
CHAMBERS GLOBAL PRACTICE GUIDES

Blockchain & Crypto-Assets 2026

Definitive global law guides offering
comparative analysis from top-ranked lawyers

USA: Law and Practice

Gregory Strong, Sarah W. Chen, Brian Farber and Amil Sumaiya Malik
Cahill Gordon & Reindel LLP





Law and Practice

Contributed by:

Gregory Strong, Sarah W. Chen, Brian Farber and Amil Sumaiya Malik
Cahill Gordon & Reindel LLP

Contents

1. Overview of Blockchain and Crypto-Assets p.4

- 1.1 Blockchain p.4
- 1.2 Crypto-Assets p.6

2. Regulation p.8

- 2.1 Regulators and International Alignment p.8
- 2.2 Crypto-Asset Regulatory Frameworks p.12
- 2.3 Regulated Firms and Legal Wrappers p.12
- 2.4 Token Issuance p.13
- 2.5 Market Abuse p.14
- 2.6 Non-Compliance p.15

3. Licensing and Set-Up Requirements p.15

- 3.1 Licensing Requirements p.15
- 3.2 Set-Up Requirements p.15
- 3.3 Change of Control p.15
- 3.4 Passporting p.15

4. Cross-Border Services p.16

- 4.1 Marketing p.16
- 4.2 White Labelling p.16

5. Decentralised Finance p.16

- 5.1 Ability to Use DeFi p.16
- 5.2 DeFi Structures p.16
- 5.3 Liability p.17

6. Payments and Stablecoins p.17

- 6.1 Payments p.17
- 6.2 Stablecoins p.17

7. Tokenisation and Real-World Assets p.18

- 7.1 Treatment p.18

Cahill Gordon & Reindel LLP is the premier destination for clients seeking counsel to help them resolve their most important, most challenging, and most sensitive legal and business problems relating to digital assets and other emerging technologies. The firm is entrepreneurial, creative, practical, responsive and relentless in its efforts to achieve clients' goals. Leveraging Cahill's more than century-long track record of excellence and innovation in guiding traditional finan-

cial institutions through seismic transformations in the structure and regulation of capital formation and trading markets, the firm's CahillNXT practice is now at the forefront of helping clients navigate the maze of risks and opportunities that flow from the world's next great financial revolution arising from the advent of blockchain technology, cryptocurrency transactions, Web3 (or Web 3.0) development, decentralised finance (DeFi) and other emerging technologies.

Authors



Gregory Strong has been advising clients engaging with blockchain and crypto-assets since 2018. He provides strategic regulatory advice with a focus on securities, commodities, and consumer

protection laws and regulations. He has successfully represented clients before the Securities and Exchange Commission, the Commodity Futures Trading Commission, state securities regulators, and various other regulators. He has also worked on cutting-edge litigation and transactions involving crypto-assets.



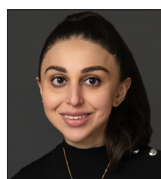
Sarah W. Chen advises clients on matters in the digital assets and emerging technology space, including M&A, venture capital investments, securities, financial regulatory and general corporate matters. She

represents clients ranging from blockchain development companies, foundation entities, digital asset marketplaces and tokenisation platforms to venture capital firms, fintech companies and traditional financial institutions, providing legal advice on securities, commodities, and other laws and regulations that apply to digital assets activity and the use of blockchain technology.



Brian Farber is counsel in the New York office of CahillNXT, Cahill's globally recognised Digital Assets and Emerging Technology practice. Brian advises clients on all matters in the space of digital assets, including

general corporate, mergers and acquisitions, capital markets transactions and securities regulatory. Brian also has deep experience of working with product and development teams to design digital asset products in a compliant manner, and guiding regulators through the products' underlying technology. Prior to joining, Brian was the general counsel of an industry-leading tokenisation platform and blockchain-enabled transfer agent.



Amil Sumaiya Malik focuses her practice on regulatory and litigation matters specific to digital assets, decentralised finance and emerging technology.

Cahill Gordon & Reindel LLP

32 Old Slip
New York
NY 10005
USA

Tel: +1 212 701 3000
Fax: +1 212 269 5420
Email: MTomsky@cahill.com
Web: www.cahill.com



1. Overview of Blockchain and Crypto-Assets

1.1 Blockchain

1.1.1 Evolution of Uses of Blockchain

The United States (USA) is home to many participants engaging with blockchain technology and crypto-assets. These include:

- crypto-asset trading platforms;
- custodians of crypto-assets; and
- developers of layer 1 blockchain networks, layer 2 networks, permissioned blockchain networks, and decentralised applications.

The USA has also been a centre of innovation when it comes to the integration of blockchain technology and crypto-assets and traditional financial services, including with respect to the tokenisation of real-world assets.

Under the Biden administration, there had been a sharp increase in enforcement actions, and litigation brought by agencies such as the Securities and Exchange Commission (SEC), the Commodity Futures Trading Commission (CFTC) and the Department of Justice (DOJ). Regulatory pressure continued through early 2025 in the lead up to the change in administration and the inauguration of President Donald J Trump.

The change in administration in early 2025, however, ushered in a meaningful shift in the US regulatory approach to digital assets. While prior years were characterised by an enforcement-driven posture – particularly by the SEC – the current approach reflects

a greater emphasis on providing forward-looking guidance, interagency co-ordination and legislative development.

Key developments include:

- the issuance of several Executive Orders related to digital assets, including Executive Order 14178 – Strengthening American Leadership in Digital Financial Technology and Executive Order 14233 – Establishment of the Strategic Bitcoin Reserve and US Digital Asset Stockpile;
- the formation of the SEC Crypto Task Force and a variety of SEC guidance with respect to crypto-assets;
- the enactment of a Memorandum of Understanding (MOU) between the SEC and CFTC to guide co-ordination and collaboration between the agencies;
- the passage of the Guiding and Establishing National Innovation for US Stablecoins (GENIUS) Act, establishing a federal framework for certain digital asset activities (including stablecoins); and
- ongoing efforts in Congress to advance broader digital asset market structure legislation.

US businesses are also using blockchain technology in a wide variety of ways, including:

- crypto-asset trading platforms;
- crypto-asset custody;
- securities issuance and record-keeping;
- securities clearing and settlement;
- gaming;
- art, collectibles and fan engagement platforms;
- protocol and software development;

- tokenised real world assets;
- payments;
- trade finance;
- logistics and tracking goods; and
- self-sovereign identity.

1.1.2 Regulatory Sandbox

There are currently no regulatory sandbox programmes in the USA specifically geared towards blockchain projects at the federal level. However, the SEC Crypto Task Force has indicated that it is evaluating whether to develop sandbox-type frameworks or other forms of tailored regulatory relief for limited, experimental blockchain and tokenisation use cases.

At the state level, several states – including Wyoming and Utah – have implemented regulatory sandbox programmes that expressly permit testing of blockchain-based products and services under modified regulatory requirements. Other states, such as Arizona, Kentucky, Florida, West Virginia and Nevada, have adopted broader sandbox frameworks for emerging technologies generally.

1.1.3 Regulation of Blockchain Technology

There is not yet a single, comprehensive regulatory regime applicable to market participants using blockchain technology or digital assets. Instead, a variety of traditional regulatory regimes may apply depending on the activities and the relevant facts and circumstances.

Recent legislative developments – particularly the passage of the GENIUS Act, which establishes a federal framework for payment stablecoins, and ongoing efforts in Congress to advance broader market structure legislation – indicate that a more defined federal regulatory framework is beginning to take shape. At the same time, US regulators continue to exercise oversight through existing authorities, reflecting an approach that seeks to balance innovation with risk mitigation rather than prohibit blockchain-based activity outright.

For an overview of the regulatory agencies in the USA that are relevant to the use of blockchain technology or digital assets, please refer to **2.1 Regulators and International Alignment**.

As discussed in **1.1.1 Evolution of Uses of Blockchain**, the current regulatory posture reflects a greater willingness to provide clarity and support innovation, while continuing to pursue enforcement where conduct falls within existing statutory frameworks.

With respect to blockchain technology used without crypto-assets, there is no dedicated regulatory framework. Its use is governed through existing legal regimes – including those relating to outsourcing, operational risk, cybersecurity and third-party service providers – under a technology-neutral approach.

Data privacy laws are enacted at the state level in the USA. There are differing obligations in each state with respect to data privacy. Practically speaking, this means that companies with a national footprint will seek to comply with the most robust state-level data privacy law. The California Consumer Privacy Act (CCPA) is one of the most robust state data privacy laws, and became effective in 2020.

Among other things, the CCPA provides consumers with the following rights:

- the right to access data collected about them by covered businesses;
- the right to delete that data; and
- the right to opt out of data collection altogether.

Covered businesses also need to provide consumers with a privacy notice, with two or more methods to opt out of the sale of personal information, and are prohibited from using opt-out mechanisms that make it difficult for a consumer to execute and have the effect of subverting the consumer's choice to opt out. The CCPA does not directly implicate blockchain, but any covered business using blockchain to gather, store or refer to customer information should have compliance with the CCPA in mind. These requirements can create tension with certain features of blockchain systems – particularly immutability – where deleting or modifying data may not be feasible, requiring firms to adopt architectural or compliance-based workarounds (such as off-chain storage or data minimisation).

Similar data protection laws have been passed in other states including Virginia, Connecticut, Texas and

Colorado, as have data breach reporting statutes. Although these laws do not specifically apply to the use of blockchain-based products or services, they contribute to an increasingly fragmented, state-level regulatory framework in the absence of a comprehensive federal regime.

1.1.4 Smart Contracts

The general view in the US legal community is that private contractual arrangements that are executable, in whole or in part, using blockchain or distributed ledger technology are valid and enforceable, assuming the elements necessary to form a contract are present – offer, acceptance, the intention to be legally bound and consideration. Whether a smart contract is coded to reflect the intentions of the parties is a separate fact-specific question.

1.1.5 Industry and Trade Bodies

There are no self-regulatory organisations in the USA specifically dedicated to blockchain or digital assets. There are a variety of trade groups dedicated to blockchain and digital assets, but none of them performs a formal regulatory or even quasi-regulatory function. Instead, these trade groups advocate on behalf of their members with respect to the adoption and regulation of blockchain technology and digital assets. There are, however, self-regulatory organisations associated with the securities and commodities industries that do have regulatory authority that may be relevant to blockchain and digital assets under certain circumstances, and these are discussed below.

The Financial Industry Regulatory Authority (FINRA)

FINRA is a government-authorised organisation tasked with the oversight of US-registered securities broker-dealers to ensure that they operate fairly and honestly. FINRA works under the supervision of the SEC and writes rules governing the activities of broker-dealers, examines broker-dealers for compliance with those rules, promotes market transparency to protect market integrity, and provides investor education.

FINRA has taken a specific interest in activities involving digital assets. It joined the SEC in putting out a joint statement regarding broker-dealer custody of

digital asset securities in July 2019. The release was withdrawn in May 2025.

The National Futures Association (NFA)

The NFA is an industry-wide self-regulatory organisation for the commodity derivatives industry. It is a registered futures association designated by the CFTC and registers a number of different participants in the commodities derivatives markets. The NFA's focus is to safeguard the derivatives markets, protect investors and ensure that members meet their regulatory responsibilities.

Trade Associations

There are a variety of trade associations in the United States that represent participants in the blockchain and digital assets space, including:

- the Crypto Council for Innovation;
- the Digital Chamber of Commerce;
- the Blockchain Association;
- the Global Blockchain Business Council; and
- the Wall Street Blockchain Association.

1.2 Crypto-Assets

1.2.1 Property Considerations

There is no definitive statutory or judicial framework governing how ownership of a digital asset is determined in the USA. In practice, though, control over the private key associated with a digital asset is often treated as evidence of ownership. However, ownership ultimately depends on the legal relationship between the parties, including custodial arrangements and contractual terms, which may diverge from on-chain control. That said, there are many instances in which the owner of a digital asset transfers control to a third party in order for the third party to perform a certain function, in which case the owner may retain its ownership right to the asset pursuant to the contractual terms of the owner's agreement with the third party.

Digital assets may be used as collateral in the USA. To that end, lenders may attempt to perfect a security interest in a digital asset pledged as collateral under the applicable provisions of the Uniform Commercial Code (UCC) — a *model statute* drafted by the Uniform Law Commission (ULC). Transacting parties typically structure the arrangement as a “security entitlement”

under the UCC – classifying the pledged asset as a “financial asset”, the borrower’s account as a “securities account” and the lender as a “securities intermediary” – which enables perfection of a security interest in the collateral by the lender.

In July 2022, amendments to the UCC were approved by the ULC that create a new Article 12 which governs the transfer of property rights in a “controllable electronic record” (CER) and revise the existing Article 9 to allow perfection of a security interest in a CER by obtaining control of the CER. Once the amendments are adopted and in effect in a particular state, the parties to a digital asset transaction under that state’s law can benefit from the new Article 12 and updated Article 9. By early 2026, approximately 30 states had adopted the 2022 amendments.

1.2.2 Access to Banking

There are no formal, categorical restrictions in the United States on the banking or payment partners that firms providing crypto-asset services may use. However, in practice, access to banking services has historically been constrained by risk-based decision-making by financial institutions, driven in part by regulatory expectations relating to anti-money laundering (AML), sanctions compliance, safety and soundness, and reputational risk. As a result, crypto-asset firms have, at times, faced challenges in obtaining and maintaining banking relationships, even where their activities are lawful.

That landscape has begun to shift, with several 2025 federal initiatives reflecting a more permissive and co-ordinated regulatory posture on digital assets. On 23 January 2025, President Trump signed an Executive Order creating the Presidential Working Group on Digital Asset Markets. This group is tasked with evaluating the potential creation of a national digital asset stockpile and proposing criteria for establishing such a reserve, among other responsibilities.

Federal banking regulators have also taken steps to reduce procedural barriers to crypto-related activities and clarify that such activities may be conducted within existing supervisory frameworks. On 7 March 2025, the Office of the Comptroller of the Currency issued Interpretive Letter 1183, confirming that

national banks and federal savings associations may engage in crypto-asset custody, certain stablecoin activities, and participation in distributed ledger networks. The letter rescinded prior guidance that had required supervisory non-objection and emphasised that banks should apply existing risk management frameworks to such activities.

On 28 March 2025, the Federal Deposit Insurance Corporation (FDIC) issued new guidance (FIL-7-2025) clarifying that supervised institutions may engage in certain permissible crypto-related activities without prior FDIC approval, provided they manage associated risks adequately.

In April 2025, the Federal Reserve withdrew prior guidance that had required state member banks to provide advance notice before engaging in certain crypto-related activities.

Subsequent OCC Interpretive Letters in 2025 provided additional clarity regarding the scope of permissible crypto-related banking activities. Interpretive Letter 1184, issued on 7 May 2025, indicated that national banks providing crypto-asset custody services may also facilitate customer execution and trading on an incidental basis. Interpretive Letter 1186, issued on 18 November 2025, addressed the ability of banks to hold de minimis amounts of crypto-assets to pay network fees (eg, “gas”) in connection with custody and payment services. Interpretive Letter 1188, issued on 9 December 2025, addressed the circumstances under which banks may engage in riskless principal crypto-asset transactions, including for tokenised securities and non-security crypto-assets, as an extension of existing brokerage and custody authorities.

These developments have coincided with increased interest among digital asset firms in obtaining OCC national trust bank charters as a potential federal pathway for engaging in crypto-related custody and related services. Anchorage Digital Bank, NA became operational as a federally chartered national trust bank in January 2021, subject to OCC supervisory conditions typical for de novo institutions. In December 2025, OCC announced its conditional approval of five national trust bank charter applications, including Circle, Ripple, BitGo, Fidelity Digital Assets and Paxos.

National trust banks operate under a limited-purpose charter focused on fiduciary and custodial activities and may engage in crypto-asset custody and related services, subject to applicable supervisory expectations. For firms with nationwide operations, these charters can offer efficiencies by pre-empting state-level licensing requirements for certain activities such as custody and money transmission.

1.2.3 ESG/Sustainable Finance

There are no ESG/sustainable finance requirements in the USA that specifically apply to digital assets. Though there have been significant mandatory ESG disclosures that the SEC has required of reporting organisations in the past, recently the SEC has been stepping back in regulating the area. Certain legislative proposals regarding ESG and crypto-assets have been introduced, but none have passed and become law.

1.2.4 Tax

In 2014, the Internal Revenue Service (IRS) issued Notice 2014-21, its first guidance on digital assets. Notice 2014-21 provides that virtual currencies are treated as non-currency property for US tax purposes, with the result that most dispositions of digital assets for cash, services or other digital assets are taxable dispositions of capital assets for US tax purposes. Since then, the Treasury Department and the IRS have continued to release piecemeal, non-binding guidance on the substantive US tax treatment of digital asset transactions. That guidance includes:

- Revenue Ruling 2019-24, which concludes that taxpayers who gain dominion and control over new tokens by reason of a hard fork are taxed at ordinary rates on the tokens at that time;
- Revenue Ruling 2023-14, which similarly treats validator rewards as ordinary income when validators gain dominion and control over them;
- Chief Counsel Memorandum 202316008, which treats the Ethereum network's upgrade to a proof-of-stake consensus mechanism as non-taxable to holders of the network's native token; and
- Revenue Procedure 2025-31, which provides rules under which "crypto ETFs" treated as grantor trusts can stake their digital assets without becoming taxable as corporations.

In addition, in July 2024, final regulations significantly expanded tax reporting by brokers in digital assets.

However, taxpayers still have very little substantive guidance on the US tax treatment of digital asset transactions. For example, while Notice 2014-21 treats virtual currencies as "property", it does not indicate what *kind* of property they are, or whether all virtual currencies are treated similarly for US tax purposes. As a result, there remains significant uncertainty as to the US tax treatment of liquid staking tokens, vault tokens, liquidity provider tokens, governance tokens and non-fungible tokens, and whether bridging, wrapping and liquidity provision are treated as taxable events. The US tax consequences for non-US and tax-exempt investors of holding and trading digital assets also remain uncertain.

1.2.5 Insolvency

There are no specific resolution or insolvency requirements or regimes for digital asset firms in the USA. Traditional bankruptcy proceedings have been used in the bankruptcies of several significant digital asset companies in the USA over the last two years. These include FTX, Voyager, Celsius and others.

1.2.6 Industry and Trade Bodies

See 1.1.5 Industry and Trade Bodies.

2. Regulation

2.1 Regulators and International Alignment

There are a number of regulatory bodies in the USA that are relevant to blockchain and digital assets.

The Securities and Exchange Commission (SEC)

The SEC has broad regulatory authority over securities transactions, securities professionals, and securities intermediaries in the USA. The threshold question that determines whether the SEC has authority with respect to blockchain or digital assets is whether a "security" is involved. The definition of the term "security" in both the Securities Act of 1933, as amended (the "Securities Act") and the Securities Exchange Act of 1934, as amended (the "Exchange Act") includes a number of enumerated types of securities, including the term "investment contract". When a contract,

transaction or scheme does not fall plainly within one of the other enumerated types of securities in the definitions of the term “security”, it may still be treated as a security if it is deemed to constitute an investment contract.

The test for whether a particular scheme is an investment contract was established in the Supreme Court’s *Howey* decision. The test looks to “whether the scheme involves an investment of money in a common enterprise with profits to come solely from the efforts of others”. Whether a particular transaction involves an investment contract is facts and circumstances dependent, grounded in the economic realities of the transaction.

The SEC has provided recent guidance on disclosure obligations in crypto-asset markets. In a 10 April 2025 statement, the Division of Corporation Finance outlined how existing registration and disclosure requirements under the Securities Act and Exchange Act apply to offerings involving crypto-assets and related businesses. The guidance emphasises that issuers must provide tailored, material disclosures regarding their business, the role of any associated network or application, and the rights and characteristics of any token or crypto-asset. It also highlights the need for clear risk factor disclosure addressing technological, operational and regulatory risks, reflecting the SEC’s continued application of traditional disclosure principles to digital asset markets.

Most recently, on 17 March 2026, the SEC and CFTC issued a joint interpretation creating a “token taxonomy” that aims to draw clear lines between the SEC’s and CFTC’s jurisdiction over crypto-assets. Though the guidance leaves questions unanswered, it does confirm the position that most crypto-assets are not themselves securities (though they may still be marketed or sold as part of an investment contract).

The Commodity Futures Trading Commission (CFTC)

The CFTC has broad regulatory authority over derivative markets for commodities, and general anti-fraud and anti-manipulation authority over the spot markets for commodities pursuant to the Commodity Exchange Act (CEA). Derivatives transactions subject

to CFTC jurisdiction include futures, options, swaps and leveraged retail commodities transactions under the CEA. In recent years, the CFTC has asserted – and courts have affirmed – that certain digital assets qualify as “commodities” under the CEA. The agency has explicitly stated that bitcoin and ether are commodities subject to its jurisdiction, a conclusion that is widely accepted.

In 2025, the CFTC signalled a shift in its regulatory approach to digital asset derivatives towards integrating these products into its existing regulatory framework, rather than treating them as a distinct or heightened risk category. On 27–28 March 2025, the CFTC rescinded Advisories 18-14 and 23-07, which had imposed heightened expectations for virtual currency derivative listings and clearing reviews, citing increased market maturity and a desire to treat digital asset products consistently with others.

On 21 April 2025, CFTC staff issued a request for information (RFI) seeking public comment on the potential uses, benefits and risks associated with perpetual futures contracts – derivatives that track the price of an underlying asset without an expiry date, which are widely used in crypto markets but raise novel questions regarding leverage, liquidity and risk transmission. The CFTC has also sought input on broader market developments, including the implications of near-continuous (24/7) trading.

Most recently, on 11 March 2026, the CFTC and SEC entered into an MOU, as referenced in **1.1.1 Evolution of Uses of Blockchain**, to enhance co-ordination and information sharing in overseeing digital asset markets, reflecting ongoing efforts to address jurisdictional overlap and promote a more unified regulatory approach.

The Treasury Department and the Financial Crimes Enforcement Network (FinCEN)

FinCEN is the arm of the US Treasury Department that is responsible, in the first instance, for enforcing the US federal laws and regulations relating to crimes involving the transmission of money, frequently working in conjunction with other federal agencies and bureaus, including the Federal Bureau of Investigation and the National Security Agency. This includes enforcing the

Bank Secrecy Act (BSA), which is a comprehensive anti-money laundering (AML)/combating the financing of terrorism (CTF) statute. The BSA mandates that “financial institutions”, which include “money services businesses” and “money transmitters”, must collect and retain information about their customers and share that information with FinCEN. FinCEN guidance from May 2019 examined a number of hypothetical business models involving digital assets to provide guidance with respect to the application of the BSA. Not surprisingly, many businesses engaging in activity involving “convertible virtual currency”, crypto-assets used as a substitute for fiat currency, have an obligation to comply with the BSA.

The Treasury Department and the Office of Foreign Assets Control (OFAC)

OFAC is a division of the US Treasury Department that administers and enforces economic and trade sanctions to promote US national security and foreign policy objectives. OFAC can take enforcement action against entities in the USA that violate sanctions programmes. OFAC has taken several such actions relating to digital asset transactions – for example, in settled actions against BitGo, BitPay and Poloniex, OFAC emphasised that US sanctions compliance obligations apply to all US persons, and encouraged companies that provide digital asset services to implement controls commensurate with their risk profile, as part of a risk-based approach to US sanctions compliance. Further, OFAC published Sanctions Compliance Guidance for the Virtual Currency Industry in October 2021 to assist participants in the virtual currency industry with navigating and complying with OFAC sanctions.

In August 2022, OFAC designated smart contracts associated with the operation of Tornado Cash, a virtual currency mixer, to the Specially Designated Nationals (SDN) list, effectively prohibiting US persons from engaging in transactions with these contract addresses. This was a significant action and the first time smart contract addresses were added to the SDN list. However, in late 2024, the Fifth Circuit ruled that OFAC exceeded its statutory authority by adding the suite of smart contract addresses comprising Tornado Cash to the SDN list, because such smart contracts are not “property” subject to the sanctions jurisdiction asserted by OFAC within the meaning of

the International Emergency Economic Powers Act. Since then, OFAC has removed the Tornado Cash smart contract addresses from the SDN list, reversing its earlier position.

The Consumer Financial Protection Bureau (CFPB)

The CFPB has authority pursuant to the Consumer Financial Protection Act (CFPA) to address unfair, deceptive or abusive acts and practices (UDAAP) with respect to financial products offered primarily for consumer use by certain “covered persons” as defined by the CFPA. To date, the CFPB has not been active in the crypto-asset space.

However, the CFPB issued significant guidance just prior to the change in administration clarifying how Regulation E of the Electronic Fund Transfer Act (EFTA) applies to digital payments, particularly in the context of rising fraud and person-to-person (P2P) payment platforms. While the CFPB had signalled plans to expand oversight – including by examining non-bank financial companies that pose consumer risks and potentially applying that scrutiny to digital asset products – its capacity to act has been substantially undermined by recent court rulings. In particular, decisions questioning the constitutionality of its funding structure have raised doubts about the CFPB’s future enforcement authority and agenda, which may delay or constrain the Agency’s ability to regulate emerging financial technologies, despite prior ambitions to increase its activity in this area.

The Department of Justice (DOJ)

The DOJ enforces federal criminal laws, including those involving securities fraud, insider trading and market manipulation, often working in parallel with civil regulators such as the SEC. While the SEC pursues civil enforcement, the DOJ has authority to bring criminal securities charges which are often paired with other alleged federal crimes such as wire fraud.

On 7 April 2025, the DOJ issued a memo, “Ending Regulation By Prosecution”, signalling a significant shift in its approach to enforcement related to blockchain technology and crypto-assets. The memo deprioritises actions against software developers in favour of targeting those who use digital assets to facilitate serious crimes such as terrorism and traf-

ficking, reflecting the Trump administration's broader policy of reducing regulatory barriers to crypto-asset innovation. This shift aligns directly with Executive Order 14178's stated goal of "protecting and promoting" access to blockchain networks and banking services for lawful users without persecution.

State Attorneys General

State enforcement actions – led by Attorneys General (AGs), securities regulators, and money transmission authorities – are expected to intensify as federal oversight of digital assets evolves. State AGs have broad authority under consumer protection laws, and some State AGs also enforce state securities laws.

For example, less than two months after the SEC dropped its lawsuit against Coinbase, on 18 April 2025 the Oregon State AG sued Coinbase for alleged violations of the Oregon Securities Law, asserting theories similar to those previously advanced by the SEC, namely that Coinbase unlawfully encouraged the sale of unregistered cryptocurrencies. As federal agencies reassess their regulatory posture, state-level enforcement is likely to become a more prominent mechanism for oversight.

State Money Transmission Regulators

Historically in the USA, states rather than the federal government have been the primary regulators of "money transmitters". Each state, other than the state of Montana, has independently passed a statute that defines the activities that constitute money transmission in that state. State laws generally define a money transmitter very broadly and typically include any entity that engages in "receiving money for transmission" or "transmitting money" or issuing or selling stored value.

The scope of each state's law, and its application to virtual currency, is dependent on how broadly the definitions of "money" and "money transmission" are interpreted by the applicable state regulator. As a result, exchanging virtual currency or facilitating payments in virtual currency may be subject to state-by-state regulation as money transmission.

While federal law requires only registration of money transmitters, state law requires licensing. It is signifi-

cant to note that money transmission regulations are extraterritorial; to engage in money transmission a person must have a licence in the state in which it is operating and every state in which it has customers. States have taken different positions with respect to whether crypto-asset activities fall within the definition of money transmission. However, many states have adopted the model Money Transmission Modernization Act, which has promoted some uniformity across those states.

State Securities Regulators

State securities regulators enforce and administer state-specific securities laws. These laws are often referred to as "blue sky" laws and are generally similar from one state to the next, but certain aspects can vary significantly. Many state securities statutes are derived from either the 1956 or 2002 version of the Uniform Securities Act.

State securities regulators have been very active in regulating cryptocurrency-related investment products and the sale of digital asset securities. In the cryptocurrency space, state securities regulators were first to file enforcement actions with respect to centralised lending businesses offering consumers interest payments in respect of cryptocurrency deposits. State securities regulators filed cases against BlockFi, Celsius and Voyager prior to their collapses, alleging that their products constituted investment contracts under the *Howey* test that were required to be registered under the Securities Act or offered pursuant to an exemption from registration.

International Standards

The USA has implemented international standards in several areas impacting blockchain. Most notably, the USA has been a proponent of applying a corollary to the "Travel Rule" – a rule under the BSA that mandates that financial institutions transmit certain identifying information (such as the sender's and recipient's name, account number and location) with transfers of funds exceeding USD3,000 – to entities known as virtual asset service providers (VASPs) that process transactions involving crypto-assets. In 2018, the Financial Action Task Force (FATF), a multi-governmental organisation that sets global standards related to anti-money laundering, clarified how the FATF

standard – a set of 40 Recommendations that form the international framework for preventing money laundering and terrorist financing – apply to activities or operations involving virtual assets, and imposed a corollary to the Funds Travel Rule on VASPs that process virtual asset transfers.

In October 2021, the FATF updated its recommended guidance regarding virtual assets and VASPs. Notably, the FATF guidance broadly interprets the definition of a VASP to include “a central party with some measure of involvement” with a decentralised application. If adopted in a specific jurisdiction, this broad interpretation would potentially bring a variety of parties within the definition of a VASP and subject them to compliance with AML/CFT laws in that jurisdiction.

It is not surprising that the US delegation to the FATF pushed for a global Funds Travel Rule corollary and the expansive interpretation of the entities that might be deemed VASPs. In doing so, the USA is attempting to promote AML/CFT compliance through global standard-setting, which would make it easier for the USA to enforce its domestic AML/CFT obligations as they apply to digital asset transactions and intermediaries.

Finally, under the Basel Committee’s prudential framework for crypto-asset exposures, member jurisdictions had previously agreed to implement standards by 1 January 2026 that would subject unbacked crypto-assets not meeting certain hedging recognition criteria to a 1250% risk weight – effectively requiring banks to hold capital equal to the full value of such exposures. However, US banking regulators have indicated that they do not intend to implement the Basel crypto-asset standards in their current form, opting instead to preserve regulatory flexibility and to promote innovation and competition.

2.2 Crypto-Asset Regulatory Frameworks

As discussed in **2.1 Regulators and International Alignment**, in the United States, there is still no single, comprehensive statutory framework governing the classification of digital assets. Broadly, securities are regulated by the SEC, while commodity derivatives are regulated by the CFTC. To the extent that fungible digital assets, or transactions in fungible digital assets,

are not regulated as securities, they would be treated as commodities and subject to CFTC’s anti-fraud and anti-manipulation jurisdiction in spot markets, as well as its broader jurisdiction over commodity derivatives.

Under existing US law, digital assets that are intended to be securities or “tokenised” securities are treated as securities. Fungible digital assets that are not themselves securities may nevertheless be transacted under circumstances that constitute “securities transactions”. Determining whether such circumstances exist requires application of the *Howey* test (discussed in **2.1 Regulators and International Alignment**), which is a facts-and-circumstances analysis and can be difficult for market participants to apply in practice.

Over the past 12–18 months, the SEC staff have issued a series of category-specific statements and interpretative materials addressing specific segments of the market, including meme coins, proof-of-work mining activities, and certain “covered stablecoins”. These statements generally reflect the view that not all crypto-assets, or activities involving them, fall within the scope of the federal securities laws, particularly where the asset does not convey rights to enterprise value or is not marketed based on the managerial efforts of others.

The Joint Interpretation (discussed in **2.1 Regulators and International Alignment**) and its accompanying taxonomy framework provide further clarity on when crypto-assets or related activities may fall within the SEC’s jurisdiction.

2.3 Regulated Firms and Legal Wrappers

In the USA, there are spot exchange-traded funds (ETFs) (eg, the SEC-approved Bitcoin and Ethereum products) that are typically organised as commodity or grantor trusts that own the underlying digital assets. Both spot ETFs and futures-based crypto funds are securities products subject to US securities laws. Both structures also face FINRA advertising standards, Exchange Act custody and anti-fraud rules, and must maintain market-surveillance agreements with their listing exchanges.

Specifically, starting in 2024, the SEC has been taking steps to facilitate institutional access to digital

assets through exchange-traded products (ETPs). Through the first quarter of 2024, the SEC approved the listing and trading of multiple spot Bitcoin ETPs, marking a significant shift in its approach to crypto-linked investment products. The SEC subsequently approved rule changes permitting the listing and trading of spot Ether ETFs in May 2024, and on 17 September 2025 approved generic listing standards for certain crypto-based ETPs, marking a shift from product-specific approvals to a more standardised, rules-based framework for market access. While these developments have contributed to increased institutional participation and inflows into crypto ETPs, the current landscape remains largely limited to bitcoin and ether, with a more limited but growing set of ETPs referencing other digital assets (such as SOL, XRP and DOT), which continue to face an evolving regulatory landscape.

2.4 Token Issuance

Tokenised securities are treated as securities in the USA. However, questions remain about the viability of tokenised securities, as they are not provided for in the UCC that gives states one set of rules for commercial transactions such as sales of goods, negotiable instruments, funds transfers, letters of credit, securities and secured lending. The UCC only recognises two categories of securities – certificated and uncertificated. Traditionally, certificated securities are represented by a physical certificate while uncertificated securities are represented as ledger entries in the books and records maintained by the issuer or its agent.

There is debate about whether a tokenised security can be certificated because the rights and obligations associated with the security are not reduced to writing on paper and electronic certificates are not provided for under the UCC. It may be possible to classify tokenised securities as uncertificated; however, there are specific rules regarding how uncertificated securities may be transacted under the UCC and recorded on the books and records of the issuer that may not be consistent with the manner in which blockchain-based assets are transferred in practice. Without clear recognition under the UCC, holders of tokenised securities may face legal risks in proving or defending their ownership rights, especially in cases

of insolvency or competing claims. This issue has been recognised by practitioners who are working on solutions under the UCC.

Guidance released on 28 January 2026 by the staff of the SEC's Divisions of Corporation Finance, Investment Management, and Trading and Markets underscores that tokenised securities may take multiple structural forms, including issuer-sponsored models in which ownership records are maintained on-chain, and third-party models that rely on custodial arrangements or synthetic exposure. In issuer-sponsored structures, the use of distributed ledger technology to maintain the "master securityholder file" does not alter the application of federal securities laws, even where ownership records are maintained partially or entirely on-chain. However, where third parties tokenise existing securities – particularly through custodial or synthetic arrangements – additional risks arise, including intermediary insolvency risk and potential divergence between the rights conveyed by the token and those associated with the underlying security.

Non-Fungible Tokens (NFTs)

There are no regulations in the USA that are specific to NFTs as such, but existing laws apply to these digital assets and activities involving them. Given their non-fungible nature, NFTs are unlikely to be considered "commodities". To the extent that an offer or sale of NFTs constitutes an investment contract under the *Howey* test, they could be classified as securities and subject to compliance with securities laws.

Additionally, offer and sale of NFTs as consumer products such as collectibles would be subject to consumer protection laws and regulations. Both federal and state consumer protection laws generally prohibit unfair or deceptive acts and practices with respect to consumer goods and services. Similar to other types of digital assets, those selling NFTs must also keep sanctions compliance in mind and take steps to avoid engaging in transactions with sanctioned individuals or individuals residing in sanctioned jurisdictions.

Meme Coins

On 27 February 2025, the SEC's Division of Corporation Finance issued a Staff Statement on Meme Coins, clarifying for the first time that typical meme coins are

presumptively not securities under federal securities laws. The SEC explained that meme coins – crypto-assets inspired by internet memes or trends and primarily purchased for entertainment, social interaction or speculation – generally do not meet the definition of a security. The Joint Interpretation (see **2.1 Regulators and International Alignment**) subsequently incorporated meme coins into a broader crypto-asset taxonomy, generally confirming this characterisation while noting that meme coins marketed with profit expectations tied to promoter efforts may still be assessed under *Howey*. At the same time, the release emphasised that meme coins marketed with profit expectations tied to promoter efforts, or otherwise embedded in a broader scheme, may still be treated as securities under a facts-and-circumstances analysis.

2.5 Market Abuse

Enforcement actions and judicial decisions arising from those actions have played an important role in shaping the application of existing laws to blockchain technology and digital assets.

Notable SEC Actions

In the securities law context, these decisions fall into two categories of cases – those involving initial allocations of digital assets and those that involve secondary transactions in tokens. Following the resignation of former SEC Chairman Gary Gensler, and the subsequent launch of the Crypto Task Force as well as the appointment of SEC Chairman Paul Atkins, in early 2025, the SEC dismissed several high-profile enforcement actions against major cryptocurrency firms, signalling a notable shift in its regulatory approach under new leadership. These dismissals, many filed “with prejudice”, indicate a significant change in the SEC’s stance towards cryptocurrency regulation, moving away from aggressive enforcement actions and towards a more collaborative and transparent approach. This includes the SEC’s enforcement actions against Coinbase, Payward (dba Kraken), Cumberland, Consensus and Dragonchain. The SEC has also closed investigations without enforcement actions against multiple firms, including reported investigation closures against Robinhood Crypto, Uniswap Labs and Crypto.com.

Separately, on 5 March 2026, the SEC filed a proposed final judgment in its action against Justin Sun, pursuant to which the SEC agreed to settle its wash trading claim against Rainberry, Inc, while dismissing, with prejudice, all remaining claims against Justin Sun, Tron Foundation Limited, BitTorrent Foundation Ltd, and Rainberry, Inc – effectively resolving one of the last remaining enforcement actions initiated under prior SEC Chairman Gary Gensler.

Notable CFTC Actions

In September 2023, the CFTC brought enforcement actions against three DeFi platforms – Opyn, Deridex and ZeroEx (0x) – alleging that each facilitated trading of derivatives or leveraged products without proper registration, regardless of decentralisation claims, in violation of the CEA. The charges included operating unregistered trading platforms, failing to register as futures commission merchants, and lacking required customer identification programmes. Each platform settled with the CFTC: Opyn paid a USD250,000 penalty, Deridex USD100,000 and ZeroEx USD200,000.

Notable Criminal Matters

On 20 November 2023, Sam Bankman-Fried was found guilty of two counts of wire fraud, two counts of conspiracy to commit wire fraud, conspiracy to commit securities fraud, conspiracy to commit commodities fraud and conspiracy to commit money laundering stemming from his activities at FTX and Alameda Research. He was later sentenced to 25 years in prison.

In August 2023, the DOJ filed a criminal indictment against two developers of Tornado Cash, an open-source privacy protocol that facilitates anonymous transactions by obscuring the origins of cryptocurrencies such as Bitcoin and Ether. The criminal case against the developers of the Tornado Cash software alleges that the developers engaged in a conspiracy to commit money laundering, conspiracy to commit sanctions violations, and conspiracy to operate an unlicensed money transmission business. The indictment alleged that the defendants created, operated and promoted Tornado Cash, a cryptocurrency mixer that facilitated more than USD1 billion in money laundering transactions, and laundered hundreds of millions of dollars for the Lazarus Group, the sanctioned

North Korean cybercrime organisation. In August 2025, a jury returned a mixed verdict, convicting one defendant of conspiracy to operate an unlicensed money transmitting business, while deadlocking on the money laundering and sanctions counts, resulting in a partial mistrial on those charges. Roman Storm now faces a potential retrial on the unresolved counts, with prosecutors seeking to proceed in October 2026.

In May 2024, the DOJ charged Anton and James Peraire-Bueno, brothers and MIT graduates, for allegedly orchestrating an illegal scheme that exploited Ethereum's transaction validation process to obtain approximately USD25 million in cryptocurrency within a span of 12 seconds. The DOJ's indictment accuses the brothers of manipulating MEV-Boost, a software used by Ethereum validators, to gain unauthorised access to pending private transactions – a practice known as Maximal Extractable Value (MEV) exploitation. This case is one of the first to target the integrity of blockchain validation mechanisms. The defendants challenged the charges, arguing that the actions were within the bounds of Ethereum's open and permissionless protocol, and that the DOJ's application of wire fraud statutes to this case represents an overreach. The case went to trial and a mistrial was declared as the jury could not reach a unanimous verdict. Prosecutors intend to retry the case.

2.6 Non-Compliance

See 2.5 Market Abuse.

3. Licensing and Set-Up Requirements

3.1 Licensing Requirements

There are no licensing regimes at the federal level in the USA that are specific to digital assets or activities in digital assets. However, there are several licensing or registration regimes that may apply, depending on the activities being undertaken. In the securities context, to the extent that digital assets or transactions in digital assets are deemed to be securities transactions, there are registration obligations with respect to intermediaries involved in those transactions, such as brokers, dealers, exchanges, investment advisers, investment companies, security-based swap dealers and clearing agencies.

With respect to activities involving derivatives on digital assets that are treated as commodities, there may be obligations to register as a futures commission merchant, designated contract market, commodity trading adviser, commodity pool operator, or swap dealer. Entities that engage in money transmission activities involving digital assets – generally defined as the acceptance of funds or value that substitutes for currency from one person and the transmission of those funds or value to another location or person by any means – may be required to obtain money transmission licences in the states in which they engage in those activities, as well as register as a money services business with FinCEN. Lastly, state licensing regimes, such as New York's BitLicense, may apply.

3.2 Set-Up Requirements

See 3.1 Licensing Requirements.

3.3 Change of Control

Digital asset firms that are licensed money transmitters and undergo a change of control will be required to engage with state money transmission regulators to provide notice of a change of control and obtain approval of the change of control.

Digital asset firms operating as broker-dealers, investment advisers, or OCC-chartered institutions are subject to analogous requirements under FINRA rules, the Investment Advisers Act of 1940, and the Change in Bank Control Act, respectively, each of which may require prior notice to or approval from the applicable regulator.

3.4 Passporting

There is no "passporting" regime in the USA. Authorisation in one state generally does not permit operation in others, and separate state-level licences are typically required. At the federal level, certain OCC charters (eg, national trust bank charters) may preempt some state licensing requirements, but do not extend extraterritorially.

4. Cross-Border Services

4.1 Marketing

There are no specific marketing requirements in the USA that apply to digital assets or activities in digital assets. The SEC prohibits touting of digital assets that it deems securities by paid promoters unless the compensation arrangements are publicly disclosed. Similarly, state securities regulators impose similar requirements. In addition, the Federal Trade Commission has put out guidance regarding the use of endorsements and testimonials in advertising and the disclosures required regarding material connections between endorsers and advertisers.

4.2 White Labelling

There is no formal “white-labelling” regime in the United States that permits an unlicensed firm to offer regulated services solely by relying on the licence of another entity.

In practice, white-label solutions are commonly used in areas such as payments, custody and trading infrastructure, where a licensed entity (eg, a bank, broker-dealer, or money transmitter) provides the regulated service, and a third-party firm offers the front-end interface or customer-facing experience. However, US regulators focus on the substance of the arrangement rather than its form. If the third party is effectively performing regulated functions – such as custody, execution or money transmission – it may be required to obtain its own licences or registrations. Licensed entities entering into white-label arrangements also remain responsible for compliance with applicable regulatory requirements, including AML, customer identification (KYC), consumer protection, and operational risk management.

5. Decentralised Finance

5.1 Ability to Use DeFi

DeFi activity is not prohibited as such in the United States. However, there is no bespoke regulatory framework for decentralised protocols. Activities conducted through DeFi infrastructure – such as trading, lending or custody – may trigger regulation under US securities laws, commodities laws, money transmis-

sion regimes, or AML and sanctions frameworks, depending on the facts and circumstances. The use of decentralised technology does not, in itself, remove an activity from the scope of applicable laws.

In practice, this means that activities conducted through DeFi infrastructure – such as trading, lending or custody – may trigger regulation under US securities laws, commodities laws, money transmission regimes, or AML and sanctions frameworks, depending on the facts and circumstances. The use of decentralised technology does not, in itself, remove an activity from the scope of applicable laws. Similarly, traditional firms may utilise DeFi infrastructure, provided they maintain compliance with applicable custody, AML/KYC, sanctions, and conduct requirements. In fact, on 13 April 2026, SEC staff issued guidance stating that certain non-custodial DeFi front-end interfaces may operate without broker-dealer registration where specified conditions are met, reflecting an effort to provide clearer parameters around permissible DeFi activity.

Regulators have also increasingly focused on the role of identifiable participants in DeFi ecosystems, including developers, governance participants, and service providers, particularly where those parties exercise control or derive economic benefit from the protocol. In practice, this results in a “function-over-form” approach, where DeFi activity is assessed based on the underlying economic activity rather than the technological structure through which it is conducted.

5.2 DeFi Structures

Consistent with the function-over-form approach described in **5.1 Ability to Use DeFi**, DeFi structures are assessed under existing regimes based on their functional characteristics.

In practice, setting up a DeFi structure in the United States typically involves forming one or more legal entities (eg, a Delaware corporation or LLC, or a Wyoming DAO LLC) and assessing the regulatory implications of the protocol's activities. Depending on the facts, this may include analysis under US securities laws (eg, whether governance tokens constitute “investment contracts”), commodities and derivatives regulation under the CEA, state-level money trans-

mission laws, and AML obligations under the Bank Secrecy Act.

Regulators have generally taken the position that the use of a DAO or other decentralised structure does not, in itself, remove an activity from the scope of applicable laws, particularly where there are identifiable persons exercising control or deriving economic benefit. Enforcement actions involving DeFi protocols have also reflected a substance-over-form approach. See **5.3 Liability** for more information.

5.3 Liability

As mentioned in **5.2 DeFi Structures**, regulators in the USA have taken the position that the use of smart contracts or DAO-based governance does not eliminate liability where there are identifiable persons or groups responsible for operating, controlling or benefiting from the protocol.

This approach is reflected in enforcement actions brought by the CFTC. In *CFTC v Ooki DAO*, the CFTC brought an action against a DAO alleged to be operating an unregistered derivatives trading platform. The court permitted the DAO to be treated as an unincorporated association and allowed service of process through the DAO's online governance forum. The court later entered default judgment against Ooki DAO.

The case also reflects the CFTC's view that participation in DAO governance may, depending on the facts, give rise to liability where individuals are sufficiently involved in the operation of the protocol.

In the civil litigation context, numerous class actions have been filed alleging that DAOs operate as general partnerships and seeking to hold significant DAO participants responsible for the activities of the DAO as general partners. For example, in *Samuels v Lido DAO*, et al in the Northern District of California, motion to dismiss was denied and the court found that the allegations in the complaint adequately alleged that the Lido DAO was a general partnership.

6. Payments and Stablecoins

6.1 Payments

Digital assets may be used for payments in the USA. There are no digital asset-specific laws or rules in this area, and use and acceptance of digital assets for payment by merchants is subject to traditional laws and rules related to payments. Many digital asset payment systems involve transmission of digital assets by an intermediary or conversion of digital assets to fiat or digital assets to other digital assets, all of which implicates US money transmission laws and rules.

6.2 Stablecoins

6.2.1 Fiat Currency and Algorithmic Stablecoins

In April 2025, the SEC's Division of Corporation Finance issued a statement clarifying how federal securities laws apply to certain "Covered Stablecoins", defined as those:

- pegged one-to-one to the US dollar;
- redeemable one-for-one for US dollar; and
- backed by low-risk, highly liquid reserves that meet or exceed their redemption value.

In the statement, the SEC shared the view that the offer and sale of Covered Stablecoins, as described, generally do not involve the offer or sale of securities under the Securities Act or the Exchange Act. To reach this conclusion, the SEC applied both the *Reves* test and the *Howey* test. Applying the "family resemblance" test under *Reves v Ernst & Young* – a Supreme Court decision that determines when a "note" qualifies as a "security" under federal securities laws – the SEC found that since Covered Stablecoins are not marketed for speculation, and are backed by risk-reducing reserves, they are unlikely to be securities. Similarly, under the *Howey* test, buyers of Covered Stablecoins do not have a reasonable expectation of profits derived from others' efforts. Nonetheless, the statement emphasised that this analysis is limited to the Covered Stablecoins described and does not apply to algorithmic stablecoins, non-US dollar pegged stablecoins, or yield-bearing stablecoins, and that each stablecoin must be assessed based on its own facts and circumstances.

The GENIUS Act reflects a statutory distinction between fiat-backed (or “payment”) stablecoins and other types of digital assets, and algorithmic and endogenously collateralised stablecoins remain outside the Act’s core regulatory framework (see **6.2.2 Stablecoin Regulation** and **6.2.3 Backing Assets** for the Act’s requirements). The Act mandates a Treasury-led interagency study of non-payment stablecoins, including algorithmic stablecoins, within one year of enactment. In the interim, because such stablecoins do not benefit from the Act’s express exclusions from securities and commodities law, they may continue to be assessed under existing federal securities, commodities and consumer protection frameworks depending on their specific features and risk profiles.

6.2.2 Stablecoin Regulation

In July 2025 Congress enacted and the President signed the GENIUS Act, establishing a federal framework for the issuance of payment stablecoins. The Act introduces requirements relating to reserve composition, redemption rights, prudential supervision, and the licensing or approval of issuers, and contemplates a dual federal–state regulatory regime. It further reinforces the treatment of certain fully reserved, fiat-backed stablecoins as payment instruments rather than securities, while subjecting issuers to bank-like oversight and compliance obligations.

6.2.3 Backing Assets

Under the GENIUS Act, permitted payment stablecoins must be backed on at least a 1:1 basis by high-quality, liquid reserve assets. The statute limits reserves to cash and cash equivalents and specifies the categories of permissible assets, including:

- US currency;
- demand deposits at insured depository institutions (including foreign branches) or approved foreign institutions;
- US Treasury bills, notes or bonds with a remaining maturity of 93 days or less;
- overnight repurchase and reverse repurchase agreements backed by such Treasury securities;
- securities issued by registered government money market funds; and
- other similarly liquid, government-issued assets approved by the relevant federal regulator.

The Act also permits certain reserve assets to be held in tokenised form, provided they comply with applicable law.

In addition, reserves must be segregated from the issuer’s operational funds and may not be commingled, and issuers are prohibited from rehypothecating reserve assets. The Act also prohibits permitted stablecoin issuers from paying interest or yield to stablecoin holders.

As to custody, reserves may be held as demand deposits at insured depository institutions (including foreign branches) or at foreign institutions approved by the relevant regulator. Foreign issuers accessing US markets must maintain sufficient reserves in a US financial institution to meet the liquidity demands of US customers.

Finally, the GENIUS Act directs federal and state regulators to impose additional capital and liquidity requirements through rulemaking, tailored to the issuer’s business model and risk profile.

6.2.4 Special Considerations

Outside the GENIUS Act, there is no dedicated framework addressing systemic stablecoin risk. However, US regulators do have tools to oversee systemically important arrangements and subject them to enhanced supervision. For instance, the Financial Stability Oversight Council (FSOC) is a federal interagency body established under the Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010 to identify and respond to risks to US financial stability. It is composed of the heads of key federal financial regulators – including the Treasury, Federal Reserve, SEC, CFTC, FDIC and OCC – along with other federal and state financial regulatory representatives. FSOC monitors systemic risks to the US financial systems and has flagged stablecoins as potential systemic risks if not properly regulated.

7. Tokenisation and Real-World Assets

7.1 Treatment

As noted in **2.4 Token Issuance**, the SEC released guidance regarding tokenisation in early 2026. The

CFTC has also released guidance on tokenised assets as well.

On 8 December 2025, the CFTC issued CFTC Letter No 25-39 (the “Guidance”), providing staff guidance on the use of tokenised assets as collateral in derivatives markets. In the Guidance, the CFTC adopts a technology-neutral approach, clarifying that the use of blockchain or distributed ledger technology to tokenise an asset “need not change the fundamental characteristics of that asset”, and that existing regulatory requirements applicable to non-cash collateral can generally accommodate tokenised assets without new rulemaking.

Consistent with this approach, tokenised assets are regulated in substantially the same manner as their non-blockchain equivalents. Assets that are eligible to serve as margin collateral – such as US Treasuries, corporate bonds or money market fund interests – remain eligible when tokenised, provided they satisfy applicable requirements relating to credit quality, liquidity and maturity.

The Guidance further emphasises that existing regulatory frameworks governing legal enforceability, custody, segregation and risk management apply equally to tokenised forms of assets. Market participants must ensure that tokenised collateral is subject to enforceable legal arrangements, held with eligible custodians, and compliant with applicable segregation and control requirements.

Similarly, risk-based methodologies – such as haircuts and valuation – apply to tokenised assets in a manner consistent with their traditional counterparts, subject to adjustments where the tokenised form introduces additional risks (eg, settlement, liquidity or operational considerations).

At the same time, the CFTC notes that tokenisation may introduce novel operational and legal risks, including cybersecurity and technological dependencies, and emphasises that tokenised assets should be assessed on a case-by-case basis depending on their structure. Taken together, the Guidance reflects the CFTC’s view that tokenisation does not alter the regulatory classification of an asset; rather, tokenised RWAs are generally subject to the same regulatory treatment as their non-blockchain equivalents, with additional analysis required only to address risks arising from the use of distributed ledger technology.

CHAMBERS GLOBAL PRACTICE GUIDES

Chambers Global Practice Guides bring you up-to-date, expert legal commentary on the main practice areas from around the globe. Focusing on the practical legal issues affecting businesses, the guides enable readers to compare legislation and procedure and read trend forecasts from legal experts from across key jurisdictions.

To find out more information about how we select contributors, email Luke.Wilson@Chambers.com