

May 12, 2025

Commissioner Hester M. Peirce
Chair, SEC Crypto Task Force
U.S. Securities and Exchange Commission
100 F Street, N.E.
Washington, DC 20549-0213

Re: Responses to the SEC Crypto Task Force's Questions

Dear Commissioner Peirce:

Thank you for the opportunity to respond to the request for information that the Securities and Exchange Commission's Crypto Task Force (the "Crypto Task Force") provided to the public on February 21, 2025 (the "Statement").¹ This letter is written on behalf of Interop Labs, the initial developer of the Axelar Network, a decentralized blockchain interoperability protocol (see Appendix for additional background). Specifically, we submit this comment letter to highlight observations related to blockchain interoperability and its significance as infrastructure for tokenized assets and tokenized capital markets. We believe that blockchain interoperability must be addressed with nuanced, functionally informed regulation. Interoperability enables assets and information to move across distinct blockchain ecosystems, unlocking liquidity, access, and innovation. However, not all interoperability networks are created equal. Some are custodial, centralized, and pose intermediary risk; while others are decentralized, non-custodial, and designed to eliminate single points of failure. We therefore urge the Commission to distinguish clearly between centralized and decentralized interoperability, and to issue guidance or a safe harbor exempting decentralized, non-custodial systems from intermediary registration requirements.

This comment letter outlines blockchain interoperability within the broader evolution of tokenized asset markets and explains why decentralized, non-custodial infrastructure warrants distinct regulatory consideration. We then examine the key differences between centralized and decentralized interoperability models and propose principles that the Commission can use to evaluate decentralization in this context. The comment letter concludes with specific responses to select questions from the Statement, with a particular focus on how decentralized interoperability informs issues such as technology neutrality, recordkeeping, and the role of intermediaries. Throughout, our aim is to support a regulatory approach that both protects investors and enables innovation in tokenized assets.

1. Blockchain Interoperability for Tokenized Assets

Tokenized assets—digital representations of real-world assets (RWAs) such as stablecoins, bonds, and equities—are increasingly being issued on a range of blockchains. These blockchains differ in consensus models, programming languages, and governance mechanisms, resulting in

¹ *There Must Be Some Way Out of Here* (2025) Hester M. Peirce, Securities and Exchange Commission (<https://www.sec.gov/newsroom/speeches-statements/peirce-statement-rfi-022125>)

fragmented ecosystems that do not communicate natively with one another. As adoption of tokenized assets grows, investors, issuers, and regulators will require seamless blockchain interoperability to ensure efficient capital flows and transparent market behavior. Blockchain interoperability is the technological foundation that enables these systems to communicate, execute trades, and enforce compliance across chains. Blockchains are built with various programming languages and consensus mechanisms, designed to verify messages and state changes within a discrete network. By themselves, they are silos, incapable of verifying a state change or message from any external network or information source. Blockchain interoperability handles this inter-blockchain verification, enabling the secure transfer of data and value across multiple, discrete blockchain environments.

2. Decentralization and Interoperability

a. *The Decentralization Spectrum in Context*

Decentralization in blockchain platforms exists on a spectrum, with different protocols exhibiting varying degrees of control, openness, and governance dispersion. Historically, the regulatory debate has focused on whether and how to define decentralization for purposes such as securities classification and compliance obligations. Today, institutional market participants are preparing asset tokenization approaches that fully embrace existing compliance obligations, by opting to build on highly centralized, privately controlled blockchains. These environments offer predictable governance and regulatory interfaces. Initiatives like the Monetary Authority of Singapore's Project Guardian exemplify how both public and private blockchains can be linked securely via interoperability protocols, in order to deliver benefits of greater access and improved liquidity that public blockchains provide.²

Connecting private blockchains in this way enables tokenized asset issuers to achieve the best of both worlds: ensuring regulatory compliance that safeguards investors, while tapping into the innovation and advantages of decentralized public blockchains. In order to preserve that combination of protection and access, interoperability protocols that facilitate this integration between private and public blockchains must be decentralized, themselves. Otherwise, they introduce a component of custodial risk that extends globally, touching all connected systems and requiring oversight that would vitiate the benefits of public blockchains. Global commerce itself is a useful analogy: the economies it links enact varying degrees of control and centralization, but international waters and airspace remain neutral to such policies.

Firms such as Deutsche Bank,³ Apollo Global Management, and Kinexys by J.P. Morgan⁴ have proposed issuance models situated at the more centralized end of the spectrum, connected to

² *Interlinking Networks Technical Whitepaper* (2023) Monetary Authority of Singapore (<https://www.mas.gov.sg/publications/monographs-or-information-paper/2023/interlinking-networks>); *Project DAMA 2 Unveiled in MAS' Project Guardian* (2024) Interop Labs (<https://www.axelar.network/blog/deutsche-bank-dama-2-announcement>)

³ *Project DAMA 2 Unveiled in MAS' Project Guardian* (2024) Interop Labs (<https://www.axelar.network/blog/deutsche-bank-dama-2-announcement>)

⁴ *Revolutionizing Asset & Wealth Management* (2023) Tyrone Lobban, Christine Moy, et al. (<https://www.jpmorgan.com/kinexys/content-hub/project-guardian>)

decentralized networks via interoperability protocols. In light of this trend, we believe it is essential that any framework or guidance developed by the Commission to evaluate decentralization be context-sensitive. Nowhere is that more important than in the interoperability layer, where the difference between centralized and decentralized approaches can have global effects, shaping the entire, emerging category of tokenized assets.

b. Centralized v. Decentralized Blockchain Networks

While we do not propose a definitive test for decentralization, we submit that certain foundational principles can serve as baseline criteria for evaluating whether a protocol operates in a decentralized manner.

- First, the protocol should be open source, with all core software components publicly accessible and auditable by any interested party.
- Second, the system should be public, meaning that any user, regardless of geographic location or affiliation, is able to access the ledger and observe transaction data in real time.
- Third, the network should be permissionless in its operation—allowing any individual or entity to participate in core functions, subject to transparent rules encoded in the protocol itself.
- Fourth, the ledger should be immutable, ensuring that all transactions are permanently recorded on an append-only blockchain and cannot be retroactively altered or deleted.
- Fifth, the protocol should be operated by a distributed set of economically incentivized participants, with a well-defined incentive structure that aligns the behavior of transaction validators and other operators with the integrity and security of the network.

These criteria are not exhaustive, but together they offer a practical foundation for assessing decentralization in the context of blockchain-based infrastructure, including interoperability networks.

c. Centralized v. Decentralized Interoperability Networks

Centralized interoperability models rely on a limited number of operators or administrators to validate and process transactions sent across discrete blockchains, also known as cross-chain transactions. These centralized models often operate through a custodial mechanism. This structure introduces material risks associated with operational failure, mismanagement, or malicious activity, as seen in the Ronin⁵ bridge and Bybit⁶ exchange hacks—both instances of centralized

⁵ *Axie Infinity's Ronin Network Suffers \$625M Exploit* (2022) Andrew Thurman, CoinDesk (<https://www.coindesk.com/tech/2022/03/29/axie-infinitys-ronin-network-suffers-625m-exploit>)

⁶ *Bybit Hacked For More Than \$1.4 Billion in Biggest Crypto Heist of All Time* (2025) Vicky Ge Huang, The Wall Street Journal (<https://www.wsj.com/livecoverage/stock-market-today-dow-sp500-nasdaq-earnings-02-21-2025/card/bybit-hacked-for-more-than-1-4-billion-in-biggest-crypto-heist-of-all-time-Od7IyKoVGsZyIfVANYbz>)

operators moving funds between blockchains, which rank among the largest known cybertheft incidents in any industry. In contrast, decentralized interoperability networks employ distributed validator sets, open-source codebases, and permissionless participation to ensure integrity without requiring custody or administrative discretion. These decentralized networks operate as public goods, eliminating intermediaries while maintaining transparency. They reduce systemic vulnerabilities and uphold investor protections through protocol-level safeguards.

Accordingly, decentralized interoperability warrants a different regulatory approach to the extent that it intersects with activity that would be regulated by federal securities laws. For example, decentralized protocols are designed to minimize or eliminate such assumptions through permissionless participation, cryptographic guarantees, and distributed control. Traditional regulatory obligations such as broker-dealer registration or transfer agent oversight are designed to constrain the behavior of intermediaries. When applied to decentralized, non-custodial infrastructure, these rules can be counterproductive by imposing burdens on systems that, by design, do not perform intermediary functions. Instead of imposing a one-size-fits-all model, the Commission should consider guidance that reflects how such systems function and the specific risks they do or do not pose. Regulatory clarity that exempts decentralized interoperability protocols from intermediary-based rules will support both innovation and investor protection.

d. Proposed Principles for Decentralization Interoperability Networks

To aid in regulatory analysis, we also propose a set of principles that define the contours of decentralized interoperability.

- First, such networks must be *non-custodial*, meaning control of software components that hold user assets must reside with diverse operator nodes, within the network.
- Second, participation in network operation—such as message transfer or governance—must be permissionless, i.e., *open to the public under transparent and objective criteria*.
- Third, the *codebase must be open source*, allowing any party to inspect, replicate, or improve the underlying software.
- Fourth, the network should *record all relevant transaction data immutably on a blockchain*, ensuring auditability and accountability.
- Fifth, network *governance processes must be distributed and transparent*, with clear mechanisms for community or tokenholder participation in decision-making.

A protocol that meets these principles should be viewed as decentralized and subject to a distinct regulatory path.

e. Regulatory Benefits of Decentralized Interoperability

Decentralized interoperability networks offer regulators unique benefits that support the Commission's core mandate to protect investors. By removing discretionary control over asset

flows, these protocols significantly reduce the risks of fraud, loss, and manipulation. All cross-chain transactions are publicly recorded, making forensic analysis and oversight more efficient and less reliant on voluntary disclosures by intermediaries. Because there is no central party with unilateral control over funds, users retain direct custody of their assets during and after a transaction. This property removes the need for certain protections that arise in custodial environments. In addition, decentralized systems that are themselves programmable—capable of running computer logic—can implement encoded rules, such as geographic restrictions or identity attestation. This capacity for programmability can make it possible to enforce regulatory requirements without compromising security or decentralization.⁷ For example, such requirements could be used by connected systems to enforce anti-money laundering (AML) measures, among other requirements, ensuring that sanctioned or criminal entities are excluded from the service in question.⁸ These tools allow for cooperation between protocol developers and regulators while preserving the core advantages of blockchain technology. As such, decentralized and programmable interoperability can both complement and advance regulatory goals.

3. Responses to Specific Crypto Task Force Questions

The following responses address specific questions raised in the Statement, with a particular emphasis on how decentralized interoperability networks should be considered within each regulatory topic. While many of the issues raised—such as decentralization, recordkeeping, and the role of intermediaries—are broad in scope, their application to the interoperability layer is both urgent and distinct. Interoperability is not merely a necessary feature for blockchain systems; it is the connective infrastructure that enables compliant tokenized markets to function across fragmented networks. Within this context, the differences between centralized and decentralized approaches have significant implications for investor protection, market integrity, and systemic risk. The responses below aim to highlight how decentralized interoperability can enhance regulatory objectives, often without requiring the same oversight or registration obligations as traditional financial intermediaries. By framing these issues through the lens of decentralized infrastructure, we hope to assist the Commission in developing policy approaches that are appropriately tailored to technical function and actual risk. Each response is designed to support principles-based guidance that preserves flexibility while reinforcing the Commission’s investor protection mission.

Question 6: How can the Commission establish a workable taxonomy while remaining merit- and technology-neutral?

Maintaining technology neutrality is a vital regulatory principle, particularly in an environment as dynamic and rapidly evolving as ours. The Commission can preserve neutrality

⁷ For a broader discussion on ways for regulators to work with interoperability layer, see *Programmable Interoperability: The Key to Standardization in Regulating Tokenized Assets* (2024) Jason Rozovsky (https://www.elevandi.io/hubfs/Programmable%20Interoperability%20-%20The%20Key%20to%20Standardisation%20in%20Regulating%20Tokenized%20Assets%20-%20July%202024_Final.pdf)

⁸ For a broader discussion on the benefits of decentralized blockchain networks to regulators, see *The New Regulatory Paradigm: How Decentralized Systems Will Improve Financial Oversight* (2024) Jason Rozovsky, Lewis Cohen (<https://www.axelar.network/new-regulatory-paradigm>)

not by treating all systems identically, but by establishing principles-based criteria that focus on outcomes—such as investor protection, transparency, and risk mitigation—rather than on technical implementation. In the context of interoperability, known parameters for assessing decentralization can serve this purpose. A clear set of attributes, such as non-custodial design, permissionless participation, and distributed governance, allows regulators to assess protocols on their merits without favoring one technology stack over another. These parameters would also help differentiate between high-risk custodial bridges and resilient, decentralized protocols. Where risks are materially different, regulatory burdens should be commensurate. Adopting a principles-based framework would empower market participants to make informed decisions and allow innovative technologies to flourish without compromising regulatory goals. Importantly, neutrality in regulation does not mean passivity—it requires proactive efforts to ensure that rules are flexible enough to accommodate multiple approaches to achieving public policy's intended outcomes. In this way, technology neutrality can coexist with strong investor protections and market integrity.

Question 14: How should the decentralization of a deployed protocol best be evaluated? How should permissioned aspects of crypto-adjacent software or participant roles, such as validators, relayers, and sequencers, be considered? Are there tech-neutral thresholds that can be agreed upon for determining thresholds for decentralization?

The decentralization of a deployed protocol should be evaluated holistically, encompassing its technical architecture, operational control, and governance model. A protocol that relies on a single entity or a tightly coordinated group for decision-making, including around maintenance and updates, should not be considered decentralized, even if it claims to be open source or non-custodial. Conversely, a protocol governed by a diverse, economically incentivized set of validators—with transparent, community-driven update mechanisms—should be presumed to meet a higher threshold of decentralization.

As noted above, decentralization is best understood as a spectrum rather than a binary state. This is especially important in tokenized asset environments, where component systems—issuance platforms, trading venues, and settlement layers—may exhibit differing levels of decentralization. Financial institutions may choose to operate on more centralized platforms for operational or compliance reasons, but they should still be able to interact with decentralized protocols that offer strong security and transparency guarantees. Establishing a principled framework will help regulators apply consistent standards across use cases, while allowing innovation to develop in both public and permissioned settings. By clearly articulating what constitutes decentralization, the Commission can both safeguard market participants and encourage responsible technological experimentation.

Question 22: Public, permissionless blockchains are being used to tokenize permissioned assets. To the extent the custody rules for broker-dealers, investment advisers, and investment companies are implicated, how should the Commission differentiate between native crypto assets of permissionless blockchains and tokenized permissioned assets? Does either type of crypto asset present greater risks of theft or loss?

Permissionless design is a cornerstone of decentralized systems and should be a key element in any regulatory framework assessing decentralization. In the context of tokenized assets,

many layers—such as the assets themselves—may require permissions or compliance-related controls due to legal or jurisdictional requirements. However, at the infrastructure level, especially for interoperability protocols, permissionlessness offers substantial benefits. A system operated by a dynamic and permissionless validator set is inherently more resistant to manipulation and failure than one controlled by a limited, fixed set of actors. Permissionless networks reduce the attack surface, eliminate gatekeepers, and return control to the users of the system. In these networks, responsibility for asset management resides with the user, not a central intermediary. This significantly reduces the potential for censorship, misappropriation, or unauthorized seizure of assets. As such, permissionless interoperability protocols offer greater alignment with the original values of blockchain—security, transparency, and neutrality—and pose fewer systemic risks. They should be viewed as more decentralized, and therefore less in need of traditional regulatory oversight applicable to custodial intermediaries.

Question 26: The recordkeeping rules for broker-dealers (17 CFR 240.17a-3 and 17 CFR 240.17a-4) require the creation and maintenance of accounting and operational records designed to assist a firm in tracking and understanding its assets, liabilities, positions, and obligations to customers (e.g., cash owed to customers and securities held for customers).

- a. What challenges, if any, do the requirements of these recordkeeping rules present with respect to crypto assets that are not an issue for traditional securities? What modifications to the rules could address these challenges?**
- b. Should crypto assets generally be treated as if they are traditional securities for purposes of these recordkeeping rules?**

Decentralized interoperability protocols inherently enhance compliance with recordkeeping requirements by publishing all relevant transaction data on a publicly verifiable blockchain. Unlike traditional intermediaries, which may rely on off-chain databases subject to tampering or human error, decentralized systems can immutably record transaction metadata—including source and destination addresses, asset types, amounts, timestamps, and fees. This comprehensive audit trail allows for continuous, automated compliance verification and reduces the burden on both regulated entities and enforcement bodies. Crucially, because the data is decentralized and append-only, no single party can alter, delete, or obscure the historical record.

Regulators and third parties can independently verify transactions without relying on intermediaries to produce reports or maintain ledgers. This architecture aligns closely with the goals of accurate, transparent recordkeeping in securities markets. Moreover, programmable compliance tools can be layered onto such protocols to further streamline data tagging and reporting. As the tokenization of assets continues to expand, the use of decentralized recordkeeping infrastructure can serve as a regulatory enabler, not a barrier. It allows regulators to shift from reactive enforcement to proactive monitoring in real-time.

Broker-dealers have historically played a central role in financial markets, acting as intermediaries that match buyers and sellers, take custody of client assets, and execute trades. However, decentralized interoperability networks alter this dynamic in fundamental ways. These protocols enable users to transact directly across blockchain ecosystems without the need for a central matchmaker or custodian. The routing, validation, and execution of cross-chain messages occur through public infrastructure, governed by transparent rules and operated by a distributed

set of validators. In this model, the traditional role of the broker-dealer—holding funds, managing counterparty risk, and facilitating settlement—is rendered obsolete. Users maintain custody of their assets throughout the process, and protocol rules ensure settlement finality without relying on discretionary judgment. While some platforms or asset types may still require regulated intermediaries for compliance or liquidity purposes, the core infrastructure no longer depends on such roles. Applying broker-dealer regulation to non-custodial, protocol-based systems would therefore be inappropriate and likely counterproductive. A better approach is to recognize the functional distinctions and tailor regulatory obligations accordingly, focusing on systems that truly intermediate transactions and present the attendant risks.

Question 41: How do the programmability and composability properties of blockchain technology and blockchain-based technologies, such as smart contracts, affect the role of a transfer agent? Are there provisions in the transfer agent rules that prevent transfer agents from using blockchain technology for this purpose to the fullest extent possible? Is an offchain record still needed as an official or a complementary record in a tokenization arrangement? Are there any legal or regulatory impediments to using onchain identity solutions?

Decentralized interoperability protocols introduce a paradigm shift in how transfer agent functions are performed. In traditional markets, transfer agents maintain centralized records of asset ownership and are trusted to ensure settlement and transfer. In a decentralized environment, these functions are embedded in the protocol itself. Cross-chain transfers are settled on a public ledger, providing a continuous and immutable chain of custody for assets across different blockchains. This transparency allows any observer, including a regulated transfer agent, to determine the ownership of a given token at any point in time. Moreover, the user retains control of their assets throughout the process, eliminating the need for custodial intervention. Should a transfer agent need to track ownership for regulatory or operational reasons, it can do so by integrating with each chain involved and using on-chain data as the definitive record. In this way, decentralized interoperability not only complements but enhances the objectives of traditional transfer agents by offering greater accuracy, resilience, and transparency.

4. Conclusion

Blockchain interoperability is essential to the success of tokenized markets and digital asset ecosystems. However, the Commission should distinguish between centralized systems that introduce intermediary risk and decentralized systems that eliminate it. We respectfully urge the Commission to issue guidance or a safe harbor clarifying that decentralized, non-custodial interoperability protocols do not require registration under intermediary regimes. We further recommend that the Commission consider convening a public roundtable or technical workshop to explore these issues with industry and academic experts. A regulatory framework that reflects technical and operational distinctions will best serve the goals of innovation, transparency, and investor protection. We remain available to provide further information or participate in future Commission discussions on this topic.

*

*

*

Thank you for your attention to this matter. We are prepared to discuss these recommendations further and provide any additional information the Commission may need.

Sincerely,

A handwritten signature in black ink that reads "Jason Rozovsky". The signature is written in a cursive style with a large initial 'J'.

Jason Rozovsky
Head of Legal and Policy
Interop Labs Inc.

cc: Sergey Gorbunov
CEO
Interop Labs Inc.

Appendix

Axelar Network Background

The Axelar protocol was founded by Sergey Gorbunov and Georgios Vlachos in 2020⁹ and launched in 2022.¹⁰ The primary objective of the Axelar Network is to use the Axelar protocol to enable decentralized interoperability among blockchain systems. Just as institutions and enterprises have historically encountered vendor lock-in with legacy IT systems, they aim to avoid replicating such limitations in modern blockchain environments. Interoperability ensures that there is no necessity to select a single blockchain, thereby preventing constraints on accessing other ecosystems.

The Axelar Network has several key architectural features.

First, it incorporates decentralized protocol characteristics similar to bitcoin. It is:

1. Open source.
2. Public.
3. Permissionless.
4. Immutable.
5. Operated by economically incentivized validators.

Second, Axelar is designed to support cross-chain message transfers, referred to as general message passing (GMP). These messages can encompass a wide array of functions, including contract calls and arbitrary data payloads such as token transfers (both "lock and mint" and "burn and mint"), governance votes, oracle updates, or application-specific instructions between blockchains.

Third, the Axelar Network records and publishes all cross-chain message transfers on an immutable blockchain, making all transfer information publicly accessible and visible. This includes information pertaining to the type of message, originating address, destination address, time of transfer, amount of transfer, and all associated fees (e.g., gas fees).

Fourth, the Axelar Network consists of a blockchain and is operated by a dynamic set of 75 validators. All cross-chain transactions are published by this set, and all cross-chain information is publicly accessible, with the blockchain recording each transaction's relevant information. Ownership of all gateways and contracts on the network is sharded (i.e., divided), distributed among and controlled by the 75 validators. Validators are incentivized to follow protocol rules through both token rewards received from the protocol and slashing penalties in the event of misconduct.

⁹ Sergey earned his B.Sc. and M.Sc. in computer science from the University of Toronto, and his Ph.D. in cryptography from the Massachusetts Institute of Technology. He was a professor of cryptography at the University of Waterloo and a member of the founding team at Algorand. Georgios earned his B.Sc. and M.Sc. in computer science from the Massachusetts Institute of Technology and was also a member of the founding team at Algorand.

¹⁰ *Axelar: Connecting Applications with Blockchain Ecosystems* (2021) (<https://www.axelar.network/whitepaper>).

Fifth, governance decisions for the Axelar Network are made by all tokenholders. This includes all modifications to the Axelar protocol, and governance over both validators of Axelar Network's core protocol and "Verifiers" for Interchain Amplifier connected networks. Tokenholders vote on changes to the Axelar Network through transparent, on-chain voting. Importantly, all actions in connection with transaction validation are subject to *quadratic voting* to ensure equitable control distribution. Specifically, voting power is tied to the square root of the total stake delegated to a validator. This mechanism significantly reduces the likelihood of any single entity or colluding entities accumulating sufficient stake to gain control over the network.¹¹

Sixth, Axelar Network provides for a programmatic layer to sit atop the protocol. This allows for complex smart contracts to execute based on information received from multiple blockchain networks.

Seventh, the Axelar Network uses a *hub-and-spoke* structure. Instead of connecting blockchains bilaterally (each chain to every other chain individually), a blockchain only needs to connect to the Axelar Network, gaining access to all other connected blockchain networks.

¹¹ Axelar Network operates a delegated proof of stake blockchain, which allows tokenholders to delegate their stake to validators without relinquishing ownership.