United States Senator Thom Tillis (R-NC)

The Proving Reserves of Others Funds (PROOF) Act

Background: The implosion of the digital asset platform FTX was largely possible due to two key organizational weakness and failures: (1) FTX co-mingled customer funds with its institutional and proprietary funds and (2) FTX diverted significant portions of its customer deposits to its subsidiary, Alameda Research, resulting in a systemic lack of adequate reserves to back its customer balances.

What It Does: The Proof Act seeks to address these dual issues by establishing clear and concrete customer protections, while also creating an important mechanism to provide greater transparency into digital asset exchange and custodial operations. Specifically, the PROOF Act would:

(1) **Establish regulatory standards on how digital asset institutions can hold customer assets, including a prohibition of the co-mingling of customer funds**

(2) **Require digital asset exchanges and custodians to submit to a Proof of Reserves** (see below) **inspection by a neutral third-party**

The PROOF Act would require any institution that provides exchange or custodial services of digital assets to submit to a monthly PoR inspection by a neutral third-party firm (with explicit preference towards an auditing firm). An attestation of the results of the inspection is then submitted to the U.S. Department of the Treasury, which is required to post the information publicly. Failure to submit to this inspection would result in a civil fine, derived through a tiered system that increases penalties for repeat offenders.

Proof of Reserves (PoR): put simply, PoR is a process used to verify whether an institution holds sufficient reserves to back its customer balances. By utilizing already-established cryptographic processes, such as Merkle trees or zero-knowledge proofs, exchanges and custodians are able to show they actually have possession of the reserves they claim. Digital asset's unique auditability properties mean that ownership can be proven to a disinterested and impartial third party with relative ease.

Though some firms have informally furnished PoR information for years, and more have promised to do so following the failure of FTX, adherence to these PoR procedures has been ad hoc, implementations have been non-standard, and not all of attestations have been overseen by CPA firms.

Bottom Line: American clients of digital asset platforms deserve better assurances regarding deposits held, and thus the solvency of these platforms. The PROOF Act would improve regulation of the cryptocurrency industry by explicitly prohibiting the co-mingling of industry funds, while also setting a strong transparency standard with the already-used industry best-practice of PoR. Combined, these two steps will help build trust that investors, both institutional and retail, can engage in digital asset markets.