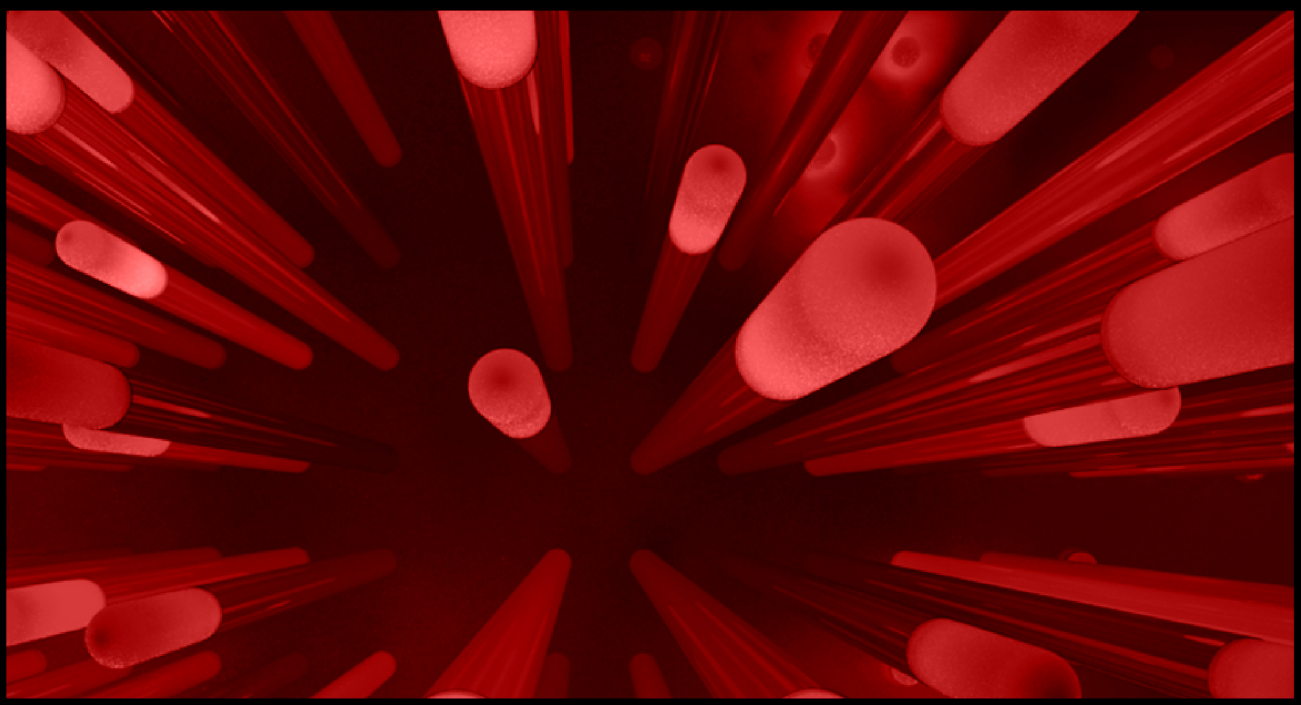
CERTIK
SKYNET

2025 SKYNET U.S. DIGITAL ASSET POLICY REPORT

The U.S. digital asset regulatory environment has transformed in 2025 to offer a much clearer statutory framework. New federal legislation and administrative reforms are now aligned around how digital assets are issued, traded, and custodied.



Executive Summary

The U.S. digital asset regulatory environment has transformed in 2025 to offer a much clearer statutory framework. New federal legislation and administrative reforms are now aligned around how digital assets are issued, traded, and custodied. The simultaneous enactment of the **GENIUS Act**, which awaits final rulemaking and becomes effective in January 2027, and the House passage of the **CLARITY Act** (which remains subject to legislative evolution), coupled with the Securities and Exchange Commission's (SEC) rescission of **Staff Accounting Bulletin 121 (SAB 121)** have established a three-part framework:

1. **A federal standard for payment stablecoins**
2. **A functional classification system for digital assets (commodities vs. securities)**
3. **A clearer operational pathway for bank and trust-company custody**

This report summarizes the legal mechanics, market-structure impacts, and operational requirements of this new regime. It also examines the remaining fragmentation at the state level (the 'Preemption Gap') and shows how a de facto 'Universal Baseline' of cybersecurity and AML/CFT expectations now governs multi-state operators. For market participants, this means:

- **Banks and trust companies now have a clearer pathway to offer digital asset custody**
- **Stablecoin issuers face tighter, unified reserve and compliance expectations**
- **Multi-state operators must plan around a de facto universal baseline of cybersecurity and AML/CFT requirements**

The Federal Stablecoin Framework

1.1 Legislative Authority and Strategic Objectives

On July 18, 2025, the **Guiding and Establishing National Innovation for U.S. Stablecoins (GENIUS) Act** established the first federal chartering and enforcement regime for payment stablecoins. The Act explicitly positions qualifying stablecoins as instruments of U.S. monetary policy and formalizes them as structural buyers of short-term U.S. Treasury securities.

1.2 Issuer Structure and the Subsidiary Mandate

A critical component of the Act is its treatment of **Insured Depository Institutions (IDIs)**. To mitigate contagion risk between digital assets and the deposit insurance fund, the Act prohibits insured depository institutions (IDIs) from issuing payment stablecoins directly. Banks must instead issue through separate, capital-segregated subsidiaries, creating a 'firewall' between insured deposits and stablecoin liabilities and addressing the 'uninsured depository flaw' cited by state regulators.

Non-bank entities may become **Federal Qualified Payment Stablecoin Issuers** supervised by the **Office of the Comptroller of the Currency (OCC)**. Foreign issuers can only access the U.S. market if their home jurisdiction enforces GENIUS-equivalent standards and the issuers can demonstrate technical compliance with U.S. sanctions requirements (e.g., address blacklisting and transaction blocking).

1.3 Prudential Standards

The Act enforces a "narrow bank" model for stablecoin issuance to ensure the singleness of money:

- **Reserve Composition:**
  Issuers must maintain reserves backed 100% by "liquid assets," defined strictly as United States coins, currency, or short-term Treasury bills. Commercial paper and corporate debt are excluded from eligible reserves.

- **No Yield:**
  Issuers are prohibited from paying interest or yield on stablecoins, preventing the emergence of shadow banking risks within the issuance model.

- **Redemption:**
  Issuers must possess the operational liquidity to honor redemptions at par (1:1) upon demand.

1.4 Technical Compliance with Role-Based Access Control (RBAC)

The GENIUS Act requires issuers to be able to 'seize, freeze, or burn' assets when ordered by law enforcement. In practice, this means implementing **Role-Based Access Control (RBAC)**, a permissions model that assigns specific privileges to pre-designated roles, in the smart contract. Issuers must define a dedicated **FREEZER_ROLE**, distinct from upgrade and treasury functions, that can block specific addresses. Best practice is to secure this role with multi-signature governance or hardware-based key management to reduce the risk of unilateral abuse while still enabling timely compliance with lawful orders.

1.5 Global Divergences: U.S. vs EU

The GENIUS Act has created a distinct liquidity pool from the European Union's Markets in Crypto-Assets (MiCA) regulation, effectively fracturing the global stablecoin market.

Requiremen	U.S. GENIUS Act	EU MiCA Regulation	Impact
Reserve Assets	100% USD HQLA (cash, short Treasuries, ≤7-day reverse repo)	Cash (60% in EU Banks) & HQLA.	**Non-Fungible:** Reserves cannot be commingled.
Jurisdiction	U.S. Domiciled or "Substantially Similar."	EU Domiciled (E-Money Token).	**Fractured Liquidity:** USDC-US vs. USDC-EU.
Redemption	Par (1:1) on demand.	Par (1:1) on demand.	**Parity:** Functional quivalence for users.
Yield	**Strictly Prohibited.**	**Strictly Prohibited.**	**Business Model:** reliance on reserve interest.

Figure 1: Regulatory Divergence (GENIUS Act vs. MiCA)



Market Structure Legislation

2.1 The CLARITY Act

The **Digital Asset Market Clarity Act (CLARITY Act)**, passed by the House of Representatives on July 17, 2025, addresses long-standing jurisdictional friction between the SEC and the Commodity Futures Trading Commission (CFTC) by classifying digital assets based on their function within a network:

- **Digital Commodities:**
  Assets intrinsically linked to the operation of a blockchain system (e.g., gas tokens, governance tokens) fall under the exclusive jurisdiction of the CFTC.
- **Investment Contract Assets:**
  Digital assets sold for capital raising remain under SEC jurisdiction.
- **Secondary Market Exemption:**
  The Act clarifies that secondary-market trades of digital commodities by non-issuers do not constitute securities offerings. This significantly reduces liability risk for exchanges that list assets which may have originated as investment contracts.

2.2 Senate Market Structure Bills

The Senate's **Responsible Financial Innovation Act (RFIA)**, released as a discussion draft on September 5, 2025, offers an alternative path. Instead of transferring jurisdiction based on a 'maturity' threshold, RFIA introduces 'Ancillary Assets,' intangible assets sold in connection with an investment contract. It proposes a tailored SEC disclosure regime for these assets, focused on project governance, code audits, and development progress, without forcing decentralized protocols into the Form 10-K reporting structure used for corporate equities.

The Senate Agriculture Committee's **Bipartisan Discussion Draft**, released on November 10, 2025, offers the complementary approach by expanding the authority of the Commodity Futures Trading Commission (CFTC). This draft establishes a comprehensive federal regulatory framework for the spot market of "digital commodities," defined generally as fungible, peer-to-peer transferable digital assets recorded on a cryptographically secured public distributed ledger, and which expressly excludes securities.

Unlike the RFIA's focus on defining Ancillary Assets for SEC oversight, the Ag Committee draft centers on the entities that facilitate commodity trading, requiring digital commodity exchanges, brokers, and dealers to register with the CFTC. These registered entities would be subject to stringent rules requiring customer fund segregation, plain language disclosures, anti-manipulation systems, and robust cybersecurity standards, mirroring consumer protections found in traditional futures markets.

2.3 The Legislative Timeline

While the House has successfully advanced the CLARITY Act with substantial bipartisan support, the Senate's corresponding market structure efforts have proceeded at a more deliberate tempo. Although both the Senate Committee on Agriculture and the Senate Banking, Housing, and Urban Affairs Committee have recently accelerated their legislative momentum, releasing discussion drafts and advancing key nominations, significant legislative hurdles remain.

Specifically, both committees must conclude their respective markups, and the resulting bills will require reconciliation and harmonization into a unified package before being considered for a full Senate floor vote. Given the current legislative calendar and the complexity of combining these regulatory frameworks, the passage of comprehensive Senate crypto market structure legislation is most realistically anticipated in Q1 of 2026.

2.4 Decentralization Audits

Although neither the CLARITY Act nor the RFIA mandates specific quantitative thresholds, the need to prove “sufficient decentralization” as a legal off-ramp has driven the rapid adoption of industry-standard **Decentralization Audits**. These audits commonly rely on metrics such as the Nakamoto Coefficient, Gini Coefficient, and geographic node distribution.

- **Nakamoto Coefficient:**
  Measuring the minimum number of validators required to compromise consensus.
- **Gini Coefficient:**
  Assessing the concentration of token wealth.
- **Geographic Distribution:**
  Evaluating the physical dispersal of nodes to assess resilience against geopolitical capture.

Feature	CLARITY Act (House Passed)	RFIA (Senate Discussion Draft)
Primary Regulator	**CFTC** (Commodity Futures Trading Commission)	**SEC** (Securities & Exchange Commission)
Asset Classification	**Digital Commodity:** Defined by functional decentralization.	**Ancillary Asset:** Intangible asset sold with an investment contract.
Transition Mechanism	**Maturity Pathway:** Explicit off-ramp to commodity status once "mature."	**Disclosure Regime:** Tailored reporting; no automatic jurisdiction transfer.
Secondary Markets	**Exempt:** Secondary sales are not securities transactions.	**Regulated:** Subject to specific SEC disclosure rules.
Key Metric	**Decentralization:** Based on voting power (<20%) and code control.	**Compliance:** Based on periodic disclosure and governance reporting.

Figure 2: Comparative Analysis of Market Structure Proposals

Institutional Custody and Accounting Reform

3.1 The Rescission of SAB 121

On January 23, 2025, the **SEC issued Staff Accounting Bulletin No. 122 (SAB 122)**, formally rescinding SAB 121. Under the prior guidance, custodians had to record client crypto assets as on-balance-sheet liabilities, which inflated their balance sheets and triggered prohibitive capital requirements for regulated banks. SAB 122 instead directs entities to apply **ASC 450 (Contingencies)**, recognizing a liability only when a loss is probable and estimable. This change removes the specific capital penalty that had effectively blocked large banks from scaling digital asset custody.

3.2 Qualified Custodian Expansion

Following this accounting reform, SEC staff issued no-action relief on September 29, 2025, clarifying that eligible state-chartered trust companies may serve as **Qualified Custodians** for Registered Investment Advisors (RIAs), provided they meet fiduciary and safety standards comparable to national banks. The guidance emphasizes operational rigor: bankruptcy-remote asset segregation, documented internal controls, and independent SOC 1 / SOC 2 audits are now baseline expectations.

Settlement Infrastructure (RLN & Project Guardian)

4.1 The Regulated Liability Network (RLN)

The U.S. banking sector has coalesced around the **Regulated Liability Network (RLN)**, a shared ledger infrastructure for settling regulated liabilities. A 12-week pilot involving the New York Federal Reserve and major commercial banks (including Citi, BNY Mellon, and Wells Fargo) successfully demonstrated "atomic settlement" of domestic and cross-border U.S. dollar payments. The pilot utilized tokenized commercial bank deposits and wholesale central bank digital currency (wCBDC) on a single interoperable chain, validating the feasibility of programmable, 24/7 fiat settlement.

Initiative	Key Participants	Primary Use Case	Technology Stack
Regulated Liability Network (RLN)	NY Fed, Citi, BNY Mellon, Wells Fargo, Swift	**Atomic Settlement:** Domestic & cross-border USD payments using tokenized deposits.	Shared Ledger (Interoperable w/ CBDC & Commercial Bank Tokens)
Project Guardian (Asset Mgmt)	JPMorgan (Kinexys), Apollo	**Discretionary Portfolios:** Automated rebalancing of 1,000+ portfolios via smart contracts.	Permissioned Blockchain (Subnet/Private Chain)
Project Guardian (FX)	Ant International, ISDA, HSBC	**FX Settlement:** Real-time cross-border exchange using tokenized bank liabilities.	Compatible with EVM standards
Project Guardian (Off-Chain)	Swift, UBS Asset Management, Chainlink	**Fund Subscription:** Settling tokenized fund transactions using legacy Swift cash rails.	Swift Integration / Chainlink CCIP

Figure 3: Institutional Pilot Programs

4.2 Project Guardian and Permissioned DeFi

Globally, the Monetary Authority of Singapore's **Project Guardian** expanded its scope in 2025 to standardize asset tokenization. Key pilots included:

- **Asset Management:**
  JPMorgan and Apollo deployed a proof-of-concept for discretionary portfolios, using smart contracts to automate the rebalancing of thousands of client portfolios instantly.
- **FX Settlement:**
  Ant International and ISDA led a workstream on using tokenized bank liabilities for real-time foreign exchange settlement, reducing settlement risk in cross-border transactions.

The State Regulatory Frameworks

5.1 The Preemption Gap

The most significant operational challenge for digital asset companies today remains the absence of a unified federal regulatory framework for all asset classes. This void has created a "Preemption Gap," forcing Multi-State Operators (MSOs), defined as firms providing services across five or more jurisdictions, to comply with a disparate patchwork of state licensing regimes. Unlike a federal bank charter which preempts state law, MSOs must navigate traditional Money Transmitter Laws (MTLs) that were designed for legacy financial services and are often ill-suited for blockchain mechanics. This results in inconsistent fee structures, varying capital reserve mandates, and significant investment in specialized legal counsel, creating a high cost of compliance that frequently prices smaller innovators out of the market.

5.2 Key State Frameworks and Unique Requirements

While many states rely on the uniform Money Transmitter Act, key jurisdictions have enacted bespoke, high-barrier frameworks:

- **New York (BitLicense):**
  The NYDFS BitLicense (23 NYCRR Part 200) remains one of the most demanding U.S. frameworks for virtual asset businesses. It imposes capital requirements tailored to specific institutional risks and mandates a dedicated compliance officer. BitLicense holders must also comply with Part 500, which requires comprehensive cybersecurity programs, multi-factor authentication, and strict incident-reporting timelines.

- **California (DFAL):**
  The Digital Financial Assets Law (DFAL) focuses heavily on consumer protection. It mandates detailed risk disclosures and imposes stringent stability requirements on stablecoin issuers, who must maintain reserves equal to the aggregate amount of all outstanding stablecoins, audited monthly.

- **Wyoming (SPDI):**
  Wyoming offers a divergent path through the **Special Purpose Depository Institution (SPDI)** charter. This limited-purpose banking framework classifies digital assets as property and allows firms to operate as qualified custodians subject to full-reserve requirements (100% fiat backing, no lending). This attempts to preempt the MTL debate by defining the entity as a bank-like institution.

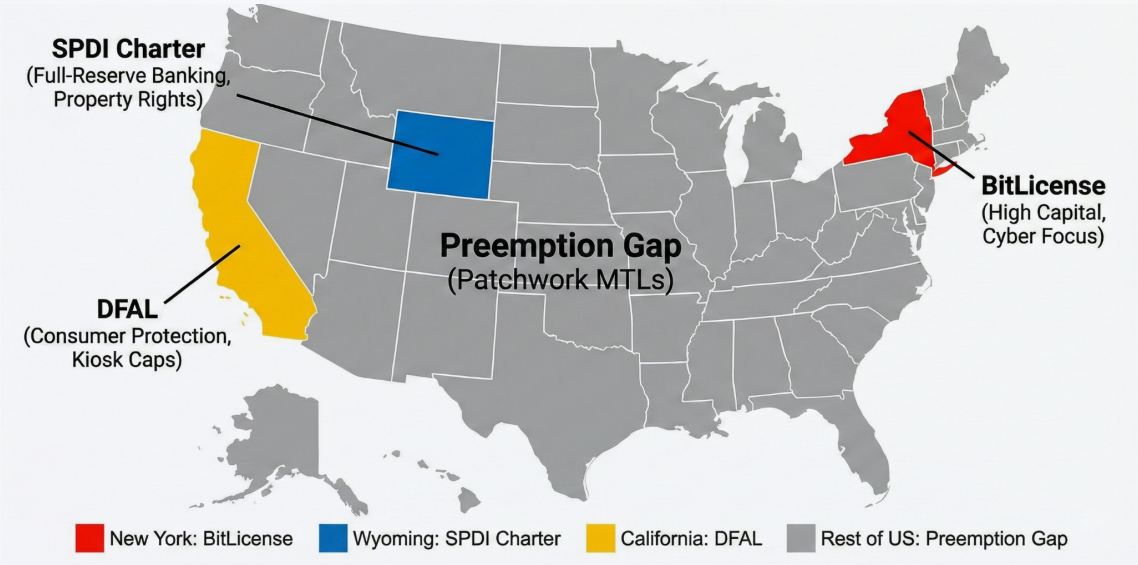


Figure 4: State Regulatory Heatmap

5.3 Operational Impacts

The complexity of these frameworks drives two primary operational behaviors. First, firms engage in **Regulatory Arbitrage**, prioritizing operations in permissive states while limiting services in high-cost jurisdictions like New York. Second, MSOs operate with a strategic eye on the **Preemption Outlook**, anticipating that forthcoming federal legislation, likely driven by the OCC or SEC, will eventually supersede this state-level patchwork with a unified chartering standard.

5.4 Essential Security & Compliance Requirements

Despite the fragmentation, a de facto 'Universal Baseline' for market entry has emerged. Regardless of whether a firm pursues an MTL, BitLicense, or SPDI charter, regulators now enforce two non-negotiable pillars for licensing and ongoing supervision:

1. **Robust Cybersecurity and Resiliency:**
   Aligned with the NIST Cybersecurity Framework, states demand mandatory incident response plans with strict reporting timelines, regular third-party penetration testing to prove system integrity, and rigorous protocols for the protection of Non-Public Information (NPI).

2. **Auditable AML/CFT Systems:**
   Reflecting federal Bank Secrecy Act (BSA) obligations, MSOs must implement sophisticated transaction monitoring systems capable of generating Suspicious Activity Reports (SARs). This includes mandatory Know Your Customer (KYC) protocols at account opening and ongoing Customer Due Diligence (CDD), overseen by a designated Chief Compliance Officer.

Firms that fail to demonstrate robust capability in these two areas are routinely denied licensure, making the "Universal Baseline" the functional minimum standard for U.S. market access.

Feature	New York (BitLicense)	California (DFAL)	Wyoming (SPDI)
Primary Focus	Prudential & Cyber: High capital/security barriers.	Consumer Protection: Disclosure & Fee Caps.	Banking Charter: Full-reserve custody.
Capital Requirement	Risk-based; determined by NYDFS per licensee.	Surety bond or trust account required.	Minimum capital for bank charter.
Asset Listing	Greenlist: Can only list pre-approved assets.	No specific "Greenlist," but disclosure required.	Assets defined as bailment (property).
Consumer Mandates	Strict disclosure; Part 500 Cybersecurity rules.	Kiosk Cap: Fees capped at $5 or 15%; receipt requirements.	100% Reserve requirement; No lending.
Key Deadline	Ongoing (Part 500 Compliance).	July 1, 2026: Full Licensure Deadline.	Continuous examination.

Figure 5: State Regulatory Compliance Matrix

Compliance and Surveillance

6.1 Forensic Market Surveillance

Regulatory agencies have integrated blockchain analytics into their enforcement toolkits.

- **Wash Trading Detection:**
  Because a significant share of reported volume on unregulated exchanges may be artificial, regulators use statistical methods such as Benford's Law to flag anomalous trading patterns for further review.

- **Clustering Algorithms:**
  Surveillance tools track **Strongly Connected Components (SCCs)**, clusters of wallets trading in closed loops, to detect coordinated market manipulation and wash trading rings on decentralized exchanges (DEXs).

6.2 Smart Contract Audits

Code auditing standards have evolved to verify regulatory logic alongside code security. For stablecoin issuers, audits now confirm the correct implementation of the GENIUS-mandated 'freeze' function, including:

- **That the FREEZER_ROLE is secured by multi-signature or hardware-based governance**

- **That it is functionally distinct from upgrade, treasury, and other administrative privileges**

The objective is to reduce unauthorized censorship risk while still enabling timely compliance with lawful orders. Code audits will grow as a key security and compliance measure for institutions to ensure alignment with the regulatory direction around centralization functions.

Conclusion

The regulatory developments of 2025 suggest a durable integration of digital assets into the U.S. financial architecture driven by both Federal and State-driven initiatives. For financial institutions, the strategic focus is shifting toward **Permissioned Digital Assets**: using blockchain-based settlement within clearly defined regulatory perimeters. As liquidity becomes segmented by jurisdiction (for example, between U.S. and EU/MiCA-compliant pools), the ability to map regulatory 'gaps' and build compliant, cross-jurisdictional infrastructure will be a key source of competitive advantage over the next few years.

Check out the **Skynet** platform today and elevate your Web3 journey by learning more about the security insights of the projects highlighted in this report and reading more on the CertiK blog hub.

Protect your community and your organization today. Visit **CertiK.com** or get in touch at **bd@certik.com**.

CERTIK
SKYNET

COMPANY INTRO

Founded in December 2017 in New York by two professors from Yale University and Columbia University, CertiK is the largest Web3 security service provider.

CertiK offers a wide range of products and services to support the Web3 industry, project teams, and users alike. CertiK's products and services span the entire lifecycle of project development, from incubation and early stages, to growth and maturity.

With a highly skilled technical team, CertiK stands out for its expertise in formal verification technology, artificial intelligence, and academia. CertiK's leaders also collaborate closely with global government bodies to develop supportive Web3 compliance and regulatory frameworks.

>$600B
ASSETS SECURED

180,000+
VULNERABILITIES DETECTED

5,000+
CLIENTS SERVED

>70% OF TOP 500 CMC PROJECTS AUDITED

DIVERSITY IN ECOSYSTEMS