CLARITY: Modernizing Tools for Law Enforcement

How CLARITY strengthens U.S. national security and financial integrity in digital asset markets.

TL;DR:

- Regulatory gaps have hindered law enforcement in digital asset markets, pushing responsible firms offshore while bad actors exploit inconsistent rules.
- The CLARITY Act brings digital asset intermediaries and semi-decentralized protocols firmly into the Bank Secrecy Act and sanctions perimeter, aligning them with traditional financial institutions.
- It updates seizure and forfeiture rules for fast-moving digital assets, extends powerful sanctions tools to onchain activity, and clarifies when private platforms can pause suspicious transactions.
- New structures for information sharing, interagency coordination, kiosk oversight, and decentralized cybersecurity standards aim to make enforcement more timely, targeted, and effective.

From regulatory gaps to a modern perimeter

For years, one of the biggest challenges facing law enforcement in the digital asset space has been the absence of a comprehensive federal framework. Legitimate companies struggled to determine which rules applied to them, while bad actors exploited gaps and inconsistencies. That dynamic pushed responsible activity offshore and left U.S. agencies without the modern tools needed to police a rapidly evolving market.

The CLARITY Act addresses that problem directly. It brings more actors into the regulatory perimeter, increases transparency, strengthens anti–money laundering (AML) obligations, and improves coordination between government and the private sector. The aim is materially stronger enforcement, focused on the actual locus of risk rather than on technology itself.

Bringing digital asset markets into the regulatory perimeter

CLARITY formally applies the Bank Secrecy Act and U.S. sanctions obligations to digital commodity brokers, dealers, and exchanges. Treating these intermediaries like traditional financial institutions means (i) robust AML programs, (ii) suspicious-activity reporting, and (iii) enhanced customer due diligence.

These are the same core structures law enforcement has long relied on to disrupt terrorist financing, drug trafficking, fraud, and organized crime.

The Act also closes a gap involving trading protocols that are not fully decentralized, creating a workable legal definition that subjects them to compliance monitoring and testing. And it directs Treasury to clarify sanctions obligations for consumer-facing application layers—user interfaces and front-end apps—so bad actors cannot hide behind technical ambiguities to evade accountability.

Modernizing asset seizure and forfeiture

CLARITY's law enforcement toolkit

BSA and sanctions obligations for digital commodity intermediaries and key protocols.
Modernized seizure and tracing rules for fungible onchain assets.
Section 311 authority and front-end sanctions clarity for digital assets.
National rules for kiosks and a NIST-led cybersecurity program for DeFi.

Many existing forfeiture statutes predate digital assets, forcing investigators to retrofit outdated tools. CLARITY updates these laws in two key ways:

- Treating digital assets as monetary instruments. This enables swift administrative, non-judicial seizures over certain financial thresholds, the same authority prosecutors have long had over cash.
- Updating tracing rules for fungible, fast-moving assets. Traditional law often required tracing specific dollars derived from a crime all the way to the account being seized. In digital asset markets—where funds are swapped, mixed, or bridged within minutes—that dollar-for-dollar tracing can be technically impossible even when the illicit origin of an account is clear from onchain analysis.

Under CLARITY, prosecutors can target the current balance in an illicitly funded account, so cases are not abandoned simply because individual dollars can no longer be linked one-to-one. In ransomware, fraud, and narcotics investigations, where speed determines whether stolen capital is recovered or lost, these updates are essential.

Strengthening sanctions and cross-border enforcement

CLARITY extends Treasury's Section 311 "special measures" authority to digital asset activity. Historically, Section 311 has been one of the federal government's most potent national security tools, allowing Treasury to designate foreign jurisdictions, institutions, or transaction types as primary money laundering concerns. Applying it to digital assets helps ensure that state-sponsored actors and international criminal syndicates cannot rely on lightly regulated offshore venues to bypass the American financial perimeter.

Complementing that authority, the bill empowers stablecoin issuers and digital asset service providers to place temporary holds on transactions when there is a reasonable, identifiable belief of unlawful activity. This defensive capability mirrors the fraud-stopping powers traditional banks have used for decades. With clear legal authority and liability protection, private platforms can act as a first line of defense—locking down suspicious funds and notifying law enforcement so investigators have time to secure a court order before assets vanish into unhosted wallets.

Information sharing and interagency coordination

Criminal networks move quickly and across jurisdictions. CLARITY establishes a Treasury-led partnership program that securely connects the Department of Justice, FBI, DEA, and other relevant agencies with private-sector participants to share information on emerging threats and suspicious activity in real time. Better data flow improves the ability to detect and stop illicit finance before it spreads.

At a strategic level, the Act creates a permanent Independent Financial Technology Working Group to Combat Terrorism, Narcotics Trafficking, and Illicit Financing. Bringing together Treasury, the Department of Justice, IRS, FBI, DEA, the Department of Homeland Security, and the Secret Service in a coordinated structure reduces siloed efforts and supports co-developed legislative and regulatory proposals that keep pace with transnational criminal organizations.

Combating localized fraud at crypto kiosks

Predatory scams targeting everyday Americans—especially elderly and other vulnerable populations—have increasingly used digital asset kiosks and ATMs to move stolen funds quickly out of victims' reach. CLARITY responds by establishing a national regulatory floor for kiosk operators, including (i) required registration, (ii) clear anti-fraud policies, (iii) customer warnings and receipts, and (iv) mandatory transaction limits and holding periods.

Crucially, kiosk operators must maintain a dedicated law enforcement point of contact. When financial fraud or elder abuse occurs at a neighborhood terminal, local police can move quickly to trace funds, identify perpetrators, and halt ongoing scams before a victim's life savings are lost.

Securing decentralized infrastructure against cyber threats

Secure by design: NIST and DeFi
Voluntary technical baselines for decentralized protocols.
Risk standards for centralized institutions connecting to DeFi.

Objective: make the safe path the default path for builders and intermediaries.

Cybersecurity vulnerabilities in decentralized finance have been exploited by transnational criminal organizations, state-sponsored hacking groups, and foreign adversaries to fund hostile operations outside the reach of U.S. sanctions. CLARITY addresses this by:

- Creating a voluntary cybersecurity program, led by the National Institute of Standards and Technology (NIST), to set clear, resilient technical baselines for developers.
- Establishing new risk management standards for centralized financial institutions that connect to decentralized protocols.

The combined effect is to build security and transaction monitoring into the technology from the outset, helping to choke off the funding channels of international cybercriminals while keeping open, interoperable infrastructure viable.

Innovation and public safety can move together

The CLARITY Act does not weaken law enforcement authority; it significantly strengthens it. By expanding transparency, bringing hidden activity into regulated channels, modernizing outdated statutes, and improving coordination, the bill equips prosecutors and investigators with tools that match the speed and complexity of digital asset markets.

The choice is not between technological innovation and public safety. It is between a regulated American market with strong oversight and an unregulated offshore market with limited visibility and fewer safeguards. CLARITY opts for the former—bringing legitimate actors into compliance while giving law enforcement the capabilities needed to pursue criminals in an onchain financial system.