April 13, 2026

By electronic submission (crypto@sec.gov)

The Honorable Hester M. Peirce

Commissioner and Crypto Task Force Lead

Members of the Crypto Task Force

U.S. Securities and Exchange Commission

100 F Street NE

Washington, DC 20549-0213

Re: Public Comment on File Number 4-894 — Cryptographic Compliance Infrastructure for Permissioned Digital Asset Markets on High-Performance Public Blockchains

Commissioner Peirce and the Crypto Task Force:

We write to share technical observations regarding the regulatory treatment of non-custodial user interfaces and permissioned market infrastructure for tokenized securities, in response to the Commission's ongoing solicitation of public input on digital asset market structure under File Number 4-894. We commend the Division of Trading and Markets' April 13, 2026 Staff Statement on Covered User Interface Providers and Commissioner Peirce's accompanying remarks, which together represent meaningful progress toward regulatory clarity.

This comment is submitted by technologists and compliance professionals who have studied the intersection of advanced cryptographic systems and securities regulation. Our purpose is to describe—at a level of technical specificity useful to both blockchain engineers and policymakers—how two classes of cryptographic infrastructure create the compliance capabilities necessary for permissioned institutional markets on high-performance public blockchains such as Solana and Sui. We do not advocate for any particular product or project; rather, we seek to educate on the architectural primitives that make compliant, non-custodial, privacy-preserving digital asset infrastructure technically achievable today.

I. The Compliance Architecture Gap

Today's regulatory framework for digital asset markets distinguishes between custodial and non-custodial systems, between intermediated and direct execution, and between opaque and transparent operations. These distinctions are appropriate and well-founded. However, the Commission's framework does not yet fully account for a third category that has emerged from

recent advances in applied cryptography: systems where compliance properties are enforced by mathematical proof rather than organizational policy.

In traditional financial infrastructure, compliance is achieved through personnel, internal controls, and auditable procedures. A broker-dealer's compliance department monitors transactions; a custodian's internal controls prevent unauthorized access; a clearing agency's procedures ensure settlement finality. These mechanisms depend on human judgment, organizational integrity, and the legal enforceability of contractual obligations. They work, but they are expensive, subject to human error, and ultimately depend on trust in the organization's good-faith operation.

Emerging cryptographic technologies offer a fundamentally different approach: embedding compliance constraints directly into the mathematical structure of the system itself, so that certain regulatory requirements are satisfied by the operation of the protocol rather than by the promises of the operator. This comment describes two such technologies—two-party computation with multi-party computation (2PC-MPC) threshold signing, and threshold fully homomorphic encryption (Threshold-FHE)—and explains how they create compliance capabilities that are directly relevant to the Commission's stated objectives.

II. Two-Party Computation with Multi-Party Computation (2PC-MPC): Trustless Non-Custody and Programmable Policy Enforcement

A. The Problem: Non-Custody as a Spectrum

The April 13 Staff Statement correctly identifies non-custodial operation as a threshold condition for Covered User Interface Provider status. We respectfully observe that "non-custodial" is not a binary category in practice. Existing systems exhibit a spectrum of custodial exposure:

- **Fully custodial:** A single entity holds and controls the complete private key material. The entity can unilaterally move assets. This is the traditional custody model (e.g., an NYDFS-licensed trust company).
- **Semi-custodial (standard MPC):** The private key is divided into shares held by multiple parties using traditional multi-party computation. However, in many commercial implementations, the platform operator holds enough shares to reconstruct the key or generate a valid signature without the user's active participation. The user's non-custody depends on the operator's contractual promise not to exercise this capability. This is custodial by architecture even if non-custodial by agreement.
- **Cryptographically non-custodial (2PC-MPC):** The private key is divided into exactly two logical shares—one held by the user, one distributed across a decentralized network of signers using threshold homomorphic encryption—such that no transaction can be signed without the user's cryptographic participation. This is non-custodial by mathematical impossibility, not by contractual promise.

The distinction between the second and third categories has direct regulatory implications. A 2023 vulnerability disclosure involving a major semi-custodial MPC platform demonstrated that

implementation flaws in traditional MPC architectures could allow private key material to be extracted through malicious signature requests. This is the type of risk that the custodial/non-custodial distinction is designed to address—and it is a risk that properly implemented 2PC-MPC architectures eliminate by design.

B. How 2PC-MPC Works: A Technical Primer for Policymakers

We provide the following technical description to help the Commission and its staff evaluate the compliance properties of 2PC-MPC architectures with precision. The protocol operates in three stages:

Stage 1: Distributed Key Generation (DKG). When a user creates a wallet, the system generates two cryptographic key shares through a cooperative protocol between the user and a decentralized network of signing nodes. One share is retained by the user; the second share is encrypted on the network using homomorphic encryption, which allows network nodes to perform computations on the encrypted share without ever decrypting it. From these shares, a public key is derived—the address from which the wallet operates on any target blockchain—but neither party ever sees, holds, or can reconstruct the complete private key. The complete private key does not exist in assembled form at any point in the system's lifecycle.

Stage 2: Collaborative Transaction Signing. When a transaction needs to be authorized, the user submits their partial signature (cryptographic data derived from their share) and the transaction message. The network then computes the signature homomorphically over the encrypted network share—meaning the network performs the mathematical operation on the share without decrypting it—and combines the result with the user's input and a precomputed presignature element. The output is an encrypted valid signature, which is then decrypted by a threshold of network participants through threshold homomorphic decryption. The final signature is valid for the target blockchain (e.g., ECDSA for Bitcoin and Ethereum, EdDSA for Solana, Sui, and Cardano). At no point in this process is the private key reconstructed.

Stage 3: Smart Contract Policy Binding. This is the step that transforms non-custodial signing into programmable compliance enforcement. The wallet can be bound to smart contract logic on a coordination blockchain (such as Sui or Solana), which defines what transactions the wallet is authorized to execute. Before generating any signature, the signing network verifies a state proof from the controlling smart contract, confirming that the requested transaction satisfies the programmed policy. If the policy is not satisfied—if the recipient wallet is not on an approved whitelist, if the transaction exceeds a defined limit, if the user has not completed required identity verification—the signature simply cannot be generated. This enforcement occurs at the cryptographic layer: it is not a software check that can be overridden by an administrator, but a mathematical precondition of the signing operation itself.

C. Compliance Capabilities Created by 2PC-MPC

The technical properties described above create specific compliance capabilities that are directly relevant to the Commission's regulatory objectives:

1. Non-custody by mathematical proof. Unlike contractual non-custody (where an operator promises not to exercise control it technically possesses), 2PC-MPC makes unilateral control

over user assets mathematically impossible. Even if the entire network of signing nodes were compromised, they could not independently generate a valid signature without the user's active cryptographic participation. This eliminates the "qualified custodian ambiguity" that arises under the Investment Advisers Act custody rule when semi-custodial MPC providers hold key shares for investment advisers' client assets.

2. Programmable, immutable policy enforcement. Because the signing operation is bound to smart contract logic, compliance policies are enforced at the infrastructure layer—not by personnel in a dashboard. An institutional access policy encoded in a smart contract cannot be overridden by an administrator, cannot be selectively bypassed, and cannot be modified without an on-chain record. This is directly relevant to the DTCC No-Action Letter's Registered Wallet requirement: a 2PC-MPC wallet bound to a smart contract that enforces DTC Participant registration makes it mathematically impossible to transfer a tokenized entitlement to an unregistered address. The signature for such a transfer cannot be produced.

3. Chain-agnostic, native asset control. Because 2PC-MPC wallets generate valid signatures for any chain supporting standard digital signature algorithms (ECDSA, EdDSA, Schnorr), a single wallet can control native assets across multiple blockchains without bridges, wrapped tokens, or custodial intermediaries. This means a user's policy-governed wallet on Sui can sign transactions on Solana, Ethereum, Bitcoin, or a permissioned chain like Canton—with the same compliance constraints enforced cryptographically across all target networks. This addresses the interoperability challenge the Commission and DTCC have identified: cross-chain asset movement that maintains compliance properties throughout the lifecycle.

4. Guaranteed output and fault tolerance. Well-designed 2PC-MPC protocols provide guaranteed output: even if some network participants are offline or behaving maliciously, as long as the required threshold of honest signers participates, the signing session completes successfully. Public verifiability ensures all operations are auditable, and identifiable abort mechanisms allow the network to detect and attribute malicious behavior. These properties make 2PC-MPC suitable for institutional operations that require high availability and auditability.

5. Scalable broadcast architecture. Advanced 2PC-MPC implementations leverage broadcast communication through blockchain consensus protocols (such as DAG-based Byzantine fault-tolerant consensus), reducing message complexity from $O(n^2)$ to $O(n)$ and enabling networks with hundreds or thousands of signing nodes to operate at sub-second latency. This makes the architecture practical for high-frequency institutional trading environments on chains like Solana, which process thousands of transactions per second.

III. Threshold Fully Homomorphic Encryption (Threshold-FHE): Privacy with Authorized Regulatory Discovery

A. The Problem: Privacy vs. Regulatory Transparency

Public blockchains expose every balance, every trade, and every position to the world. This is a compliance and competitive impossibility for institutions bound by confidentiality obligations

under Regulation NMS, MiFID II, and fiduciary duties. Conversely, fully opaque privacy chains—where no party, including regulators, can observe transaction details—face justified regulatory scrutiny because they preclude the oversight that securities laws require.

The Commission has rightly identified this tension. The ideal outcome is a system that provides privacy by default during normal operations while maintaining the ability for authorized parties to access specific records when legally required—a property that might be described as "privacy with a compliance trapdoor." Threshold-FHE is the cryptographic technology that makes this possible.

B. How Fully Homomorphic Encryption Works: A Technical Primer

Fully Homomorphic Encryption (FHE) is a class of encryption schemes that allows computation on encrypted data without decrypting it first. This is not a theoretical concept—it is a property demonstrated in published, peer-reviewed cryptographic research that has advanced significantly in the past five years.

In a standard encryption scheme, if you want to add two encrypted numbers, you must first decrypt them, perform the addition, and then re-encrypt the result. This means the computation engine must have access to the plaintext—a fundamental privacy limitation. In an FHE scheme, addition and multiplication (and therefore any computation expressible as a combination of these operations) can be performed directly on the encrypted values (called ciphertexts). The result, when decrypted, is the same as if the operations had been performed on the plaintext values. The computation engine never sees the underlying data.

For digital asset markets, this means:

- Account balances can be stored on-chain in encrypted form. Validators, indexers, block explorers, and all other public observers see only ciphertexts—not the actual balances.
- Trades can be matched and executed on encrypted order data. A matching engine can determine that a buy order meets a sell order's price without knowing either party's actual price, quantity, or identity.
- Portfolio positions, collateral ratios, and risk calculations can be computed on encrypted state, enabling institutional operations on public chains without exposing competitive or confidential information.

C. The Critical Innovation: Ring-Enhanced FHE for Practical On-Chain Computation

Traditional FHE schemes have faced a fundamental trade-off: schemes optimized for arithmetic operations (addition, multiplication) perform poorly on logical operations (comparisons, conditional branching), and vice versa. This trade-off made FHE impractical for most financial applications, which require both arithmetic (adjusting balances, computing fees) and logic (comparing prices, evaluating policy conditions, determining order matching).

Recent advances in ring-enhanced FHE (RE-FHE) have eliminated this trade-off. RE-FHE schemes support unified arithmetic and logical operations on encrypted 64-bit machine-word values—enabling encrypted programs to switch seamlessly between math and logic, much like

a conventional CPU operates on plaintext data. This means comparisons (greater-than, equal-to, less-than), conditional branching (if/else), scoring, and policy decisions all work natively on encrypted inputs.

For the securities market context the Commission is evaluating, RE-FHE makes the following operations practical on encrypted data: verifying that a counterparty's wallet satisfies KYC/AML requirements without exposing identity data; computing whether a proposed trade falls within regulatory position limits; evaluating whether a transfer would violate lock-up periods or maximum holding constraints; and performing the price-comparison logic necessary for trade matching and best-execution analysis.

Published benchmark improvements over the previous leading FHE framework (TFHE, which dominated since 2016) include ciphertext sizes roughly 100 times smaller, multiplication approximately 20 times faster, and addition approximately 1,000 times faster. These performance characteristics make encrypted computation on high-throughput blockchains like Solana technically viable for the first time.

D. Threshold-FHE: Decentralized Decryption as Regulatory Architecture

Standard FHE has a critical limitation from a regulatory perspective: someone must hold the decryption key. If a single entity holds that key, FHE merely shifts the trust problem from the computation layer to the key-holder—a centralized point of trust and failure that undermines both the privacy guarantee and the decentralization properties that public blockchains are designed to provide.

Threshold-FHE solves this problem by distributing the decryption key across a decentralized network of participants using threshold cryptography. No single participant holds the complete decryption key. A threshold of participants (e.g., two-thirds of the network by stake weight) must cooperate to decrypt any specific ciphertext. This distribution creates three properties of direct regulatory relevance:

1. Privacy by default. During normal operations, encrypted data remains encrypted. No single party—not the platform operator, not any individual network participant, not any validator or indexer—can access the plaintext. This satisfies institutional confidentiality requirements and prevents front-running, information leakage, and unauthorized surveillance of trading positions.

2. Authorized regulatory discovery. When a lawful discovery order requires access to specific transaction records, the threshold decryption mechanism can be invoked to decrypt the targeted records—and only the targeted records—through a multi-party cooperation protocol. This requires the coordinated participation of a threshold of network participants, creating a process that is auditable, attributable, and resistant to abuse. It is architecturally analogous to the multi-party approval requirements for wiretap orders or bank secrecy act record requests, but enforced cryptographically rather than procedurally.

3. Aggregate reporting without individual decryption. Because FHE allows computation on encrypted data, aggregate statistics—total trading volume, position concentration metrics, compliance exception counts—can be computed and reported to regulators from encrypted transaction data without decrypting any individual record. This enables the quarterly reporting

obligations contemplated in the DTCC No-Action Letter while preserving participant-level privacy during normal operations.

E. The 2PC-MPC and Threshold-FHE Synergy

These two technologies are not merely complementary—they are architecturally synergistic when deployed together. A 2PC-MPC signing network already employs threshold homomorphic encryption for its core signing operations: the network's key share is encrypted homomorphically, and signing is performed as a computation on encrypted data, with the result decrypted by a threshold of participants. This same infrastructure—the same decentralized network of MPC nodes, the same threshold decryption protocol, the same Byzantine fault-tolerant consensus layer—naturally extends to serving as the decryption committee for FHE computations on the application layer.

The combination creates a unified cryptographic architecture in which non-custodial signing, programmable policy enforcement, private execution, and authorized regulatory discovery are all provided by a single decentralized infrastructure layer. This is not a stack of separate products bolted together—it is a coherent cryptographic system where each layer reinforces the security and compliance properties of the others.

IV. Application: Creating Permissioned Markets on High-Performance Public Blockchains

With these cryptographic primitives established, we now describe—at a high level—how they combine to create permissioned institutional markets on public, permissionless, high-throughput blockchains like Solana and Sui. This is the architectural pattern we believe is most relevant to the Commission's innovation exemption framework and the DTCC Tokenization Services pilot.

A. Smart-Contract-Enforced Access Control at the Token Level

Modern blockchain token standards—such as Solana's Token-2022 extensions—enable programmable transfer restrictions to be embedded directly into the token itself. A tokenized security can be configured so that every transfer instruction is evaluated against an on-chain compliance module before execution. The module checks whether the sender is verified (KYC/AML), whether the receiver holds the required accreditation, whether the transfer violates jurisdictional restrictions, lock-up periods, or maximum holding limits. If any check fails, the transfer reverts at the contract level—it does not execute. This is enforcement at the protocol layer, analogous to the DTCC's Registered Wallet requirement, but enforced by the mathematics of the blockchain rather than by the policies of an intermediary.

B. Zero-Knowledge Identity Verification

Zero-knowledge proof systems enable a user to prove compliance attributes—jurisdictional eligibility, accredited investor status, OFAC clearance, proof of personhood—without revealing the underlying personal data to the protocol, the counterparty, or the public blockchain. The

verification is mathematically sound: the proof demonstrates that the prover possesses a valid credential from an approved issuer, without revealing the credential itself. This creates portable, privacy-preserving identity that can be verified on Solana, Sui, Ethereum, and permissioned chains without duplicating KYC processes across each environment—addressing one of the most significant operational burdens for institutional participants in multi-chain environments.

C. Cross-Chain Coordination Without Bridges or Wrapped Assets

2PC-MPC wallets generate valid native signatures for any target blockchain. An institutional wallet governed by a smart contract on Sui can sign transactions on Solana, Ethereum, Bitcoin, or a permissioned settlement chain—using the native signature algorithm of each target chain (EdDSA for Solana and Sui, ECDSA for Ethereum and Bitcoin, Schnorr where required). Assets move as native tokens, not as wrapped or bridged representations, eliminating the counterparty risk, smart contract vulnerability exposure, and liquidity fragmentation that bridges introduce. The compliance policy defined on the coordination chain travels with the wallet across all target networks.

D. Private Execution with Public Settlement

FHE adds a confidential execution lane alongside the public settlement lane of a high-throughput blockchain. The lifecycle of a private transaction proceeds as follows:

1. Inputs are encrypted client-side before submission to the blockchain.
2. The encrypted work is dispatched to a confidential execution environment coordinated by the MPC signing network.
3. Programs evaluate logic on encrypted state—computing trade matches, evaluating policy conditions, adjusting balances—without decrypting any underlying data.
4. Only authorized outputs are revealed or trigger external actions, governed by the policy layer described above.
5. Final state transitions and settlement are committed to the public blockchain, maintaining composability with the existing on-chain ecosystem.

This architecture preserves the auditability, composability, and finality properties of public blockchains while adding the confidentiality protections that institutions require. Encrypted programs can interact with non-encrypted programs on the same chain—the privacy is additive, not isolating.

E. The Result: A Permissioned Environment on a Permissionless Chain

The combination of these four elements—smart-contract-enforced access control, zero-knowledge identity, 2PC-MPC policy-bound signing, and FHE with threshold decryption—creates a permissioned institutional environment operating on public, permissionless blockchain infrastructure. Participation is gated by cryptographic proof of compliance attributes. Transfers are constrained by protocol-level enforcement. Execution is private. Regulatory discovery is available through threshold decryption. And the entire infrastructure is non-custodial: the platform operator never holds key material, never sees

plaintext transaction data, and cannot unilaterally override the compliance policies encoded in the smart contracts.

This is the architectural paradigm that the Commission's innovation exemption and Covered User Interface Provider frameworks are, in our view, designed to accommodate.

V. Recommendations for the Commission

Based on the technical analysis above, we respectfully offer the following recommendations:

1. Recognize cryptographic non-custody as a distinct category. Systems where non-custody is guaranteed by mathematical proof (2PC-MPC with user-required participation) provide stronger investor protection than systems where non-custody depends on contractual promises. The Commission's framework should recognize this distinction and calibrate compliance burdens accordingly. A system that is non-custodial by mathematical impossibility should face lower organizational compliance requirements than one that is non-custodial by contractual agreement.

2. Recognize smart-contract-enforced compliance as equivalent to organizational controls. When a compliance policy is encoded in a smart contract and enforced at the signing layer through 2PC-MPC binding—such that a non-compliant transaction cannot generate a valid signature—the enforcement is more reliable than organizational controls subject to human override. The Commission should consider safe harbor treatment for systems where access control, transfer restrictions, and KYC/AML enforcement are embedded at the protocol level rather than maintained through organizational policies.

3. Recognize Threshold-FHE regulatory discovery as a legitimate transparency mechanism. The Commission's reporting and transparency requirements can be satisfied by threshold-FHE architectures that provide aggregate reporting without individual decryption and targeted record disclosure through multi-party cooperation protocols. This approach provides privacy during normal operations while preserving the regulatory access that securities laws require—and does so through a process that is auditable, attributable, and resistant to abuse.

4. Provide permanent, rule-based clarity for user interface providers. Commissioner Peirce's call for a more permanent fix to the broker definition is well-taken. Market participants building on the cryptographic architectures described in this comment need durable legal certainty to justify the engineering investment these systems require. A five-year, non-binding, staff no-objection posture—while a welcome step—does not provide the foundation for the institutional-grade infrastructure the Commission is seeking to foster.

5. Encourage technology-neutral, function-based regulation with compliance-burden calibration. We echo SIFMA's March 30, 2026 submission in endorsing function-based regulation. We would add that the compliance burden associated with each function should be calibrated to the architectural properties of the system performing it. A non-custodial, policy-enforced-by-code, privacy-with-discovery system should bear a materially lighter organizational burden than a custodial, policy-enforced-by-personnel, privacy-by-access-control

system performing the same function—because the architectural approach provides equivalent or superior investor protection with lower operational risk.

VI. Conclusion

The Commission's trajectory from the DTCC No-Action Letter through the innovation exemption framework to the April 13 Covered User Interface Provider Statement represents a thoughtful, incremental approach to integrating blockchain technology into the existing securities market structure. We support this approach.

We respectfully urge the Commission to recognize that the cryptographic infrastructure described in this comment—2PC-MPC threshold signing and Threshold-FHE—represents not merely a technology choice, but a compliance architecture. These systems do not avoid regulation; they implement it at a deeper layer than organizational controls can reach. The policy question is not whether these systems should be compliant—they are designed to be—but whether the compliance burden imposed on them should reflect the strength of their architectural guarantees.

The goal should be frameworks where the most architecturally compliant systems bear the lightest organizational burden, creating market incentives for the adoption of investor-protective technology. We believe the cryptographic primitives described in this comment make that goal achievable for permissioned digital asset markets on public, high-performance blockchains.

We appreciate the opportunity to share these observations and welcome further engagement with the Crypto Task Force on these topics.

Respectfully submitted,

Metabyte Labs, Inc.