

CLARITY: Integrating the Security and Commodity Frameworks

How a lifecycle model can align U.S. securities and commodities law with onchain

TL;DR:

- Digital assets evolve over time, often starting with securities-like capital raising and maturing into decentralized, commodity-like networks, which today do not fit cleanly in either the securities or commodities regime.
- The CLARITY Act creates a single, lifecycle-based framework that defines digital assets at each stage and brings issuers and intermediaries under harmonized SEC–CFTC oversight.
- The bill's six core outcomes—lifecycle jurisdiction, a harmonized intermediary perimeter, stronger market integrity and illicit finance rules, developer safe harbors, and sustainable agency funding—are designed to deliver regulatory clarity, investor protection, and durable innovation in U.S. digital asset markets.

Digital assets and the need for a lifecycle regime

Digital assets do not fit neatly into the regulatory frameworks Congress originally designed for securities and commodities. Many begin life with securities-like characteristics: they are sold by a centralized team to raise capital and build a network. Over time, if that network decentralizes and the asset's primary function shifts to facilitating transactions or access on an open protocol, the asset can come to resemble a digital commodity.

Other assets, such as Bitcoin, may be created and traded from inception with no securities-like features at all. The current regime was not built for that range of lifecycle paths. It lacks the flexibility to put appropriate guardrails around issuers and around intermediaries—exchanges, brokers, dealers, custodians—that handle these assets once they are widely traded.

The CLARITY Act addresses this mismatch by creating a comprehensive federal framework tailored to digital assets. It defines assets at each stage of their lifecycle and incorporates issuers and intermediaries into a unified U.S. regulatory perimeter. In doing so, it delivers six major outcomes that together form a cohesive market structure for onchain finance.

Jurisdictional lifecycle: defining the SEC–CFTC boundary

The first outcome is a clear, lifecycle-based answer to the “security vs. commodity” question. Instead of forcing a permanent label at launch, the framework ties jurisdiction to how the asset operates.

- SEC phase. The Securities and Exchange Commission retains jurisdiction in the initial, centralized capital-raising phase. During this period, the asset is treated as a security and subject to securities-law protections. Metrics such as network decentralization and common-control thresholds determine when the asset no longer functions as a security.
- CFTC phase. Once an asset meets those decentralization thresholds, jurisdiction transitions to the Commodity Futures Trading Commission. The asset becomes a “digital commodity,” and the CFTC assumes exclusive spot-market authority.

A harmonized intermediary perimeter

This dynamic hand-off is designed to ensure that an asset is regulated as a security when it behaves like one, and as a commodity when it operates as a decentralized, tradable network token.

The second outcome is a harmonized perimeter for platforms and intermediaries, intended to close gaps and avoid regulatory arbitrage.

- Securities platforms. For assets under SEC jurisdiction, the framework modernizes broker-dealer and disclosure rules for digital assets. It strictly applies insider trading laws and primary-offering transparency to token markets, updating securities norms for onchain contexts.
- Commodity platforms. For assets under CFTC jurisdiction, the bill establishes a new federal registration regime for digital commodity exchanges, brokers, and dealers. This brings centralized spot crypto exchanges into a federal perimeter for the first time, with obligations for market surveillance and system safeguards.

By setting parallel, matching standards, the framework seeks to ensure that similar risks are treated similarly, whether the platform lists securities-phase assets or digital commodities.

Initial Phase	Intermediate Phase	Mature Phase
Capital-raising, centralized control (SEC)	Decentralizing Network (transition zone)	Decentralized digital Commodity (CFTC)

Market integrity and investor safeguards

The third outcome is a set of ecosystem-wide guardrails aimed at preventing mismanagement and systemic failures.

- Asset segregation. All registered digital asset intermediaries must segregate customer funds from corporate accounts and use qualified custodians. This is meant to prevent commingling and protect customer assets in stress scenarios.
- Conflict prohibitions. Digital commodity exchanges are barred from trading against their customers or running proprietary market-making on their own venues, reducing conflicts that can undermine fair markets.
- Retail advocacy. A Digital Commodity Retail Advocate provides a permanent institutional voice for everyday users and helps identify and address predatory practices.

These protections are designed to give digital asset users baseline expectations comparable to those in traditional financial markets.

A fortified illicit finance perimeter

The fourth outcome focuses on national security and illicit finance. The framework modernizes anti-money laundering guardrails by making all digital asset service providers—whether overseen by the SEC or CFTC—fully subject to the Bank Secrecy Act.

That includes robust Customer Identification Programs and suspicious-

activity reporting. The bill also grants law enforcement targeted authority to request temporary transaction pauses where there is evidence of illicit activity or compromised protocols. The goal is a consistent defensive perimeter around digital asset intermediation, without fragmenting rules along agency lines.

Shielding the technological layer

The fifth outcome is explicit protection for the open-source foundation of the digital economy. The framework recognizes that writing and publishing code are distinct from providing regulated financial services.

It creates a clear safe harbor for: (i) software developers and core protocol contributors, (ii) node validators who secure decentralized networks, and (iii) designers of non-custodial wallets and related tools.

Under the harmonized SEC–CFTC framework, these actors cannot be treated as financial intermediaries or forced to register as brokers solely because they publish software or maintain decentralized infrastructure. This aims to preserve the open, permissionless innovation that underpins onchain finance, while focusing regulatory obligations on custodial and transactional service providers.

Protecting builders, targeting intermediaries:

Developers, validators, and non-custodial wallet designers benefit from a statutory safe harbor. Regulatory obligations are concentrated where custom-er funds and transactions are handled.

Sustainable funding and agency harmonization

The sixth outcome is institutional: ensuring that the CFTC and SEC can sustain their expanded roles and stay aligned over time.

Self-sustaining CFTC funding. The bill establishes a dedicated funding stream through initial and annual fees on registered digital commodity entities, designed to expand CFTC capacity without new burdens on taxpayers.

Permanent joint advisory committee. A standing SEC–CFTC Advisory Committee is tasked with coordinating requirements and updating the regime as technology and markets evolve.

These measures aim to make the unified framework durable—supported by adequate resources and formal coordination, rather than one-off rulemakings or ad hoc guidance.

Toward a cohesive, future-proof market structure

By integrating the securities and commodities frameworks into a single, lifecycle-based regime, the CLARITY Act turns a set of disparate digital asset issues into a cohesive market structure. It gives institutional investors the structural certainty they need to engage responsibly in U.S. onchain markets, while providing retail users with uniform federal safeguards.

At the same time, the framework strengthens anti–money laundering defenses and national security tools, and protects the open-source technology layer that enables onchain innovation. If implemented as designed, it would help ensure that the infrastructure of digital finance can grow within a clear, durable U.S. regulatory perimeter, rather than migrating to jurisdictions with looser standards or greater ambiguity.