BLOCKCHAIN ASSOCIATION

July 9, 2026

Submitted via Regulations.gov

Christopher Kirkpatrick, Secretary of the Commission
Commodity Futures Trading Commission
Three Lafayette Centre
1155 21st Street NW
Washington, DC 20581

Re: Request for Information: Identifying Regulations To Facilitate Innovation and Competition to Financial Products and Services for Fintech Firms (RIN 3038-ZA24)

Dear Mr. Kirkpatrick:

The Blockchain Association ("BA") appreciates the opportunity to respond to the Commodity Futures Trading Commission's (the "Commission" or "CFTC") Request for Information: Identifying Regulations To Facilitate Innovation and Competition to Financial Products and Services for Fintech Firms (the "RFI").[1] BA is the leading nonprofit membership organization dedicated to advancing a pro-innovation policy environment for the digital asset industry. BA is composed of more than 100 members, including software developers, infrastructure providers, investors, and others supporting the public blockchain ecosystem. BA works with its broad-based membership to seek regulatory clarity and to educate policymakers, regulators, and the courts about how blockchain technology can support a more secure, competitive, and consumer-friendly digital marketplace.

BA supports the Commission's effort to identify regulations, guidance, orders, no-action letters, and other regulatory items that may unnecessarily impede responsible innovation and fair competition. The Commission is appropriately focused not only on barriers to entry for fintech firms, but also on preserving safety and soundness, customer protection, market integrity, financial stability, and oversight.[2] Those objectives are not in tension with blockchain-enabled infrastructure. Properly regulated, blockchain systems can advance the Commodity Exchange Act's ("CEA") core purposes: financially secure trading facilities, effective oversight, financial integrity of transactions, protection against misuse of customer assets, market integrity, responsible innovation, and fair competition.[3]

Below, BA makes eleven recommendations. All recognize the overriding importance of ensuring that responsible innovation does not require weakening regulatory oversight of market participants that custody assets, solicit trades, intermediate transactions, operate markets, clear transactions, provide advice, or exercise discretion. Those functions should remain subject to appropriate CFTC oversight when performed in CFTC-regulated markets. At the same time, the Commission should not apply legacy regulated entity

[1] Request for Information: Identifying Regulations To Facilitate Innovation and Competition to Financial Products and Services for Fintech Firms, 91 Fed. Reg. 36774 (June 18, 2026) (RIN 3038-ZA24) (hereinafter "RFI").
[2] Id. at 36774-75.
[3] Commodity Exchange Act § 3(a)-(b), 7 U.S.C. § 5(a)-(b).

categories[4] to neutral technology infrastructure providers that do not perform those regulated functions. Rather, consistent with its principles-based approach to the regulation of such organizations, the Commission should adopt a technology-neutral regulatory framework that permits such regulated entities to operate blockchain-enabled infrastructure while maintaining compliance with the CEA.

BA's recommendations rest on the principle that the Commission should regulate functions and outcomes consistent with the principles-based structure of the CEA. Where a person performs traditional market functions, the relevant CFTC framework should apply. But where a regulated entity uses blockchain-enabled infrastructure to satisfy the same statutory and regulatory objectives as legacy infrastructure, the Commission should evaluate that infrastructure by whether it achieves the CEA's outcomes, not by whether it resembles traditional offchain architecture. Likewise, neutral technology providers should not be treated as regulated intermediaries merely because they provide software, connectivity, data display, transaction-preparation tools, or other non-custodial infrastructure.

To translate those principles into concrete regulatory action, BA recommends that the Commission:

1. **Permit a two-rulebook approach for regulated entities operating both legacy and blockchain-enabled systems.** The Commission should allow DCMs, DCOs, SEFs, FCMs, SDs, (each, as defined herein) and other regulated entities, where appropriate, to maintain separate rulebook provisions, procedures, or technical appendices for blockchain-enabled operations, including rules addressing access, margin, settlement, recordkeeping, business continuity, forks, validator or oracle dependencies, smart-contract upgrades, wallet whitelisting, private-key administration, and incident response.

2. **Clarify how Part 40 applies to blockchain-enabled system changes.** The Commission should provide predictable standards for when smart-contract upgrades, wallet-permissioning changes, collateral-token parameters, settlement workflow changes, or other technical modifications require self-certification, approval, notice, or no filing.

3. **Permit tokenized real-world-asset collateral and payment stablecoins for margin and settlement where objective risk standards are met.** The Commission should expand upon its efforts to date to modernize its collateral framework so that tokenized forms of otherwise eligible collateral, tokenized RWA collateral, and payment stablecoins can be used where they satisfy appropriate liquidity, valuation, custody, transferability, legal-rights, reserve, redemption, default-treatment, and operational-risk standards.

4. **Adapt rules and supervisory expectations for 24/7 trading, margining, clearing, and settlement.** The Commission should permit regulated entities to demonstrate compliance through continuous margining, automated collateral movements, real-time or intraday settlement, and other blockchain-native workflows, provided that financial-integrity, customer-protection, default-management, and Commission-visibility objectives are preserved.

[4] Unless otherwise indicated, this comment letter uses the term "regulated entity" to encompass trading and clearing organizations (*e.g.*, designated contract markets and derivatives clearing organizations) as well as registrants that act as intermediaries (*e.g.*, futures commission merchants and introducing brokers).

5. **Support direct participant-access and non-intermediated clearing models where customer protections are preserved.** The Commission should identify circumstances in which direct access can be permitted subject to risk-based conditions, including participant eligibility, margin and default resources, automated liquidation controls, segregation, operational resilience, and clear responsibility for errors, outages, and defaults.

6. **Recognize onchain records where they satisfy books-and-records and reporting objectives.** The Commission should allow onchain records to satisfy applicable recordkeeping and reporting obligations where they are complete, accurate, accessible, searchable, reproducible, protected from unauthorized alteration, retained for the required period, and linked to necessary offchain metadata.

7. **Create predictable review procedures for blockchain-related registrations, designations, rule submissions, no-action requests, and exemptive requests.** The Commission should establish completeness checks, Staff response deadlines, opportunities to cure deficiencies, escalation paths, technical-review protocols, and, where appropriate, a dedicated blockchain-infrastructure review channel.

8. **Tailor KYC/AML-compliance, sanctions, cybersecurity, and operational-resilience expectations to blockchain-native systems.** The Commission should preserve equivalent regulatory outcomes while recognizing wallet-based access, smart contracts, public networks, validator or sequencer risks, oracle integrity, private-key governance, code-upgrade processes, and other blockchain-specific controls.

9. **Develop tailored pathways for DeFi and protocol-based systems.** The Commission should distinguish between identifiable persons performing regulated functions and decentralized or protocol-based systems where no person performs such functions, and should use interpretive guidance, exemptions, exceptions, or rulemaking as appropriate.

10. **Issue durable guidance or rulemaking for front-end interfaces, self-custody wallets, APIs, and institutional technology providers.** The Commission should confirm that neutral, non-custodial technology providers are not required to register merely because they provide software, connectivity, messaging, data display, transaction-preparation tools, or user-directed access to regulated markets.

11. **Continue to Focus on Harmonization Efforts.** The Commission should continue to focus on the harmonization of the CEA and the federal securities laws, as well as on the harmonization of potentially conflicting and confusing definitions used across different CFTC rules (*i.e.*, the definition of a "U.S. person").

The CFTC's oversight is rightly known as the global gold standard for derivatives regulation. Each of the foregoing recommendations would further advance the agency's mission to promote the integrity, resilience, and vibrancy of the U.S. derivatives markets through sound regulation—in a technology-neutral fashion—all while allowing compliance with the CEA's principles-based regime.

I. Blockchain infrastructure is becoming an element of financial market infrastructure, not merely the underpinnings of digital asset classes.

Blockchain technology is already being adopted across traditional finance, including derivatives, payments and settlement tools, collateral management, custody-adjacent workflows, and institutional connectivity. Meanwhile, native digital asset markets, such as spot crypto, tokenized assets, crypto derivatives, and prediction markets, continue to grow and mature. Market participants are no longer considering blockchains only as they relate to digital assets. Increasingly, they are considering public and private blockchains as infrastructure used for settlement rails, recordkeeping systems, collateral movement tools, and programmable market architecture.

The Commission should respond to this development by encouraging activity to occur in the United States, subject to U.S. registration and supervision when required and appropriate, while fostering U.S.-based innovation. Regulatory uncertainty creates incentives for next-generation market infrastructure to migrate offshore, an outcome that is decidedly contrary to the public interest and detrimental to the industry. Indeed, the current Administration has also prioritized "support[ing] growth and innovation in the digital assets industry . . . and keep[ing] the United States at the forefront of digital asset development."[5] Offshore migration does not eliminate risk; it reduces U.S. regulatory visibility, reduces domestic accountability, weakens the Commission's ability to shape market standards, and deprives U.S. market participants of the benefits of responsible innovation under U.S. law.

A technology-neutral framework would instead allow market participants to bring blockchain-enabled infrastructure into the regulated perimeter when they perform regulated functions, while allowing neutral technology providers to support those entities without being misclassified as intermediaries. This balance protects the Commission's oversight authority and the CEA's customer-protection and market-integrity objectives, while allowing innovation to develop within the United States.

II. The CEA supports a principles-based approach and a technology-neutral framework.

The CEA is well suited to accommodate blockchain-enabled financial market infrastructure. Congress recognized that the derivatives markets serve a national public interest, and it directed that the CEA serve that interest through a system of effective self-regulation under Commission oversight.[6] The CEA's purposes include deterring and preventing price manipulation and other attacks on market integrity, ensuring the financial integrity of transactions, avoiding systemic risk, protecting market participants from misuse of customer assets, and promoting responsible innovation and fair competition.[7]

Those purposes are outcome-oriented. They do not require a particular database architecture, clearing workflow, settlement rail, collateral ledger, interface design, or custody technology. Nor do they require legacy intermediated workflows where a different technical architecture can satisfy the same or better regulatory outcome.

---

[5] *Fact Sheet: The President's Working Group on Digital Asset Markets Releases Recommendations to Strengthen American Leadership in Digital Financial Technology*, The White House (July 30, 2025), https://www.whitehouse.gov/fact-sheets/2025/07/fact-sheet-the-presidents-working-group-on-digital-asset-markets-releases-recommendations-to-strengthen-american-leadership-in-digital-financial-technology/.

[6] CEA § 3(a)-(b), 7 U.S.C. § 5(a)-(b).

[7] CEA § 3(b), 7 U.S.C. § 5(b).

Consistent with these principles, the Commission has long administered statutory core-principles frameworks for regulated entities. Designated contract markets ("DCMs") and derivatives clearing organizations ("DCOs"), for example, operate under statutory core principles and implementing regulations that require compliance with substantive outcomes rather than rigid technical specifications.[8] Such a principles-based regulatory approach affords the Commission substantial flexibility to evaluate blockchain-enabled systems on their merits.

The Commission should use that flexibility and evaluate a blockchain system on the basis of whether it satisfies the relevant CEA objectives, including, but not limited to:

1. Impartial access;
2. Market surveillance;
3. Protection against manipulation;
4. Transparency;
5. Books and records;
6. Auditability;
7. Execution integrity;
8. Customer asset protection;
9. Financial integrity;
10. Operational resilience; and
11. Appropriate Commission visibility.

In many cases, blockchain infrastructure can further these objectives, and in some cases may do so more effectively than legacy infrastructure. A tamper-resistant ledger can improve auditability. Smart contracts can automate margining, settlement, access restrictions, and collateral movements. Public transaction histories can support surveillance and after-the-fact analysis. Wallet and permissioning tools can support whitelisting, access controls, and segregation of functions. Regulated entities can use these features of blockchain infrastructure to fulfill their regulatory obligations more effectively, rather than as a substitute for regulation.

The Commission has existing statutory authority and regulatory tools to implement this approach. These include the DCM and DCO core-principles frameworks; the Commission's rulemaking authority; its authority over regulated entities; its interpretive and no-action processes; and, where appropriate, its exemptive authority under CEA section 4(c).[9] The Commission should use these tools to provide durable, technology-neutral standards.

[8] CEA § 5, 7 U.S.C. § 7; 17 C.F.R. pt. 38; CEA § 5b, 7 U.S.C. § 7a-1; 17 C.F.R. pt. 39.

[9] CEA § 4(c)(2), 7 U.S.C. § 6(c)(2); 17 C.F.R. § 140.99.

III. The Commission should modernize existing rules to permit regulated entities to operate onchain.

a. Permit a two-rulebook approach and clarify Part 40 treatment of blockchain-enabled system changes.

Existing Commission regulations, regulated entity rulebooks, and related regulatory review practices often assume a single offchain technical stack. That assumption creates unnecessary ambiguity for a regulated entity that wants to add a blockchain-enabled system while maintaining its legacy system.

The Commission should permit a regulated entity to maintain separate rulebooks, procedures, or technical appendices for traditional infrastructure and blockchain-enabled infrastructure, subject to Commission review and ongoing examination, to ensure both environments meet applicable core principles. Instead of reducing Commission oversight, a two-rulebook approach would make oversight more precise by allowing the Commission and the regulated entity to identify which rules should govern each technical environment and how each environment satisfies the applicable core principles.

For example, a DCM or DCO operating both legacy and blockchain-enabled systems should be permitted to maintain distinct rule provisions addressing access, margin, settlement, recordkeeping, business continuity, incident response, forks, validator or oracle dependencies, smart-contract upgrades, wallet whitelisting, private-key administration, and other onchain operational issues. Forcing those systems into a rulebook written for a different technology increases uncertainty without improving customer protection or market integrity.

The Commission should also clarify how Part 40 rule certifications and approvals apply to blockchain-enabled system changes. Regulated entities need predictable standards for identifying when a smart-contract upgrade, wallet-permissioning change, collateral-token parameter, or settlement workflow change requires self-certification, approval, notice, or no filing. The Commission can provide this clarity without weakening its ability to review material changes.

b. Permit tokenized RWA collateral, tokenized eligible collateral, and payment stablecoins for margin and settlement where objective risk standards are met.

BA applauds the Commission Staff's recent actions to modernize the clearing system through the careful use of tokenized assets and payment stablecoins to collateralize derivatives transactions. As the Commission continues to modernize the treatment of these assets, the relevant question should not be whether collateral is represented on a blockchain, but whether the collateral satisfies the applicable risk, liquidity, valuation, custody, transferability, legal-rights, and financial-resource standards.

As CFTC Staff has already indicated in the Tokenized Collateral Guidance, a tokenized form of eligible collateral may be used where the asset satisfies applicable requirements and provides legal and economic rights that are the same as or functionally equivalent to the rights associated with the asset in traditional form.[10] CFTC Staff also has issued no-action relief relating to certain non-securities digital assets accepted as margin collateral by futures commission merchants ("FCMs"), including payment stablecoins under

[10] CFTC Staff Letter No. 25-39, Tokenized Collateral Guidance (Dec. 8, 2025).

specified conditions.[11] Those are important interim steps. The Commission, however, should address certain gaps that remain. In particular, as reflected in Commission Staff FAQs, Commission Regulation 23.156 does not currently include payment stablecoins in the enumerated list of eligible collateral for uncleared swap margin. The Staff has confirmed that Staff Letter 26-05 does not alter the enumerated list and that crypto assets, including payment stablecoins, are not included as eligible collateral for uncleared swaps under Regulation 23.156.[12] That result is not technology-neutral. It permits a tokenized representation of an otherwise eligible asset to be used as collateral where functional-equivalence standards are met, but it leaves payment stablecoins outside the collateral framework even when they satisfy appropriate reserve, redemption, custody, transfer, valuation, and risk controls.

BA recommends that the Commission consider rulemaking, or appropriate coordinated guidance, to permit payment stablecoins to be used for margin and settlement where they meet objective standards. Those standards could include, as appropriate:

1. full reserve backing with high-quality liquid assets;
2. legally enforceable redemption rights;
3. transparent reserve reporting;
4. segregation from issuer estate risk to the extent feasible;
5. transferability and settlement finality standards;
6. operational resilience and incident-response controls;
7. valuation, haircut, concentration, and wrong-way-risk controls;
8. sanctions, wallet-screening, and access controls where applicable; and
9. clear treatment in default, insolvency, and recovery scenarios.

This recommendation does not mean that every digital asset should qualify as eligible collateral. Nor does it mean that collateral standards should be weakened. Rather, it means that the Commission should evaluate tokenized collateral and payment stablecoins by risk characteristics and legal rights, not by technological form.

c. Adapt rules and supervisory expectations for 24/7 trading, margining, clearing, and settlement.

Many Commission rules and market practices assume traditional business hours, batch processing, end-of-day settlement, and daily variation-margin cycles. Blockchain markets and blockchain-enabled infrastructure can operate continuously. They may support intraday or real-time margining, automated collateral movements, and settlement outside traditional business hours.

The Commission should adapt operational requirements to recognize continuous markets while preserving financial integrity. A DCM, swap execution facility ("SEF"), DCO, FCM, or swap dealer ("SD") using blockchain-enabled infrastructure should be able to demonstrate how its system satisfies margin, default-management, settlement, liquidity, risk-management, and customer-protection requirements in a continuous environment. Requirements should focus on outcomes: whether margin is adequate, settlement

[11] CFTC Staff Letter No. 26-05, Staff No-Action Position Regarding Digital Assets Accepted as Margin Collateral (Feb. 6, 2026).

[12] CFTC, Registrant and Registered Entity Activities Relating to Crypto Assets and Blockchain Technologies FAQs, Question 5 (Mar. 20, 2026); 17 C.F.R. § 23.156.

is final with clear and enforceable legal effect, risk controls operate effectively, operational incidents are managed promptly, customer assets are protected, and the Commission has appropriate visibility.

In adapting these requirements, the Commission should recognize that in some respects a continuous model may actually reduce certain risks by decreasing settlement latency, improving collateral mobility, and providing more frequent risk measurement. On the other hand, BA recognizes that new technologies can create new risks. In this context, such risks may include smart-contract vulnerabilities, oracle or data dependencies, liquidity disruptions, network congestion, validator disruption, key-management failures, cyber incidents, and operational demands outside traditional staffing hours. The regulatory framework should address those risks directly rather than forcing continuous systems into rules designed for batch processing.

d. Support direct participant-access models that preserve customer protections.

The Commission should encourage pathways for direct participant access and direct-to-DCO or non-intermediated clearing models, subject to risk-based conditions equivalent to FCM customer-protection, margin, default-management, and segregation standards; including default-management, financial-integrity, and risk-management outcomes required by the CEA.

This issue should be handled carefully. BA does not recommend weakening customer protections, segregation requirements, risk controls, or the Commission's oversight of trading activity. Where an entity accepts customer funds, solicits or accepts orders, carries customer positions, intermediates transactions, or performs other regulated functions, that entity should be subject to the applicable registration and customer-protection regime. But blockchain-native structures may allow certain participants to interact with markets, collateral, and settlement systems without every function being performed by a traditional intermediary. Such structures can help reduce costs and democratize markets under the Commission's jurisdiction without compromising strong oversight. The Commission should identify circumstances in which direct access can be permitted subject to appropriate risk-based conditions. Those conditions could include participant eligibility standards, disclosures, margin and default resources, automated liquidation controls, independent governance, operational resilience, customer asset protections, segregation or functional segregation, and clear responsibility for errors, outages, and defaults.

The overarching regulatory objective should be to preserve the protections associated with intermediated models, rather than protecting the architecture of intermediation for its own sake.

e. Recognize onchain records where they satisfy books-and-records and reporting objectives.

The Commission should recognize that onchain records satisfy books-and-records and reporting requirements where such records are complete, accurate, accessible, searchable, capable of being reproduced, protected from unauthorized alteration, and retained for the required period. Regulation 1.31 and Part 45 swap-data reporting requirements should be applied in a manner that permits blockchain records to satisfy regulatory objectives and reduce duplicative reporting where appropriate.[13]

[13] 17 C.F.R. § 1.31; 17 C.F.R. pt. 45. *See also*, Executive Order 14405: Integrating Financial Technology Into Regulatory Frameworks, 91 Fed. Reg. 30475 (May 22, 2026) (Instructing Federal financial regulators to identify existing regulations that can be updated to facilitate innovation, and competition to financial products and services for fintech firms.); and *Strengthening American Leadership in Digital Financial Technology* (July 30, 2025) at p. 53

Immutable or tamper-resistant blockchain records can have significant advantages over traditional systems. For example, ledgers can improve auditability and data integrity. Where a regulated entity demonstrates that onchain records provide complete, regulator-accessible information meeting retention and integrity standards, the Commission should consider reducing duplicative offchain records to avoid unnecessary costs. The Commission should create a pathway for regulated entities to demonstrate that onchain records satisfy books-and-records and reporting outcomes and to avoid duplicative recordkeeping where doing so is consistent with the CEA.

BA acknowledges that a blockchain ledger is not automatically sufficient for all regulatory purposes. The Commission should require regulated entities to demonstrate that onchain records include or are linked to all required data fields; that they can be associated with the relevant legal entity, account, customer, transaction, and product; that offchain metadata is preserved where necessary; that privacy and confidentiality obligations are satisfied; and that the Commission can readily access information in usable form.

IV. The Commission should provide predictable review procedures and a dedicated blockchain-infrastructure review channel.

The RFI asks whether registration, designation, and authorization processes may not be fit for purpose for fintech firms and how they should be streamlined.[14] BA recommends that the Commission create clear procedural expectations for blockchain-related applications, rule submissions, requests for interpretive relief, and no-action or exemptive requests.

Firms should not face open-ended uncertainty when they seek to modernize regulated systems. To address this uncertainty, the Commission should establish:

1. predictable application timelines;
2. transparent review milestones;
3. defined Staff response periods (*e.g.*, between 45 and 60 days);
4. an initial completeness review (*e.g.*, within 30 days of receipt);
5. written identification of deficiencies;
6. a defined opportunity to cure;
7. an escalation path where Staff review stalls;
8. clear standards for when technical demonstrations are needed; and
9. publication of anonymized or generalized Staff views where recurring interpretive issues arise.

These procedures would benefit the Commission as well as applicants. They would create a better record, improve accountability, and reduce the reliance on Staff no-action letters. They would also support the Commission's objective of identifying regulatory items that impede fintech partnerships or delay eligible fintech firms seeking registration, designation, or authorization.

The Commission should also consider a dedicated blockchain-infrastructure review channel for regulated entities seeking to deploy onchain systems. A specialized channel, attended by the Commission's experts

(Specifically instructing the CFTC to consider using its rulemaking, interpretative and exemptive authority under the CEA to advance the initiative of using blockchain technology to satisfy recordkeeping obligations under CFTC Regulation 1.31.)

[14] RFI, 91 Fed. Reg. at 36775.

in fintech and blockchain technology, would provide an efficient pathway to the safe and successful deployment of innovative systems. These efficiencies would be beneficial to the Commission itself and the parties it regulates. The process should be structured to demonstrate how a proposed architecture satisfies applicable legal requirements.

V. The Commission should tailor requirements that assume legacy technology, including KYC/AML-adjacent controls and cybersecurity.

A technology-neutral framework should evaluate safety based on demonstrable risks and controls, regardless of whether infrastructure is centralized or blockchain-based. It should require each regulated entity to identify its risks, implement controls, test those controls, maintain records, report material incidents, and demonstrate operational resilience.

Some regulatory and supervisory expectations in this regard, however, assume centralized account systems, centralized custody, batch settlement, perimeter-based cybersecurity, and traditional vendor-management models. These assumptions are ill-suited to blockchain systems that may rely on wallet-based access, smart contracts, public networks, validator sets, or third-party infrastructure that does not fit those assumptions.

The Commission should identify requirements that need technical tailoring while preserving the relevant regulatory outcome. For KYC, AML, sanctions, and related controls, the Commission should coordinate with NFA, FinCEN, OFAC, and other authorities where appropriate. The key question should be whether customer identification, access controls, sanctions compliance, suspicious-activity escalation, and recordkeeping objectives are achieved, not whether they are achieved through a legacy account-opening workflow.

For cybersecurity and operational resilience, the Commission should recognize blockchain-native risk models, which necessarily differ from traditional models. A framework for blockchain-enabled registrants should address smart-contract security, private-key governance, wallet permissioning, validator or sequencer risks, oracle integrity, bridge risks, code upgrade governance, network congestion, denial-of-service risks, incident response, rollback or fork scenarios, business continuity, and third-party infrastructure dependencies. Requirements calibrated to the efficacy of relevant controls should address these and similar risks transparently.

VI. The Commission should develop appropriate pathways for decentralized systems and protocol-based activity.

The RFI asks whether current registration, designation, or authorization categories are inadequate for decentralized finance protocols or applications, and whether existing categories may be too broad for certain fintech activity.[15]

Existing regulated entity categories such as FCM, introducing broker ("IB"), DCM, SEF, DCO, commodity pool operator ("CPO"), and commodity trading adviser ("CTA") generally assume that there is a centralized person performing a regulated function, *e.g.*, custodying assets, soliciting or accepting orders, operating a market, clearing transactions, providing advice, exercising discretion, or otherwise intermediating activity. Some protocol-based systems do not fit neatly into those categories, if at all. Others may involve sufficient centralized governance, operation, interface control, upgrade authority, fee control, custody, discretion, or

[15] Id. at 36776.

market operation that oversight is appropriate. The Commission should distinguish among these various cases. Where a person or group operates a facility for trading CFTC-regulated products, clears transactions, solicits or accepts orders, provides advice, exercises discretion, intermediates transactions, or custodies assets, the Commission should apply the relevant regulatory framework. Blockchain technology should not be a basis to avoid oversight of regulated functions.

On the other hand, where a protocol is genuinely decentralized and/or no person performs a regulated-entity function, forcing the protocol into a legacy category may be both impractical and inconsistent with the structure of existing categories, and unnecessary to achieve the Commission's regulatory purposes. In those circumstances, the Commission should consider whether an exemption, exception, interpretive clarification, or targeted pathway is appropriate, and whether any regulated touchpoints, such as custodians, intermediaries, registered venues, clearing entities, or persons exercising meaningful control over front-end interfaces, provide a more appropriate locus for oversight.

Where a system sits between those poles, for example, a protocol with identifiable governance, upgrade keys, fee control, admin controls, front-end control, or centralized risk management, the Commission should consider a tailored pathway. That pathway could be grounded in the Commission's existing authority over regulated entities, the core-principles framework, rulemaking authority, interpretive authority, and, where applicable, section 4(c) exemptive authority.[16] The pathway should specify which obligations apply, who bears them, and how compliance can be demonstrated in a protocol-based environment.

This approach would avoid two errors. It would avoid weakening oversight where regulated functions are being performed. And it would avoid imposing legacy intermediary categories on software or protocols that do not perform those functions.

VII. The Commission should provide durable guidance for front-end interfaces, self-custody wallets, APIs, and institutional technology providers.

BA was pleased with Staff's issuance of CFTC Letter No. 26-09, known after its requester as the "Phantom Letter," which permitted a front-end software provider to perform its non-custodial services without being required to register as an IB.[17] The letter recognized that Phantom was not proposing the sorts of activities that would justify direct Commission oversight: it would not hold, control, or take into custody any customer assets; generate "buy" or "sell" signals; or exercise any discretion with respect to the routing or execution of user orders. As a result, Commission Staff permitted Phantom to provide its passive services without registration, so long as it observed specific guardrails.

This is the right approach. The Phantom Letter, however, was necessarily limited to only the set of facts presented by the requester. The Commission should extend its approach to other situations where, coupled with appropriate guardrails, there is no need for regulation as a traditional registrant. The need for action remains acute for self-custody wallet providers, front-end interface providers, API and connectivity providers, and other software providers that support institutional market participants but do not perform regulated intermediary functions.

[16] CEA § 4(c)(2), 7 U.S.C. § 6(c)(2).

[17] CFTC Letter No. 26-09 (Mar. 17, 2026); CFTC Press Release No. 9197-26, CFTC Staff Issues No-Action Position to Self-Custodial Crypto Asset Wallet Software Provider (Mar. 17, 2026).

The need is also acute for other technology providers. The Commission should clarify that such a provider is not required to register in any registration category, merely because it provides software functionality, connectivity, messaging, data display, or transaction-preparation tools. The analysis should turn on function. A technology provider should not be treated as an intermediary where it does not:

1. solicit trades;
2. recommend products, counterparties, or venues;
3. open customer accounts;
4. accept orders as an intermediary;
5. exercise independent trading discretion;
6. custody assets;
7. sit in the flow of funds;
8. act as counterparty;
9. control execution or routing to a preferred counterparty;
10. restrict users from accessing venues or intermediaries directly;
11. provide buy or sell signals; or
12. receive compensation for causing customers to trade with a particular venue, counterparty, or intermediary.

The Commission should also clarify that, based on a facts-and-circumstances analysis, technology-based fee models do not, by themselves, create registration risk. A fee should be permitted to be calculated by reference to transactions, messages, notional volume, executed volume, API usage, connectivity usage, or other objective measures of platform utilization without becoming brokerage compensation, so long as the fee is charged for access to and use of the software or connectivity layer and is not paid for solicitation, recommendation, introducing, accepting orders, steering to a preferred counterparty, or sharing in execution commissions.

The distinction is between compensation for technology services and compensation for brokerage or intermediation. Consistent with the conduct-based analysis above, fixed fees, usage-based fees, volume-based fees, per-message fees, and per-transaction technology fees should not automatically convert a technology provider into an IB or other intermediary where the provider is not receiving commission splits, referral fees, spread capture, payment for order-flow steering, or other compensation tied to causing customers to trade with a particular venue, counterparty, or intermediary.

The Commission should consider an institutional technology provider framework. Many CFTC customer-protection concepts are designed for entities that handle customer funds, intermediate transactions, or serve retail or less sophisticated market participants. Non-custodial technology providers serving only institutional clients present different risks that can appropriately be managed by the entity using the technology. The appropriate regulatory focus should be cybersecurity, API security, access controls, auditability, data integrity, operational resilience, business continuity, conflicts management, and incident response.

This framework would not—and should not—create a loophole for entities performing intermediary functions. If a provider solicits orders, recommends trades, exercises discretion, handles customer funds, routes to preferred venues for compensation, acts as counterparty, or otherwise performs a regulated function, it should be regulated accordingly. But neutral software and connectivity should not be forced into intermediary categories simply because the software facilitates user access to a regulated market.

VIII. Concerns about structured oversight, routing transparency, and regulatory arbitrage support a targeted technology-provider framework, not overbroad intermediary classification.

Some have argued in related regulatory contexts that user interfaces and wallet providers raise concerns about "structured oversight," "routing transparency," "display bias," "market coverage," "operational and technology risk," and "regulatory arbitrage." Those are serious considerations. They do not, however, justify treating every front-end, wallet, or technology interface as a regulated intermediary for five reasons.

First, the Commission can obtain appropriate visibility through the regulated entities that use the technology, through recordkeeping and audit rights, vendor-management expectations, cybersecurity and operational-resilience standards, and targeted notification or attestation frameworks for technology providers where warranted. This will avoid imposing unwarranted costs that may stifle innovation and allow the Commission to focus its resources on its core missions of ensuring stable markets and protecting customer assets.

Second, conduct-based standards should address concerns about display bias and implicit recommendations. A neutral interface that displays user-selected venues, provides objective data, or enables user-directed connectivity is different from an interface that ranks venues based on undisclosed compensation, steering arrangements, affiliation, or conflicted routing. The Commission should prohibit misleading disclosures, undisclosed conflicts, and steering that amounts to solicitation or recommendation. It should not presume that all display functionality is intermediation.

Third, transaction-based technology fees should not be conflated with brokerage compensation. In legacy markets, transaction-based compensation can be a relevant indicator of broker or intermediary status because it may reflect compensation for inducing or effecting transactions. But in software markets, usage-based pricing is ordinary. API calls, messages, bandwidth, transaction preparation, and system utilization may all be measured by volume. The regulatory question should be what the fee compensates. If the fee compensates software access or connectivity, it should not create registration risk. If it compensates solicitation, steering, order acceptance, trade recommendation, execution, or commission sharing, the analysis is different.

Fourth, avoiding regulatory arbitrage does not require imposition of legacy architecture on new systems. Regulatory arbitrage occurs when functionally equivalent risks are treated differently without justification. A technology-neutral framework avoids such arbitrage by applying the same regulatory principles to the same regulated functions, regardless of technology. It also avoids a different form of arbitrage: forcing blockchain-based firms into poorly fitting categories while allowing legacy technology vendors to provide analogous connectivity without registration or otherwise being subject to regulatory scrutiny. And if new technology in fact makes it easier to comply with the CFTC's regulations than legacy approaches do, the markets will naturally gravitate in that direction without compromising regulatory oversight. That is not regulatory arbitrage.

Fifth, durable rulemaking is preferable to indefinite reliance on Staff statements and individualized no-action letters. BA agrees that significant market-structure issues deserve public input, legal durability, and Commission-level standards. That is why the Commission should use the input received from the RFI to move from *ad hoc* relief to technology-neutral guidance and, where appropriate, notice-and-comment rulemaking. A durable framework should integrate blockchain-enabled infrastructure into the CFTC

regulatory system without imposing intermediary registration on neutral technology providers that do not perform intermediary functions.

IX. Responses to the Commission's specific questions.

Question 1: Registration, designation, and authorization processes not fit for purpose.

Fintech firms and existing registrants face uncertainty when proposing blockchain-enabled systems because current processes often lack defined timelines, technical milestones, and transparent criteria for assessing novel infrastructure. This is a request for clearer process.

The Commission should create predictable review timelines, completeness checks, Staff response deadlines, opportunities to cure deficiencies, and escalation procedures. The Commission should also provide technical-review protocols for blockchain systems, including smart-contract audits, wallet controls, oracle dependencies, cybersecurity testing, settlement-finality analysis, collateral-risk analysis, governance documentation, and incident-response plans.

For regulated entities using Part 40 submissions, the Commission should clarify how blockchain-related system changes are classified for certification or approval purposes, and when changes may be handled through technical appendices or rulebook supplements rather than full-scale reauthorization.

Question 2: Regulatory items that impede partnerships with CFTC regulated entities.

Regulatory uncertainty around intermediary status impedes partnerships between fintech firms and CFTC regulated entities. The most obvious example is uncertainty over when a front-end interface, wallet provider, API provider, data provider, or connectivity provider is treated as an IB or other intermediary. The Commission should provide interpretive guidance confirming that non-custodial technology providers are not intermediaries solely because they provide neutral software functionality, connectivity, transaction preparation, or user-directed access.

Rules and supervisory expectations concerning records, reporting, collateral, settlement, and cybersecurity may also impede partnerships when applied as if all systems use legacy architecture. The Commission should modernize Regulation 1.31, Part 45 reporting expectations, Part 39 requirements, Regulation 1.25, Regulation 23.156, and related guidance to recognize onchain records, tokenized collateral, payment stablecoins, continuous settlement, and blockchain-native risk controls where the relevant regulatory objectives are satisfied.

Question 3: Regulatory items not fit for blockchain-native regulated entities.

Regulations and supervisory expectations are not fit for purpose where they assume business hours, batch settlement, daily variation-margin cycles, centralized databases, centralized custody models, or offchain-only records. A blockchain-native regulated entity should be permitted to demonstrate compliance through continuous margining, automated settlement, smart-contract controls, onchain records, wallet permissioning, and other blockchain-native controls.

The Commission should not require blockchain-native regulated entities to recreate legacy architecture solely to demonstrate compliance. It should require them to demonstrate the same regulatory outcomes: impartial access, market integrity, surveillance, customer protection, financial integrity, operational resilience, recordkeeping, reporting, and Commission access.

Question 4: Adequacy of registration, designation, and authorization categories, including DeFi.

Existing categories are adequate for many activities where an identifiable person performs a regulated function. If a person operates a DCM, SEF, or DCO; acts as an FCM, IB, SD, CPO, or CTA; solicits trades; accepts orders; clears transactions; custodies assets; provides advice; or exercises discretion, existing categories can apply.

But existing categories do not fit every protocol-based or decentralized system. Some systems have no central intermediary that can satisfy obligations designed for a centralized person. Others have governance, upgrade authority, front-end control, fee control, custody, or operational discretion sufficient to justify oversight.

The Commission should develop a tailored framework for protocol-based systems. That framework should identify factors showing sufficient centralization to support registration or designation, and factors showing that an exemption or exception is appropriate because no intermediary exists. The Commission can rely on existing authority under the CEA's core-principles framework, rulemaking authority, interpretive authority, and section 4(c) exemptive authority, while recognizing that some gaps may require congressional action if the Commission concludes that a new category is needed beyond existing statutory authority.

Question 5: Categories that may be too broad and activity that should qualify for exemption or exception.

Application of the IB category can become overbroad if applied reflexively to neutral technology providers that merely provide software, connectivity, or transaction-preparation tools. The Commission should clarify that a provider is not an IB solely because it supplies self-custody wallet software, front-end interface software, APIs, connectivity, or other technology that enables a user to access a registered market, provided the provider does not solicit trades, recommend products or counterparties, accept orders as an intermediary, exercise discretion, custody assets, control execution, sit in the flow of funds, or receive compensation for causing customers to trade with a particular venue or intermediary.

Similarly, DeFi protocols or applications should qualify for exemption, exception, or tailored treatment where there is no person performing the regulated function. Where there is a person performing the function, the Commission should regulate that function. Where there is neutral technology without intermediation, the Commission should not create registration obligations based on technological form alone.

X. Continue to Focus on Harmonization Efforts.

Fintech firms often seek to engage with and/or offer technological products to market participants subject to dual registration/regulation under the CEA and the federal securities laws. Such firms may benefit from harmonization of the CEA and the federal securities laws that reduces the costs and burdens of offering technological products to such market participants.

Accordingly, BA encourages the Commission to continue to focus on the harmonization of the CEA and the federal securities laws, including the initiative recently undertaken with the U.S. Securities and Exchange Commission.[18] Furthermore, BA believes that the engagement of fintech firms in these harmonizations may afford benefits to the broader financial markets and market participants.

[18] Joint Request for Comment: Joint Request for Comment on Further Definition of ''Swap'' and ''Security- Based Swap'' and on Alternative Compliance, 91 Fed. Reg. 37873 (June 24, 2026) (RIN 3235–AN79); and Joint Request

As a related matter, BA supports additional harmonization efforts that focus on potentially conflicting and confusing definitions used across different CFTC regulations. An example of such a situation exists with respect to the use of the definition of a U.S. Person in the context of CFTC Regulation 23.23, Part 30 (FCM registration), CFTC Regulation 3.10 (foreign intermediary exemption), and CFTC Regulation 48.2(c) (foreign board of trade registration).

BA anticipates that one or more of its members may submit additional comments in further support of these and other harmonization efforts.

Conclusion

Blockchain technology can support the CEA's core objectives. It can improve transparency, auditability, settlement efficiency, collateral mobility, and market access. It also can introduce new operational, cybersecurity, governance, and market-integrity risks. The Commission should address those risks directly through a technology-neutral framework.

Accordingly, BA respectfully recommends that the Commission:

1. adopt a technology-neutral framework for blockchain-enabled regulated entities;
2. modernize rules that assume legacy infrastructure;
3. permit a two-rulebook approach for registrants operating both traditional and blockchain-enabled systems;
4. permit tokenized collateral and payment stablecoins for margin and settlement where objective risk standards are met;
5. adapt rules for 24/7 trading, clearing, margining, and settlement;
6. recognize onchain records where they satisfy books-and-records and reporting objectives;
7. provide predictable registration, designation, authorization, and Staff review timelines;
8. tailor KYC/AML-adjacent and cybersecurity expectations for blockchain-native systems while preserving regulatory outcomes;
9. develop appropriate pathways for DeFi and protocol-based systems;
10. move beyond individualized no-action relief by issuing broader interpretive guidance or conducting formal rulemaking for front-end interfaces, self-custody wallets, APIs, and neutral technology providers; and
11. continue to support harmonization efforts among the CEA and the federal securities laws, and among various CFTC regulations.

BA appreciates the Commission's consideration of these comments and would welcome the opportunity to engage further with the Commission and Staff.

Respectfully submitted,
The Blockchain Association
By: /s/Ashok M. Pinto
Executive Vice President Legal and Government Relations

for Comment: Joint Request for Comment on Further Implementation of Portfolio Margining and Cross-Margining of Securities and Derivatives, 91 Fed. Reg. 39579 (June 26, 2026) (RIN 3235-AN80).