The False Choice of Innovation vs. Compliance in the Digital Asset Marketplace

March 5, 2026

Written by

John Auerbach

Kevin Strenski

Despite growing market headwinds, this has been a transformational year in the US digital asset sector, as crypto's homegrown leaders jostle for position with traditional finance giants in mainstreaming blockchain finance. And, following through on its 2024 campaign promise of a much more salutary posture towards crypto, the Trump Administration has relaxed regulatory pressure and championed legislation designed to accelerate and broaden accessibility of cryptocurrency in the US market. As a first step, President Trump signed the GENIUS Act in July 2025. The first major piece of US legislation focused on digital assets and established a comprehensive federal regulatory system for stablecoins. In the months following its passage, traditional financial institutions rushed to bring long-standing products onto the blockchain. By late 2025, firms including Goldman Sachs, JPMorgan Chase, Bank of New York Mellon, and State Street unveiled tokenized offerings that allow clients to hold digital tokens representing shares in money market funds. And, in January 2026, the New York Stock Exchange announced plans to develop a platform for trading tokenized securities—effectively bringing the stock market on-chain **[1]**. In February 2026, additional US banks, including Huntington Bancshares, First Horizon, and M&T Bank all announced plans to build tokenized deposit networks **[2]**.

However, in recent weeks the Digital Asset Market CLARITY Act, which was passed with largely bipartisan support in the House of Representatives at the same time as the GENIUS Act, has stalled in the Senate. By dividing oversight responsibilities between the Securities and Exchange Commission and the Commodity Futures Trading Commission, the CLARITY Act aims to create a comprehensive regulatory framework for digital assets, establish registration requirements for digital-commodity exchanges, and introduce a modern "maturity test" to classify tokens more accurately. Designed to end years of regulatory jurisdictional uncertainty, it should establish guidance, providing developers, investors, and institutions metaphorical "rules of the road" and adding predictability to crypto enforcement. However, several major crypto companies have opposed the bill in the Senate writeup process, arguing that late-stage changes go too far in establishing jurisdiction

over decentralized finance operators and impose compliance burdens misaligned with how open blockchain networks operate. Industry participants withdrew support in January 2026, which has caused the Senate to delay the bill's markup.

The impasse over the CLARITY Act exposes fault lines between the traditional finance, or TradFi, giants – which have had to live within the highly proscribed world of fiat banking and securities regulation – and blockchain-native firms – which have matured largely within a more permissive compliance and enforcement gray zone. Both seek greater predictability from the US regulatory regime but differ on the scope and standards of enforcement.

The current debate, framed as a binary choice between the supposedly diametrically opposed interests of innovation and compliance, is short-sighted as the industry faces existential risks to growth; to wit, operational risk vulnerabilities and financial crime. With wide consumer reach comes equally widescale potential liability – legal, financial and reputational. Conversely, fair, transparent, and lawful operations reliably build mass market trust and appeal over the long term. This is especially true in periods of extreme price volatility, such as the industry is currently experiencing, reminiscent of 2022's 'Crypto Winter,' sparked by the Terra/Luna collapse, which led to the high-profile failure of FTX and other major industry players. Today, with the opportunity to balance growth and the establishment of controls to ensure crypto's long-term viability, i.e., innovation in compliance, the industry should not necessarily wait for government to lead the way.

The risks are evident. Lighter government oversight can provide the freedom of action needed to drive rapid growth, yet the pseudonymity and speed of blockchain finance leaves companies more vulnerable to exploitation by financial criminals seeking to move funds across borders with minimal friction. Data from blockchain intelligence firms illustrates the scale of the challenge, with TRM Labs reporting more than $158 billion in illicit cryptocurrency transactions in 2025, a nearly 145% increase in one year, and Chainalysis identifying over $17 billion stolen in 2025 from cryptocurrency scams and fraud. **[3]** The highly sophisticated global money laundering networks that serve as banks to transnational criminal organizations and narcotics traffickers are rapidly adopting crypto networks as their preferred value transfer vehicle. **[4]**

The threat is not limited to money laundering. Digital asset platforms also face unprecedented levels of hacking activity. In 2025, illicit actors stole $2.87 billion through more than 150 hacks. **[5]** In the largest incident, the Bybit hack – responsible for half the total, more than $1.4 billion in losses – attackers accessed the exchange's hot wallet and withdrew the stolen funds in just two transactions. **[6]** Cryptocurrency exchanges such as Bybit are far from the only targets for sophisticated cybercriminal actors. Decentralized Finance, or DeFi, protocols and smart contracts are prime targets for flash loan and governance attacks. In January 2026, cyber actors exploited a vulnerability in the smart contract code of the DeFi protocol Truebit to mint unlimited quantities of TRU tokens, resulting in losses of over $26 million. **[7]**

In 2025, illicit actors stole $2.87 billion through more than 150 hacks.[5]

As blockchain companies innovate, threat actors evolve in parallel. New services create new targets, which sophisticated attackers are quick to exploit. Mistakes have market-shaking impacts, as was demonstrated this month by Bithumb's accidental distribution of $43bn in Bitcoin, which contributed to a 17% drop in the price of BTC. **[8]** The trend is clear: as innovation in the blockchain industry fuels rapid growth, it simultaneously expands the attack surface for bad actors and increases the consumer damage from internal control failures.

Thus, blockchain technology requires innovative

compliance strategies and security controls built to address the pace and virtual, distributed operating model of the industry. Successful compliance strategies and security controls will creatively address four facets of the blockchain experience:

- **Customer identification.** The inherent pseudonymity of blockchain transactions makes it persistently difficult to link on-chain activity to real-world individuals. Unreliable attribution of crypto holdings presents huge opportunities to financial criminals. In addition, traditional Know Your Customer processes are frustrated by the ability of bad actors to spoof legitimate credentials by using AI deepfakes to generate identity documents and defeat "customer selfie checks," biometric photograph comparisons to government-issued identification. These synthetic identities, now generated at scale by transnational criminal organizations and state actors and used in tandem with internet protocol, or IP, geo-masking using Virtual Private Network, or VPN, platforms, can increasingly fool automated verification systems, overwhelm manual review teams, and facilitate high volume money laundering or market exploits. The more-established exchanges and the TradFi stablecoin issuers are increasingly being targeted by money launderers seeking "off-ramps" to convert their more speculative crypto holdings into stablecoins, tokenized securities, and/or fiat holdings.
- **Suspicious activity detection.** Digital asset providers face significant obstacles in monitoring suspicious activity, particularly when trying to identify money laundering and market manipulation in high velocity pseudonymous markets. High transaction volumes, cross-chain bridges, and the use of mixers or privacy tools can obscure illicit flows, making it difficult to distinguish trading from laundering. Market manipulation—such as wash trading, pump-and-dump schemes, or spoofing—can be hard to detect without advanced surveillance tools that correlate on-chain activity with exchange order-book behavior. These challenges are amplified by resource constraints and varying regulatory expectations that leave compliance teams struggling to maintain meaningful oversight at scale. Decentralized exchange protocols, liquidity pools, and cross-chain bridges have become increasingly attractive methods for laundering digital assets, given that they obscure the origin and destination of funds and offer token swapping functionality without meaningful KYC requirements.
- **Cybersecurity.** Digital asset providers face increasing pressure to tighten cybersecurity as sophisticated adversaries deploy advanced techniques like the supply-chain attack that enabled the Bybit breach, where malicious code was injected into a third-party wallet interface to trick authorized signers into granting access to cold storage. Similarly, DeFi protocols and smart contract issuers are vulnerable to hackers looking to exploit smart contract code and poor security controls to steal millions, as in the case of Truebit. Preventing similar incidents requires rigorous vendor security assessments, continuous code-integrity monitoring, and strict access controls. Exchanges and DeFi platforms alike must harden their infrastructure, adopting multi-layer authentication, hardware-backed key management, and real-time anomaly detection. Equally important is implementing independent security audits and red team exercises—e., self-due diligence by simulated adversaries—to uncover vulnerabilities before attackers do. Platforms, which tend to focus on the front-end user experience, must pay equal attention to back-end security to ensure the security of customer assets.
- **Operational risk controls**. Like any rapid growth industry, crypto exchanges face challenges in maintaining strong internal operational controls, particularly segregation of duties, as small, rapidly growing teams often allow the same individuals to initiate, approve, and reconcile transactions—creating opportunities for abuse. Weak or fast-changing accounting controls can lead to inaccurate asset reconciliation across wallets and delayed recognition of liabilities, as well as gaps and timing differences between on-chain and off-chain ledgers. Additionally, securing truly independent audit oversight is difficult, as many exchanges lack mature governance structures or rely on auditors who lack crypto-native expertise, audit experience, or both. When these shortcomings compound, they increase operational risk and undermine trust with regulators, customers, and institutional partners.

Luckily, the crypto toolbox is growing rapidly. On the front end, AI-driven identity-verification tools are being deployed to strengthen customer onboarding and make it significantly harder to spoof identities. Know Your Transaction surveillance models employed by blockchain intelligence providers are moving beyond single-wallet screening to include cluster analytics, i.e., looking at extended upstream and downstream links to high-risk actors. Behavior-based analytics are now able to detect at earlier stages coordinated geo-masking and signs of market manipulation such as wash trading.

Ongoing independent compliance audits—of internal accounting controls, customer onboarding, private-key management, and privileged-access systems—help reduce the risk of hacks, material losses, and accidental credits. Both centralized exchanges and DeFi platforms can further mitigate risk through external reviews of their smart-contract code, including red team exercises designed to uncover vulnerabilities before exploiters can.

As some risk incidents are inevitable, firms are upgrading their rapid response capabilities to gather facts in reaction to potential exploits, using a multidisciplinary approach of on-chain tracing, cyber response, forensic data analytics, open source intelligence, and human source intelligence. With risks and countermeasures both rapidly evolving, the successful platform will coordinate oversight functions and seek continuous improvement in tools and processes.

In the end, the firm establishment of the digital asset industry will come not through a legislative framework or the pace of tokenization but through the ability to modernize its guardrails as quickly as it innovates. There can be great temptation to use the light regulatory environment to justify a failure to invest in strong compliance and internal controls, and while this may lead to greater short-term profits, it almost guarantees a far less profitable long-term future. Building a racecar without functioning brakes is not a viable long-term strategy. The platforms that treat compliance, security, and operational discipline as strategic advantages rather than regulatory chores to be avoided will be the ones that win consumer trust, attract institutional capital, and withstand the next Crypto Winter. The companies that can effectively strike this balance will emerge as leaders of the industry's next era.

Endnotes

1. https://www.wsj.com/finance/currencies/nyse-to-launch-24-7-trading-platform-for-blockchain-based-securities-8313526a.
2. https://www.bloomberg.com/news/articles/2026-02-18/us-banks-build-tokenized-deposit-network-to-guard-their-turf.
3. https://www.trmlabs.com/reports-and-whitepapers/2026-crypto-crime-report; https://www.chainalysis.com/blog/crypto-scams-2026/.
4. https://www.chainalysis.com/blog/2026-crypto-money-laundering/.
5. https://www.trmlabs.com/reports-and-whitepapers/2026-crypto-crime-report.
6. https://www.elliptic.co/blog/bybit-exploit-six-months-on.
7. https://protos.com/legacy-defi-platforms-lose-27m-as-hacking-spree-continues-into-2026/.
8. https://www.reuters.com/world/asia-pacific/crypto-firm-accidentally-sends-44-billion-bitcoins-users-2026-02-07/.

Nardello & Co.

For press inquiries

Contact Elizabeth Anscombe at
eanscombe@nardelloandco.com

Chambers TOP RANKED Litigation Support 2025 Nardello & Co.

Nardello & Co. is the only Chambers Band 1 Investigative Firm in the US, UK, and APAC.

GIR

Winner of GIR's 'Investigations Consultancy of the Year' 2024.