and evaluate due diligence procedures employed at other agencies to identify best practices. For example, in the securities markets, a private market actor seeking to acquire a broker-

dealer is obliged to undertake extensive due diligence, with the oversight and guidance of the SEC, FINRA and other SROs.[1]

While this process is not perfect, a comparative analysis of it and other processes employed by sister agencies could yield useful insights and could also be a steppingstone towards enhanced coordination with other regulators - given that many companies likely to acquire CFTC-registered entities are primarily regulated by a different agency.

Our second recommendation is to explore the topic of cybersecurity threats for blockchain products in general and for crypto derivative markets more specifically. Currently crypto derivatives trading (at least that under CFTC purview) does not typically occur directly on the blockchain, but on more conventional trading platforms. But the underlying assets for these trades do exist on the blockchain, which means that the cybersecurity risks found there can translate into operational and market risks.

The rhetoric around blockchain technology often asserts that, at least at its core, the immutability of blockchain protocols somehow provides, or will provide, a higher level of security for financial platforms than currently exists with traditional finance. We know the current reality is often far different. Like any software program or computer network, crypto platforms are just as vulnerable -if not more so - to the cyber security risks faced by more conventional computing tools.

- The code can contain bugs that offer hackers opportunities to breach platforms and steal assets. Sometimes, blockchain developers themselves use code to orchestrate inside jobs.
- Other times, flaws in code can execute transactions or activities that end up being harmful to exchange participants, despite participants' best efforts stop them.
- New layers of code that bypass the layer 1 chains to deal with slow transaction speeds introduce new complexity and vulnerabilities. Bridges created to deal with interoperability challenges have become one of the most vulnerable points of attack.
- And these are just the operational security challenges these platforms face; this doesn't touch structural vulnerabilities found underlying these chains – related to ISPs or data storage - or the examples of more traditional affinity fraud, phishing attacks, and ransomware exploits that have migrated to blockchain platforms and often thrived.

Additionally, these so-called decentralized networks often struggle to achieve 'true' decentralization, leaving them vulnerable to manipulation, without the benefit that can come from more formal intermediation. For example:

- The mining and validating activities on many major chains are concentrated in the hands of a few major mining pools.
- Token ownership both across platforms and even within the DAOs that 'govern' decentralized platforms and protocols are often disproportionately held by a small number of wallets.
- Maintenance for the source code that supports Bitcoin (and others) is managed by a handful of programmers.

As such, we recommend that the MRAC review the linkages between the cybersecurity risks found in blockchain platforms tied to existing crypto derivatives - both the operational risk found within chains

[1] https://www.davispolk.com/sites/default/files/2017-09-20_so_now_you_own_broker_dealer.pdf

housing the underlying assets, as well as the structural risks found within the information technology infrastructure supporting such platforms. The MRAC's review could identify actions that would better ensure integrity of movement and pricing of assets on the blockchain and help better protect customer funds as well as identify standards of custody that could guard against cybersecurity breaches.

The MRAC could also explore what risk emerges from crypto derivatives built off underlying assets that are not Bitcoin or Ethereum. Given that the definitions of crypto assets as securities, commodities or other classifications is sometimes contested, it would be helpful to understand the scale of cybersecurity risk that might be present should more crypto assets be deemed under the jurisdiction of the CFTC.

Ultimately the review could help recommend how to strengthen the CFCTs cybersecurity requirements for the platforms that house and generate the assets underlying these derivatives markets.

Thank you for your time and would be happy to provide any follow up thoughts on these topics for discussion.

-Mark Hays

Senior Policy Analyst
AFREF and DPEF
markhays@ourfinancialsecurity.org