May 1, 2025

MORTAR STRATEGIES

Response to SEC Crypto Regulatory Questions

This report addresses Commissioner Hester Peirce's questions on crypto assets within the securities regulatory framework, adopting a pro-innovation stance while prioritizing investor protection. It follows Peirce's taxonomy: Security Status and Scoping Out, with analysis, recommendations, and insights supported by case law (e.g., SEC v. Howey), SEC guidance, academic research, industry whitepapers, and international comparisons.

Technical concepts like staking and proof-of-reserves are explained plainly for policymakers. The focus is on regulatory clarity, decentralization, and compliance efficiency without compromising investor safeguards.

Sections

Mortar Strategies Overview

Government Relations & Public Affairs for Blockchain Innovators

WHO WE ARE

Mortar Strategies is dedicated to empowering blockchain companies with the strategic insights and advocacy needed to thrive in a complex regulatory and legislative environment. Our decades of experience in legislative advocacy, regulatory guidance, stakeholder engagement, and strategic communications transforms challenges into opportunities—helping you shape a future where innovation meets favorable policy.

Experience Forged By...
40+ years lobbying and public affairs
15+ years blockchain industry
15+ years political campaigns
15+ years serving Capitol Hill

THE CHALLENGE

Regulatory Complexity: Fragmented federal agency activity creates regulatory uncertainty.

Legislation: Vacuum of knowledge on benefits of blockchain technology coupled with a polarized environment where bipartisanship is required.

Alignment: Coordinating diverse stakeholders requires massive trust.

OUR SERVICES

Policy Monitoring: Collect real-time intelligence and provide 24/7 guidance to tailor strategy.

Policy Advocacy: Directly engage policymakers to promote blockchain-friendly frameworks.

Stakeholder Relations: Coalition engagement with allied industry, non-profit, and other leaders to increase awareness, boost credibility, and complement existing trade association memberships.

Strategic Communications: Craft policy focused messaging to showcase blockchain innovations and leadership.

OUR APPROACH

Discovery & Analysis: Identify legislative, regulatory, and stakeholder opportunities.

Strategic Planning: Develop tailored advocacy and communications strategies.

Engagement & Implementation: Execute on stakeholder legislative and regulatory goals.

Review & Optimization: Evaluate outcomes and refine strategies for ongoing success.

LET'S CONNECT

Website: https://mortarstrategies.com | Washington, D.C. Based: Global Reach

MORTAR STRATEGIES

Executive Summary

1. Security Status

- **Predictable Taxonomy:** Define clear categories (e.g., tokenized securities, investment-contract tokens, pure utility tokens, non-security assets) aligned with Howey, MiCA, FINMA models.
- **Non-Howey Instruments:** Issue guidance applying Reves to stablecoins and lending notes, distinguishing payment-focused (non-security) vs. investment-oriented stablecoins.
- **Functional & Staking Tokens:** Clarify that consumptive tokens and pass-through liquid staking tokens (LSTs) are non-securities if structured transparently.

2. Scoping Out

- **Non-Security Assets:** Confirm fiat-backed stablecoins, wrapped non-securities (e.g., WBTC), and consumptive NFTs fall outside SEC jurisdiction.
  Dynamic Taxonomy: Establish outcome-based criteria ("payment," "utility," "investment") with periodic review and global alignment.

3. Public Offerings

- **Tailored Disclosure:** Adapt S-1/Reg A/Crowdfunding frameworks with token-specific disclosures (tokenomics, code status, roadmap).
- **Ongoing Reporting:** Design streamlined, web-based "token issuer" reports (quarterly/semiannual) covering protocol updates and adoption metrics.

4. Safe Harbor

- **Time-Limited Exemption:** Propose "Safe Harbor X" (3-year window) with objective decentralization thresholds, required disclosures, and anti-fraud guardrails—retroactively available to compliant projects.

5. Trading

- **New Platform Category:** Create a "Digital Asset Trading Platform" or amend Reg ATS to permit dual trading of securities and non-securities with appropriate segregation.
- **Best Execution & MEV:** Issue guidance addressing MEV, gas fees, and slippage; invest in on-chain/off-chain surveillance and data aggregation.

6. Custody

- **Modernized Rules:** Amend Rules 15c3-3 and 206(4)-2 to recognize multi-sig wallets, self-custody with safeguards, and state-chartered custodians; update net-capital haircuts based on liquidity/volatility.
- **Recordkeeping & Audits:** Update Rules 17a-3/17a-4 for blockchain-specific logs and endorse AICPA PoR practices with crypto-expert auditors.

7. Crypto Lending

- **Differentiated Oversight:** Light-touch guidance for over-collateralized DeFi lending; require registration or tailored exemptions for pooled centralized lending.

8. Crypto ETPs

- **Integrity Framework:** Use multi-factor metrics (market cap, volume, spreads) over SSAs; treat spot ETPs on par with futures ETFs leveraging CME linkage & robust indices.

9. Tokenized Securities

- **Regulatory Updates:** Exempt on-chain settlement from clearing agency rules; update transfer-agent provisions (Rule 17Ad-15) to recognize blockchain records; grant 40 Act relief for tokenized funds.

10. Sandbox & International Coordination

- **Domestic Sandbox:** Launch accredited-investor pilots for DeFi, tokenized offerings, and compliance tech under no-action relief.
- **Cross-Border Collaboration:** Partner via GFIN with FCA/MAS to harmonize testing, data-sharing, and rule development.

Security Status

Defining a Predictable Taxonomy

Question Addressed: How can regulators classify crypto assets to determine security status predictably?

Analysis: The Howey test defines a security as "an investment of money in a common enterprise with a reasonable expectation of profits from others' efforts." While flexible, its application to crypto can be inconsistent, causing uncertainty. A clear taxonomy could categorize assets as: (1) tokenized securities (e.g., stocks), (2) assets offered as investment contracts, (3) tokenized traditional securities, and (4) non-security crypto assets. This aligns with economic reality, remaining merit- and technology-neutral. International models like the EU's MiCA (utility, asset-referenced, e-money tokens) and Swiss FINMA (payment, utility, asset tokens) offer precedents.

Recommendations: Adopt a taxonomy with clear criteria for each category, ensuring flexibility for new asset types. Engage industry for feedback to refine classifications.

Insight: A taxonomy reduces litigation risks by providing predictability, fostering innovation while enabling targeted enforcement against fraud.

Clarifying When Tokens Are "Securities"

Question Addressed: How do non-Howey security definitions (e.g., notes, derivatives) apply to crypto?

Analysis: The Securities Act includes "notes" and "evidences of indebtedness." The Reves test could clarify when crypto lending or stablecoin arrangements are notes. For example, algorithmic stablecoins with repayment promises might be securities, while fully-backed payment stablecoins (e.g., USD-pegged, 1:1) are not, as per recent SEC guidance. Clarifying non-Howey categories reduces over-reliance on investment contract analysis.

Recommendations: Issue guidance on applying Reves to crypto lending and stablecoins, confirming non-security status for payment-focused stablecoins.

Insight: Clear non-Howey guidance prevents misclassification, ensuring only true securities face registration burdens, enhancing market efficiency.

Technology Functions vs. Securities Law

Question Addressed: Should tokens with technical functions (e.g., staking, gas fees) be treated differently?

Analysis: Tokens enabling network functions (e.g., ETH for gas, staking rewards) are often non-investment-focused. If distributed without fundraising or profit promises, they resemble commodities. The SEC's FinHub Framework notes consumptive use and decentralization as non-security indicators. However, fundraising sales may trigger Howey. Block rewards earned through mining/staking are not securities, but third-party staking pools could raise issues.

Recommendations: Clarify that functional tokens earned via network participation are not securities. Address staking pools separately to assess investment product risks.

Insight: Recognizing utility tokens encourages decentralization and network security, balancing innovation with fraud prevention.

Liquid Staking Tokens (LSTs)

Question Addressed: Are liquid staking tokens securities?

Analysis: LSTs (e.g., Lido's stETH) represent staked assets, allowing trading while earning rewards. Like warehouse receipts for commodities, they are claims on user assets, not investments in a promoter's efforts. Courts and SEC no-action letters support non-security status for similar arrangements (e.g., gold storage receipts). Exceptions arise if platforms promise additional profits beyond protocol rewards.

Recommendations: Issue guidance treating LSTs as non-securities when structured as pass-through claims, with transparency requirements for risks (e.g., slashing).

Insight: Supporting LSTs enhances liquidity for proof-of-stake networks, critical for decentralization, while transparency mitigates investor risks.

Recommendations (Security Status)

1. Publish a framework defining crypto asset categories.
2. Clarify non-Howey security applications (e.g., notes, swaps).
3. Confirm functional tokens are not securities absent investment promises.
4. Address LSTs via no-action letters, treating them as commodity receipts.
5. Seek public input to evolve the taxonomy.

Scoping Out

Identifying Non-Security Crypto Assets

Question Addressed: Which crypto assets fall outside SEC jurisdiction?

Analysis: Clarifying non-security assets reduces compliance burdens and directs issuers to appropriate regulators. Key categories include:

- **Stablecoins**: Fully-backed, fiat-pegged stablecoins (e.g., USDC) used for payments are not securities, per 2025 SEC CorpFin guidance, if they lack investment intent. Asset-backed stablecoins may require investment company analysis.
- **Wrapped Tokens**: Tokens like WBTC represent non-security assets (e.g., Bitcoin) and should not be securities unless additional promises are made. Tokenized securities inherit their underlying's status.
- **NFTs**: NFTs for art or collectibles are not securities unless marketed as investments (e.g., Impact Theory case). Consumptive NFTs lack common enterprise or profit expectations.

Recommendations: Issue a policy statement confirming non-security status for payment stablecoins, wrapped non-securities, and consumptive NFTs, with caveats for facts-based analysis.

Insight: Scoping out non-securities clarifies regulatory boundaries, reducing overreach and enabling other regulators (e.g., CFTC, Treasury) to address relevant risks.

Toward a Workable Taxonomy

Question Addressed: How can a technology-neutral taxonomy accommodate innovation?

Analysis: A taxonomy based on rights/expectations (e.g., payment, utility, investment tokens) ensures flexibility. Avoid blockchain-specific terms, using "transferable units on a distributed ledger." International models (MiCA, UK FCA) provide alignment opportunities. Periodic reviews can address new assets (e.g., social tokens).

Recommendations: Develop a taxonomy with outcome-based criteria (e.g., decentralization as no single controller). Establish an advisory committee for updates. Align with global regulators to prevent arbitrage.

Insight: A dynamic, neutral taxonomy fosters global consistency, reducing compliance costs and supporting cross-border innovation.

Recommendations (Scoping Out)

1. Confirm non-security status for payment stablecoins, wrapped non-securities, and consumptive NFTs.
2. Identify other regulators' roles (e.g., CFTC for commodities).
3. Create a review mechanism to update the taxonomy.
4. Engage internationally for consistent definitions.

Public Offerings

Tailored Disclosure and Relief

Question Addressed: Can the SEC address high costs and ill-fitting disclosure requirements for token offerings via guidance, relief, or new forms?

Analysis: Traditional disclosure forms (e.g., S-1) assume established issuers, misaligning with early-stage, open-source token projects. Guidance could tailor disclosures to crypto-specific elements: token functionality, protocol technology, tokenomics (supply, burns), development roadmap, and risks (cybersecurity, regulatory). Targeted relief could waive irrelevant requirements (e.g., management details for decentralized networks). Precedents like Regulation A (simplified for small offerings) and Regulation Crowdfunding (streamlined for micro-offers) support this approach. If existing forms remain inadequate, a new "Token Offering" form could formalize tailored disclosures, potentially piloted with volunteer projects.

Recommendations: Issue crypto-specific disclosure guidance and grant relief for inapplicable requirements. Pilot a bespoke token offering form if needed.

Insight: Tailored disclosures reduce compliance costs, enabling small projects to access public markets while providing investors with relevant information.

Tailored Ongoing Disclosure

Question Addressed: Should the SEC develop ongoing disclosure requirements for token offerings, and what information should be included?

Analysis: Token networks evolve rapidly, requiring continuous investor updates unlike static IPOs. A "token issuer ongoing report" (semiannual or quarterly) could cover tokenomics changes, development progress, adoption metrics (e.g., active users), financial status, and incidents (e.g., breaches). Initial sale disclosures should detail plans, team, use of proceeds, and risks. Ongoing reports could be posted on public websites or blockchain systems, complementing EDGAR filings. Anti-fraud standards must apply to ensure accuracy.

Recommendations: Design a streamlined ongoing report for token issuers, balancing frequency (e.g., semiannual) with accessibility (e.g., web-based). Enforce anti-fraud rules.

Insight: Ongoing disclosures align with crypto's dynamic nature, enhancing transparency without overburdening resource-constrained projects.

Using Regulation A (Tier 1/Tier 2) for Tokens

Question Addressed: Is Regulation A viable for token offerings, and could revisions improve it?

Analysis: Regulation A (up to $75M) allows public solicitation and tradeable tokens, as shown by Blockstack's 2019 Reg A+ offering ($23M). However, the process was costly and slow (10 months), deterring others. Revisions could clarify token applicability, relax audited financial requirements for pre-revenue projects, and confirm trading on digital asset platforms. Alternatively, Regulation CF ($5M cap) or a new exemption could suit smaller projects.

Recommendations: Publish a Reg A compliance guide for tokens, relax financial audit rules, and clarify secondary trading. Explore raising Reg CF caps for tokens.

Insight: Enhancing Reg A fosters broad community participation in token sales, aligning with decentralization goals while maintaining investor protections.

Recommendations (Public Offerings)

1. Compile lessons from past token offerings (e.g., Blockstack, INX) to issue compliance guidance.
2. Launch a "Token Offering" pilot to test tailored processes.
3. Support new mechanisms (e.g., safe harbor) if existing rules fall short.
4. Ensure disclosures balance investor needs with project feasibility.

Safe Harbor from Registration

Implementing a Safe Harbor (Rule 195 or "Safe Harbor X")

Question Addressed: Should the SEC adopt a safe harbor like Rule 195 or Safe Harbor X?

Analysis: A safe harbor offers a time-limited exemption (e.g., 3 years) for token projects to decentralize without immediate registration, requiring public disclosures and good-faith efforts. Safe Harbor X refines this with stricter transparency (e.g., insider sales) and objective decentralization criteria. Key features include non-exclusivity, clear disclosures (project, tokenomics, team, risks), a defined time limit with exit conditions, and anti-fraud provisions. Global sandboxes provide precedent.

Recommendations: Propose an interim safe harbor rule combining Rule 195 and Safe Harbor X, soliciting public comment.

Insight: A safe harbor breaks the regulatory logjam, encouraging compliant innovation and community-driven networks.

Retroactive Application

Question Addressed: Should the safe harbor apply retroactively to existing projects?

Analysis: Retroactive application could allow pre-safe harbor projects to comply by filing disclosures, reducing enforcement overhang and benefiting token holders with transparency. It should exclude projects under investigation or guilty of fraud, with precedent in SEC amnesty programs (e.g., 1990s Section 16(a)).

Recommendations: Allow retroactive safe harbor for compliant projects initiated before the rule, excluding those with enforcement actions.

Insight: Retroactivity incentivizes compliance, leveling the playing field and reducing litigation risks for good-faith projects.

Disclosure Requirements in a Safe Harbor

Question Addressed: What disclosures are feasible for early-stage projects, and how should updates be provided?

Analysis: Initial disclosures should cover project purpose, tokenomics, team, use of funds, roadmap, code status, risks, and optional legal analysis. Ongoing updates (quarterly, web-based, EDGAR-filed) should report roadmap progress, team changes, token issuances, fund status, and partnerships. Blockchain-based disclosure (e.g., hashed reports) could enhance transparency.

Recommendations: Require initial and quarterly disclosures focusing on transparency, accessible via websites and EDGAR. Explore blockchain disclosure options.

Insight: Lightweight disclosures align with investor needs (progress, not profits), fostering trust without stifling innovation.

Measuring Decentralization – Objective Thresholds

Question Addressed: Should the SEC define objective decentralization thresholds, and is dispersion of control a better framework?

Analysis: Objective thresholds (e.g., no entity controls >20% tokens, <50% insider holdings, diverse governance) clarify decentralization. Dispersion of control focuses on power distribution (tokens, voting), accounting for delegation. Multi-factor tests (token distribution, code contributions, governance) and qualitative caveats prevent gaming. Third-party audits could verify compliance.

Recommendations: Set quantitative benchmarks (e.g., token/governance dispersion) with qualitative oversight. Allow third-party audits for verification.

Insight: Clear thresholds reduce uncertainty, enabling verifiable decentralization while deterring manipulation.

Evaluating Decentralization in Practice

Question Addressed: How should decentralization be evaluated, considering permissioned roles (e.g., validators, sequencers)?

Analysis: Evaluation includes node distribution (e.g., validator diversity), infrastructure (e.g., admin keys), permissioned roles (e.g., sequencers' decentralization plans), and forkability. Tech-neutral thresholds (e.g., no unilateral control) ensure flexibility. Projects must disclose centralized roles and decentralization timelines.

Recommendations: Require disclosure of centralized roles and plans to decentralize. Use tech-neutral metrics (e.g., node diversity, no single-entity control).

Insight: Multidisciplinary evaluation ensures robust decentralization, supporting network autonomy while addressing regulatory concerns.

Recommendations (Safe Harbor)

1. Propose a safe harbor rule with clear disclosures and exit criteria.
2. Include quantitative decentralization benchmarks with flexibility.
3. Allow retroactive application for compliant projects.
4. Require initial and periodic disclosures, with a final decentralization report.
5. Enable third-party audits and self-certification for compliance.

Trading

New Trading Platforms Registration Category

Question Addressed: Should the SEC create a new registration category for crypto trading platforms or adapt existing exchange/ATS frameworks?

Analysis: Platforms trading crypto asset securities must register as national securities exchanges or Alternative Trading Systems (ATSs), but these rules assume traditional securities and intermediated access. Crypto platforms (e.g., Coinbase) trade both securities and non-securities (e.g., Bitcoin), complicating compliance. A new "Digital Asset Trading Platform" category could allow listing both asset types with tailored rules (e.g., segregation, anti-manipulation, custody protections). Alternatively, adapting Reg ATS to permit direct retail access or creating a "notational exchange" with scaled requirements could work. A regulatory sandbox could test relaxed rules while maintaining oversight. Inter-agency cooperation with the CFTC could unify oversight for mixed platforms, as proposed by Coinbase in 2022.

Recommendations: Propose a new platform category or amend Reg ATS for retail access and dual-asset trading. Pilot a sandbox for crypto exchanges.

Insight: Build frameworks to reduce compliance barriers for innovation & ensure investor protection.

Side-by-Side Trading and Interoperability

Question Addressed: What updates enable side-by-side trading of securities and non-securities to enhance interoperability and composability?

Analysis: Composability allows seamless token interactions (e.g., tokenized stocks as DeFi collateral). Strict separation of securities and non-securities fragments markets, reducing blockchain benefits. Updates could include allowing broker-dealers/ATSs to handle both asset types, clarifying custody rules, and encouraging consolidated price feeds for all tokens. Exemptive rules or safe harbors could permit DeFi protocols handling security tokens to operate under oversight, avoiding bans. Coordination with FINRA could standardize dual-activity firms.

Recommendations: Permit broker-dealers/ATSs to trade both asset types. Develop consolidated data feeds and DeFi safe harbors.

Insight: Interoperability supports DeFi innovation, enabling efficient markets while maintaining regulatory clarity.

Best Execution in On-Chain and Off-Chain Trading

Question Addressed: Do on-chain/off-chain trading complexities affect best execution, and should rules be modified?

Analysis: Best execution requires brokers to seek optimal trade terms, but on-chain trading (e.g., DEXs) introduces challenges like MEV (e.g., front-running), gas fees, and block timing. Guidance could clarify that brokers consider MEV risks, gas costs, and slippage, using tools like private relays (e.g., Flashbots) to mitigate harm. Disclosures to clients about on-chain risks (e.g., network fees, delays) are needed. A principles-based approach could account for crypto market dynamics, encouraging smart order routers for best pricing.

Recommendations: Issue best execution guidance for crypto, emphasizing MEV mitigation and client disclosures. Promote flexible, principles-based standards.

Insight: Updated guidance ensures fairness in crypto trading, aligning broker duties with blockchain realities without stifling DEX use.

Open-Source Data for Market Monitoring

Question Addressed: Can open-source blockchain data enhance market monitoring, and what are its limitations?

Analysis: Blockchain transparency enables tracking of transactions and patterns (e.g., pump-and-dumps) via analytics tools (e.g., Chainalysis). Regulators could run nodes to monitor real-time data, flagging anomalies. However, centralized exchange internal trades are off-chain, requiring exchange cooperation. Proof of Reserves (PoR) and Proof of Solvency enhance transparency but are limited (e.g., snapshots, no liability coverage), needing auditor oversight. Regulators could use crowd-sourced tips and require standardized exchange data feeds.

Recommendations: Invest in blockchain analytics for surveillance. Encourage PoR with auditor disclosures. Standardize exchange data feeds.

Insight: Blockchain data empowers proactive oversight, reducing reliance on firm reports while addressing off-chain gaps through cooperation.

Regulatory Ingestion of Order Book Data

Question Addressed: How should regulators ingest and analyze order book data from APIs and ledgers?

Analysis: Centralized exchanges provide APIs, while DEX order books are smart contract states. Regulators could aggregate public APIs and decode DEX transactions, avoiding new reporting burdens. Standardization (e.g., a crypto FIX protocol) would ease data integration. AI and analytics could detect anomalies (e.g., spoofing). PoR verifications could be automated as data points, reducing compliance costs.

Recommendations: Build API aggregation systems and DEX decoders. Promote data standardization via industry groups. Use AI for anomaly detection.

Insight: Leveraging public data streamlines oversight, minimizing firm burdens while enabling real-time market monitoring.

Maximal Extractable Value (MEV) Considerations

Question Addressed: How should registrants assess MEV, delineate its types, and address its impact?

Analysis: MEV (profit from transaction ordering) includes benign arbitrage (e.g., price equalization) and predatory forms (e.g., sandwich attacks). Brokers must assess MEV risks to meet best execution, using tools like private relays or order splitting. Regulators could categorize predatory MEV as manipulative, encouraging anti-MEV solutions (e.g., Flashbots, batch auctions). Market efforts like MEV-Boost and proposer-builder separation mitigate harm. Guidance could mandate MEV mitigation for security token venues.

Recommendations: Issue MEV guidance for registrants, recognizing anti-MEV tools. Encourage batch auctions and fair sequencing.

Insight: Addressing MEV ensures fair trading, aligning crypto markets with traditional regulatory standards while supporting technical solutions.

Recommendations (Trading)

1. Create a “Digital Asset Trading Platform” category or amend Reg ATS for dual-asset trading and retail access.
2. Issue best execution guidance addressing MEV, gas fees, and on-chain risks.
3. Invest in blockchain analytics and API aggregation for surveillance, standardizing exchange data feeds.
4. Encourage PoR and Proof of Solvency with auditor oversight, integrating into regulatory data systems.
5. Provide MEV guidance, mandating mitigation for security token trading and supporting fair sequencing solutions.
6. Coordinate with CFTC and FINRA for unified oversight and industry standards (e.g., consolidated transaction tape).

Custody

Modernizing Custody Rules for Crypto

Question Addressed: Should the SEC amend rules, propose new ones, or issue guidance for crypto custody, including self-custody, and differentiate between securities and non-securities?

Analysis: Existing SEC custody rules target traditional assets, not key-controlled crypto, and SPBD relief ends in 2025. The SEC should amend Rule 15c3-3 to let broker-dealers hold crypto under strict controls (multi-sig, cybersecurity, audits) and update Rule 206(4)-2 to permit adviser self-custody (offline storage, consent, surprise exams). A unified digital-asset custody rule would ensure consistent protection, interim guidance could recognize multi-sig as control, and expanding "qualified custodian" to include state/OCC-chartered crypto firms would broaden options.

Recommendations: Amend Rules 15c3-3 and 206(4)-2 for crypto custody and self-custody. Issue interim guidance and recognize specialized QCs.

Insight: Flexible rules foster secure custody innovation, reducing reliance on nascent custodians while maintaining robust protections.

Tokenized Permissioned vs. Native Assets

Question Addressed: How should custody rules differentiate between native crypto assets and tokenized permissioned assets, and which poses greater risks?

Analysis: Native assets (e.g., ETH) exist solely on permissionless chains, with no central recourse if stolen, posing higher theft risk due to irreversibility. Tokenized permissioned assets (e.g., tokenized stocks) may have issuer controls (e.g., freezing), reducing theft impact but introducing counterparty risk. Custody risks (hacking, key loss) are similar, but permissioned assets may leverage issuer safeguards. Rules should require BDs/IAs to analyze asset features (e.g., freeze functions, admin keys) to tailor custody controls, ensuring equal safeguarding rigor for both types.

Recommendations: Mandate asset-specific custody analysis. Apply consistent safeguarding standards, leveraging permissioned asset features where applicable.

Insight: Uniform rules with tailored controls balance risks, ensuring native assets' irreversibility is mitigated by robust security.

Auditing, Accounting, and Valuation Standards

Question Addressed: Are there accepted practices for auditing/accounting crypto assets, and should the SEC propose specific requirements?

Analysis: AICPA guidance outlines crypto accounting (intangible assets under GAAP, fair value for trading) and auditing (proof-of-ownership via key signing, blockchain confirmation). Valuation uses exchange data, but GAAP's cost-minus-impairment model lags market reality. PCAOB notes proof-of-reserve (PoR) reports lack audit rigor. The SEC could enhance trust by requiring auditors with crypto expertise, mandating enhanced verification (e.g., in-person key signing), and endorsing FASB's fair value proposals. Non-CPA attestations (e.g., cybersecurity) could supplement audits.

Recommendations: Issue guidance endorsing AICPA practices, require crypto-expert auditors, and support FASB fair value rules. Allow supplemental attestations.

Insight: Standardized auditing boosts investor confidence, aligning crypto reporting with traditional rigor while addressing unique risks.

Broker-Dealer Custody and Financial Responsibility

Special Purpose Broker-Dealer (SPBD) Framework

Question Addressed: Should the SEC modify or withdraw the SPBD Statement, and how should Rule 15c3-3 accommodate crypto?

Analysis: The SPBD Statement's restrictions (only digital asset securities, no mixed custody) limit adoption. Expanding it to cover both securities and non-securities, with conditions (e.g., key control, daily reconciliations, insurance), would align with customer needs. Amending Rule 15c3-3 to include "secure digital wallets" as good control locations, with audit standards, ensures compliance. Withdrawing SPBD without replacement risks pushing custody to unregulated entities. Capital charges for crypto volatility could enhance safeguards.

Recommendations: Expand SPBD into a permanent Rule 15c3-3 amendment for mixed custody, defining secure wallets as control locations.

Insight: A unified custody rule supports integrated platforms, enhancing investor access while maintaining protection.

Net Capital Treatment of Crypto Assets

Question Addressed: How should crypto assets be evaluated for liquidity and haircuts under Rule 15c3-1?

Analysis: Liquid crypto (e.g., BTC, ETH) is "readily convertible to cash" if it has high trading volume and multiple venues. Metrics (e.g., market cap, exchange listings) could define liquidity. Haircuts should reflect volatility: BTC/ETH at 20-40%, volatile altcoins at 50-100%, and stablecoins at 0-10%. Stress testing (e.g., historical volatility) ensures conservatism. Concentration charges could address overexposure.

Recommendations: Define liquidity criteria (volume, venues) and tiered haircuts based on volatility. Apply stress-tested haircuts and concentration charges.

Insight: Tailored haircuts balance capital safety with market realities, encouraging BD crypto adoption without undue risk.

Recordkeeping and Operational Controls

Question Addressed: What recordkeeping challenges do crypto assets pose, and should they be treated like traditional securities?

Analysis: Rules 17a-3/17a-4 require tracking trades and positions, but crypto introduces new data (e.g., transaction IDs, wallet addresses). Records must capture DeFi interactions (e.g., smart contract details) and events (e.g., airdrops). Blockchain data could be retained via hashes, with parsed records for audits. Crypto should align with securities for customer statements and confirms, but rules need updates for wallet schedules and key logs. WORM storage applies, with standard formats for longevity.

Recommendations: Update Rule 17a-3 for wallet schedules and blockchain transaction logs. Clarify DeFi and event recordkeeping. Ensure standard formats.

Insight: Adapted recordkeeping ensures auditability, aligning crypto with securities while addressing blockchain nuances.

Recommendations (Custody)

1. Amend Rules 15c3-3 and 206(4)-2 for BD/IA crypto custody, permitting self-custody with safeguards (multi-sig, audits, disclosures).
2. Issue guidance recognizing specialized QCs and multi-sig controls, followed by permanent rules.
3. Apply consistent custody standards for all crypto, with asset-specific controls (e.g., leveraging permissioned features).
4. Endorse AICPA auditing practices, require crypto-expert auditors, and support FASB fair value accounting.
5. Expand SPBD into a Rule 15c3-3 amendment for mixed custody, defining secure wallets as control locations.
6. Set liquidity criteria and volatility-based haircuts for crypto under Rule 15c3-1.
7. Update Rules 17a-3/17a-4 for crypto-specific records (wallets, blockchain data, DeFi interactions).

Broker-Dealer Custody and Financial Responsibility

Special Purpose Broker-Dealer (SPBD) Framework

Question Addressed: Should the SEC modify or withdraw the SPBD Statement? If modified, how, and should Rule 15c3-3 accommodate crypto assets?

Analysis: The 2020 SPBD Statement's restrictions (only digital asset securities, no other business) limit its adoption, with only one FINRA member approved by late 2023. Expanding it to allow BDs to custody both securities and non-securities (e.g., Bitcoin) under one entity aligns with customer demand for unified platforms. Amending Rule 15c3-3 to include a "Digital Asset Custody" provision could formalize conditions: exclusive private key control, on-chain segregation (e.g., omnibus accounts with sub-ledgering), daily reconciliations, risk disclosures (e.g., no SIPC coverage), and theft insurance. Withdrawing SPBD without replacement risks pushing custody to unregulated entities or non-BD channels (e.g., banks), undermining oversight. Adding "secure digital wallets" as good control locations under Rule 15c3-3, with audit standards, ensures compliance. Capital charges for crypto volatility could enhance safeguards.

Recommendations: Expand SPBD into a permanent Rule 15c3-3 amendment for mixed custody, defining secure wallets as control locations. Require custody statistics reporting.

Insight: A unified custody framework supports integrated platforms, enhancing investor access while maintaining robust protections.

Net Capital Treatment of Crypto Assets

Question Addressed: How should crypto assets be evaluated for liquidity and haircuts under Rule 15c3-1?

Analysis:

- **Liquidity**: A crypto asset is "readily convertible to cash" if it has high daily trading volume (fiat/stablecoin terms), multiple reputable exchange listings, and minimal price impact on sale. Metrics (e.g., market cap >$X, listed on Y platforms) could define liquidity. Bitcoin and Ether qualify; small-cap tokens may not, requiring stress-tested convertibility (e.g., stablecoin redeemability).
- **Haircuts**: Haircuts should reflect volatility and liquidity risks. Tiered approach: Bitcoin/Ether at 20-40% (higher than equities due to ~80% historical crashes), volatile altcoins at 50-100%, stablecoins at 0-10% (if fully collateralized). Stress testing (e.g., 30-day volatility multiple) ensures conservatism. Concentration charges address overexposure.

Recommendations: Establish liquidity criteria (volume, listings) and tiered haircuts based on volatility. Apply stress-tested haircuts and concentration charges.

Insight: Tailored net capital rules balance BD stability with crypto market realities, encouraging participation without undue risk.

Recordkeeping and Operational Controls

Question Addressed: What recordkeeping challenges do crypto assets pose under Rules 17a-3/17a-4, and should they be treated like traditional securities?

Analysis:

- **Challenges**: Crypto introduces new data (e.g., transaction IDs, smart contract addresses) not covered by traditional ledgers. DeFi trades lack contra-party confirmations, requiring records of transaction hashes. Airdrops/forks need tracking as new assets. Communications via decentralized protocols (e.g., Discord) and blockchain data retention (e.g., hashes vs. full ledgers) pose storage/format issues. WORM compliance (17a-4) applies but needs clarification for crypto keys/signatures.
- **Treatment**: Crypto should align with securities for customer statements and trade confirms, ensuring accurate asset/liability tracking. Additional requirements (e.g., wallet address schedules, on-chain reconciliation logs) enhance auditability. Standard formats ensure future readability despite tech changes.

Recommendations: Update Rule 17a-3 for wallet schedules, transaction logs, and DeFi/airdrop records. Clarify WORM application to crypto data. Require standard formats.

Insight: Adapted recordkeeping ensures transparency and auditability, aligning crypto with securities while addressing blockchain nuances.

Recommendations (Broker-Dealer Custody and Financial Responsibility)

1. Expand SPBD into a Rule 15c3-3 amendment for mixed crypto custody, defining secure wallets as good control locations and requiring insurance, disclosures, and reconciliations.
2. Establish liquidity criteria (volume, exchange listings) and tiered haircuts (20-40% for BTC/ETH, 50-100% for altcoins, 0-10% for stablecoins) under Rule 15c3-1, with stress testing and concentration charges.
3. Update Rules 17a-3/17a-4 to include wallet schedules, blockchain transaction logs, and DeFi/airdrop records, ensuring WORM compliance and standard formats.
4. Require periodic custody statistics reporting to enhance SEC oversight.
5. Issue interim guidance clarifying SPBD expansion and recordkeeping practices pending rule changes.

Investment Adviser Custody and Other Requirements

Challenges Under the Advisers Act & Current Practices

Question Addressed: What challenges do RIAs face with Advisers Act compliance for crypto assets, and what practices address these? Can obligations like best execution, recordkeeping, and Form ADV/PF disclosures be clarified? Do crypto characteristics increase risks?

Analysis:

- **Custody Rule (206(4)-2)**: RIAs trigger custody if they control client crypto (e.g., private keys or withdrawal authority), requiring a qualified custodian (QC). Few QCs historically supported crypto, leading RIAs to use state-chartered trust companies (e.g., Coinbase Custody) or avoid custody via client-held assets. The 2023 Safeguarding Rule proposal tightens requirements, potentially limiting crypto engagement.
- **Form ADV/PF**: Crypto lacks a specific asset class, requiring "Other" categorization. Tailored guidance could clarify reporting staking, liquidity provision, or unregistered tokens.
- **Best Execution**: RIAs must seek optimal trade terms, but crypto venues (e.g., DEXs) raise regulatory uncertainty. Practices include using centralized exchanges or OTC desks, with sophisticated RIAs employing execution algorithms.
- **Recordkeeping (204-2)**: DeFi trades (e.g., transaction hashes) and crypto communications (e.g., Discord) require new archiving solutions. RIAs use blockchain explorers and API data for records.
- **Risks**: Crypto's bearer nature heightens theft/loss risks via key compromise or smart contract bugs. RIAs mitigate with multi-sig wallets, cybersecurity training, and insured custodians.

Recommendations: Issue guidance clarifying best execution (e.g., DEX use, 24/7 monitoring), Form ADV/PF (add "digital assets" category), and recordkeeping (include transaction hashes, DeFi logs). Require crypto custody internal controls audits.

Insight: Clear guidance aligns RIA practices with fiduciary duties, reducing compliance uncertainty while addressing crypto's unique risks.

Enabling Participation in Networks (Staking, Voting, etc.)

Question Addressed: Can RIAs stake, vote, or participate in crypto networks without moving assets from QCs? Should the Custody Rule allow temporary asset movement?

Analysis: Some QCs (e.g., Anchorage) offer staking while retaining custody, but not all support voting or DeFi interactions, requiring asset movement to smart contracts. Amending Rule 206(4)-2 to permit short-term movement (e.g., 7 days) for staking/voting, with conditions (e.g., smart contract due diligence, client consent, records), would enable participation without custody violations. Non-custodial smart contracts (e.g., locked staking) mitigate misappropriation risks.

Recommendations: Amend Rule 206(4)-2 for temporary movement exemptions with safeguards (records, time limits, client notification). Encourage QCs to expand staking/voting services.

Insight: Flexible custody rules unlock blockchain opportunities, aligning RIA fiduciary duties with client value maximization.

Cold vs. Hot Wallet Custody Clarifications

Question Addressed: What clarifications are needed for cold vs. hot wallet custody? What requirements apply, and how do they impact RIA strategies?

Analysis: Cold storage (offline) minimizes hack risks but slows trading, while hot wallets (online) enable fast transactions but increase exposure. Mandating all cold storage would hinder high-frequency strategies. Requirements could include policies balancing security/liquidity (e.g., 90% cold), client disclosures, and hot wallet safeguards (multi-sig, whitelisting, insurance). These ensure safety without dictating wallet type.

Recommendations: Issue guidance requiring cold/hot storage policies, client disclosures, and hot wallet controls (multi-sig, rate limits, HSMs). Avoid prescriptive mandates.

Insight: Balanced wallet guidance supports diverse RIA strategies, ensuring security without compromising market agility.

Investment Company Custody

Challenges Under 17(f) for Funds Holding Crypto

Question Addressed: What challenges do funds face with Section 17(f) for crypto custody? Are requirements inconsistent, and do funds expect eligible custodians?

Analysis: Section 17(f) requires bank/BD custodians, but crypto custodians were initially non-traditional. Banks (e.g., BNY Mellon) and state trust companies now offer solutions, often qualifying as "banks." Challenges include staking/trading outside custody and valuation for 24/7 markets. No requirements are categorically inconsistent, but operational alignment (e.g., DeFi segregation) is needed. Funds expect custodians to support crypto via partnerships.

Recommendations: Confirm state trust companies as 17(f) custodians. Issue guidance on staking/trading within custody frameworks.

Insight: Recognizing evolving custodian options ensures funds can hold crypto compliantly, leveraging existing rules.

Staking/Voting by Funds and Potential Rule Changes

Question Addressed: Can funds stake/vote while complying with 17(f)? Should Rule 17f-2 or others be updated?

Analysis: Custodians offering staking maintain 17(f) compliance, but unsupported activities (e.g., DAO voting) risk custody breaches. Updating Rule 17f-2 to allow limited self-custody for staking/voting (e.g., weekly audits, multi-sig with board approval) could enable participation. Trading requires custodian-aligned systems (e.g., tri-party agreements). Guidance could encourage custodian voting services.

Recommendations: Modernize Rule 17f-2 for crypto self-custody with strict controls. Promote custodian staking/voting solutions.

Insight: Targeted rule updates empower funds to engage in blockchain governance, balancing innovation with oversight.

Unique Fund Activities (Staking, Mining, Airdrops)

Question Addressed: Should custody rules address staking, mining, or airdrops, and do they hinder these activities?

Analysis: Airdrops/forks create new assets custodians may not support, risking value loss. Staking involves smart contract/slashing risks, and mining requires secure reward sweeps. Guidance could allow temporary self-custody for airdrops (e.g., 30 days, board oversight) and staking delegation to vetted contracts. Mining rewards should sweep to custodians daily. Boards must assess risks (e.g., slashing insurance).

Recommendations: Issue guidance for temporary airdrop self-custody, staking delegation, and mining sweeps. Require board risk oversight.

Insight: Flexible custody provisions capture crypto-native value, ensuring funds protect shareholders without regulatory conflicts.

Recommendations (Investment Company Custody)

1. Confirm state trust companies as Section 17(f) custodians and issue guidance on staking, trading, and 24/7 valuation for crypto.
2. Amend Rule 17f-2 to allow limited self-custody for staking/voting with audits, multi-sig, and board approval.
3. Promote custodian staking/voting services to minimize self-custody needs.
4. Issue guidance for temporary airdrop self-custody (30 days), staking delegation, and daily mining sweeps.
5. Mandate board oversight for crypto risks (e.g., slashing insurance) and require robust cybersecurity and recordkeeping.

Crypto Lending

Fostering Opportunities in Crypto Lending

Question Addressed: How should the SEC approach crypto lending to avoid stifling opportunities?

Analysis: Centralized lending (e.g., BlockFi) often resembles unregistered securities offerings, requiring registration or exemptions (e.g., Reg D). DeFi lending (e.g., Aave), with over-collateralized, algorithmic loans, mirrors securities lending and may not involve securities. The SEC could permit DeFi lending with transparency and anti-fraud oversight, while requiring centralized offerings to register or use tailored exemptions (e.g., "Crypto Yield Product" safe harbor). Coordination with CFTC/banking regulators could clarify stablecoin lending.

Recommendations: Issue guidance distinguishing DeFi lending (light-touch) from centralized offerings (registration/exemption). Propose a safe harbor for compliant yield products.

Insight: Nuanced regulation supports safe lending models, fostering yield opportunities without unchecked risks.

Comparing Crypto Lending to Traditional Securities Lending

Question Addressed: How do crypto lending programs compare to traditional securities lending?

Analysis:

- **Similarities**: Both involve lending assets for interest, with collateral, expecting return from borrower payments, not platform efforts. Over-collateralization and recall rights align structures.
- **Differences**: Centralized crypto lending (e.g., Celsius) often pools assets, relying on platform management, resembling investment contracts. Traditional securities lending uses regulated brokers with strict collateral rules, avoiding rehypothecation risks. DeFi lending's transparency (on-chain) contrasts with centralized opacity.

Recommendations: Clarify via no-action letter that over-collateralized, non-pooled crypto lending (e.g., DeFi) is not a security, akin to securities lending. Require registration for pooled, effort-dependent programs.

Insight: Aligning DeFi lending with securities lending encourages innovation, while regulating centralized models protects investors.

Recommendations (Investment Adviser Custody and Other Requirements)

1. Issue guidance clarifying best execution (DEX use, 24/7 monitoring), Form ADV/PF (add "digital assets"), and recordkeeping (transaction hashes, DeFi logs).
2. Amend Rule 206(4)-2 for temporary asset movement for staking/voting, with safeguards (e.g., 7-day limit, client consent).
3. Require cold/hot wallet policies, client disclosures, and hot wallet controls (multi-sig, insurance) without mandating storage type.
4. Confirm state trust companies as 17(f) custodians and modernize Rule 17f-2 for limited crypto self-custody by funds.
5. Issue guidance for airdrop self-custody (30 days), staking delegation, and mining sweeps, with board oversight.
6. Permit DeFi lending with transparency and anti-fraud oversight; require centralized lending to register or use exemptions.
7. Propose a "Crypto Yield Product" safe harbor for compliant lending, coordinating with CFTC/banking regulators.

Crypto Exchange-Traded Products (ETPs)

Addressing Fraud/Manipulation without an SSA

Question Addressed: Can a listing exchange address fraud/manipulation concerns without an SSA, using size/liquidity measures or other means?

Analysis: Without a surveillance-sharing agreement (SSA), exchanges can demonstrate market maturity to mitigate manipulation risks. Bitcoin's ~$500B market cap and tens of billions in daily volume (2025) suggest scale where sustained manipulation is costly and quickly arbitraged. Metrics like high volume-to-market-cap ratio, tight bid-ask spreads, and low price divergences (e.g., <1–2% across exchanges) indicate liquidity and arbitrage efficiency. Exchanges could implement surveillance using blockchain analytics and API data to monitor anomalies, or design ETPs with robust pricing indices (e.g., volume-weighted, outlier-resistant). Coordination with CME futures markets, indirectly tied to spot, could enhance oversight.

Recommendations: Establish safe harbor thresholds (e.g., volume >10% market cap, spreads <1%) and encourage exchange-led surveillance and index-based pricing.

Insight: Market maturity and alternative surveillance reduce reliance on SSAs, enabling spot ETPs while addressing fraud concerns.

Key Factors for Market Integrity

Question Addressed: What factors should the SEC consider for evaluating a crypto market's integrity?

Analysis: A holistic evaluation includes:

- **Market Cap**: High cap (e.g., BTC's ~$2T) signals broad ownership, deterring manipulation.
- **Unique Wallets**: Diverse, non-concentrated addresses suggest decentralized control, reducing cornering risks.
- **Trading Volume**: High organic volume (e.g., 10% of market cap daily) across venues ensures liquidity.
- **Number/Geography of Spot Markets**: Trading on many exchanges (none >30% volume) globally fosters 24/7 arbitrage.
- **Price Divergences/Arbitrage Speed**: Low divergence (<1% median) and rapid convergence (minutes) counter manipulation.
- **Arbitrage Mechanisms**: Futures, OTC desks, and stablecoin flows normalize prices.

Recommendations: Adopt a multi-factor framework prioritizing volume, distribution, and arbitrage efficiency for integrity assessments.

Insight: Comprehensive metrics ensure objective evaluations, aligning crypto ETP approvals with other commodities.

Interaction with Existing Crypto ETFs under 40 Act

Question Addressed: How should the SEC consider spot ETPs for assets in existing 40 Act ETFs (e.g., Bitcoin futures ETFs)?

Analysis: Consistency avoids regulatory arbitrage. Bitcoin futures ETFs (approved 2021) rely on CME surveillance, implying spot market integrity (futures track spot). Spot ETPs (1933 Act trusts) offer similar exposure without roll costs. The Grayscale ruling criticized SEC's inconsistent spot/futures standards. Spot ETPs should leverage futures SSA indirectly, with robust custody/pricing. Existing ETF performance (tight spot tracking) supports spot market orderliness.

Recommendations: Treat spot ETPs comparably to futures ETFs, leveraging CME SSA and market data to streamline approvals.

Insight: Parity ensures fairness, recognizing spot market maturity via futures linkage for investor benefit.

Factors for Surveillance Sharing Agreements (SSAs)

Question Addressed: What factors should the SEC consider for an SSA with a spot crypto market?

Analysis: Key factors include:

- **Market Scope**: SSA partner (e.g., Coinbase) must influence global pricing significantly.
- **Regulatory Status**: Partners should be regulated (e.g., BitLicense) with strong surveillance.
- **Data Depth**: Real-time order book/trade data and customer info sharing are critical.
- **Integrity Measures**: Partner's KYC/AML and anti-manipulation controls (e.g., wash trade monitoring) enhance SSA value.
- **Coverage**: Focus on ETP's underlying asset; multiple SSAs or group sharing (e.g., ISG-like) could suffice.
- **CME Proxy**: CME futures SSA may indirectly cover spot via reference rate linkage.

Recommendations: Prioritize SSAs with major, regulated exchanges offering deep data. Explore multiple SSAs or CME linkage.

Insight: Flexible SSA criteria balance oversight with market realities, supporting ETP approvals.

Pricing Information and Reliability

Question Addressed: How should the SEC weigh pricing information reliability, frequency, and dissemination for ETP assets?

Analysis:

- **Reliability**: Use independent, audited indices (e.g., CME CF Bitcoin Reference Rate) with multi-exchange inputs and outlier detection to ensure robust NAV calculation.
- **Frequency**: Real-time feeds (every 15 seconds) support intraday indicative values, enabling arbitrage to align ETP price with NAV.
- **Dissemination**: Publish NAV/IIV via Consolidated Tape, public websites, and redundant vendors to ensure accessibility. Use TWAP (e.g., 1-hour at 4pm EST) for closing NAV to limit manipulation.

Recommendations: Require ETPs to use audited indices, real-time feeds, and public dissemination via standard channels.

Insight: Robust pricing ensures ETPs track underlying assets accurately, protecting investors from dislocations.

Recommendations (Crypto ETPs)

1. Establish safe harbor thresholds (e.g., volume >10% market cap, spreads <1%) and encourage exchange-led surveillance for ETPs without SSAs.
2. Adopt a multi-factor integrity framework (market cap, volume, arbitrage speed) for objective market evaluations.
3. Treat spot ETPs comparably to futures ETFs, leveraging CME SSA and market performance data.
4. Prioritize SSAs with major, regulated exchanges; explore multiple SSAs or CME linkage.
5. Require ETPs to use audited, multi-exchange indices, real-time pricing (15-second updates), and public NAV/IIV dissemination.
6. Issue guidance formalizing integrity metrics and pricing standards to streamline ETP approvals.

Tokenized Securities

Legal Provisions Impeding Tokenization & Steps to Enable Innovation

Question Addressed: Do federal securities laws impede tokenized securities in blockchain applications? How can the SEC facilitate innovation while mitigating risks, ensuring tech-neutrality? Does blockchain type matter?

Analysis:

- **Exchange Act (Trading Venues)**: Peer-to-peer trading platforms risk being unregistered exchanges/ATSs. Regulation ATS assumes centralized intermediaries, misaligning with decentralized systems.
- **Clearing Agencies**: Blockchain's T+0 settlement bypasses clearinghouses, but Rule 15c6-1 assumes T+1 processes. Unregistered netting systems may trigger clearing agency needs.
- **Transfer Agents**: Rules (e.g., Rule 17Ad-15) assume traditional ledgers, not blockchain-based ownership records.
- **Custody**: Existing rules (e.g., 15c3-3, 206(4)-2) apply but need clarity for self-custody or digital custodians; SIPC coverage for tokenized securities is uncertain.
- **Securities Act**: Tokenized offerings require wallet delivery mechanisms and key loss disclosures.
- **FINRA**: Broker confirmations need blockchain transaction adaptation (e.g., hash confirms).
- **Blockchain Type**: Permissioned chains offer control (e.g., KYC, rollback) but centralize trust; permissionless chains enhance security but complicate compliance (e.g., pseudonymity, forks).

Recommendations:

1. Create a Regulation ATS safe harbor for peer-to-peer trading with on-chain reporting.
2. Exempt blockchain T+0 settlement from clearing agency registration if transparent and DvP-compliant.
3. Update Rule 17Ad-15 to recognize blockchain ledgers as official records.
4. Clarify custody rules for self-custody and SIPC coverage.
5. Issue guidance for tokenized offerings (e.g., key management disclosures).
6. Remain tech-neutral, requiring chain-specific safeguards (e.g., transfer restrictions for permissionless, continuity plans for permissioned).

Insight: Targeted rule updates remove barriers, enabling blockchain efficiencies while maintaining investor protections.

Programmability, Composability, and Transfer Agents

Question Addressed: How do smart contracts affect transfer agents? Are there impediments to blockchain use or on-chain identity solutions?

Analysis: Smart contracts automate transfer agent functions (e.g., ownership tracking, dividends, voting), shifting agents to oversight roles. Rules (e.g., 17Ad-10) permit blockchain but assume manual processes. Delaware DGCL (§224) allows blockchain ledgers, but SEC rules need alignment. Off-chain backups are prudent for continuity (e.g., chain failures). On-chain identity (e.g., ERC-725, whitelisting) ensures compliance but faces privacy/AML challenges. No explicit prohibitions exist, but clarity is needed for decentralized identity systems.

Recommendations:

1. Update Rule 17Ad-15 to allow blockchain ledgers as primary records, with off-chain backup requirements.
2. Permit transfer agents to oversee smart contracts, certifying compliance.
3. Issue guidance recognizing on-chain identity (e.g., KYC-linked whitelists) if verified by regulated entities.

Insight: Clarifying blockchain's role modernizes transfer agents, enhancing efficiency while ensuring regulatory compliance.

Tokenized Funds and Unique 40 Act Issues

Question Addressed: Do tokenized 1940 Act fund shares raise unique issues? Is relief needed for secondary trading?

Analysis: Tokenized mutual fund shares trading peer-to-peer violate Section 22(d) and Rule 22c-1 (NAV-based pricing), requiring ETF-like exemptions. Issues include 12b-1 fee distribution, liquidity risks (e.g., money market fund price fluctuations), and compliance with fund limits (e.g., 12(d)(1)). Structuring as ETFs or closed-end funds simplifies tokenization. Conditions (e.g., arbitrage mechanisms, gating features) ensure compliance.

Recommendations:

1. Grant exemptive relief from Section 22(d)/22c-1 for tokenized funds with ETF-like arbitrage.
2. Pilot tokenization with closed-end funds to avoid redemption conflicts.
3. Require smart contracts to enforce liquidity fees/gates for money market funds.

Insight: ETF-style relief enables tokenized funds, balancing innovation with 40 Act protections.

Tokenized Stable-Value Securities (for Payments/Settlement)

Question Addressed: How should the SEC approach stable-value tokenized securities for payments? What challenges exist, and should they be treated differently?

Analysis: Tokenized money market funds or bank deposits functioning as stablecoins face friction as securities transactions. Challenges include transaction speed, settlement finality, and off-chain issuer redemption tracking. Treating every transfer as a securities trade is impractical. Exemptions (e.g., no-action relief for low-value, non-investment transfers) and coordination with banking regulators (for tokenized deposits) reduce barriers. Conditions ensure stability and anti-fraud oversight.

Recommendations:

1. Exempt low-value payment transfers from broker-dealer/exchange registration via Section 28/36 authority.
2. Treat stable-value tokens as currency-like for non-investment use, focusing on issuer regulation.
3. Require disclosures on redemption risks and non-FDIC status.

Insight: Flexible treatment fosters payment innovation, prioritizing prudential oversight over trading rules.

Other Laws Posing Challenges to Tokenization

Question Addressed: Do other laws challenge tokenized securities?

Analysis:

- **State Corporate Law**: Some states lack blockchain ledger provisions (unlike Delaware's DGCL §224), risking shareholder recognition.
- **UCC**: Non-uniform Article 12 adoption creates inconsistent token transfer rules.
- **Tax**: Payment use may trigger taxable events, pending IRS de minimis exemptions.
- **AML/Sanctions**: Peer-to-peer transfers require KYC/whitelisting to comply with OFAC/BSA.
- **Blue Sky Laws**: Non-preempted tokens face state registration complexities.
- **40 Act/Advisers Act**: Tokenized pools risk unintended fund/adviser status.

Recommendations:

1. Encourage state adoption of UCC Article 12 and blockchain-friendly corporate laws.
2. Support AML-compliant identity solutions (e.g., whitelisting).
3. Clarify blue sky exemptions for ATS-traded tokens.

Insight: Coordinated regulatory updates mitigate non-SEC barriers, supporting tokenized securities adoption.

Recommendations (Tokenized Securities)

1. Adapt Regulation ATS for peer-to-peer trading and exempt T+0 blockchain settlement from clearing agency rules.
2. Update Rule 17Ad-15 to recognize blockchain ledgers, requiring off-chain backups and on-chain identity guidance.
3. Grant 40 Act relief for tokenized fund trading, piloting with closed-end funds and enforcing liquidity controls.
4. Exempt low-value stable-value token payments from securities trading rules, coordinating with banking regulators.
5. Encourage state law modernization (UCC, corporate) and AML-compliant identity solutions.
6. Clarify custody, SIPC, and FINRA rules for tokenized securities, ensuring tech-neutrality.

Sandbox and International Coordination

Benefits and Focus of a Crypto Sandbox

Question Addressed: Would a sandbox foster tokenization and blockchain innovation? What products/services would firms test, and what barriers hinder progress? Can a sandbox mitigate these?

Analysis: A sandbox provides regulatory relief and SEC engagement, enabling innovation. Firms could test:

- **Decentralized Trading**: DEXs or AMMs for tokenized securities, navigating exchange/ATS rules.
- **Tokenized Offerings**: Micro-IPOs or utility tokens with tailored disclosures.
- **DeFi Integration**: Smart contracts for settlement or stablecoin dividends by traditional firms.
- **Interoperability**: Cross-chain recordkeeping reconciled with legacy systems.
- **Compliance Tech**: On-chain trade reporting to regulators.
- **Products**: 24/7 crypto index fund tokens, programmable bonds, or micro-loan networks.

Barriers:

- **Regulatory**: Uncertainty and high compliance costs deter startups.
- **Technical**: Scalability, interoperability, and security require real-world testing.
- **Operational**: Integrating blockchain with legacy processes lacks standards.

Mitigation: Sandboxes offer no-action relief, phased scaling, and SEC feedback, reducing regulatory fears and enabling technical/operational refinement.

Recommendations:

1. Launch a sandbox for limited-scale testing (e.g., accredited investors, capped investments) with relief from registration/clearing rules.
2. Target DeFi, tokenized offerings, and compliance tech, requiring enhanced disclosures.
3. Facilitate knowledge-sharing among participants to standardize practices (e.g., custody).

Insight: A sandbox accelerates innovation by resolving regulatory and technical hurdles in a controlled environment, informing permanent rules.

Cross-Border Sandbox Collaboration

Question Addressed: Could a cross-border sandbox address multi-jurisdictional challenges? How should the SEC structure it, and do foreign sandboxes provide models?

Analysis: Global crypto projects face fragmented regulations. A cross-border sandbox via the Global Financial Innovation Network (GFIN) enables unified testing across jurisdictions (e.g., U.S., UK, Singapore). Firms benefit from single applications, while regulators share data to align rules. Examples include tokenized bond issuances or cross-border payment tokens. Models like the UK FCA's sandbox (tested custody, STOs) and Singapore MAS's (payment tokens) show success in informing regulations. Structure involves MOUs for data-sharing, aligned timeframes, and joint oversight.

Recommendations:

1. Join GFIN to co-host a "Global Digital Asset Sandbox" with FCA/MAS, testing cross-border payments or STOs.
2. Use MOUs to unify conditions, relief, and reporting across regulators.
3. Evaluate outcomes jointly to harmonize rules, avoiding arbitrage.

Insight: Cross-border sandboxes streamline global innovation, leveraging shared expertise to create consistent, investor-friendly regulations.

Recommendations (Sandbox and International Coordination)

1. Establish a domestic sandbox with no-action relief for DeFi, tokenized offerings, and compliance tech, limited to accredited investors and capped scales.
2. Require sandbox participants to provide enhanced disclosures and share operational data with the SEC.
3. Join GFIN for a cross-border sandbox, testing global products (e.g., tokenized bonds, payment tokens) with FCA/MAS.
4. Use MOUs to align regulatory relief, timelines, and data-sharing across jurisdictions.
5. Leverage UK/Singapore sandbox outcomes to inform U.S. rules, prioritizing investor protection and market integrity.
6. Pilot a blockchain settlement system for broker-dealers, evaluating efficiency and errors to guide Exchange Act updates.

Conclusion

In closing, this comprehensive framework lays the groundwork for a forward-looking, innovation-friendly regime that responsibly integrates crypto assets into our securities laws. By embracing clear classifications, tailored disclosures, calibrated safe harbors, and collaborative sandboxes—both domestic and international—the SEC can reduce uncertainty, foster healthy competition, and drive technological progress, all while upholding its core mandate to protect investors and preserve market integrity. As digital asset markets evolve, continued dialogue with industry participants, aligned global standards, and adaptive rule-making will ensure that U.S. policy remains both rigorous and resilient in the face of tomorrow's challenges.