



April 2, 2025

The Honorable Hester M. Peirce  
Commissioner  
U.S. Securities and Exchange Commission  
100 F Street, NE  
Washington, D.C. 20549

By submission to <https://www.sec.gov/about/crypto-task-force/submit-written-input>

**RE: Written Input to the Crypto Task Force**

Dear Commissioner Hester M. Peirce:

We appreciate the opportunity to provide written input to the questions the SEC's Crypto Task Force is considering. This submission provides responses to the Task Force's questions #18 regarding the monitoring of custodial storage of customers' digital assets and #23 regarding commonly accepted practices and standards for auditing and accounting for crypto asset investments and transactions.

*About Taxbit*

Taxbit is a software technology company that specializes in tax compliance and financial reporting for digital assets. We assist businesses and governments with navigating the complexities of digital assets, specifically, the challenges of accurately reporting taxable gains, losses, and income from digital asset activities, complying with Generally Accepted Accounting Principles applicable to digital assets for companies following both US GAAP and IFRS, and broadly helping companies with portfolio tracking and management reporting. Our tax and accounting platform is used by some of the largest digital asset exchanges, payment processors, Fortune 500 adopters of digital assets, accounting firms, and government organizations worldwide. Companies rely on Taxbit to ensure that their tax and financial reporting results from digital asset activities are accurate, complete, transparent, and fully auditable.

*Relevant Task Force Questions*

**Question 18:**

*The crypto markets are inherently transparent because they use open-source data, from public blockchains to open application programming interfaces ("APIs"). Are there programmatic/technological ways that crypto market participants, intermediaries, potential self-regulatory organizations, or regulators can monitor crypto markets using open-source data? How would this take into consideration nested accounts on centralized exchanges, given that this activity may not appear in public ledgers? Is open-source data sufficient for the market to monitor trading and therefore what non-public information might warrant mandatory disclosure? What sort of open-source tools can be used for enhanced transparency, such as proof of reserves, or proof of holdings? What are the limitations of such tools and such data?*

Yes. Existing technology allows for real-time accounting and reporting of digital asset quantities and values held in any combination of wallets in a customer-facing enterprise or any other entity possessing digital assets. When facing a regulator, or even the general public at large, such accounting can be used to prove that entities possess the digital assets they claim to possess, a concept generally known as proof of reserves (“PoR”). A PoR practice serves to prove that those entities are solvent and have the necessary liquidity to fulfill their redemption obligations to their customers on demand. The vast majority of digital asset trading activity takes place on centralized exchanges that maintain customer assets in omnibus wallets, making reliance on blockchain data alone somewhat incomplete for consumer asset-protection purposes. Furthermore, custodial wallet addresses are not necessarily a matter of public knowledge (nor should they necessarily be), so observing asset movements among wallets also does not provide the requisite visibility for ensuring the protection of customer assets.

The digital assets industry is experiencing a resurgence in global acceptance, having suffered financially and reputationally from high-profile bankruptcies and criminal malfeasance by a small number of players only a few short years ago. To maintain this positive momentum and to ensure the continued vitality of the sector and its promise of democratizing finance, the SEC might adopt the wisdom of former President Ronald Reagan with his strategy of, “Trust but verify.”<sup>1</sup> The idea behind that saying was simple: checking on a counterparty to follow through on its agreements, even when the parties might want to trust one another, breeds ongoing trust, which further enhances their relationship over time. The SEC might adopt this wisdom with digital asset custodial entities it regulates and will regulate, as the existing technology allows them to report PoR in real-time the digital assets they hold on behalf of others. As alluded to in the question above, such reporting can be done by API directly from custodian to regulator at any given time rather than in delivery of reports at preset increments.

In recent years, bipartisan legislation has been introduced to require PoR reporting by digital asset custodians. During the last Congress, Sens. Tillis (R-N.C.) and Hickenlooper (D-CO) introduced the PROOF Act,<sup>2</sup> which would have required digital asset exchanges and custodians to submit a periodic PoR inspection by a neutral third-party to Treasury. It also would have established regulatory standards for how digital asset entities can custody customer assets, which included a prohibition on commingling customer-owned assets with entity-owned assets.<sup>3</sup> The senators introduced the PROOF Act in the wake of the FTX scandal, which involved misappropriating billions of dollars worth of digital assets belonging to FTX customers. This scandal remains fresh in our collective memory. According to Sen. Tillis,

The FTX fiasco was a direct result of mismanagement and grossly unethical decision-making, leading to significant fraud and loss of investor funds... The PROOF Act would improve regulation of the cryptocurrency industry by explicitly prohibiting the co-mingling of funds, while also setting a strong transparency standard with the already-used industry best practice of PoR.<sup>4</sup>

---

<sup>1</sup> President Ronald Reagan, Remarks on Signing the Intermediate-Range Nuclear Forces Treaty (Dec. 8, 1987), *available at* <https://www.reaganlibrary.gov/archives/speech/remarks-signing-intermediate-range-nuclear-forces-treaty>.

<sup>2</sup> Proving Reserves Of Others’ Funds Act (PROOF) Act, S. 3087, 118th Cong. (2023).

<sup>3</sup> *Id.*; *see also*, Proving Reserves Of Others’ Funds Act (PROOF) Act, Section by Section, *available at* <https://www.tillis.senate.gov/services/files/D9B718BB-53B8-4060-9B27-031902972ED2>.

<sup>4</sup> Press Release, Sen. Tom Tillis, Tillis, Hickenlooper Introduce Bipartisan Legislation to Prevent Another FTX Disaster (Oct. 20, 2023), *at* <https://www.tillis.senate.gov/2023/10/tillis-hickenlooper-introduce-bipartisan-legislation-to-prevent-another-ftx-disaster>.

Real-time on-chain PoR reporting might have prevented the misappropriation of assets at FTX. At its core, the misconduct was relatively straightforward: transferring assets equitably belonging to FTX customers from one wallet to another entity's wallet. In 2022, FTX proprietor Sam Bankman-Fried reportedly lent approximately \$10 billion worth of customer assets to his investment firm, Alameda Research, in an attempt to cover losses stemming from unrelated digital asset bankruptcies. This ultimately triggered a customer run on FTX.<sup>5</sup> Had FTX existed under a regulatory framework requiring real-time PoR visibility into its customer omnibus wallet(s), that regulator could have theoretically picked up the phone to FTX and asked the company what it was doing with those assets – or simply have stopped that transfer from occurring without further explanation by the company, depending on the stringency of the reporting requirement. In a blockchain environment where transfers occur within minutes, delayed or periodic PoR disclosures might offer little protection. Given the speed of blockchain activity, PoR reporting should be real-time or near real-time. A PoR report to a regulator sent weeks later could very well be useless in protecting customer assets.

Complete on-chain PoR reporting could include (1) a regulating agency having real-time knowledge about the universe of assets held in customer omnibus accounts, (2) the total values of those assets, (3) the universe of blockchains associated with those assets, (4) the wallet addresses corresponding to customer omnibus accounts, (5) the individuals at the regulated entity authorized to move assets into and out of those wallets, and (6) a notification protocol for statistically large outbound transfers of customer assets.

Still, the efficacy of asset-side PoR reporting on its own ends at the edge of blockchain activity. Off-chain commitments – such as rehypothecation of collateral assets – do not appear in PoR reporting, and custodial entities' liabilities to their customers are necessary for a complete accounting intended to protect customers. To the extent the SEC requires custodial entities to provide Merkle-tree analyses regarding customer accounts to help inform that liability side of an accounting, the SEC should strongly resist any impulse toward a reporting requirement that would be tantamount to revealing customer-specific information such as assets held and balances.

Generally, PoR should be considered one part of a broader, multidimensional custodial reporting framework. While PoR can provide visibility at the wallet level, it may not disclose asset-level details for nested accounts such as other exchanges using omnibus wallets. Such a hurdle could be overcome, however, to the extent future regulations might require wallet segregation for nested accounts.

Despite these limitations, a PoR requirement would serve as an essential foundation for digital asset custodians when adding up their off-chain commitments involving on-chain assets. Whatever those custodians might do with those assets off-chain, those commitments would still have to complement their known on-chain holdings. Ultimately, such a requirement would breed trust in investors and consumers, knowing that their digital asset custodians' reserve holdings match what they claim to manage.

---

<sup>5</sup> Vicky Ge Huang, Alexander Osipovich, Patricia Kowsmann, *FTX Tapped Into Customer Accounts to Fund Risky Bets, Setting Up Its Downfall*, WALL STREET JOURNAL (Nov. 11, 2022), available at <https://www.wsj.com/articles/ftx-tapped-into-customer-accounts-to-fund-risky-bets-setting-up-its-downfall-11668093732>.

**Question 23:**

*Are there commonly accepted practices and standards for auditing and accounting for crypto asset investments and transactions, including those related to valuation? How about with respect to verifying the existence and valuation of crypto assets, both among auditors and attestation providers (including non-accountant providers)? Should the Commission propose additional or specific requirements to address the unique nature of crypto assets?*

FASB and IFRS treat digital assets as intangible assets and, under ASC 350-60, entities that hold certain digital assets must account for them at fair value with changes included in net income each reporting period. As general matters, auditors of digital assets should be able to verify them by tracking and confirming the existence of those assets on entity-owned and -controlled blockchain wallet addresses. Auditors follow a confirmation process today to verify cash balances (as an example) and validate the assets a company owns. This same concept can readily apply to digital asset holdings that are held in self-custody wallets, the existence of which can be confirmed against the relevant blockchain. If those holdings are custodied by a centralized entity such as an exchange, then the centralized party can verify existence in a similar way that banks provide confirmation support today.

Furthermore, pricing and fair value accounting standards are outlined in ASC 820 and have been used for many years in traditional markets. These pricing and valuation principals are currently applied to and should continue to apply to digital assets. This includes the requirement to identify a Principal Market from which a price is used to determine the fair value of held assets.

\* \* \*

Again, we appreciate the SEC's commitment to developing a practical regulatory framework for digital assets and the various entities within the digital asset ecosystem. Should you have any questions about this submission, please feel free to contact us.

Sincerely,



John Schoenecker  
Head of Policy



Aaron Jacob  
Head of Accounting