

CLARITY: Protecting Consumers and Investors

How CLARITY hardwires baseline safeguards for U.S. crypto users.

TL;DR:

- Jurisdictional clarity is a means to an end: consumer protection. Tens of millions of Americans already use digital asset platforms, but today face a patchwork of state rules and after-the-fact federal enforcement.
- The CLARITY Act replaces “regulation by enforcement” with consumer protection by default, establishing five baseline protections for every federally regulated digital asset platform.
- These protections require asset segregation, conflict-of-interest bans, mandatory public disclosures, a dedicated retail advocate, and strong identity and anti-money laundering controls to address cyber-theft and scams.

From patchwork oversight to consumer protection by default

Jurisdictional clarity is the foundation of CLARITY, but it’s also a means to an end—the end is consumer protection. Tens of millions of Americans already participate in digital asset markets. Until now, many have done so under a patchwork of state regimes and ad hoc federal enforcement actions that leave systemic gaps. When no one is clearly responsible for oversight, no one is clearly accountable.

The CLARITY Act shifts the regulatory focus from “regulation by enforcement” after problems emerge to consumer protection by default. It defines five baseline protections, applied uniformly across every federally regulated digital asset platform, to give American consumers a level of safeguard comparable to what they expect in traditional financial markets.

Five baseline protections for digital asset users

Requiring asset segregation

Crypto platforms would be legally required to keep customer funds completely separate from corporate operational accounts. Customer deposits could not be used to pay corporate debts or leveraged for platform profits.

By mandating strict qualified custody and segregation rules, CLARITY is designed to ensure that even if an exchange goes bankrupt, customer assets are legally protected and fully retrievable—whether the custodian is an affiliate or an external entity.

Preventing conflicts of interest

The framework bans exchanges from trading against their own users or manipulating prices for platform benefit. It also applies strict insider-trading laws to digital asset markets. Executives and developers face severe penalties if they use non-public technical or operational data to enrich themselves at the expense of regular buyers.

These measures aim to align incentives between platforms and users, reducing opportunities for self-dealing and restoring trust in market integrity.

Mandating public disclosures

To reduce information asymmetries, platforms are prohibited from listing a token unless the project provides continuous, audited updates. This disclosure regime is uniquely tailored to the risk factors of digital assets, rather than to corporate financials. Disclosures must clearly describe the underlying source code, who controls the token supply, and the asset's transaction history, so that buyers have a transparent view of what they are purchasing.

The goal is to prevent situations where insiders hype an asset while masking technical, governance, or concentration risks that could materially affect its value.

Creating a dedicated government watchdog

The legislation establishes an Office of the Digital Commodity Retail Advocate—a permanent retail-focused watchdog inside the regulatory system, as neither the CFTC's nor the SEC's parent regime has an equivalent: The CFTC handles retail concerns through general enforcement and the Office of Customer Education, while the SEC diffuses investor protection across its broader mandate. This office would track predatory market patterns, analyze emerging consumer risks, and provide a direct portal for the public to report corporate abuse or fraud.

By institutionalizing a dedicated advocate, CLARITY ensures that individual investors have a sustained voice in how digital asset markets are supervised.

Freezing cyber-theft and scams

Finally, the framework requires platforms to enforce strict identity-verification and anti-money laundering controls to keep criminal actors out of the financial system. Where a network suffers a cyber-breach or exploit, the bill provides targeted authority for regulators and law enforcement to request temporary pauses in transactions. Securities laws don't contain crypto-specific tools of this kind, instead addressing misconduct post hoc through enforcement and clawbacks.

This pause power is intended to give authorities a narrow window to trace and freeze stolen capital before it can be moved out of reach, complementing onchain transparency with traditional investigative tools.

Together, these five protections turn digital asset oversight from reactive enforcement into a proactive, rules-based regime. They standardize expectations for basic safeguards across platforms, address the most visible drivers of consumer harm—commingling, conflicts, opacity, and scams—and do so without shutting down onchain innovation.

For U.S. policymakers, the choice is not between crypto and consumer protection. The CLARITY framework shows how a unified federal regime can deliver both: preserving the benefits of digital asset markets while giving Americans the baseline protections they already associate with regulated finance.

From patchwork rules to default safeguards

Today: uneven state regimes and ad hoc enforcement.

Under CLARITY: uniform federal baseline protections across all registered platforms.

Why this matters for policymakers