



2025 Industry Guide for Lawyers and Dev Teams: **Introduction and Overview**

DLx Law PLLC

January 13, 2025

(updated Jan. 14, 2025)

In light of how fast this year is moving—*ALREADY*—DLx Law is kicking off 2025 by releasing this three-part *U.S. Industry Guide for Lawyers and Dev Teams* to help our friends and clients navigate the rapidly changing U.S. regulatory and political landscape. In the *Industry Guide*, our attorneys include much of their own policy insights and perspectives on the new Congress and Donald Trump’s second presidential term, as well as the potential implications for digital assets and emerging technologies and industries.

Here is what our *Industry Guide* contains:

Part 1. Ongoing Industry Trends and Challenges: Offers an overview of key trends and innovations in digital assets, blockchain, distributed ledger technologies and industries, analyzing some of the most significant challenges standing in the way of further advancements and broader adoption and use.

[Read on webpage](#) or [read document as PDF](#).

Part 2. Recent and Existing Policy and Enforcement: Recaps policy under the outgoing presidential administration and surveys key legal and regulatory events at the federal and state levels during this time, revealing how fragmented oversight and aggressive enforcement have intensified debates over compliance obligations.

[Read on webpage](#) or [read document as PDF](#).

Part 3. Current Legal Trends and Developments: Examines changing political tides as the United States enters a new era of governance, identifying how congressional gridlock, geopolitical tensions, and shifting priorities of the incoming presidential administration affect the future of digital assets, decentralized systems, and emerging technologies.

[Read on webpage](#) or [read document as PDF](#).

Read on for a summary of the *Industry Guide*’s conclusions and key takeaways—

Throughout the last several years, digital assets, decentralized systems, and new technologies and industries have evolved from a niche market to a force driving significant financial and technological change in society. Even after having taken major strides in recent years to advance scalability, interoperability, and institutional adoption, these industries face persistent uncertainties. In the United States, piecemeal legal

frameworks, uneven enforcement priorities, and potentially widening political fissures have clouded the path forward for blockchain and distributed ledger networks, DeFi and Web3 application programmers, other industry innovators and advocates.

Shifting market demands and evolving global geopolitical pressures—coupled with the return of a now possibly evolved, yet still unconventional, Trump White House—give cause for speculation. Nonetheless, incoming U.S. market regulatory leadership could potentially help to maintain stability and adjust rules and enforcement to safely restore market confidences, and they are widely anticipated to open up major opportunities for change and growth in new digital technologies and industries. Although business sectors focused on digital assets and decentralized systems also still face formidable challenges with regulatory compliance, sustainability, public perception, and wide-scale adoption, the regulatory outlook is largely positive for the first time in a long time.

Ultimately, 2025 will likely mark a pivotal moment in history for digital assets, decentralized systems, and many other emerging technologies and the industries they support. Despite remarkable growth and significantly favorable regulatory promises, however, these sectors could remain tempered in the near-term, fueled by unpredictability over many elements of the incoming Trump administration, growing international tensions, and evolving economic conditions in the U.S. and around the globe. Importantly, if demands for these technologies and industries continue to grow at their current trajectory, then incentives will also increase for government actors, industry leaders, and diverse stakeholders to collaborate and forge sustainable frameworks that can ensure their long-term viability and success.

Overview of outstanding challenges.

Regulatory ambiguity and inconsistency aside: As they continue to mature, digital assets and emerging technologies and industries will likely be confronted with a range of critical challenges. Successfully balancing privacy concerns with oversight interests will probably be one of the most significant challenges for standard-building and regulation. For example, the rapid growth and increasing sophistication of blockchain and DeFi platforms have attracted not only entrepreneurs and investors but also cyber criminals.

High-profile exploits, including smart contract breaches and cross-chain bridge hacks, have collectively resulted in billions of dollars in losses over recent years.¹ Malicious actors employ methods ranging from phishing attacks against network participants to ransomware schemes that target the custodians of digital assets, disrupting operations and extorting funds.² Additionally, decentralized infrastructures can be challenging to police, because the absence of central intermediaries complicates efforts to trace illicit activities or recover stolen funds.

Industry and government responses to these threats have evolved in tandem. Some blockchain projects now undergo rigorous code audits before launch, and bug bounty programs incentivize independent researchers

¹ See Chainalysis Team, *Funds \$2.2 Billion Stolen from Crypto Platforms in 2024, but Hacked Volumes Stagnate Toward Year-End as DPRK Slows Activity Post-July*, CHAINALYSIS: BLOG: CRIME (Dec. 19, 2024), <https://www.chainalysis.com/blog/crypto-hacking-stolen-funds-2025/>; Chainalysis Team, *2024 Crypto Crime Mid-year Update Part 1: Cybercrime Climbs as Exchange Thieves and Ransomware Attackers Grow Bolder*, CHAINALYSIS: BLOG: CRIME (Aug. 15, 2024), <https://www.chainalysis.com/blog/2024-crypto-crime-mid-year-update-part-1/>; Chainalysis Team, *Funds Stolen from Crypto Platforms Fall More Than 50% in 2023, but Hacking Remains a Significant Threat as Number of Incidents Rises*, CHAINALYSIS: BLOG: CRIME (Jan. 24, 2024), <https://www.chainalysis.com/blog/crypto-hacking-stolen-funds-2024/>.

² See FED. BUR. INVESTIGATION, *Cryptocurrency Fraud Report 2023*, FBI: INTERNET CRIME COMPLAINT CTR., at 6, 11-12, 20 (Sep. 9, 2024), https://www.ic3.gov/AnnualReport/Reports/2023_IC3CryptocurrencyReport.pdf.

to disclose vulnerabilities rather than exploit them.³ Regulatory bodies, law enforcement agencies, and international standard-setters have stepped up oversight, increasingly adopting frameworks like the Financial Action Task Force’s (FATF) Travel Rule,⁴ which is meant to enhance the traceability of digital asset transactions and deter money laundering but is burdensome⁵ and can threaten user privacy.⁶

Striking a balance between robust enforcement and allowing room for innovation and competition remains imperative yet challenging. Overly burdensome measures can deter legitimate innovation or potentially undermine important underlying technological principles, whereas a laissez-faire approach risks emboldening bad actors and undermining public confidence in the sector.

In fact, one of the most significant challenges facing digital assets and permissionless systems more broadly involve overcoming barriers to wider adoption—chief among those barriers likely being public perception. For example, the complexity of current interfaces, the difficulty in safely storing private keys, and frequent user confusion with concepts like gas fees and wallet addresses present daunting hurdles. Moreover, negative news coverage of scams, frauds, and volatile markets contributes to public mistrust, making many consumers reluctant to embrace digital assets or engage with decentralized applications (“dApps”). For enterprises, concerns about scalability and interoperability persist, as high transaction fees, slow network speeds, and fragmented platforms can impede the efficient processing of millions of daily transactions.

Wider adoption of these emerging technologies is likely essential for industry advocates to gain broad enough political support to ensure that policy, both in the U.S. and abroad, is designed to preserve the integrity of decentralized systems and the security and privacy principles on which they stand. Nevertheless, addressing these adoption-related challenges requires a multi-pronged approach. Educational initiatives can demystify blockchain and improve general financial and technological literacy, and investments in user

³ See Adeleke Ayobami, *How Blockchain Technology is Revolutionizing Audit and Control in Information Systems*, ISACA: RESOURCES: NEWS & TRENDS: INDUSTRY NEWS (Oct. 31, 2024), <https://www.isaca.org/resources/news-and-trends/industry-news/2024/how-blockchain-technology-is-revolutionizing-audit-and-control-in-information-systems>; CyberSanctus, *The Role of Bug Bounty Programs in Web3 Security*, PENTEST MAG. & COURSES (Apr. 10, 2024), <https://pentestmag.com/the-role-of-bug-bounty-programs-in-web3-security/>.

⁴ FATF Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers, FIN. ACTION TASK FORCE (Oct. 2021), <https://www.fatf-gafi.org/content/dam/fatf-gafi/guidance/Updated-Guidance-VA-VASP.pdf.coredownload.inline.pdf>; FATF, *Report: Virtual Assets: Targeted Update on Implementation of the FATF Standards on VAs and VASPs*, FIN. ACTION TASK FORCE: PUBS. (Jul. 9, 2024), <https://www.fatf-gafi.org/en/publications/Fatfrecommendations/targeted-update-virtual-assets-vasps-2024.html>.

⁵ The FATF Travel Rule requires virtual asset service providers (VASPs) to collect and share extensive customer information for every cross-border transaction, leading to significant operational costs, technological integration challenges, especially for smaller companies struggling to implement the necessary systems, while also facing inconsistencies in how different jurisdictions interpret and enforce the rule; this can hinder innovation and market entry for new businesses, developers, and users in the sector. See Lana Schwartzman, *Key Takeaways from FATF’s Fifth Targeted Update of Travel Rule Implementation: July 2024*, NOTABENE: REG. INSIGHTS (Jul. 10, 2024), <https://notabene.id/post/key-takeaways-from-fatfs-2024-targeted-update-of-travel-rule-implementation-for-virtual-assets-and-service-providers---july-2024>; NOTABENE: CRYPTO TRAVEL RULE 101, *Crypto Travel Rule Compliance: Challenges and Opportunities for VASPs*, <https://notabene.id/crypto-travel-rule-101/crypto-travel-rule-compliance-challenges-and-opportunities-for-vasps>.

⁶ Even if a transaction is legitimate, personal data is collected and shared with multiple entities, increasing the risk of misuse or unauthorized access. Additionally, database transactions on blockchain networks, including financial transactions are intended to be pseudonymous, meaning they ought not to inherently reveal users’ identities. The Travel Rule undermines this principle by linking personal information to blockchain addresses, significantly increasing the risk of the information’s improper exposure and use, which has been the focus of subsequent FATF guidance. The requirement creates centralized databases that become attractive targets for cyberattacks, attempts at which grow increasingly frequent, exposing millions of individuals to identity theft and financial fraud. Depending on how it is applied across various jurisdictions globally, variations of the Travel Rule have the potential to threaten the very principles on which blockchain technology and security stands (*i.e.*, decentralization, permissionlessness), as well as uses of many privacy-preserving tools and techniques (e.g., mixers, privacy coins, or zero-knowledge proofs), which are critical to innovation in this sector and are overwhelmingly purposed solely for lawful uses. See Suzie Violet Ward, *New EU Rules Could Threaten Your Security: What You Need to Know*, FORBES: DIGITAL ASSETS (Jan. 7, 2024), <https://www.forbes.com/sites/digital-assets/2025/01/07/new-eu-rules-threaten-your-security--what-you-need-to-know/>; SHYFT NETWORK: NEWSROOM, *The FATF Travel Rule: Implications for Privacy and Data Protection* (Apr. 6, 2023), https://www.shyft.network/newsroom/the-fatf-travel-rule-implications-for-privacy-and-data-protection?utm_source=chatgpt.com; 21ANALYTICS: BLOG, *GDPR and Privacy within the FATF Travel Rule* (Jan. 24, 2022), https://www.21analytics.ch/blog/gdpr-and-privacy-within-the-fatf-travel-rule?utm_source=chatgpt.com;

interface design can make interacting with decentralized services more intuitive. Institutions that lend credibility and stability—such as reputable custodians, insurance providers, and standardized compliance frameworks—may encourage risk-averse consumers and businesses to test the waters. Improvements in underlying protocols, combined with industry-led best practices and regulatory clarity, will likely help reassure skeptics. As trust deepens, interfaces improve, and scalability solutions come online, digital assets and blockchain infrastructure will likely gradually become indispensable components of daily commerce and information exchange.

Future trends in emerging industries and technologies.

Despite regulatory uncertainty and a wide array of other significant challenges, innovation in blockchain and related technologies is poised to advance. The tokenization of real-world assets (“**RWAs**”)—such as real estate, carbon credits, or supply chain inventory—promises to broaden access to previously illiquid markets, accelerate settlement times, and diversify investment opportunities. Plus, further developments in decentralized physical infrastructure networks (“**DePINs**”) could encourage cross-industry collaborations, aligning incentives among infrastructure providers and end users, and catalyzing a wave of bottom-up infrastructure deployment in telecommunications, energy grids, and beyond.

Interoperability solutions will gain traction as developers refine cross-chain protocols, enabling seamless asset transfers and communication between disparate networks. Combined with continued integration with AI (*artificial intelligence*), machine learning, and internet of things (“**IoT**”) technologies, blockchain- and distributed ledger-based systems could one day in the near future become the digital backbone of highly automated, data-driven environments.

Forthcoming developments might include further advancements in machine-to-machine payments, information provenance verifications, and the overall resilience of decentralized systems. In tandem, ongoing evolutions in decentralized governance structures could reshape how industry participants structure business operations, decision-making requirements, and community participation. Collectively, these changes might influence the way future projects perform protocol upgrades or make treasury allocations, or they could help ensure the efforts of developers are better aligned with user interests and more adaptable to market changes.

Global considerations.

The U.S. regulatory approach, or lack thereof, will shape its global influence. The EU’s MiCA framework is now in full force, and jurisdictions like Singapore, Hong Kong, and Dubai are actively refining their policies. If U.S. lawmakers remain mired in partisan stalemates and fail to offer a competing regime soon, then they risk ceding the nation’s leadership in emerging technologies and potentially global finance. Abroad, forward-looking governments are courting entrepreneurs in these industries with stable, innovation-friendly regulations. The cross-border nature of digital assets magnifies these dynamics, because capital, talent, and business models are increasingly mobile.

The industry’s original ethos—challenging entrenched wealth and power structures—has met with the complexities of real-world implementation. Incumbent financial institutions have adapted to leverage permissioned networks and private infrastructures, often with government support, while open, permissionless protocols face consistent regulatory skepticism. Nevertheless, core attributes of blockchain

technology and distributed systems—resilience, transparency, and decentralization—could prove invaluable amid rising inflationary pressures, supply chain uncertainties, and geopolitical tensions. As adoption continues to grow, the U.S. will need to navigate the delicate balance between enabling technological progress and safeguarding the public interest.

A call to action.

As this article has illustrated, the path forward for digital assets, blockchain technology, and associated emerging industries is neither linear nor guaranteed. Regulatory uncertainty, cybersecurity risks, privacy pressures, and reputational hurdles complicate the terrain. Yet, these challenges also represent opportunities for stakeholders to engage in meaningful dialogue and work toward principle-based frameworks that nurture innovation while preserving consumer protections, economic stability, and the rule of law.

Policymakers and regulators must recognize that the traditional, reactive approach to financial rulemaking would likely be ill suited to adapt to rapidly evolving technology sectors. Instead, proactive and flexible, principles-based policies can help guide the industry toward responsible growth, ensuring that the U.S. remains a competitive environment for development.

Regardless of what other factors might be at play, industry participants, advocacy groups, regulators, and international standard-setters should seek to collaborate on common standards and ethical guidelines, channeling the collective energy of the community into constructive outcomes. By pursuing clarity, inclusivity, and foresight, the U.S. and other global players can seize the promise of these transformative technologies.

The years ahead could prove pivotal, as today’s debates and decisions shape the financial systems, markets, and economic structures of tomorrow. If all stakeholders commit to balancing innovation with prudence, decentralized architectures can serve as catalysts for equitable growth, engendering trust, efficiency, and resilience within the international economy.

Have questions or want to chat? Feel free to [get in touch](#).

DISCLAIMER

By visiting DLx Law’s website (at <http://https://dlxlaw.com/>) or reading this or other content included on the website, regardless of whether you read it in other formats or in other locations, you represent that you acknowledge and understand the website’s legal disclaimer (<https://dlxlaw.com/legal-disclaimer/>) and agree to its terms & conditions (<https://dlxlaw.com/terms-and-conditions/>).
