Metabyte Labs, Inc.

April 15, 2026
Via Electronic Submission

Commissioner Hester M. Peirce and Members of the Crypto Task Force
U.S. Securities and Exchange Commission
100 F Street NE
Washington, DC 20549-0213

Re: Cryptographic Compliance Architecture for Tokenized Securities Markets: Two-Party MPC Signing, Fully Homomorphic Encryption, and the Regulatory Framework for Trustless Decentralized Infrastructure

Commissioner Peirce and the Crypto Task Force:

Metabyte Labs, Inc. respectfully submits this advisory letter to the Crypto Task Force, in response to the Commission's ongoing solicitation of public input on digital asset market structure. 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.[1]

Metabyte Labs is a financial technology research and development company focused on cryptographic compliance infrastructure for digital asset markets. We do not write to advocate for any particular protocol, blockchain network, or commercial product, but rather to offer the Commission an educational perspective on a class of cryptographic technologies that, in our view, fundamentally alter the regulatory analysis applicable to tokenized securities, automated market makers, non-custodial wallet classification, and institutional digital asset management.

We have reviewed the public comment record with care, including the submissions of the Solana Policy Institute and DeFi Education Fund, the Securities Industry and Financial Markets Association, Galaxy Digital, Coinbase, Ondo Finance, Fidelity Investments, Douro Labs, the Blockchain Association, the Crypto Council for Innovation, and numerous other parties. We have also reviewed the Commission's published speeches, guidance, and staff statements, as well as the academic economic analyses submitted by Dr. Craig Lewis and Dr. James Overdahl. This letter is informed by that full body of work.

We write because the current debate has largely presented the Commission with a binary choice: either apply existing intermediary-based regulatory frameworks to on-chain tokenized securities markets in full, or provide broad exemptive relief from those frameworks. We believe this framing is incomplete. A third option exists, one that the Solana Policy Institute has most clearly articulated[2], in

which the Commission evaluates compliance *outcomes* rather than compliance *structures*, and recognizes that certain cryptographic architectures can achieve regulatory objectives with stronger guarantees than the organizational trust relationships they are designed to replace.

This letter proceeds in ten parts, organized to build a progressive understanding of the relevant technologies, their regulatory implications, and their application to the specific questions the Commission has raised. We have endeavored to cite primary sources throughout and to distinguish clearly between established law, Commission guidance, commenter advocacy positions, and our own analysis.

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. The Regulatory Question the Comment Record Has Not Yet Fully Addressed

The comment record reveals a productive but fundamentally polarized debate. On one side, the securities industry's leading trade association argues that "the starting assumption should be that established Regulations ATS and NMS should continue to apply in full to all otherwise applicable securities, including tokenized securities and the intermediaries that transact with them, regardless of the technology used."[3] On the other, the Solana Policy Institute and the DeFi Education Fund argue that regulatory obligations should attach based on *function*, specifically, whether an entity takes

custody, exercises discretion, or acts as an agent on behalf of users, not based on the mere existence of a user interface or the receipt of transaction-based compensation.[4]

Galaxy Digital has offered a cogent middle position, proposing that "outcome equivalence, not structural equivalence, is what neutrality demands."[5] We endorse this formulation and submit that the Commission should evaluate it through the lens of the specific cryptographic technologies described in the following sections.

The question the record has not fully addressed is: what happens to the regulatory analysis when the compliance properties that organizational structures are designed to provide are instead delivered by cryptographic architecture, provably, immutably, and without the possibility of human override? The answer, we submit, is that the regulatory analysis changes fundamentally. Not because the regulatory objectives change, they do not, but because the means of achieving them are materially stronger, and because many of the risks that justify intermediary regulation are eliminated at the architectural level.

The April 13 Covered User Interface Provider Statement is an important step in this direction. By recognizing that interfaces which merely "convert user-identified crypto asset securities transaction parameters into blockchain-legible commands" are not brokers[6], the Commission has implicitly acknowledged that software performing deterministic, non-discretionary functions occupies a different regulatory category than entities exercising judgment over client assets. The technologies described in this letter extend that principle from the interface layer to the signing layer, the execution layer, and the compliance enforcement layer.

III. Two-Party Multi-Party Computation Threshold Signing: A Technical Primer and Its Regulatory Implications

A. 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:[7]

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.

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.[8] 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.[9]

Stage 2: Collaborative Transaction Signing. When a transaction needs to be authorized, the user submits their partial signature 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, 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.[10]

C. Compliance Capabilities Created by 2PC-MPC

1. Non-custody by mathematical proof. Unlike contractual non-custody, 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.[11]

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 registration makes it mathematically impossible to transfer a tokenized entitlement to an unregistered address.[12]

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 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.

5. Scalable broadcast architecture. Advanced 2PC-MPC implementations leverage broadcast communication through blockchain consensus protocols, 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 on chains that process thousands of transactions per second.

D. Regulatory Implications: The Broker-Dealer Analysis

The SEC v. Coinbase decision, the only judicial application of the broker-dealer analysis to non-custodial wallet functionality, found that allegations of brokerage activity failed where there was no custody, discretion, negotiation, or agency.[13] The joint Solana Policy Institute and DeFi Education Fund submission correctly observes that the Commission subsequently dismissed, with prejudice, its broker-dealer claims against a non-custodial wallet provider.[14]

2PC-MPC threshold signing strengthens the non-custodial, non-intermediary analysis considerably. Where smart contract-bound policies enforce compliance deterministically without human discretion, the wallet infrastructure is functionally analogous to a compliance-enforcing vending machine: it applies predefined rules to determine whether to participate in signing, but exercises no judgment, discretion, or agency in doing so. The question of whether such a system constitutes "effecting transactions in securities for the account of others" should be answered by examining who initiates, controls, and benefits from the transaction, and in a 2PC-MPC architecture, the answer is unambiguously the user.

A potential counterargument is that smart contract-bound signing policies constitute a form of "control" or "discretion." This argument fails for the same reason that a transfer restriction embedded in a security's smart contract is not "discretion" exercised by the smart contract developer. The policies are defined once, published transparently, and execute deterministically. No human decision-maker intervenes at the point of transaction. This is precisely the model of compliance-by-architecture that the ERC-7943 standard proposes for token-level transfer controls[15], extended to the signing layer for defense-in-depth.

IV. Threshold Fully Homomorphic Encryption: Privacy with Authorized Regulatory Discovery

A. The Privacy-Transparency Tension

The comment record reveals a fundamental tension. Proponents of on-chain tokenized securities trading correctly observe that public blockchains provide "more comprehensive, more timely, and more universally accessible trade and quote data than the consolidated tape and securities information processors."[16] Simultaneously, the securities industry association's letters identify real risks arising from this same transparency: front-running, sandwich attacks, and MEV exploitation.[17] Institutional market participants require execution privacy, approximately 40% of equity trading and nearly all bond trading occurs in private dark pool and RFQ systems.[18]

The binary framing, either accept full transparency with its attendant MEV risks, or reintroduce traditional intermediaries to provide execution privacy, is a false dichotomy.

B. How Fully Homomorphic Encryption Works

Fully Homomorphic Encryption ("FHE") is a class of cryptographic schemes that allow computation to be performed directly on encrypted data without first decrypting it. The result of the computation, when decrypted, is mathematically identical to the result obtained by performing the same computation on the unencrypted data.[19]

For digital asset markets, this means: account balances can be stored on-chain in encrypted form; trades can be matched and executed on encrypted order data; 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. 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. Published benchmark improvements over the previous leading FHE framework 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 technically viable for the first time.

D. Threshold Decryption: The Compliance Trapdoor

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. Threshold-FHE solves this by distributing the decryption key across a decentralized network using threshold cryptography. No single participant holds the complete decryption key. A threshold of participants 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, can access the plaintext. This satisfies institutional confidentiality requirements and prevents front-running, information leakage, and unauthorized surveillance.

2. Authorized regulatory discovery. When a lawful discovery order requires access to specific 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 is architecturally analogous to the multi-party approval requirements for wiretap orders, 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 quarterly reporting obligations while preserving participant-level privacy.[20]

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

These two technologies are not merely complementary, they are architecturally synergistic. 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 computation on encrypted data. This same infrastructure, the same decentralized network, 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.

V. The Anatomy of a Compliant Automated Market Maker for Tokenized Securities

Galaxy Digital's submission defines a narrow class of AMMs that fall outside the statutory definition of "exchange": those exhibiting absence of discretionary control, transparency and verifiability, self-executing settlement, and neutral access.[21] We agree with this analysis and submit that the Commission should further distinguish among AMM architectures based on the compliance controls embedded within them.

A. Three Layers of Compliance Enforcement

A fully compliant AMM for tokenized securities can incorporate compliance controls at three independent, mutually reinforcing layers:

Token-Level Transfer Restrictions. The ERC-7943 standard standardizes eligibility checks, freeze mechanisms, and enforcement transfer paths.[22] Token-2022 extensions on high-performance blockchain networks provide programmable transfer hooks enforcing compliance logic at the runtime level on every transaction.[23]

Signing-Layer Enforcement via 2PC-MPC. As described in Section III, smart contract-bound signing policies prevent non-compliant transactions at the cryptographic signing layer, before a transaction is even submitted to the network. This provides defense-in-depth.

Encrypted Execution via FHE. As described in Section IV, FHE-encrypted execution eliminates information leakage and MEV exploitation, addressing the specific concerns raised by the securities industry association.

These three layers operate independently and reinforce each other. A tokenized security protected by all three achieves compliance properties that surpass both traditional intermediary-enforced compliance and single-layer on-chain compliance.

B. AMMs and RFQ Systems Are Complementary, Not Competing

The Commission should recognize that AMMs and request-for-quote systems serve different segments of the tokenized securities market, just as lit exchanges and dark pools serve different segments of the traditional equity market. For retail and moderate-size orders, transparent AMMs with compliant access controls provide efficient, autonomous execution. For institutional-size orders, encrypted RFQ systems provide execution privacy, zero market impact, and atomic settlement. A regulatory framework accommodating both models will better serve the full spectrum of market participants.

VI. The Intersection of Permissioned and Permissionless Infrastructure

The Commission's comment record has largely treated permissioned and permissionless systems as separate domains. We submit that the most significant innovations will emerge at their intersection.

A. Cross-Chain Signing and Unified Compliance

2PC-MPC threshold signing networks are inherently cross-chain: a single wallet can produce valid signatures for transactions on any supported network, permissioned or permissionless, from a single compliance-verified identity. This means a user who has completed KYC verification once can transact on a high-performance permissionless network, settle on a permissioned institutional network, and manage positions across both, all under the same compliance constraints. This directly addresses the market fragmentation concerns raised by the securities industry association.[25]

B. Compliant On-Ramps Between Markets

A KYC-verified wallet on a public blockchain can access tokenized securities on a permissioned institutional network through 2PC-MPC cross-chain signing, without re-intermediation at the bridging layer. The compliance constraints are enforced at the signing layer, and the asset moves as a native token rather than a wrapped representation. This eliminates the bridging risks and wrapped-token complexities that the securities industry association's December 2025 letter identified as sources of fragmentation.

C. Collateralized Lending with Institutional Assets

Permissioned institutional assets, tokenized Treasury securities, investment-grade credit, fund units, can serve as collateral for lending protocols on permissionless infrastructure, provided that compliance constraints are maintained at the signing layer. The collateral does not leave the institutional custodial framework; rather, a 2PC-MPC signed attestation of the collateral position authorizes borrowing on the permissionless side. This enables institutional assets to unlock liquidity

in permissionless DeFi markets without compromising custody, compliance, or regulatory reporting properties.

D. Zero-Knowledge Identity and Portable Accreditation

Fairmint's February 2026 submission proposes "portable accreditation", where an investor's verified compliance status becomes a reusable credential.[26] Zero-knowledge KYC protocols implement this cryptographically: a user proves compliance attributes (accredited investor status, jurisdiction, sanctions clearance) without revealing underlying personal data. The proof is portable across any blockchain network, creating an "investor credential" that is verifiable, reusable, and privacy-preserving. The Commission should consider how such credentials can be integrated into the innovation exemption framework.

E. The Result: Permissioned Environments on Permissionless Chains

The combination of 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. 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.

VII. The Solana Policy Institute's Regulatory Framework: Why It Points Toward the Correct Approach

The Solana Policy Institute's submissions represent, in our view, the most clearly articulated and technically informed regulatory framework in the comment record.[27] The SPI framework rests on a core principle: regulatory obligations should attach based on function, custody, discretion, agency, not form. The technologies described in this letter provide the Commission with tools to verify whether these functions are present or absent with mathematical certainty.

This transforms the Commission's classification inquiry from a factual investigation into organizational structures, which can be complex, contested, and subject to change, into a technical verification of architectural properties, which can be audited, tested, and mathematically proven.

The SPI's historical analogy to Regulation ATS is apt: the Commission developed the ATS regime in 1998 because emerging electronic trading platforms did not fit within the legacy exchange framework.[28] The Commission recognized that "substantial changes in the way securities are traded" required accommodation rather than conformity.[29] The current moment is directly analogous. Just as Regulation ATS provided a middle-ground solution, the Commission should develop a framework that recognizes cryptographic compliance architecture as a legitimate means of achieving regulatory objectives.

The SPI identifies itself as a member of Project Open, a consortium enabling tokenized securities on public blockchains consistently with existing regulations.[30] The Project Open model, where public blockchain infrastructure serves as the transaction layer, non-custodial wallets enable user-directed activity, smart-contract protocols facilitate secondary trading, and a registered transfer agent maintains the authoritative ownership record, is a practical implementation of the principles we describe.

VIII. Addressing the Principal Objections in the Comment Record

A. "Technology Neutrality" and the Incumbency Problem

Galaxy Digital correctly identifies the "technology neutrality" argument as deployed by incumbents: rules drafted for one architecture must be mechanically transposed onto another, which, as Galaxy observes, "is not neutrality; it is incumbency."[31] Commissioner Peirce has recognized this dynamic.[32] We add: the technologies described in this letter achieve *superior* outcomes in several material respects. A genuinely technology-neutral framework should recognize superior compliance architecture, not penalize it for failing to reproduce inferior organizational structures.

B. Blockchain Performance

The securities industry association's assertion that blockchains "may be significantly slower than traditional compute technology"[33] reflects an outdated understanding. Purpose-built high-performance Layer 1 networks achieve sub-second block times and process thousands of transactions per second.[34] The Commission should evaluate performance network-by-network.

C. MEV and Manipulation

Galaxy Digital provides public data indicating sandwich attacks imposed costs of approximately 0.0000005% of traded volume.[35] While MEV is a legitimate concern for institutional-size orders, FHE-encrypted execution eliminates the MEV attack vector entirely by encrypting transaction parameters until settlement. This is a technological solution to a technological problem; it does not require re-intermediation. Further, where tokenized securities are restricted to whitelisted, KYC-verified wallets, fraudulent or manipulative conduct would be especially discoverable.

D. Liquidity Provision and the Dealer-Trader Distinction

We agree with Galaxy's analysis that Liquidity Providers on qualifying AMMs are traders, not dealers, confirmed by the Northern District of Texas's decisions vacating Rule 3a5-4.[36] Passive liquidity provision is functionally analogous to securities lending, which has never been classified as dealing.

IX. Recommendations for the Commission

1. Adopt an outcome-equivalence standard for evaluating compliance in tokenized securities markets. Where cryptographic architecture achieves regulatory objectives with provable guarantees, the Commission should not require additional organizational intermediary structures addressing the same risks through weaker means.

2. 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 should calibrate compliance burdens accordingly.

3. Recognize smart-contract-enforced compliance as equivalent to organizational controls. When 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.

4. Recognize Threshold-FHE regulatory discovery as a legitimate transparency mechanism. Aggregate reporting without individual decryption and targeted record disclosure through multi-party cooperation satisfy the Commission's reporting and transparency requirements while preserving privacy.

5. Accommodate both AMM and RFQ execution models within the innovation exemption framework, reflecting the existing coexistence of lit and dark venues in traditional equity markets.

6. Develop a framework for cross-chain compliance consistency, recognizing that unified signing-layer enforcement across multiple blockchain networks addresses market fragmentation while maintaining regulatory standards.

7. Engage with privacy-preserving identity standards (zero-knowledge KYC, portable accreditation) as mechanisms that enhance both compliance and privacy simultaneously.

8. Evaluate the intersection of permissioned and permissionless infrastructure as a feature, not a regulatory liability. The most promising innovations emerge at this intersection.

9. 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.[37]

10. Continue to support the approach championed by the Solana Policy Institute: tailored, functional regulation that evaluates what actors do rather than what technology they use, with compliance-burden calibration reflecting architectural guarantees. The most architecturally compliant systems should bear the lightest organizational burden, creating market incentives for the adoption of investor-protective technology.

X. Conclusion

The Commission stands at a historic inflection point. The technologies described in this letter, 2PC-MPC threshold signing, fully homomorphic encryption with threshold decryption, zero-knowledge identity verification, cross-chain cryptographic signing, and smart contract-bound compliance enforcement, are not theoretical. They are in active development and approaching production deployment. They will define the architecture of institutional digital asset markets regardless of regulatory posture; the question is whether that architecture develops under the Commission's oversight, within a clear and workable framework, or offshore, beyond the Commission's reach.

We have endeavored to provide the Commission with a technically grounded, brand-neutral understanding of how these technologies work, why they matter for the regulatory analysis, and how they resolve many of the tensions that have occupied the comment record. We do not ask the Commission to lower its standards. We ask it to recognize that cryptographic architecture can meet those standards, and, in important respects, exceed them.

We respectfully urge the Commission to recognize that the cryptographic infrastructure described in this comment 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.

We appreciate the Commission's engagement with these issues and the work of the Crypto Task Force in creating a thoughtful, inclusive process for addressing them. We welcome the opportunity to discuss any aspect of this letter at the Commission's convenience.

Respectfully submitted,

Metabyte Labs, Inc.

Endnotes

[1] SEC Division of Trading and Markets, Staff Statement on Covered User Interface Providers, File Number 4-894 (Apr. 13, 2026); Commissioner Hester M. Peirce, Statement on Covered User Interface Providers (Apr. 13, 2026) ("People have shown great ingenuity in developing crypto wallets and front ends that serve users well. It would be a shame if investors in crypto asset securities transactions were unable to use these tools because of an overly broad reading of the term 'broker.'").

[2] See Solana Policy Institute, Request for Information Regarding National Securities Exchanges and Alternative Trading Systems Trading Crypto Assets (Apr. 1, 2026); Solana Policy Institute and DeFi Education Fund, Non-Custodial Wallet Software and Neutral User Interfaces (Feb. 10, 2026). SPI is a member of Project Open, a consortium working to enable tokenized securities on public blockchain networks in a manner consistent with existing regulations.

[3] SIFMA, RFI Response to SEC RFI "And Then Some" and Linked FAQ, at 2 (Mar. 17, 2026), https://www.sec.gov/files/ctf-written-sifma-ats-rfi-letter-03-17-2026.pdf.

[4] Solana Policy Institute, supra note 2, at 2, 4; DeFi Education Fund, Response to Request for Information Regarding National Securities Exchanges and Alternative Trading Systems Trading Crypto Assets (Apr. 1, 2026), https://www.sec.gov/files/ctf-written-input-defi-education-fund-040126.pdf.

[5] Galaxy Digital Inc., Automated Market Makers, Tokenized Securities, and Technology Neutrality, at 3 (Apr. 14, 2026), https://www.sec.gov/files/ctf-written-input-galaxy-digital-041426.pdf.

[6] Staff Statement on Covered User Interface Providers, supra note 1 (describing Covered User Interfaces as software that "convert[s] user-identified crypto asset securities transaction parameters… into blockchain-legible commands for signature and transmission via the user's self-custodial wallet").

[7] See SEC Division of Trading and Markets, Statement on the Custody of Crypto Asset Securities by Broker-Dealers (Dec. 17, 2025), https://www.sec.gov/newsroom/speeches-statements/trading-markets-121725-statement-custody-crypto-asset-securities-broker-dealers; Exchange Act Rule 15c3-3(b)(1).

[8] See Fireblocks, Inc., Disclosure of MPC Vulnerability (Aug. 2023) (publicly documented vulnerability in semi-custodial MPC implementation allowing private key material extraction through malicious signature requests).

[9] See generally Yehuda Lindell, Fast Secure Two-Party ECDSA Signing, in Advances in Cryptology – CRYPTO 2017 (2017); Rosario Gennaro and Steven Goldfeder, Fast Multiparty Threshold ECDSA with Fast Trustless Setup, in Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security (2018).

[10] This architecture is described at a general level in the Move programming language documentation for smart-contract-bound signing systems. See, e.g., developer documentation for dWallet-based signing networks describing smart contract policy binding architecture.

[11] See, e.g., Commissioner Hester M. Peirce, Getting Smart – Tokenization and the Creation of Networks for Smart Assets: Opening Remarks for Tokenization Roundtable (May 12, 2025); SEC Division of Trading and Markets, Frequently Asked Questions Relating to Crypto Asset Activities and Distributed Ledger Technology (Feb. 19, 2026).

[12] SEC Division of Trading and Markets, No-Action Letter re: DTCC Tokenization Services (Dec. 11, 2025), https://www.sec.gov/files/tm/no-action/dtc-nal-121125.pdf (requiring tokens only transferable to Registered Wallets).

[13] SEC v. Coinbase, Inc., 726 F. Supp. 3d 260, 305-07 (S.D.N.Y. Mar. 27, 2024).

[14] SEC v. Consensys Software Inc., No. 1:24-cv-04578, Joint Stipulation to Dismiss (E.D.N.Y. Mar. 27, 2025). See also Solana Policy Institute and DeFi Education Fund, supra note 2, at 4-5.

[15] See Dario Lo Buglio, Written Input to the SEC Crypto Task Force: ERC-7943 (uRWA), Open, Interoperable Compliance Primitives for Tokenized Real-World Assets (Feb. 23, 2026).

[16] Galaxy Digital, supra note 5, at 15.

[17] SIFMA, Automated Market Makers and the Consistent Application of Securities Market Regulations, at 2 (Mar. 30, 2026), https://www.sec.gov/files/ctf-written-input-sifma-033026.pdf.

[18] See FINRA, OTC Transparency Data (2025); Greenwich Associates, Fixed-Income Trading in 2024.

[19] See Craig Gentry, A Fully Homomorphic Encryption Scheme (Stanford University Ph.D. dissertation, 2009); Brakerski, Gentry, and Vaikuntanathan, (Leveled) Fully Homomorphic Encryption Without Bootstrapping, in Proceedings of the 3rd Innovations in Theoretical Computer Science Conference (2012).

[20] This capability is directly relevant to the quarterly reporting obligations contemplated in the DTCC No-Action Letter, supra note 12.

[21] Galaxy Digital, supra note 5, at 3-6.

[22] Lo Buglio, supra note 15.

[23] See Groovy Company, Inc. dba OTCM Protocol, Supplemental Letter to SEC, at 4 (Apr. 2, 2026) (describing 42 Transfer Hook controls enforced at the Solana runtime level, integrated with Chainalysis KYT and TRM Labs).

[24] SIFMA, supra note 17, at 2.

[25] SIFMA, RFI Response, supra note 3, at 10.

[26] Fairmint, Inc., Written Input to the SEC Crypto Task Force: Modernizing Investor Accreditation for On-Chain Capital Markets (Feb. 4, 2026).

[27] Solana Policy Institute, supra note 2; Solana Policy Institute and DeFi Education Fund, supra note 2.

[28] Solana Policy Institute, supra note 2, at 5-6.

[29] Regulation of Exchanges and Alternative Trading Systems, 63 Fed. Reg. 70844, 70845 (Dec. 22, 1998).

[30] Solana Policy Institute, supra note 2, at 1, n.1.

[31] Galaxy Digital, supra note 5, at 2.

[32] Commissioner Hester M. Peirce, Bees, Ts, and NFTs: Remarks at the Coin Center Dinner (Sept. 26, 2025), https://www.sec.gov/newsroom/speeches-statements/peirce-remarks-coin-center-dinner-092525.

[33] SIFMA, RFI Response, supra note 3, at 10.

[34] See Token Terminal, Solana Block Time (Mar. 30, 2026) (average block time under 400ms); Solana Policy Institute, supra note 2, at 7.

[35] Galaxy Digital, supra note 5, at 16, n.35, citing Sandwiches, https://sandwiched.me/sandwiches.

[36] Crypto Freedom Alliance of Texas v. SEC, No. 4:24-cv-00361-O, 2024 WL 4858590 (N.D. Tex. Nov. 21, 2024); Commissioner Hester M. Peirce, Dealer, No Dealer? (Feb. 6, 2024), https://www.sec.gov/newsroom/speeches-statements/peirce-statement-dealer-trader-020624.

[37] Commissioner Peirce, supra note 1 (expressing preference for "a more permanent fix" to the broker definition).