METRIKA

April 11, 2025

Commissioner Hester M. Peirce
Chair
SEC Crypto Task Force
U.S. Securities & Exchange Commission
100 F Street NE
Washington, D.C. 20002

Re: Operational Risk Considerations for Digital Asset Innovation in Traditional Financial Markets

Dear Commissioner Peirce and Members of the SEC Crypto Task Force (the "Task Force"):

Metrika[1] appreciates the Crypto Task Force's request for information included in Commissioner Peirce's statement, entitled, "***There Must be Some Way Out of Here***"[2]. Metrika embraces the opportunity to share our perspective on the evolving risk landscape in digital assets, particularly the operational risks impacting the resilience and reliability of blockchain-based financial infrastructure. The growing ability to tokenize traditional securities – then trade, clear, settle and distribute them to investors on blockchain protocols will prompt a revolution in financial markets. This revolution will be driven by the reduced costs and efficiencies of decentralized finance ("DeFi") and the use of smart contracts.

About Metrika:

Metrika is at the forefront of the rapid developments in blockchain technology and its adoption. More specifically, Metrika provides critical risk management tools that enable traditional financial services and crypto-native firms to monitor their risks in this new technology environment. Metrika is the leading provider of real-time, dynamic risk management solutions for digital assets and blockchain technology. Our Software as a Service ("SaaS") platform enables financial institutions, enterprises, and regulatory bodies to proactively monitor, assess, and mitigate risks across tokenized assets, stablecoins, crypto, and blockchain networks. By leveraging advanced analytics, automated risk frameworks, and industry-aligned Key Risk Indicators ("KRIs"), we empower organizations to enhance transparency, compliance, and operational resilience in the evolving digital asset ecosystem. Already trusted by many leading global financial

---

[1] https://www.metrika.co/

[2] Commissioner Hester M. Peirce, "*There Must Be Some Way Out of Here,*" U.S. Securities & Exchange Commission (Feb. 21, 2025), *available at* https://www.sec.gov/newsroom/speeches-statements/peirce-statement-rfi-022125?utm_medium=email&utm_source=govdelivery (Last visited on April 7, 2025).

firms, Metrika is redefining risk management for the future of finance. Our firm is backed by top venture firms, including Coinbase Ventures, M12 (Microsoft's venture arm), Neotribe, NYCA Partners, and Samsung Next, among others.

I. Technology Resolves Many Traditional Compliance Risks While Introducing New Challenges for Firms to Address

The revolution in digitizing traditional financial markets through "tokenization" offers the opportunity for market participants to gain efficiencies in transactions while also increasing transparency. Tokenization allows the creation of a digital token backed by the rights of a security or other asset, that can be held, sold, and traded on a blockchain. When a tokenized asset is combined with the instant settlement capabilities of blockchain technology, it enables "atomic" transfers and the use of those tokens, including tokenized securities, across various decentralized finance (DeFi) services on multiple blockchain protocols. These DeFi services include decentralized exchanges and investment pools automated and governed by smart contracts.

The Task Force Chair has recognized that "tokenization also may give rise to unique risks and challenges" [3], given the movement of securities on-chain. These risks and challenges are driven by tokenized assets' use of new, open technology infrastructure. It is important to note that these risks and challenges can be addressed with minimal disruption to capital formation, providing robust investor protection with low-cost tools that innovators like Metrika have already been actively deploying in the marketplace. Tokenization-specific risks can be divided into four areas – (a) blockchain network risks; (b) inherent digital asset risk, (c) cross protocol risks; (d) risks in DeFi; and (e) atomic settlement risks. This letter addresses each of these topics in more detail below. Sections (a) – (c) are also responsive to question 40 proposed by the SEC in Commissioner Peirce's speech:

40. *Tokenization enables dematerialized securities to be mobilized (i.e., not held in and confined to a single centralized ledger). Are there any provisions under the federal securities laws that prevent these securities from being used in new blockchain-based transactions and applications, and, if so, what steps should the Commission consider taking to facilitate this innovation while* ***mitigating any related risks?*** *Are there amendments or new rules that the Commission should consider to ensure a merit- and technology-neutral approach to tokenization? Does the type of blockchain used (i.e., permissioned versus permissionless)* ***bear on this risk assessment?***

---

[3] Commissioner Hester M. Peirce, *There Must Be Some Way Out of Here,* U.S. Securities & Exchange Commission (Feb. 21, 2025), Question 40, *Question on General Risks of Tokenized Securities. "Creating a digital representation of a security on a blockchain or issuing a security directly on a blockchain does not change the substance of the security but may benefit issuers and investors. Moreover, the use of a blockchain-based database may be more secure in some respects than using a centralized database with a single point of failure.* ***Tokenization also may give rise to unique risks and challenges." (Emphasis Added)***

(a) Blockchain Network Risks

The nature of a blockchain network—whether permissionless or permissioned, public or private—significantly influences the types and severity of associated risks. A fundamental concern across all blockchain networks is technology risk. Given the relative novelty of blockchain technology and its continuous evolution to support financial innovation, vulnerabilities may emerge during the integration of new features and capabilities.

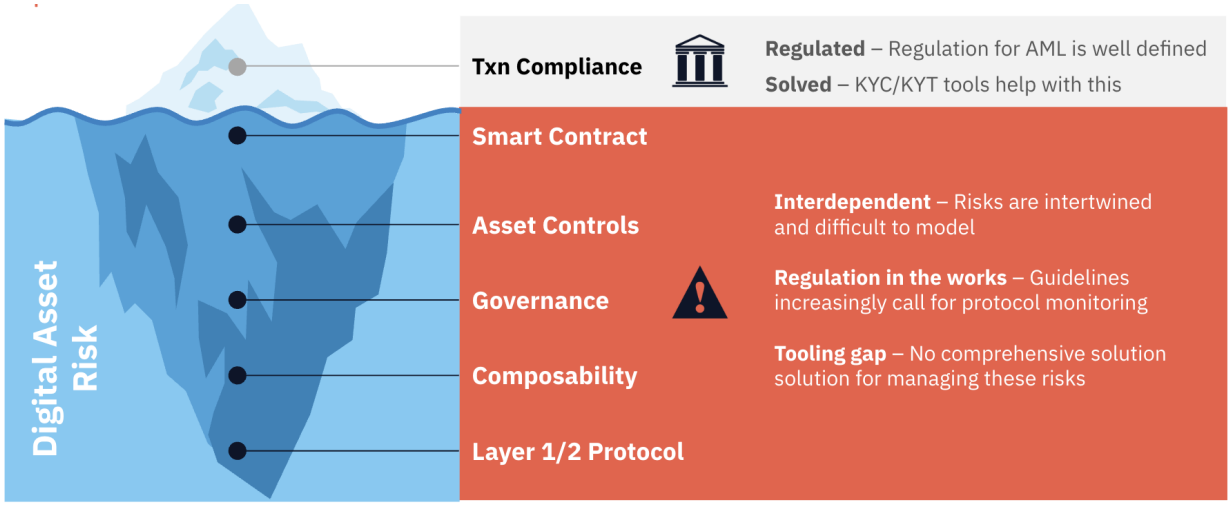


Figure 1: Updated Digital Asset Risk "Iceberg"[4]

Public Blockchain Networks:

Public blockchain networks, either Layer 1 or Layer 2, characterized by their open and decentralized nature, present several unique challenges. These include: (1) decentralization risks, (2) operational and technological risks, (3) governance risks, and (4) protocol security and reliability risks.

(1) Decentralization Risks. These encompass various dimensions, including geographic distribution of nodes, staking mechanisms, reliance on cloud services, and diversity of client software. For decentralization to be successful, a threshold level of adoption is required, creating a diverse network of nodes that are not controlled by the founders of the protocol. While decentralization improves governance risk (risk which must be managed by traditional finance firms engaged with the protocol), the network must have technological resilience as it is not controlled by a centralized actor.

(2) Operational and Technological Risks. The continuous operation of blockchain networks without maintenance windows (operating 24/7/365) necessitates network

[4] Nathan, A., Kaponis, D., & Lustgarten, S. (2023). *Understanding and managing blockchain protocol risks.* *Journal of Risk Management in Financial Institutions*, 16(4), 337–353. https://doi.org/10.48550/arXiv.2310.10797

upgrades to introduce new features. Such upgrades, executed without downtime, can introduce unforeseen risks. For instance, in May 2023, the Ethereum network experienced two brief periods of non-finalization. The first incident occurred on May 11, lasting for approximately 25 minutes, and the second took place about 24 hours later, lasting around an hour. During these periods, while blocks were proposed, they were not finalized, leading to temporary disruptions for some applications and infrastructure providers. Firms must be prepared for and understand these operational challenges.

(3) Governance Risks. Decisions regarding technological and ecosystem improvements are often made through community proposals. Challenges such as voter apathy or the concentration of voting power among a few influential participants can result in suboptimal governance outcomes.

(4) Protocol Security & Reliability Risks. Blockchain protocols that underpin tokenization processes (including issuance, transfer, and settlement) present foundational risks. Issues such as consensus vulnerabilities, validator centralization, protocol governance, and upgrade compatibility can all affect system reliability. Network downtime or forks may disrupt operations, while limited decentralization can undermine trust. Evaluating these risks requires assessing validator participation, governance transparency, and resilience to operational disruption.

Permissioned or Private Blockchain Networks:

While permissioned or private blockchain networks typically have a reduced attack surface compared to public networks, they are also not immune to certain risks. The risks include technology risks and security risks that must also be understood and addressed.

(1) Technology Risks & Continuous Evolution. Despite their restricted access, private blockchains must continually evolve to incorporate new features and maintain competitiveness with rapidly innovating public networks. This ongoing development can introduce unforeseen vulnerabilities as these technological updates may not be visible to users of the chain.

(2) Security Risks. Non-public blockchain networks may introduce additional risks that impact their security. Permissioned networks depend on the behaviors of the entities authorized to maintain and secure them and must ensure strong governance processes to avoid the risk of collusion. Private networks may lack transparency in their infrastructure, posing the risk that security exploits in the software used to maintain the blockchain remain undetected. In general, the lack of a financial requirement, such as a staked deposit, to participate in the consensus process of Permissioned and Private networks poses the risk of attacks at a lower cost.

- **Smart Contract Vulnerabilities.** Smart contracts on private blockchains can contain logical errors or security weaknesses (part of the inherent digital asset risk)

- **Interoperability Risks**. Although permissioned networks present a starting point of reduced risk for financial institutions, there is a continuous push to enable interoperability across those networks to make the offered financial services more attractive for the customers. As a result, there will be new risks being introduced that will gradually expand the overall risk profile similar to that of public, permissionless blockchain networks. This is the equivalent of private intranet networks in the 2000s that were being interconnected between enterprises, which eventually led to all of them being connected through the public internet.

In summary, while private blockchain networks offer enhanced control and privacy, they must diligently address technological and security challenges to ensure robust and secure operations.

(b) Inherent Digital Asset Risks

The use of smart contracts to tokenize assets on the blockchain enhances transparency, unlocks automation, and fosters innovative financial operations. However, these smart contracts also embed critical controls that define an asset's functionality, governance, and operational procedures, each of which introduces specific risks that are inherent to the tokenized asset itself.

Chief among these is the *access control framework* within the contracts, which dictates who can mint tokens, authorize or freeze asset transfers, vote on governance matters, or execute administrative actions. Weaknesses or inadequate protections in these access controls can grant unauthorized actors disproportionate or unintended authority, harming the security, integrity, and governance of the digital asset system. Additionally, the precise asset implementation within smart contracts—including token issuance processes, redemption (burning), freezing functionality, and rules governing token transfers—is critical, as it directly influences the asset's behavior, economic stability, and regulatory compliance. Since smart contracts frequently inherit functionality from existing contracts or rely on interdependent code structures, operational vulnerabilities can inadvertently propagate, leading to unintended behaviors or operational disruptions not anticipated by the issuer. Furthermore, although the transparency inherent to blockchain enhances oversight, it simultaneously amplifies the potential consequences of any implementation error, as mistakes are permanently recorded and immediately actionable. Thus, rigorous governance oversight, secure access control protocols, and meticulous operational design are essential for managing these blockchain-specific risks, preserving asset integrity, and realizing the technology's transformative potential safely and effectively.

(c) Cross Protocol Risks

When specific tokenized assets are issued across multiple blockchain protocols, assessing the cumulative risk becomes complex. There are examples of state-of-the-art tokenized securities, such as Government Money Market Funds (e.g., Franklin Templeton's, BENJI), which have been deployed across as many as eight different blockchains. Each protocol may have distinct properties and vulnerabilities, and the interplay between them can introduce additional risks. Transferring shares of these funds from blockchain A to blockchain B is increasingly common in these multi-chain tokenized funds. Orchestrating token issuance and redemptions seamlessly across chains, all while maintaining a consistent total supply, however, introduces significant operational complexity and risk. Each cross-chain transfer involves multiple points of potential failure, including reliance on bridging protocols, accurate synchronization of supply, and continuous reconciliation of blockchain and off-chain ledgers. This complexity necessitates constant, proactive monitoring and robust risk management practices to ensure asset integrity, prevent double issuance, and swiftly identify anomalies or compliance breaches. Therefore, a comprehensive risk assessment must consider the specific characteristics and potential vulnerabilities of each underlying blockchain infrastructure. This is essential to mitigating both protocol-specific risks in isolation and the additional risks affecting tokenized assets whose supply is distributed across multiple protocols. While tokenization and blockchain technology offer innovative avenues for financial services, they also introduce a spectrum of risks. Understanding and mitigating these risks is crucial for the sustainable development of DeFi ecosystems.

(d) Risks in DeFi

The principle of composability in DeFi—often described as financial "Lego blocks"—enables tokenized securities to seamlessly integrate into sophisticated and innovative financial instruments and protocols. For instance, it allows tokenized fund shares to serve as underlying assets for stablecoins, collateral for loans, or even backing assets for other tokenized funds. This interconnectedness, however, creates substantial composability risk: vulnerabilities in one component can quickly propagate, causing impacts across multiple linked platforms. A technical failure, liquidity crisis, or compliance breach within a single fund or asset could lead to cascading effects, potentially destabilizing stablecoins or DeFi protocols relying on those assets as collateral. Effective management of composability risk demands deep visibility into asset interdependencies, rigorous stress testing, continuous monitoring for anomalies, and proactive contingency planning to mitigate contagion effects in interconnected blockchain ecosystems.

For example, if a digital asset interacts with various DeFi services—such as liquidity pools, staking mechanisms, oracles, or cross-chain bridges—the risks associated with each service can propagate and compound, potentially affecting the asset's stability and security. A growing example in the market is the use of tokenized money market funds as reserves for the issuance of stablecoins or as collateral in DeFi lending pools. In both cases, the use of additional smart contracts, multi-protocol distribution and bridging

further increases the operational risk for firms investing on behalf of themselves or third-party investors.

(e) Atomic Settlement Risks

Near Instant atomic settlement is a fundamental breakthrough enabled by blockchain technology, as opposed to the current T+1 or T+2 clearing and settlement process in traditional financial markets. Atomic settlement brings significant efficiencies while reducing central counterparty risk.

Commissioner Peirce highlighted this issue in her statement under Question 45:

Question 45, *Question on Risks of Atomic Settlement. "The Commission recently adopted rule amendments to shorten the standard settlement cycle for most broker-dealer transactions from 'T+2' to 'T+1,' subject to certain exceptions. Tokenization is often characterized as an innovation that facilitates instant or simultaneous settlement ("atomic settlement") if all parts of a transaction are executed and settled on the same blockchain. What are the benefits of* ***atomic settlement,*** *and* ***what are the risks?*** *Should the Commission consider taking any actions that would encourage adoption of atomic settlement?"*

On Solana, for example, transactions typically finalize in 12 seconds, while on Ethereum, finality takes approximately 15 minutes (65–90 blocks at 12 seconds per block). Compared to the multi-day settlement cycles in traditional finance, these speeds represent a 100x improvement, marking a fundamental shift in financial infrastructure.

This efficiency comes with new real-time risks, however, that differ from the periodic or batch risks of traditional finance. Smart contracts can be upgraded at any moment, potentially altering asset controls. Risk management, once reliant on quarterly or annual spreadsheet-based assessments aligned with financial reporting cycles, must now adapt to a 24/7/365 environment where assets, protocols, and services continuously evolve on-chain. This shift necessitates real-time risk management platforms with embedded risk criteria and controls to keep pace with the rapid transformation of finance.

The ability to conduct atomic settlement of transactions across multiple blockchains is a key benefit of asset tokenization. At the same time, this additional capability also introduces risk associated with mismatched finality guarantees and time to finalization between different protocols. This underscores the need for parallel risk monitoring with coverage across many blockchains to maximize the utility of tokenized assets while minimizing risk.

II. Digital Assets Require a New Approach to Existing Custody and Control Rules

The unique characteristics of digital assets necessitate a reevaluation of traditional custody and control frameworks, particularly regarding activities like staking and voting.

Unlike physical assets, digital assets are managed through cryptographic keys and decentralized networks, introducing novel risks that traditional frameworks may not adequately address. The SEC should consider the following:

(1) **Custody and Control.** The management of digital assets relies on private keys. If these keys are compromised, assets can be irretrievably lost. Beyond key management, the integrity of the underlying blockchain network is crucial. Events such as "hard forks"—where a blockchain splits into separate paths—can alter the fundamental properties of an asset, affecting its value and legal standing. In addition, malicious modifications to smart contracts can redirect or siphon assets without the owner's consent, posing significant threats to asset security.

(2) **Staking and Voting Risks**. These risks were discussed in Commissioner Peirce's statement under Question 31: *Can a fund comply with the requirements of section 17(f) and the rules thereunder when trading, staking, voting, or otherwise engaging with crypto assets in which it invests? Should the Commission consider any changes to rule 17f-2 (the self-custody rule) or any other rules to facilitate transactions in crypto assets, and if so, what tailored conditions should the Commission propose to mitigate any related risks?"* Engaging in staking (participating in transaction validation) and voting (making governance decisions) exposes assets to additional layers of risk. These activities often require interacting with smart contracts or delegating control, which can be exploited if vulnerabilities exist. Moreover, these mechanisms could potentially be leveraged for illicit activities, inadvertently involving asset holders in transactions that could violate sanctions or regulatory requirements.

(3) **Network-Related Threats.** The decentralized nature of blockchain networks means that consensus attacks or vulnerabilities in the protocol can directly impact asset security. Unlike traditional assets, where risks are often isolated to specific custodians or intermediaries, digital assets are susceptible to network-wide events that can compromise their safekeeping.

Broker-Dealer Custody

The net capital rule for broker-dealers also should be considered differently in its treatment of digital assets, particularly crypto assets.

Question 25(b) in Commissioner Peirce's statement addressed this issue: *"**Under the net capital rule,** securities and commodities are treated as readily convertible into cash. However, they are subject to deductions (known as haircuts) to account for the market, credit, liquidity, basis, and **other risks inherent in the instrument.** The haircuts range from 0 to 100 percent. For example, exchange-traded equity securities have a 15 percent haircut, while securities without a ready market (e.g., securities that are not exchange traded) are subject to haircuts as high as 100 percent. Commodities are subject to a 20 percent haircut. How should crypto assets be evaluated to determine the appropriate haircut to apply?"*

To determine the appropriate haircut for crypto assets under the net capital rule, SEC-regulated institutions should adopt a comprehensive risk-based approach that addresses both traditional financial risk metrics (e.g., market, credit, and liquidity risks) and the unique risks inherent to digital assets (e.g., smart contract vulnerabilities, decentralization risks, and custody considerations) to adjust to the new paradigm.

A structured way to assess these risks is through established risk frameworks (each financial institution has its own), such as the DTCC's Digital Asset Securities Control Principles (DASCP), which identifies 30 risks and 50 controls to align digital asset risk management with traditional finance. These frameworks can help quantify the inherent volatility, market depth, and technological risks of crypto assets to determine appropriate haircuts.

To operationalize these risk frameworks, platforms like Metrika enable SEC-regulated institutions to generate live risk scores for digital assets. These scores provide real-time assessments of factors such as network stability, liquidity fluctuations, and security threats, allowing firms to dynamically adjust haircuts based on evolving market conditions rather than relying on static risk assumptions.

III. Tailored, Scalable Solutions Exist to Mitigate These Compliance Risks for Market Actors

Given the immense and rapidly changing technological landscape, Metrika has been at the forefront of developing new tools for leading SEC-regulated firms. As the SEC moves to consider rule changes that embrace blockchain technology and identify the new risks presented by some digital assets, it should also consider tools, like Metrika's, that are available to effectively monitor and address these risks. Looking at the best practices that have been developed by innovators in the financial industry so far, along with the solutions they are actively using to meet their obligations, can be a helpful roadmap for the SEC as it considers tailored and efficient compliance obligations.

Firms like Metrika provide an end-to-end risk management platform for SEC-regulated firms engaging with digital assets, which provides more coverage with less administrative costs. Our platform allows firms to define their own risk frameworks and assessments (including those that would be mapped to their SEC regulatory obligations) and allows those firms to monitor their KRIs in real-time. The platform provides a solution for a wide variety of digital asset use cases, as set forth below.

For example, in the following case study, a leading asset manager with an SEC-registered broker-dealer developed a risk framework for evaluating blockchain protocols for tokenizing assets. The asset manager integrated the client's existing framework and identified Key Risk Indicators ("KRIs") by analyzing protocol-level data, secondary markets for selling tokenized assets, and financial and governance information related to the digital asset. The implementation was completed in eight weeks, reducing internal workload through automation, enhancing visibility into operational risks and supporting the firm's regulatory compliance obligations.

As the SEC considers compliance obligations for SEC-regulated firms managing and custodying digital assets, it should encourage those firms to develop KRIs that align with the risks highlighted above. Real-time monitoring of KRIs should be a key component of

any regulatory framework to ensure that the additional risks of the underlying technology are covered.

IV. Targeted SEC Requirements Can Ensure Safe Adoption of Low-Cost, Low-Burden Monitoring Solutions to Ensure Efficient & Safe US Digital Financial Markets

Metrika encourages the SEC to consider adopting a tailored regime that encourages the adoption of low-cost, low-burden monitoring solutions, which will support strong capital formation with robust market and appropriate investor protections. As part of the Crypto Task Force's proposed changes, Metrika makes the following specific recommendations:

(1) **Create Specific Digital Asset Custody Requirements for Investment Advisers and Broker-Dealers:** The SEC should implement clear digital asset custody requirements that encompass both key management and the risks inherent to operating on a novel financial market infrastructure such as a blockchain network. This includes setting standards for how custodians should handle digital asset risk consisting of: (a) the inherent asset risk; (b) protocol or multi-protocol risk; and, (c) third-party risks arising from providers of other digital asset services (e.g., staking).

(2) **Create Appropriate Issuer Obligations for Digital Asset Securities:** The SEC should require minimum issuer obligations of digital asset securities that require issuers to conduct risk assessments of the implementation of the asset on the specific blockchain protocol. This could be incorporated into the traditional securities registration requirements, updated for the tokenized nature of these assets.

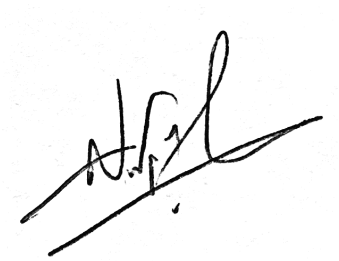
(3) **Implement Efficient Real-Time Risk Management:** Given the rapid pace at which digital asset ecosystems evolve; traditional periodic assessments are insufficient. Adoption of real-time risk management strategies at investment advisers, broker-dealers and custodians dealing with digital asset securities is essential to promptly identify and respond to emerging threats, ensuring the ongoing security of digital assets. The SEC and FINRA should also implement real-time risk management and market surveillance to ensure they have a full view of the digital asset marketplace. The SEC can access the relevant information, which is publicly available on the blockchain, through third-party tools like Metrika without burdening registrants with reporting obligations.

By acknowledging and addressing these unique risks, the SEC can develop more robust frameworks that ensure the safekeeping of digital assets, aligning with the evolving landscape of digital finance.

***

Thank you for the opportunity to submit our views on these important issues. We look forward to working with the Crypto Task Force to help provide insight and expertise on these issues in the future.

Sincerely,



Nikos Andrikogiannopoulos
Founder & CEO
Metrika Inc.