

From Regulatory Uncertainty to Clarity: U.S. Laws Governing Stablecoins, Network Coins, and Retail Participation in Cryptocurrency

Author: Daniel Benham, Certified Paralegal

Disclaimer

This document is provided for informational and educational purposes only and does not constitute legal, financial, or investment advice. The author, Daniel Benham, Certified Paralegal (GPA 4.0 Blackstone), has prepared this content based on publicly available sources and professional expertise. Readers should consult qualified professionals for advice tailored to their specific circumstances. The information herein reflects developments as of March 2026 and may become outdated due to evolving regulations. No liability is assumed for any reliance on this material.

Executive Summary

This report examines the transformation of U.S. cryptocurrency regulations from a period of ambiguity prior to 2025 to the structured frameworks established by the Guiding and Establishing National Innovation for U.S. Stablecoins (GENIUS) Act and the Digital Asset Market Clarity (CLARITY) Act. These laws provide clarity on the classification, issuance, and oversight of Stablecoins and network coins, while preserving retail investor rights to self-custody and staking. The analysis highlights how these regulations mitigate risks, promote compliance, and facilitate safe participation in the cryptocurrency ecosystem. Key risks, including de-pegging, volatility, and security vulnerabilities, are addressed with risk management strategies to guide readers toward informed engagement.

Introduction

Cryptocurrency emerged in 2008 with the publication of the Bitcoin whitepaper by Satoshi Nakamoto, introducing a decentralized peer-to-peer electronic cash system intended to enable direct transactions without intermediaries such as banks, thereby promoting financial sovereignty, privacy, resistance to censorship or inflation through centralized control, and reducing intermediary fees and friction (3rd party fees). Bitcoin's original intention was to serve as a trustless, borderless digital currency secured by proof-of-work consensus and cryptography.

Since inception, cryptocurrency has evolved dramatically. From Bitcoin's launch in 2009 as the first blockchain-based asset, the ecosystem expanded to include thousands of tokens with diverse utilities: smart contracts (e.g., Ethereum), cross-border payments (e.g., XRP for Ripple's network and XLM for Stellar's), stable value storage (Stablecoins), and decentralized applications. This evolution has driven global impact, including trillions in market capitalization, adoption in remittances, DeFi protocols managing billions in value, and integration into traditional finance through institutional investments and tokenized assets. Network coins like XRP (designed for fast, low-cost international settlements via Ripple) and XLM (focused on affordable cross-border transfers and financial inclusion via Stellar) exemplify this shift toward practical utility beyond mere speculation.

This report outlines the regulatory progression in the United States, focusing on the GENIUS Act (enacted July 2025) for Stablecoins and the CLARITY Act (enacted 2025) for broader digital assets. It emphasizes retail participation, including self-custody (direct control of private keys) and staking (validating transactions for rewards), within a framework designed to balance innovation with consumer protection.

Problem Context: Regulatory Uncertainty Pre-2025

Prior to 2025, U.S. cryptocurrency oversight was fragmented, with agencies such as the Securities and

Exchange Commission (SEC) (e.g., in the Ripple v. SEC lawsuit), Commodity Futures Trading Commission (CFTC), and Office of the Comptroller of the Currency (OCC) applying inconsistent classifications. Stablecoins faced debates over whether they constituted securities or money transmission instruments, leading to enforcement actions and investor hesitation. Network coins were often scrutinized under the Howey Test, a U.S. Supreme Court-derived standard from SEC v. W.J. Howey Co. (1946) to determine if an asset qualifies as an "investment contract" (and thus a security). The Howey Test requires four elements: (1) an investment of money, (2) in a common enterprise, (3) with a reasonable expectation of profits, (4) derived primarily from the efforts of others. Assets failing these criteria, such as fully decentralized network coins, are generally not securities. In the Ripple v. SEC case, the court ruled that XRP sold on public exchanges (programmatic sales) does not constitute a security under the Howey Test, though institutional sales were deemed unregistered securities offerings.

Retail investors encountered risks from unregulated platforms, including asset loss during exchange failures like FTX. This uncertainty stifled innovation and deterred mainstream adoption, underscoring the need for comprehensive legislation.

Overview of the Failures

- **Mt. Gox (2014):** Once the dominant Bitcoin exchange handling approximately 70% of global Bitcoin transactions, Mt. Gox filed for bankruptcy after a series of hacks resulted in the loss of around 850,000 BTC (valued at about \$450 million at the time). The incident stemmed from inadequate security measures, internal mismanagement, and delayed disclosure, leading to prolonged creditor proceedings that continue to affect distributions as of 2026.
- **Terra Labs (TerraUSD/LUNA, 2022):** Terraform Labs' algorithmic stable coin, TerraUSD (UST), which was designed to maintain a \$1 peg through arbitrage with its sister token LUNA, experienced a catastrophic de-pegging amid market volatility and large-scale redemptions. This triggered a death spiral where LUNA's value hyperinflated and collapsed to near zero, approximately \$40–60 billion in total market value erased, with significant realized losses contributing to broader contagion, including the failures of entities like Celsius and Three Arrows Capital.
- **FTX (2022):** The FTX exchange imploded due to revelations of commingled customer funds with its affiliated trading firm, Alameda Research, coupled with fraudulent practices and a liquidity crisis. This resulted in an estimated \$9 billion in losses, criminal convictions for key executives, and widespread market turmoil.

Similarities

These failures share several core attributes that amplified risks in an unregulated environment:

- **Massive Financial and Market Impact:** Each event precipitated significant investor losses and contributed to "crypto winters"—prolonged periods of depressed prices and reduced activity. For instance, Mt. Gox's collapse marked the first major winter, while Terra and FTX exacerbated the 2022 downturn, with Terra's losses alone surpassing FTX's in scale (\$20.5 billion realized losses for Terra versus \$9 billion for FTX, per blockchain analytics). Industry observers, including blockchain founders, have equated Terra's damage to that of Mt. Gox in terms of eroding public confidence.
- **Erosion of Trust and Contagion Effects:** All three incidents highlighted opacity in operations, leading to panic withdrawals and spillover to interconnected entities. Mt. Gox and FTX involved centralized platforms where users entrusted assets, only to face insolvency due to internal failures, while Terra demonstrated vulnerabilities in algorithmic designs that promised stability but delivered systemic risk.
- **Regulatory Gaps as a Common Thread:** The absence of clear federal guidelines allowed these risks to fester. Issues like inadequate reserves (Terra), poor security (Mt. Gox), and fund misuse (FTX) thrived in a fragmented oversight landscape, fueling calls for reforms that culminated in the

GENIUS and CLARITY Acts.

Differences

Despite parallels, the mechanisms differed markedly:

- **Nature of Failure:** Mt. Gox was primarily a security breach (hack), Terra involved inherent protocol design flaws in a decentralized system, and FTX centered on deliberate fraud and governance lapses in a centralized exchange.
- **Scope and Ecosystem:** Mt. Gox affected early Bitcoin adopters, Terra disrupted DeFi and stable coin markets, and FTX impacted a broader institutional and retail base, including through its native token FTT.
- **Recovery and Legal Outcomes:** Mt. Gox's ongoing bankruptcy has seen partial recoveries, Terra led to lawsuits against Terraform Labs (with founder Do Kwon facing extradition as of 2026), and FTX resulted in swift criminal prosecutions.

These crises collectively illustrate the perils of unregulated crypto activities, directly influencing the development of post-2025 frameworks to enhance transparency, reserve requirements, and investor protections.

Risk Management Considerations in the Pre-2025 Era

Without clear guidelines, investors faced heightened risks such as counterparty exposure on centralized exchanges and volatility in unbacked assets, potentially leading to liquidity failures. Effective risk management involved diversifying holdings, using hardware wallets for self-custody, and monitoring regulatory updates to avoid non-compliant platforms.

Current U.S. Legislative Framework (updated paragraph on CLARITY Act)

The CLARITY Act, passed by the U.S. House of Representatives in 2025, seeks to regulate non-stablecoin digital assets as "digital commodities" under primary CFTC jurisdiction. If enacted, it would require registration for exchanges, brokers, and custodians (third parties), mandate asset segregation, and require customer consent for services such as staking. The proposed legislation aims to distinguish decentralized network coins from securities, thereby reducing classification ambiguity. As of March 2026, the bill remains under consideration in the Senate, with delays in markup potentially extending into mid-2026 due to ongoing debates regarding final language, implementation details, and industry impacts. Notably, banking lobbies are advocating for amendments to prohibit stablecoin yields or rewards, viewing them as potential threats to traditional deposit bases and financial stability.

Note: The CLARITY Act provisions described reflect the version that passed the House in 2025 and are presented here for educational purposes. Final enactment and implementing rules are pending Senate action and potential reconciliation as of March 2026, amid pressures from banking interests to restrict yield-generating features.

Table caption / note (optional – add below the table if desired)

Note: The CLARITY Act provisions described reflect the version that passed the House in 2025 and are presented here for educational purposes. Final enactment and implementing rules are pending Senate action and potential reconciliation as of March 2026.

Future Implications and Guidance (updated paragraph)

Ongoing implementations of the GENIUS Act, including the OCC's proposed rulemaking issued in

February 2026 addressing capital floors, AML requirements, and other operational standards, are expected to progress toward final rules by mid-to-late 2026. The FDIC has extended the comment period for GENIUS-related proposals to May 2026, allowing additional stakeholder input. These measures are anticipated to foster greater institutional adoption, reduce fraud risk, and facilitate integration of compliant stablecoins into traditional finance, potentially paving the way for broader tokenized asset frameworks. The CLARITY Act, while advancing through the House, faces continued Senate deliberation with potential delays pushing markup into mid-2026; its eventual passage (or modifications) could further clarify treatment of network coins and staking activities, though banking lobby efforts to prohibit yields on stablecoins may influence amendments. Key challenges include resolving yield/reward prohibitions under GENIUS and achieving harmonization between state and federal oversight.

GENIUS/CLARITY Comparison Table

Aspect	GENIUS Act (Stablecoins)	CLARITY Act (Network Coins)
Primary Regulator	OCC / Federal Reserve	CFTC
Key Requirements	1:1 reserves, monthly reporting, no interest payments (non-banks)	Asset segregation, consent for staking, disclosures
Asset Classification	Payment instruments	

Integration of Stablecoins and Network Coins

Stablecoins function as stable value-transfer tools in decentralized finance (DeFi) and payments, compliant with anti-money laundering (AML) rules under the Bank Secrecy Act (BSA)—a U.S. federal law (codified primarily at 31 U.S.C. §§ 5311–5336) that requires financial institutions to maintain records, report suspicious activities, and assist in detecting money laundering and terrorist financing. Network coins, such as XRP, XLM, ETH, or SOL, enable blockchain functions like governance and transaction fees, classified as commodities if decentralized under the CLARITY Act. Intersections include using Stablecoins as collateral in network-based staking, enhancing liquidity.

Risk Management for Stablecoins and Network Coins

Stable coin de-pegging risk Arises from reserve mismanagement, liquidity shortages during market stress, or issuer operational failures. **Mitigation:** Verify monthly attestations and third-party audits; diversify across multiple reputable issuers.

- **Network coin volatility risk** Driven by market sentiment, technological changes, regulatory developments, and macroeconomic factors, amplified by the asset class’s relative novelty. **Mitigation:** Diversify portfolio across uncorrelated assets; use stop-loss or trailing-stop orders; actively monitor protocol upgrades, governance proposals, and security audits.
- **Custodial (third-party) risk** Exposure to centralized exchanges or custodians through insolvency, mismanagement, or security breaches. **Mitigation:** Select platforms with comprehensive insurance and regular independent reserve audits.
- **Self-custody-specific risks** Full responsibility shifts to the individual; no counterparty risk but significant personal exposure. Primary threats include:
 - Private key compromise (phishing, malware, social engineering, device theft)
 - Permanent loss from lost seed phrases or forgotten wallet credentials
 - User error (wrong address transfers, poor configuration)
 - Software/hardware vulnerabilities (exploits, supply-chain attacks)
 - Phishing and impersonation scams targeting wallet interfaces

Mitigation:

- Use hardware wallets for significant holdings
- Store seed phrases offline in multiple secure, geographically dispersed locations
- Employ multi-signature wallets where feasible
- Verify all software/firmware updates from official sources only
- Perform small test transactions before larger transfers
- Apply multi-factor authentication and remain vigilant against phishing (domain checks, avoid unsolicited links)

Consistent application of these layered controls materially reduces—but does not eliminate—risks associated with Stablecoins, network coins, and self-custody in the current regulatory environment.

Retail Investor Considerations: Self-Custody and Staking in the Legal Structure

U.S. regulations affirm retail rights to self-custody, where individuals control private keys via wallets, exempt from BSA obligations as non-intermediaries. Self-custody staking in decentralized networks is non-securities activity, with rewards permissible without SEC oversight if not pooled. Tax implications may treat rewards as income; consult jurisdiction-specific rules.

In self-custody, individuals effectively become their own bank, assuming full responsibility for security and operations without third-party intermediaries. This eliminates "third-party friction" (e.g., fees for account management, withdrawal restrictions, or platform policies) but requires diligent execution of all steps:

- **Acquire cryptocurrency:** Purchase via a compliant exchange or peer-to-peer method, transferring to a personal wallet.
- **Set up a wallet:** Choose a software (hot) or hardware (cold) wallet; generate and securely back up the seed phrase (a 12–24 word recovery phrase).
- **Secure private keys:** Store the seed phrase offline (e.g., in a fireproof safe); never share it or store digitally unprotected.
- **Transfer funds:** Send assets from the exchange to your wallet address; confirm transactions on the blockchain explorer.
- **Stake (if applicable):** Lock assets directly on the network or via a decentralized validator; monitor for rewards and potential slashing penalties.
- **Manage ongoing:** Use multi-factor authentication, update software, and test small transactions first.

Future U.S. laws do not restrict individual self-custody or staking rights but enhance institutional adoption by providing regulatory clarity. This clarity enables greater institutional buy-in, influencing network market caps through increased supply-demand dynamics and potential price appreciation.

Risk Management for Retail Participation

Self-custody eliminates counterparty risk but introduces personal responsibility for key security; best practices include multi-factor authentication, hardware wallets, and backup seed phrases. Staking risks include slashing (penalties for downtime); mitigate by selecting reliable validators and understanding network protocols. Retail investors should assess their risk tolerance and consider professional advice.

Future Implications and Guidance

Ongoing implementations, such as OCC's proposed rulemaking for GENIUS Act details (e.g., capital floors and AML requirements), are expected by mid-2026. These will foster institutional adoption, reduce fraud, and integrate Stablecoins into traditional finance, potentially expanding to tokenized assets. Challenges include resolving yield prohibitions and harmonizing state-federal oversight.

Forward-Looking Risk Management

Anticipate regulatory evolution by maintaining compliance programs, conducting regular audits, and staying informed via SEC bulletins. Diversify across assets to hedge against policy shifts.

Conclusion and Recommendations

The GENIUS and CLARITY Acts (passed by House in 2025 and under consideration in the Senate) mark a pivotal shift toward regulatory clarity, enabling secure institutional and retail participation in cryptocurrency. Readers are encouraged to prioritize risk management, utilize self-custody responsibly, and seek expert guidance. For further resources, consult SEC investor alerts and CFTC advisories.

Appendices

Glossary

- **Stable coin:** A digital asset designed to maintain a stable value by pegging to a fiat currency or asset basket.
- **Network Coin:** A native cryptocurrency token used for operations on a specific blockchain, such as transaction fees or governance.
- **Self-Custody:** Direct control of cryptocurrency private keys by the owner, without third-party intermediaries.
- **Staking:** The process of locking cryptocurrencies to support blockchain operations and earn rewards.
- **De-Pegging:** When a stable coin's value deviates from its intended peg, often due to reserve issues.
- **Howey Test:** A U.S. Supreme Court-derived test to determine if an asset is a security, requiring investment of money in a common enterprise with expectation of profits from the efforts of others.
- **Bank Secrecy Act (BSA):** Federal law requiring financial institutions to assist in detecting and preventing money laundering through record keeping and reporting.

Timeline of Key Events

- October 2008: Bitcoin whitepaper published.
- July 2025: GENIUS Act enacted.
- 2025: CLARITY Act passed by House in 2025 and under consideration in the Senate
- February 2026: OCC proposes GENIUS Act rulemaking.
- Mid-2026: Expected finalization of implementing regulations.

References

This report draws from congressional bills, federal agency publications (e.g., SEC, CFTC, OCC), court rulings (e.g., Ripple v. SEC outcomes), and industry analyses cited inline. Full sources are available via referenced web links and official government websites.