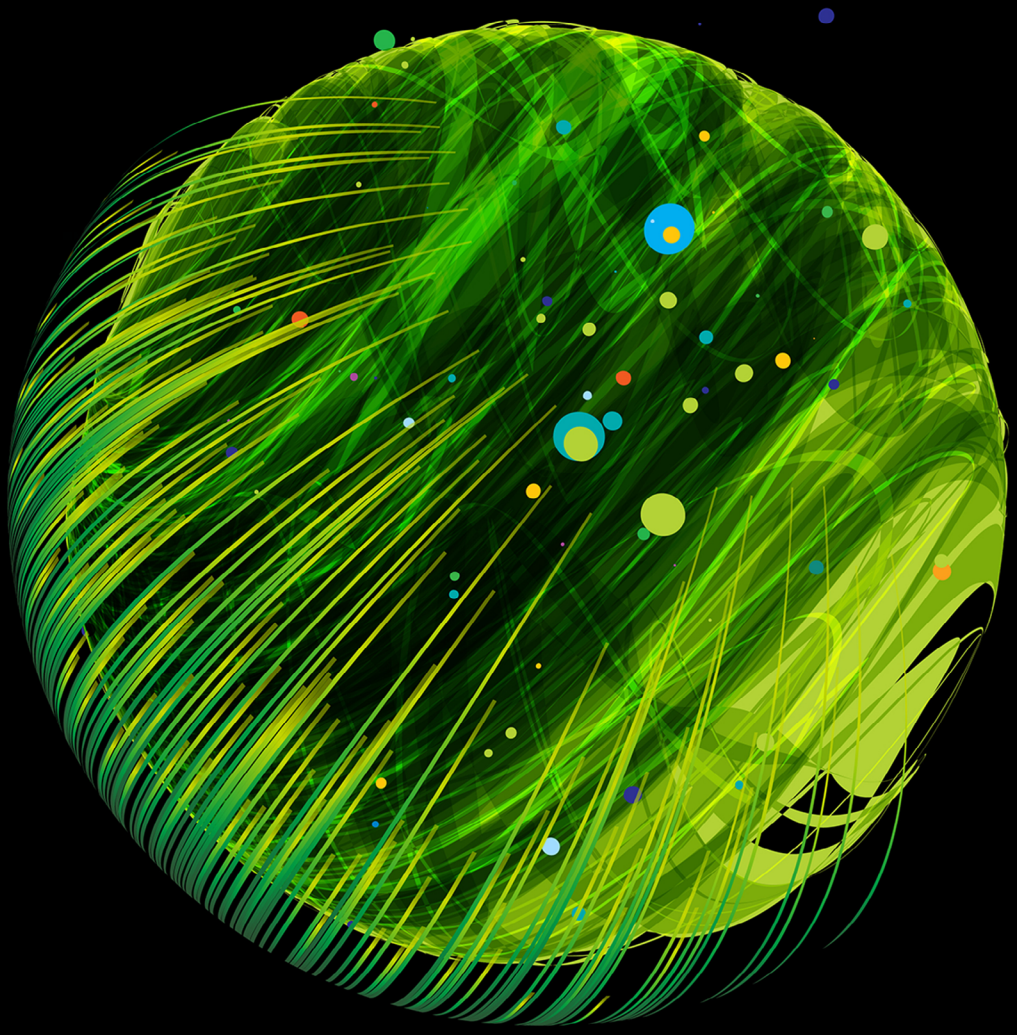
Deloitte.



2025 – the year of payment stablecoins

Laying the foundation

In our 2023 publication, *Engaging with Stablecoins*, and our inaugural piece in 2021, *So You Want to be a Stablecoin Issuer*, we explored the dynamics of this innovative digital asset class, highlighting complexities, market disruptions, and the evolving regulatory landscape both in the United States and globally.[1] Fast forward to 2025, and multiple forces appear to be encouraging "traditional" financial (non-crypto-native) companies to consider becoming stablecoin issuers, from the recent surge and market capitalization and transaction volume of fiat-backed stablecoins, combined with signaling from the new administration, banking regulators and movement in the U.S. Congress towards a "payment stablecoin" ("PSC") law and regulatory regime. A potential payment stablecoin issuer ("PSCI") should strategically assess market opportunities, regulatory requirements, and required capabilities to successfully launch a PSC.

We anticipate 2025 to be different than 2021 for a few reasons:

- The **administration's stated priority** in supporting USD-backed stablecoins[2]
- **Forthcoming legislation** with the potential to create further regulatory clarity[3]
- **Early signs of market adoption and market activity** with banks looking to become issuers and activity among venture capital and private equity firms

As a result, we expect 2025 to be "The year of the payment stablecoin," potentially creating new opportunities for a wide range of market participants.

In this next installment in our stablecoin series, we will delve deeper into the current state of pivotal regulatory developments while also presenting a revised "impact and response framework," grounded in leading industry practices. This framework can serve as a self-assessment tool for financial service companies and others that are starting from "the ground up" in building out capabilities to support the issuance of PSCs.

Definition – "Payment stablecoin"

The proposed Guiding and Establishing National Innovation for US Stablecoins (GENIUS) Act defines a "payment stablecoin" as follows:

(A) means a digital asset— (i) that is or is designed to be used as a means of payment or settlement; and (ii) the issuer of which—(I) is obligated to convert, redeem, or repurchase for a fixed amount of monetary value, not including a digital asset denominated in a fixed amount of monetary value; (II) represents that such issuer will maintain or creates the reasonable expectation that it will maintain a stable value relative to the value of a fixed amount of monetary value; or (III) has complied with the authorization requirements of this Act; and

(B) that—(i) is not a national currency; (ii) is not a deposit (as defined in section 3 of the Federal Deposit Insurance Act), including a deposit recorded using distributed ledger technology; (iii) does not offer a payment of yield or interest; and (iv) is not a security, as defined in section 2 of the Securities Act of 1933 (15 U.S.C. 77b), section 3 of the Securities Exchange Act of 1934 (15 U.S.C. 78c), or section 2 of the Investment Company Act of 1940 (15 U.S.C. 80a–2), other than a bond, note, evidence of indebtedness, or investment contract satisfying the conditions described in subparagraph (A).

As reported to the Senate on March 18, 2025

Recent developments

Administration developments

Since taking office, the Trump administration has begun to reframe US policies toward the digital asset industry. In an early step, President Trump signed an executive order entitled "Strengthening American Leadership in Digital Financial Technology" that called for a new approach and set a 60-day deadline for agencies to identify any relevant past guidance on digital assets.[4] With respect to PSCs, the executive order put explicit emphasis on promoting the global growth of dollar-backed PSCs. In terms of policy details for achieving this end, the new administration is still formulating an approach.

Regulatory developments

To date, federal agencies have taken some initial steps to rescind and adjust past guidance and adjust their supervisory approach and re-evaluate their approach to cryptocurrency.[5]

On March 7, 2025, on top of the slew of recent administrative developments, the Office of the Comptroller of the Currency (OCC) rescinded its Interpretive Letter 1179 (which outlined the agency's supervisory nonobjection process for banks to engage in digital asset activities) and reaffirmed that national banks may engage in crypto-asset custody, distributed ledger, and stablecoin activities, as discussed in prior interpretive letters.[6]

Legislative developments

As of February 2025, three bills have been introduced in Congress that would set up a legal and regulatory framework for "payment stablecoins": (1) the GENIUS Act introduced in the Senate by Senator Bill Hagerty (R-TN), with some bipartisan co-sponsorship; (2) the Stablecoin Transparency and Accountability for a Better Ledger Economy (STABLE) Act introduced in the House by Representative French Hill (R-AR); and (3) an as yet unnamed bill introduced in the House by Representative Maxine Waters (D-CA).[7] The probability of PSCs legislation being enacted in 2025 has increased significantly, which could drive more companies to issue PSCs and encourage others to leverage them within their business operations. This political shift is also expected to influence the regulatory landscape, reinforcing legitimacy of the underlying technology and product, and creating opportunities for new market entrants.

In Congress, each of the three PSC bills that has been introduced establishes a federal regulatory framework for PSCs, which would be a critical step. Common elements of these bills include one-to-one backing of reserve assets to tokens in circulation, restrictions on asset types for PSC reserves, and regular auditing and certification of reserves. As noted above, permitted PSC issuers are limited under these bills to nonbank entities (NBEs) and insured depository institution (IDI) subsidiaries.

State frameworks and the role of state regulators

In the interim, state-based frameworks, like the New York Department of Financial Services (NYDFS) BitLicense regime and state money service business licensing requirements, remain the primary licensing and registration avenue for those issuing PSCs in the United States.

The debate on the role of federal and state regulators for PSCIs remains a significant sticking point in Congress. The roles of the Federal Reserve Board of Governors (FRB) and the OCC differ under the proposed bills, as do the roles of state regulators. If the approach proposed under the current iterations of the GENIUS and STABLE bills prevail and becomes the law, the OCC would become the exclusive federal regulator for NBEs that are not operating under a State-only option. There are, however, a diversity of views on the subject, including those who may not support the issuance of PSCs by entities subject to only state approval and supervision (a "state-only" option), regardless of whether state-only issuers are subject to limits on the amount of tokens they may issue or not. Related federal and state issues include the extent to which a new federal regime may preempt state laws. These issues will need to be resolved before a final law becomes reality.

Definition – "Payment stablecoin Issuer"

Under the three current PSC acts under consideration in Congress, permitted payment stablecoin issuers would be limited to nonbank entities (an entity that is not an insured depository or a subsidiary of an insured depository, each an "NBE") and subsidiaries of insured depository institutions (IDIs). NBEs could be controlled by a bank holding company, or a company that does not control an IDI. Under these proposed regimes, while IDIs would be permitted to issue tokenized deposits, they would not be permitted to issue payment stablecoins.

How do you want to engage?

Companies will encounter multiple opportunities to engage with PSCs and must continuously assess which part of the value chain to participate in. Some entities will aggressively seize market share with a first-mover strategy, while others will react when external use of PSCs demands their involvement. Executives need to evaluate market conditions, competitive positioning, and long-term objectives to navigate this evolving landscape effectively. Firms should begin taking into consideration which role(s) to play:

Issuance of PSCs

- **Issuer:** Organizations can create and distribute PSCs, assuming responsibility for their issuance and redemption as well as managing the strategy of reserve asset allocation.
- **Transaction bank:** Facilitate ongoing collection and disbursement of fiat related to mints and redemption of PSCs.
- **Reserve bank:** Entities can function as reserve banks, holding and managing reserve assets that back PSCs.

Enabling the Ecosystem

- **Custodian of PSCs:** Firms can safeguard PSCs on behalf of clients and users, providing secure storage and the ability to use PSCs on platforms that allow their use.
- **Building platforms for use:** Companies can act as the platform which builds the interface enabling the use of PSCs for settlement, processing, and integration.
- **Providing ecosystem services:** Businesses can offer a range of support services to the PSC ecosystem, including technology solutions, compliance assistance, and advisory services.

The use of a distributed and decentralized blockchains for issuance and transactions using PSCs will enable participants to be nimble within the ecosystem. Lower barriers to entry and higher competition between platforms will foster innovation and provide opportunities for entities to strategically position themselves in the evolving PSC landscape.

Opportunities

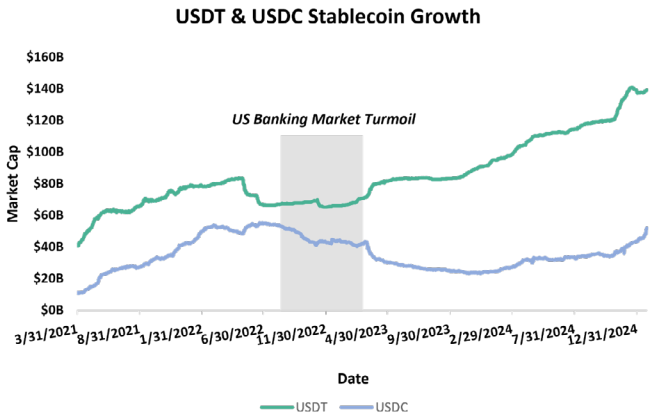
PSCs offer specific advantages by allowing instant settlement at reduced costs across borders and entities. They incentivize users to transition from traditional financial systems (and payment rails) to blockchain networks, all while avoiding the volatility associated with non-fiat-backed cryptocurrencies (ex. bitcoin). As market capitalization of PSCs has grown to over $200 billion, more business are creating platforms to enable payments using PSCs.[8] The growing demand in PSCs by the market presents significant opportunities for prospective issuers.

Payment stablecoin market capitalization and volume have been driven to date largely by trading activities involving cryptocurrencies and digital assets, with PSCs providing a stable medium of exchange, especially during periods of increased market volatility. Emerging use cases for PSCs, however, extend far beyond digital asset trading. They are increasingly being utilized in remittances and payments unrelated to digital asset transactions, offering a faster, more cost-effective alternative to transactions reliant on legacy financial infrastructure and traditional payment rails. PSCs are being used as substitutes for fiat currency, highlighting their evolution from use in crypto native transactions to being a digital extension of the dollar.

For PSCs to realize their promise, further strides should be made to reduce obstacles that limit current usage in retail and commercial payments. This includes enhancing technological infrastructure and fostering broader acceptance among financial institutions, merchants, and consumers. By addressing these challenges, PSCs may lead to significant changes in the way value is transferred globally, making financial transactions quicker and cheaper to execute.

Figure 1 paints the picture of PSC market caps of the two largest USD PSCs: USDT (known as "Tether") and USDC. The graph reflects how USDC and USDT have continued to grow, representing more than half of the USD PSCs total market cap, despite market volatility and other digital asset events:

Figure 1: Stablecoin growth[9]



Source: DefiLlama, "Stablecoins circulating," accessed March 11, 2025.

Excluding USDT and USDC, and including certain "algorithmic" stablecoins that will not be permitted under the USD PSC regulatory regimes now before Congress, the remaining top 10 stablecoins have a combined market capitalization of $15 Billion. Within this mix include other fiat-backed stablecoins (i.e., USDS, FDUSD), crypto-backed stablecoins (i.e., USDX), synthetic stablecoins (i.e. USDe), and algorithmic stablecoins (i.e., USDD). While the mix within the top 10 continues to shift, fully reserved and fiat-backed PSCs continue to have the largest share of the market.

In exchange for being a guardian of the dollar peg of a PSC, issuers can earn yield on the collateral reserves backing the token. Issuers have the ability, and under the pending Congressional bills will be required, to invest the reserves in high-quality, liquid assets. These assets can potentially generate a consistent return through interest payments. For example, yields on reserve assets can be generated through payments on short-term U.S. Treasury instruments, as well as U.S. Treasury repurchase ("repo") agreements in which the issuer lends cash overnight to global financial institutions, collateralized by U.S. Treasury securities. This reserve model not only helps to ensure the stability of the PSC, but also allows issuers to fund operations and profit from interest earned on the reserve securities held directly, as well as the spread of the buy and sell on overnight repo transactions.

Taking the next step

Stablecoins are transitioning from niche user-to-user transactions to mainstream B2B and B2C payment applications, transforming traditional payment rails, a space traditionally owned by banks. As reliance on these products grows, so does the risk of disintermediation of existing financial systems. With a clear federal framework in place, banks will have an opportunity to create reliable solutions (whether B2B or B2C) that leverage payment stablecoins to streamline operations with faster, secure payments, while customers may increasingly demand their use. As offerings and adoption grow, stablecoins could challenge the value chain of traditional payment infrastructure, reshaping the financial landscape.

To date, PSC issuance has primarily been done by non-banking entities and crypto native companies outside of a U.S. federal legal or regulatory regime. The competitive landscape, however, is shifting as the likelihood of a U.S. national regulatory framework for PSCs increases. A clear and consistent U.S. legal and regulatory framework will support entities exploring PSC issuance.

Existing financial institutions and payment processors should consider how they might leverage their existing platforms to integrate a native PSC into their operations to drive efficiencies and meet customer opportunities and demands, consistent with the emerging federal regulatory regime. At the same time, PSC users should benefit from interacting with an issuer subject to a clear national legal and regulatory regime that ensures consistent protections, a defined supervisory framework, and transparent periodic reporting requirements regarding the PSC's reserve. As more organizations integrate and build upon an infrastructure meeting the requirements of the evolving federal regulatory regime, the enhanced network effects may contribute to a more robust and versatile financial ecosystem, attracting further participation and investment.

Risks

While PSCs unlock various opportunities, they also introduce significant risks that issuers must handle, encompassing those associated with operating within the traditional financial regulatory environment as well as the new crypto-native ecosystem. Depending on the role an entity plays in the PSC ecosystem, the applicability and severity of risks are expected to vary. A good practice for firms to manage the risks posed by being in the PSC ecosystem is to establish or enhance its risk and control frameworks through conducting a digital asset risk assessment[10] specific to the characteristics of the underlying products and technologies.

Cybersecurity and data protection: Issuers should safeguard their digital infrastructure against cyber-attacks, which could lead to the theft of PSCs and loss of private keys. Such breaches can result in significant financial losses, legal liabilities, and erosion of user trust. To mitigate these risks, issuers should implement robust cybersecurity measures, including multi-factor authentication, regular vulnerability assessments, and comprehensive incident response plans. Furthermore, the risk of technological failures, such as malfunctions in the blockchain network or issues with the underlying protocol, can disrupt PSC operations and lead to transaction delays or failures. Issuers must confirm that their technological infrastructure is resilient and capable of handling high transaction volumes, especially during periods of market volatility in addition to continually monitoring the underlying protocols they operate. Regular stress testing and contingency planning are essential to maintaining operational stability and ensuring the reliability of PSC services.

Anti-money laundering: Issuers should comply with stringent regulations related to anti-money laundering (AML), know-your-customer (KYC), and applicable state laws. Failure to comply can result in enforcement actions by regulatory bodies, which may include fines, restrictions on operations, and even the required cessation of business activities. Non-compliance can also lead to reputational damage and loss of customer trust. To mitigate these risks, issuers must confirm develop and implement comprehensive compliance programs that include robust AML and KYC processes. This involves conducting thorough customer due diligence, maintaining detailed records of transactions, and reporting suspicious activities to the relevant authorities.

Blockchain and smart contract risk: The reliance on blockchain technology and smart contracts introduces unique risks. Smart contracts can contain vulnerabilities or bugs that may be exploited by malicious actors. Additionally, the underlying blockchain network may experience forks, congestion, or other technical problems that can impact the performance of transaction on the network. Such issues can lead to delays, failures, and potential financial losses. To mitigate these risks, issuers should frequently assess the reliability of smart contracts and blockchains. Implementing comprehensive incident response plans specifically for smart contract and blockchain network issues is crucial. Furthermore, issuers should establish a process to evaluate prospective blockchain networks they plan to issue their PSC. Continuous monitoring of blockchain infrastructure is essential to ensure the stability and efficiency of the technology stack supporting the issuance and management of PSCs.

Depegging of stablecoin: The primary risk associated with PSCs is the potential for depegging, where the units of the PSC in circulation diverge from its intended peg (e.g., 1:1 dollar value to its underlying fiat reserves). Depegging can occur due to on-chain factors, including minting and burning operations and reserve management. To mitigate this risk, issuers should maintain a robust control environment that ensures accurate minting and burning activities and effective reserve management. Effective communication, through the issuance of transparency reports, demonstrates the mechanisms in place to maintain the peg of the PSC, which is necessary to maintain trust and confidence.

Tax considerations: While stablecoins may be used as a means of payment and carry a value similar to fiat currency, they may not be considered money or currency for US income tax purposes. Rather, stablecoins may be considered general property or even a debt obligations for tax purposes depending on the structure of the stablecoin and interpretations of existing US treasury regulations developed prior to the advent of blockchains and digital assets. Further, payments in stablecoins may be subject to the same informational requires as other digital assets (Form 1099-DA).

Accounting considerations: From an accounting perspective, holders of stablecoins will need to assess the terms to identify whether those stablecoins represent financial assets or intangible assets, which will impact classification, subsequent measurement, and the accounting for subsequent transfers. For stablecoins concluded to be intangible assets, entities will also need to consider whether such assets are within the scope of the new US GAAP accounting guidance for crypto assets, including the new required disclosures. Finally, for entities that are issuers of stablecoins, entities will need to determine whether those stablecoins represent financial liabilities.

Operational and market risks: Issuers also face operational risks, such as the potential for human error, fraud, or internal misconduct, which can affect the stability and reliability of PSC operations. Additionally, market risks, including fluctuations in the value of reserve assets, can affect the stability and value of PSCs. These risks can lead to financial losses, operational disruptions, and erosion of user trust. To mitigate these risks, issuers must implement robust internal controls, risk management frameworks, and governance structures. This includes developing metrics to monitor the performance of APIs and partners in accordance with established rules and limits, including profitability and marketplace impacts. Regular stress testing and contingency planning are essential to ensure operational stability and resilience during periods of market volatility. Providing ongoing training to employees on operational procedures and risk management practices can help minimize the risk of human error and misconduct. Additionally, maintaining a diversified portfolio of reserve assets can help manage market risks and ensure the stability of the PSC.

Regulatory non-compliance: The regulatory landscape for PSCs is complex and continuously evolving. Non-compliance with relevant laws and regulations can lead to severe penalties, legal actions, customer harm, and reputational damage, significantly affecting the issuer's operations and financial stability. To mitigate these risks, issuers must stay informed about changes in the regulatory environment and ensure compliance with all applicable laws and regulations. This involves engaging with regulators, participating in industry forums, and seeking legal and compliance expertise. Regular reviews of compliance programs can help identify and address potential gaps or issues. Proactive engagement with regulators and transparent communication about compliance efforts can further mitigate the risk of regulatory non-compliance.

Essential capabilities

In this rapidly evolving landscape of digital finance, payment stablecoin issuers face an array of challenges that demand robust operational frameworks, ongoing compliance, and sophisticated risk management strategies. As detailed above, the regulatory landscape for PSCs is complex and dynamic, with different jurisdictions and authorities having varied approaches and requirements. Issuers and entities providing services to issuers should be aware of these requirements and their impact on various aspects of their PSC offerings and services, including business strategy, governance, enterprise risk management (ERM), compliance, audit, and treasury. This awareness should include and consider the key components and common features of the PSC frameworks (including permitted issuers and the federal and state approval and supervision frameworks) reflected in the PSC Senate and House bills in play in the current Congress.

Payment stablecoin issuers and non-issuers* should articulate business strategies supported by ongoing analysis of the regulatory and competitive risk landscapes A formalized risk management framework is essential to identify, measure, monitor, and mitigate risks associated with PSC and blockchain-based activities. These risks may include regulatory non-compliance, market volatility, operational inefficiencies, and cybersecurity threats. A risk governance framework should be established to define a formal risk appetite and maintain effective controls to ensure compliance with the current regulatory environment, and is able to respond in a timely manner as the regulatory requirements change in this dynamic and evolving environment. It is essential to implement a nimble risk response program that promptly identifies and implements net new capabilities.

For issuers, strong governance arrangements are crucial and include defined organizational structures, effective board and management committees, and clear roles and responsibilities. Effective management of underlying PSC reserves is essential to ensuring the stability and liquidity of PSCs, requiring robust treasury policies, regular stress testing, and contingency planning to maintain the peg and support timely redemption. The issuer should perform a roll-forward of tokens in circulation and a reconciliation to underlying reserves. Issuers should publicly release a transparency report that includes this roll-forward and reconciliation, enhancing the confidence and trust of, and accountability to, PSC users. These measures address risks such as liquidity shortfalls, reserve mismanagement, and failure to maintain the PSC peg.

By developing and maintaining these essential capabilities, issuers and non-issuers can better navigate the complex risk landscape, ensuring compliance, operational efficiency, and consumer trust in their PSC issuance and related services, respectively. Financial institutions looking to participate in the ecosystem must prioritize these areas to thrive in this rapidly evolving market. Leveraging expertise in regulatory compliance, operational excellence, and risk management can help position institutions for success in the PSC ecosystem.

* A "non-issuer" is an entity engaged in activities relating to and supporting a payment stablecoin issuance, but which is not the issuer of the payment stablecoin. Examples of non-issuers in this context include an entity acting as a custodian, a payment processors, a depository for payment stablecoin cash reserves, or a liquidity provider.

Impact and response framework

As mentioned previously, the regulatory landscape for PSCs is complex and dynamic, as different jurisdictions and authorities have different approaches and requirements. Payment stablecoin issuers and users must be aware of the requirements and associated impact to their offering whether issuing or using a PSC. This section explores some of the key federal and state regulatory expectations that payment stablecoin issuers may face, and how these expectations affect the capabilities that issuers need to develop and maintain across areas such as business strategy, governance, enterprise risk management framework, compliance, audit, treasury, etc. These expectations reflect the existing requirements from US regulators and global bodies in addition to monitoring development and evolution of the regulatory framework for PSCs.

Potential regulatory expectations	Applicability to participate		Considerations (based on industry experience)
	Issuers	Non-issuers	
Business strategy			
• Articulate business strategies, supported by scenario-based, pro-forma projections, and the creation and maintenance of a business plan • Analyze a range of impact scenarios regarding PSCs covering the regulatory, risk, and competitive landscapes • Ensure that the financial resources, managerial and technical expertise, and governance practices are in place • Consider additional factors, including evaluating the benefits to the public, the stability of the financial system, the needs of the community to be served, and the plan to promote financial inclusion			• Definition and documentation of approach to engage with PSCs including detailed steps and existing capabilities • Determine impact on overall business strategy owing to broader adoption of deposit tokens, blockchain-based deposits issued by a licensed depository institution tied to a customer's cash deposit and redeemable at 1:1 • Documented operating model (people, process and technology, in-house vs outsourced) and key technology architecture, including applicable processes and flows of funds • Risk and control framework in accordance with PSC specific risk management capabilities required by regulatory requirements • Third party risk management framework, including policies and procedures for TPRM, controls across vendor lifecycle

High impact Medium impact Low impact

Potential regulatory expectations	Applicability to participate		Considerations (based on industry experience)
	Issuers	Non-issuers	
Risk management			
• Establish or adapt enterprise-wide risk-management framework, including a risk management policy, to identify, measure, monitor, and mitigate risks associated with the PSC and other blockchain-based activities • Establish or adapt a risk governance framework that provides an appropriate organizational structure, escalation mechanism, and reporting framework for the risk management of the PSCs • Define a formal risk appetite with thresholds that contain risk appetite limits/ statements for PSC activities • Conduct a top-down, enterprise-wide risk assessment and due diligence • Identify legal risks considered by the board and document how they can be managed/ mitigated • Maintain effective controls to conduct the PSC activity in a safe and sound manner in compliance with the applicable regulations, including the Bank Secrecy Act and the USA Patriot Act • Enhance enterprise risk reporting capabilities, including PSC metrics • Document approach to managing the different risks related to PSCs, including operational, market, liquidity, cybersecurity and fraud, blockchain technology, and third-party service provider • Evaluate the ability to meet obligations, monitor reserves, assess arbitrage risks, analyze asset shifts, identify recourse protections, and compare on-chain with bank transfers • Ensure adequate insurance coverage by banks issuing PSCs • Include industry risk, risk from negative public perception, sensitivity to market risk, and impact on examination ratings in the risk assessment			• Enhanced ERM framework and articulation of an updated risk appetite statement to account for the unique risks associated with PSCs • Resources with expertise in managing operational and liquidity risks by addressing interoperability issues, ensuring thorough testing of new technologies across platforms, and identifying blockchain-related risks traditionally not applicable to financial institutions • Board and senior management with experience and expertise in risks associated with activities in the PSC value chain • New product approval and governance processes that care for the risks posed by the PSC • Approval process addressing PSC-specific risks, including those related to smart contracts, immutability, and key management • Demonstrate the capability to regularly review the material risks arising from PSC arrangements and identify and implement appropriate mitigants, taking an integrated and comprehensive view of risks • Create and implement procedures for handling claw back incidents in case of organizational bankruptcies

High impact Medium impact Low impact

Potential regulatory expectations	Applicability to participate		Considerations (based on industry experience)
	Issuers	Non-issuers	
Risk management			
• Document approach to managing the different risks related to PSCs, including operational, market, liquidity, cybersecurity and fraud, blockchain technology, and third-party service provider • Evaluate the ability to meet obligations, monitor reserves, assess arbitrage risks, analyze asset shifts, identify recourse protections, and compare on-chain with bank transfers • Ensure adequate insurance coverage by banks issuing PSCs • Include industry risk, risk from negative public perception, sensitivity to market risk, and impact on examination ratings in the risk assessment • New, modified or expanded product approval (NPA) • Implement robust risk management of modifications made to products, including full risk assessment and approval of products • Establish NPA process to ensure that risk associated with a new product/ service is identified and managed accordingly • Document governance framework for the proposed activity • Ensure board and senior management oversight relating to the development of policies and procedures • Conduct comprehensive compliance and legal reviews, including specific documentation and regulatory frameworks, for new programs at banking entities • Create and document a project plan covering expected volumes of activity, cost-benefit analysis, and any other analysis supporting the financial feasibility of the PSC services			

High impact Medium impact Low impact

Potential regulatory expectations	Applicability to participate		Considerations (based on industry experience)
	Issuers	Non-issuers	
Operational – Blockchain & digital assets			
• Establish procedures for minting and burning • Issue public reports that reconcile outstanding supply to underlying reserve balances • Implement transaction monitoring and sanction screening for addresses associated with mint and burn requests • Enable the ability to freeze and unfreeze holdings of designated parties not allowed to hold stablecoins due to sanctions screening			• Evaluate reliability of blockchains and smart contracts utilized • Establish preventive and detective processes for minting and burning activities • Conduct compliance checks of users and related blockchain addresses during onboarding and on an ongoing basis • Secure private keys to wallets using self-custody or custodial solutions • Develop functionality to track all wallets, including any required updates to account configurations within the application • Track internal wallets used by the company and external wallets of onboarded customers to ensure accurate monitoring and management of all relevant transactions • Enable the ability to provide customers with their USD and PSC balances in real-time

High impact Medium impact Low impact

Potential regulatory expectations	Applicability to participate		Considerations (based on industry experience)
	Issuers	Non-issuers	
Regulatory			
• Regulatory and legal interpretation • Obtain an approval/license from the appropriate federal PSC regulator before issuing PSCs • Notify the appropriate federal PSC regulator within 30 days after making the related service contract or performing the activity for third parties/vendors that provide services integral to the functioning of payment stablecoin issuers • Engage with regulators for required approvals and non-objections			• Resources with expertise in evaluating necessary licenses for relevant institutional roles and achieving high standards to mitigate future regulatory risks • Regulatory inventory with list of regulators and requirements to which the entity will be subject as per the planned PSC operations and establish capability to incorporate regulatory feedback • Regulatory engagement plan, including a detailed understanding of pre-filing requirements and the preparation of a business plan for regulatory approval (if applicable) • Regulatory tracking and change management process for PSCs, to ensure the bank's policies and processes are updated in accordance with evolving regulatory requirements and expectations

High impact Medium impact Low impact

Potential regulatory expectations	Applicability to participate		Considerations (based on industry experience)
	Issuers	Non-issuers	
Compliance			

• Payment stablecoin issuers can either be structured as a:
  ◦ Non-depository trust company registered with a board and can issue PSCs whose outstanding value does not exceed $10 billion, or
  ◦ Federally chartered or depository institution chartered by the OCC or a state bank supervisor, with no limit on the value of outstanding PSCs
• Compliance framework updates to effectively manage specific compliance obligations posed by PSCs, including privacy, consumer protection, and other key impacts
• Payment stablecoin issuers in New York are expected to come into compliance with the NYDFS guidance, including reserve requirements, within three months except for the annual attestation requirement
• Issuers must obtain an annual attestation report by an independent CPA on their control effectiveness, structures, and compliance procedures
• Issuer would be subject to federal regulation if market capitalization is greater than $10 billion, while for issuers with market capitalization less than $10 billion, there is an option of state regulation as long as it meets certain federal standards
• Nonbank entities issuing PSCs will be subject to restrictions on transactions with affiliates as stated under the BHC Act
• Identify and disclose fees and charges that will be imposed on customers using the system to conduct transactions
• Ensure e-sign consent, licenses, and commercial entity agreement are aligned with regulatory and operational requirements
			• Consumer Protection Policy and Procedures tailored to stable PSCs to help explain to consumers the unique risks along with prioritizing risk assessment methodology, transparency, and risk mitigation to safeguard consumer interests
			• Consumer complaints response process to address consumer concerns and identify emerging operational problems, mitigating larger compliance or reputational risks associated with PSCs and retail adoption
			• Compliance framework for PSC arrangements, ensuring issuers, payment processors, and banks adhere to lending restrictions, risk management, liquidity and capital requirements, and limits on commercial affiliations and use of customer data
			• Regulatory tracking system, allowing the integration and upgrade of compliance programs as new regulatory developments arise
			• Extensive KYC, Bank Secrecy Act /AML, and transaction monitoring capabilities, for issuers supporting non-custodial wallet capabilities (ie, beyond closed ecosystem)
			• Due diligence process for counterparties of third-party service providers, focusing on on-ramp and off-ramp banking partners
			• Contractual relationship established with a depository institution as a sub-custodian for the reserves
			• Policies, procedures, and compliance programs akin to banks, with a compliance program that addresses new obligations arising from obtaining a bank charter
			• Registration with Securities and Exchange Commission (SEC) and compliance with securities rules, as PSCs may be classified as securities

High impact Medium impact Low impact

Potential regulatory expectations	Applicability to participate		Considerations (based on industry experience)
	Issuers	Non-issuers	
Compliance			
• Communicate with the FDIC regarding new crypto-related activities • Assess the adequacy of systems for compliance risk assessments and monitoring, reporting, and remediation processes			• Compliance with potential risk management and capital/ liquidity rulemaking by federal regulators • Updates to compliance framework for banks (acting as issuer or a non-issuer), potentially requiring major changes given the regulatory uncertainty and new risks that come into scope • Less stringent regulatory requirements for non-issuers (excluding banks) because they do not carry PSCs on the balance sheet; however, cognizance required to any amendments to state specific MTLs (money transmitter licenses)

High impact Medium impact Low impact

Potential regulatory expectations	Applicability to participate		Considerations (based on industry experience)
	Issuers	Non-issuers	
BSA/AML program			

• Update the risk assessment to include all crypto activities, addressing BSA, KYC, AML / non-AML considerations such as -
  ◦ Office of Foreign Assets Control (OFAC) and sanctions
  ◦ Bank Secrecy Act
  ◦ USA Patriot Act
  ◦ Identifying and assessing money laundering (ML) and countering the financing of terrorism (CFT) risks
  ◦ Transaction monitoring, including suspicious activity reporting (SAR)
  ◦ Record keeping
• Update current monitoring and auditing processes to include PSC activities, and document any new AML/CFT controls and include in the audit plans
			All participants
			• BSA/AML compliance capabilities such as client onboarding with enhanced due diligence and KYC requirements to prevent the misuse of blockchain rails or PSCs for fraud and illicit money transfers along with robust sanctions screening program including transactions blocking, reporting, recordkeeping, sanctions operational controls such as geolocation tools, IP blocking controls, etc, to ensure compliance with OFAC regulations
			• Blockchain analytics tools to supplement existing transaction monitoring tools
			• Assessment and identification of ML/TF risks prior to PSC launch, with appropriate measures to manage and mitigate these risks before go-live
			• Improved compliance for private-sector entities and/or enforcement actions for non-compliance; All PSC participants who are subject to enforcement actions will be held accountable for non-compliance with AML/CFT and sanctions obligations
			• Perform regular testing of AML transaction monitoring controls
			Non-Bank Payment Stablecoin Issuers and Payment Processors
			• Improved compliance for private-sector entities and/or enforcement actions for noncompliance; all PSC participants who are subject to enforcement actions will be held accountable for noncompliance with AML/CFT and sanctions obligations
			• Perform regular testing of AML transaction monitoring controls
			Nonbank payment stablecoin issuers and payment processors
			• Preparation for classification as financial institutions, treating issuers and service providers of PSCs as financial institutions under the BSA

High impact Medium impact Low impact

Potential regulatory expectations	Applicability to participate		Considerations (based on industry experience)
	Issuers	Non-issuers	
Governance			
• Define organizational structure having clear business line and legal entity structure, and key interrelations and dependencies between institution subsidiaries and nonbank affiliates • Ensure strong governance arrangements with effective oversight and internal controls that allows for timely human intervention, as and when needed • Establish effective board and management committees with clear information on participants who have the ability to make binding decisions and handle objections • Define roles and responsibilities for key personnel - the board, management committees, second-line committees and business to ensure risk-taking activities are in line with the organization's strategic objectives and risk appetite • Define interbank relationships, communication protocols and compliance measures • Document discussions, analyses, approvals, and any related items for each PSC activity			• Updated and defined governance structures with clear and direct lines of responsibility and accountability • Resources with skills required to support end-to-end PSC management activities • Strong governance through the adoption of a Three Lines model to enable significant operational impacts and reduce risk of fraud or abuse of reserves • Updates to corporate governance (including committees and cross-functional internal advisory bodies) may be needed for banks when including PSCs in their portfolio; demonstrating effective challenge of new business and ongoing monitoring of crypto risks will be key • Overarching governance structures for all market participants with clear and direct lines of responsibility and accountability as well as integrated and comprehensive risk management frameworks • Oversight process to ensure PSC reserves align with the outstanding number of PSCs, for investor and consumer protection • Establishment of a board and management team that benefits from a wide range of skills, experiences, and perspectives

High impact Medium impact Low impact

Potential regulatory expectations	Applicability to participate		Considerations (based on industry experience)
	Issuers	Non-issuers	
Third party risk and intercompany governance			
• Ensure processes are up-to-date to meet regulatory expectations, including inventory, risk rating, due diligence, and ongoing performance monitoring • Consider service level agreements to document performance expectations and controls for oversight and monitoring when payment stablecoin issuers leverage other affiliate services • Subject third parties/vendors (eg, custodians, wallets) leveraged by PSCI's to perform any services or activities integral to the functioning of PSCs to regulation and supervision by the appropriate federal PSC regulator • Establish minimum financial requirements for third parties/vendors integral to the functioning of the PSC • Manage risk of theft or compromise due to utilizing a third party with weak key management policies and procedures for key/seed generation, leading to unauthorized access to assets, potential financial losses, and damage to the reputation of the involved parties • Define access rights to third parties including data / transaction restrictions • Define vendor review process to thoroughly assess key elements like financial analysis and operating controls			• TPRM and oversight capabilities to monitor critical functions related to PSCs • Intercompany governance processes and related controls to manage affiliate relationships • Enhanced oversight over clients/customers to avoid risk of non-compliance with regulations • Third-party service provider management/onboarding policy and procedures, including (i) a list of all engaged third parties, (ii) a description of their services, and (iii) a summary of due diligence performed prior to engagement • Service level agreements (SLAs)/written contracts with clear roles and responsibilities, ongoing monitoring, contingency plans for terminations, and performance monitoring • Updates to existing TPRM processes will be needed for banks as they onboard new types of vendors to enable settlement • Contracting with third parties to perform functions that have been in-house previously, • Capabilities to comply with bank like regulations, FRB supervision and capital requirements, for third-party vendors supporting issuers

High impact Medium impact Low impact

Potential regulatory expectations	Applicability to participate		Considerations (based on industry experience)
	Issuers	Non-issuers	
Treasury			
• Ensure capital adequacy and capital management processes demonstrate the ability to withstand significant stress • Establish liquidity management, including measurement of liquidity and contingency planning • Balance sheet management • Contingency planning • Reserve management • Payment stablecoin issuers must ensure they hold reserves at least equivalent to the nominal value of all outstanding units of the PSC as of the end of each business day • Ensure reserves consist only of assets permitted by applicable law and regulations (eg, treasuries, repurchase agreements (complying with the applicable conditions for maturity duration, central counterparties (CCP) or board approval) • Creation of endogenously collateralized PSCs (algorithmic PSCs) will be deemed unlawful • Redemption management • Issuers must have clear policies in place covering the redemption rights of a PSC holder clearly disclosing the meaning of redemption and timing of timely redemption (no more than one day after the redemption request) • Custody oversight policies and procedures • Stress testing to manage PSC risk • Financial planning and analysis			**Bank and non-bank payment stablecoin issuers** • Adequate capital and liquidity to support heightened standards addressing safety, soundness, and financial stability concerns • Standards and policies to ensure maintenance of sufficient capital and liquidity • Forecasting capabilities, including stress testing and sensitivity analysis, to establish contingency capital and funding plans • Treasury policies that define reserve composition and redemption rights, with contingency plans of additional funding sources for timely redemptions during stress periods, maintain reserves on a one-to-one basis, ensuring these reserves are not pledged, reused, or rehypothecated, except for creating liquidity to meet redemption requests • Pre-approved repurchase agreements by the board, OCC, or state bank regulators for cleared repos as reserve assets • Documented procedures and controls directing issuers not to sell, transfer, assign, lend, hypothecate, pledge, or otherwise use or encumber assets, except when directed by the customer • One-day redemption capabilities • Segregation of customer and issuer assets for custodial services • Monthly attestations and disclosures

High impact Medium impact Low impact

Potential regulatory expectations	Applicability to participate		Considerations (based on industry experience)
	Issuers	Non-issuers	
Treasury			
• Define whether reserves will be held in connection with liabilities, the form of these reserves and if they serve as collateral • Establish clear procedures for administering the omnibus account and ensure it accurately reflects customers' purchased crypto assets • Publish the total number of outstanding PSCs along with details of the amount and compositions of the reserves, every month • Ensure examination of the reserve details for the prior month by a CPA along with certification from the CEO/ CFO who would be subject to criminal penalties for false certifications			• Custodial policies, procedures, and contracts to protect reserve assets and ensure prompt access for redemptions • Scenario analysis and stress testing to evaluate risks in PSC processes, inform limits and liquidity management, and facilitate periodic reviews by senior management • Strategic planning and forecasting at both enterprise and legal entity levels, considering the organization's current state, future strategy, and economic environment/tax jurisdictions • Assess applicable treatment of PSCs on their balance sheet and impacts to liquidity requirements • For banks, demonstrate to the supervisors how the PSC is considered applicable to the respective RWA treatment • Liquidity risks may be posed to all market participants due to misalignment of the settlement timing between PSC arrangements and other traditional systems, causing temporary mismatches in the quantity of PSCs available that need to be managed • Assess whether the PSC provides its holders with a direct legal claim on the issuer, or claim in the underlying reserve assets for timely convertibility at par into other liquid assets in both normal and stressed times

High impact Medium impact Low impact

Potential regulatory expectations	Applicability to participate		Considerations (based on industry experience)
	Issuers	Non-issuers	
Technology and information security			
Information security and business continuity planning (BCP) • Implement disaster recovery and business continuity planning • Establish an information security program supporting IT controls and risk management process • Establish a cybersecurity framework to ensure delivery of critical services and manage issues relating to cyber and data security incidents • Chief information security officer • Implement effective controls, such as multi-factor authentication. • Maintain privacy and information security policies detailing rights and responsibilities including management of privacy and data security violations. • Manage risk of private key extraction and subsequent loss of assets due to improper hardware security module configuration and risk of private key loss and/or destruction with no potential for recovery due to inadequate backup/storage processes, resulting in permanent loss of access to PSCs owned. • Manage risk of compromised security and/or network service outages due to the use of outdated/incorrect versions of protocol/node software that is out of sync with the main network, potentially leading to an increased vulnerability to attacks and disruptions.			**All participants** • Entities providing custody wallet services for PSCs would need appropriate processes to comply with limits on using customers' transaction data • IT controls and IT governance practices (in line with existing FFIEC (Federal Financial Institutions Examination Council) expectations relating to technology, IT risk, and IT governance) • Systems to support tax, compliance, risk, and financial processes (e.g., transaction monitoring) • Plan to mitigate risk from adverse events due to the usage of PSCs, for non-issuers. • Update to information security and business continuity plan should include PSC-related specifics. **Bank and non-bank payment stablecoin issuers** • Chief information security officer who will be responsible for implementing and overseeing the security program and continuity plan • Multi-factor authentication, transaction reconstruction, and audit trails • Capabilities to periodically assess and identify information security vulnerabilities in company systems • Capabilities to deal with interoperability as PSCs face issues when operating across different blockchains (for example using bridges that are protocols that connect separate blockchain networks) or by wrapping which involves locking the original PSC and minting a new one • Key management capabilities and asset safeguarding policies, including access restrictions, private key storage monitoring, and wallet security controls • Policies for managing customer complaints

High impact Medium impact Low impact

Potential regulatory expectations	Applicability to participate		Considerations (based on industry experience)
	Issuers	Non-issuers	
Technology and information security			
Technology and IT Risk • Implement broader technology and IT risk management impacts and controls supporting digital currency processes • Perform ongoing vulnerability assessments • Manage risk of malfunctions in the ingestion of blockchain data/transactions into books and records due to changes made to the underlying blockchain infrastructure or legacy systems, potentially resulting in data discrepancies and compliance issues • Manage risk of transaction failure or delay due to blockchain network congestion, leading to inefficiencies, financial losses, and frustration for users • Manage risk of inadequate node verification processes leading to unauthorized nodes accessing the network and/or validating transactions • Manage risk of adverse impacts (e.g., network instability) resulting from software upgrades implemented through hard or soft forks, potentially disrupting the operation of the blockchain network and causing user inconvenience • Describe the interaction between the bank, its operating systems, APIs, and other relevant systems • Issuance of PSCs through public, permissionless blockchain networks			• Backup recovery system to ensure that the entity maintains continued access to the private key in case of system failure • Enhancing legacy systems to ensure alignment with new industry standards • Process for periodic review of blockchain node software for quates to detect like off-chain transactions • Process to conduct regular analysis/simulation of the network's current and anticipated future capacity to determine whether the network is capable of scaling to meet current and future volume and hashing demands • Process to ensure that signing nodes are available online and in line with the associated network speed at any given time for a customer's cluster; implement strategy layers in infrastructure that prioritizes downtime mitigation above all else with the availability of secondary nodes and implement node verification processes • Process for review and testing of system configurations and communicate vulnerabilities discovered post-software upgrade to appropriate committee and/ or senior management • Ensure technologies are tested annually by qualified internal personnel or a third party • dentification of risks from integration with existing fiat currency models poses challenge, particularly in transaction validation and integrity of the distributed ledger that are utilized to support end-to-end processes

High impact Medium impact Low impact

Potential regulatory expectations	Applicability to participate		Considerations (based on industry experience)
	Issuers	Non-issuers	
Accounting, reporting & and internal controls			

• Regulatory reporting
• Financial reporting
  ◦ Define how funds exchanged are reflected in the balance sheet
  ◦ Define whether and how the assets themselves are or will be reflected on the balance sheet
• Tax informational reporting
• Accounting and internal controls
• Transparency provided by external audits
• Income tax treatment
• General ledger impact
  ◦ Maintain sample general ledger entries for various transactions (transfers, asset burning, etc.)
• Record retention
			• Understand income tax treatment of PSCs from both issuer's and holder's perspectives, considering the terms, conditions, and operational design in the absence of specific tax guidance on PSCs
			• Legal framework that acknowledges and supports the finality of a transfer, ensuring that once legal finality is achieved, it is maintained regardless of any competing states of the ledger
			• Process for reconciling misalignment between technical settlement and legal finality, with measures to address potential losses from reversals due to such misalignment infrastructure for record-keeping of non-completed, outstanding, or inactive accounts or transactions for a minimum of five years and for recording related to PSC business activities for at least seven years
			• Financial reporting system to track and report composition of assets and liabilities, capable of generating call reports, quarterly and annual financial statements, including audited financial statements, as required
			• Internal control and quality assurance frameworks to ensure complete, timely, and accurate reporting, aligning with the standards followed by insured depository institutions
			• Processes to ensure transparency in asset reserve composition and internal controls, aligning with emerging leading practices among payment stablecoin issuers and anticipating future regulatory requirements
			• Monthly review and attestation reports
			• Process to monitor requirements and produce additional regulatory and financial reports or create new internal controls to deal with risks arising from PSCs

High impact Medium impact Low impact

Potential regulatory expectations	Applicability to participate		Considerations (based on industry experience)
	Issuers	Non-issuers	
Accounting, reporting & and internal controls			

• Reserve reporting and attestation
  ◦ Payment stablecoin issuers must obtain a monthly attestation report by a licensed CPA regarding end-of-day market value of the reserve (with breakdowns by asset class), end-of-day quantity of PSC units in circulation, whether the reserve was adequate to fully back all outstanding PSC units
  ◦ Submit an annual report to the appropriate federal regulator detailing: joint ventures, partnerships, other engagements by the issuer during the report period and efforts of the issuer to promote inclusion, for payment stablecoin issuers with more than $150,000,000 in total PSC value
• Define segregation and identification of crypto-related balance sheet assets
• PSCs would not be considered as securities and agencies such as NCUA and SEC are prohibited from assets held in custody as liabilities
			• Reporting mechanisms (financial, tax and regulatory) of banks (acting as an issuer or non-issuer) should be updated to include PSCs in alignment with existing and developing regulatory expectations
			• Internal controls should be updated, and additional controls may be added (if required) to manage risks Controls should be designed to ensure sufficient reserves against outstanding PSC units
			• Enhancements to data and reporting frameworks, robust accounting practices, safekeeping procedures, proper segregation of assets and internal controls for the entities providing custody wallet services
			• Define the point at which transfer on the ledger becomes irrevocable and unconditional and technical settlement happens. Identify risk of misalignment between technical settlement and legal finality

High impact Medium impact Low impact

Conclusion

"The Year of the Payment Stablecoin" presents abundant promising opportunities for market participants interested in engaging in stablecoin activities. Regulatory tones have seen significant shifts recently, with authorities across the globe increasingly acknowledging the transformative potential of stablecoins within the financial system. Concurrently, potential legislative advancements appear on the horizon, which may offer greater clarity and certainty for businesses and investors through a more tailored regulatory framework.

Organizations looking to integrate into the stablecoin ecosystem should conduct a detailed assessment of their market opportunities and pay careful consideration to their operational strategies, risk controls, and governance structures. By doing so, they can better strategically position themselves to capitalize on these burgeoning advancements in financial technology. Moreover, proactive engagement with regulatory developments and adherence to best practices in compliance and risk management will be crucial in navigating this evolving landscape. By investing in a robust foundation, organizations will be better positioned for sustained long-term success.

Endnotes

1. Rob Massey et al., "Engaging with stablecoins?," Deloitte, March 2023; Rob Massey et al., "So, you want to be a stablecoin issuer?," Deloitte, 2021.

2. The White House, "Strengthening American leadership in digital financial technology," January 23, 2025. See also Deloitte, "President Trump issues executive order to advance digital assets," 2025.

3. US Congress, "S.394 – GENIUS Act of 2025," February 4, 2025; US House Committee on Financial Services, "Hill and Steil release discussion draft for stablecoins," press release, February 6, 2025; US House Committee on Financial Services Democrats, "Ranking Member Maxine Waters unveils bipartisan stablecoins legislation," press release, February 10, 2025.

4. The White House, "Strengthening American leadership in digital financial technology"; *see also* Deloitte, "President Trump issues executive to advance digital assets."

5. Federal Reserve Board of Governors (FRB), Governor Christopher J. Waller, "Reflections on a Maturing Stablecoin Market," speech given at A Very Stable Conference (San Francisco, CA, February 12, 2025); Securities and Exchange Commission (SEC), "Staff Accounting Bulletin No. 122," January 23, 2025; SEC, "SEC Crypto 2.0: Acting Chairman Uyeda announces formation of new crypto task force," press release, January 21, 2025.

6. Office of the Comptroller of the Currency (OCC), "OCC clarifies bank authority to engage in certain cryptocurrency activitiesv," news release, March 7, 2025.

7. US Congress, "S.394 – GENIUS Act of 2025"; US House Committee on Financial Services, "Hill and Steil release discussion draft for stablecoins"; US House Committee on Financial Services Democrats, "Ranking Member Maxine Waters unveils bipartisan stablecoins legislation."

8. DefiLlama, "Stablecoins circulating," accessed March 11, 2025.

9. Ibid.

10. Roy Ben-Hur et al., "Digital asset risk assessment: A new paradigm in risk management," Deloitte, 2022.

Works cited

- US House of Representatives, "Stablecoin Transparency and Accountability for a Better Ledger Economy (STABLE) Act of 2025," discussion draft introduced February 6, 2025.
- Financial Stability Board (FSB), "FSB Global Regulatory Framework for Crypto-asset Activities," July 17, 2023.
- Monetary Authority of Singapore (MAS), "MAS Finalises Stablecoin Regulatory Framework," press release, August 15, 2023; MAS, "Response to Public Consultation on Proposed Regulatory Approach for Stablecoin-related Activities," August 15, 2023.
- HM Treasury, "Update on Plans for the Regulation of Fiat-backed Stablecoins," October 2023."Update on Plans for the Regulation of Fiat-backed Stablecoins,", October 2023., Update on plans for the regulation of fiat-backed stablecoins - GOV.UK (www.gov.uk)
- Bank of England, "Regulatory regime for systemic payment systems using stablecoins and related service providers", November 2023.
- Hong Kong Monetary Authority (HKMA), "Legislative Proposal to Implement the Regulatory Regime for Stablecoin Issuers in Hong Kong," December 2023.
- US Senate, "Lummis-Gillibrand Payment Stablecoin Act," 118th Cong., introduced April 2024.
- Bank for International Settlements (BIS), "Stablecoins: regulatory responses to their promise of stability," April 2024.
- Circle Group, "Circle Announces USDC Smart Contract for Transfers by BlackRock's BUIDL Fund Investors," press release, April 11, 2024.
- Circle Group, "USDC Reserve Report," February 27, 2025.
- Office of the Comptroller of the Currency (OCC), "Comptroller's Licensing Manual: Charters," December 2021.
- Ripple, "Championing Blockchain and Crypto Utility with Ripple's USD-backed Stablecoin," April 4, 2024.
- Circle Group, "An Overview of USDC and Circle's Stablecoin Infrastructure," October 24, 2023.
- CoinDesk, "*PayPal to Issue Dollar-Pegged Crypto Stablecoin Based on Ethereum and Issued by Paxos*," August 8, 2023.
- Solana, "Case Study: Helio's Shopify x Solana Pay Plugin Powers Phone Sales," April 25, 2024.
- Federal Reserve Board of Governors (FRB), Speech by Governor Christopher J. Waller, "Reflections on a Maturing Stablecoin Market," February 12, 2025.
- Total Stablecoins Market Cap, "Stablecoins Circulating - DefiLlama. January 27, 2025, March 6, 2025
- OCC, "Interpretive Letter 1183," March 7, 2025. *See also* OCC, "Interpretive Letter 1179," November 18, 2021.

Contacts

Richard Rosenthal
Business & Entity Transformation Leader
Principal
Deloitte & Touche LLP
rirosenthal@deloitte.com

Roy Ben-Hur
Managing Director
Deloitte & Touche LLP
rbenhur@deloitte.com

Rob Massey
Global Tax Leader - Blockchain and Cryptocurrency
Deloitte Tax LLP
rmassey@deloitte.com

Tim Davis
Principal
Deloitte & Touche LLP
timdavis@deloitte.com

Irena Gecas-McCarthy
FSI Director, Deloitte Center for Regulatory Strategy, US
Deloitte & Touche LLP
igecasmccarthy@deloitte.com

Richard Mumford
Independent Senior Advisor to Deloitte & Touche LLP
rmumford@deloitte.com

Arpita Mukherjee
Senior Manager
Deloitte & Touche Assurance & Enterprise Risk Services
India Private Limited
arpimukherjee@deloitte.com

CJ Burke
Manager
Deloitte & Touche LLP
cjburke@deloitte.com

Jacob Lewtan
Manager
Deloitte Services LP
jlewtan@deloitte.com

Meghan Burns
Manager
Deloitte Services LP
megburns@deloitte.com

Neeraj AS
Manager
Deloitte & Touche Assurance & Enterprise Risk Services
India Private Limited
neeas@deloitte.com

Reishi Kumaar T
Manager
Deloitte & Touche Assurance and Enterprise Risk Services
India Private Limited
reist@deloitte.com

Rajat Sharma
Senior Consultant
Deloitte & Touche Assurance & Enterprise Risk Services
India Private Limited
rajatsharma6@deloitte.com

Zach Peterson
Consultant
Deloitte & Touche LLP
zpeterson@deloitte.com

Palash Gupta
Lead Solution Advisor
Deloitte & Touche Assurance and Enterprise Risk Services
India Private Limited
palashgupta@deloitte.com

Deloitte.