KPMG

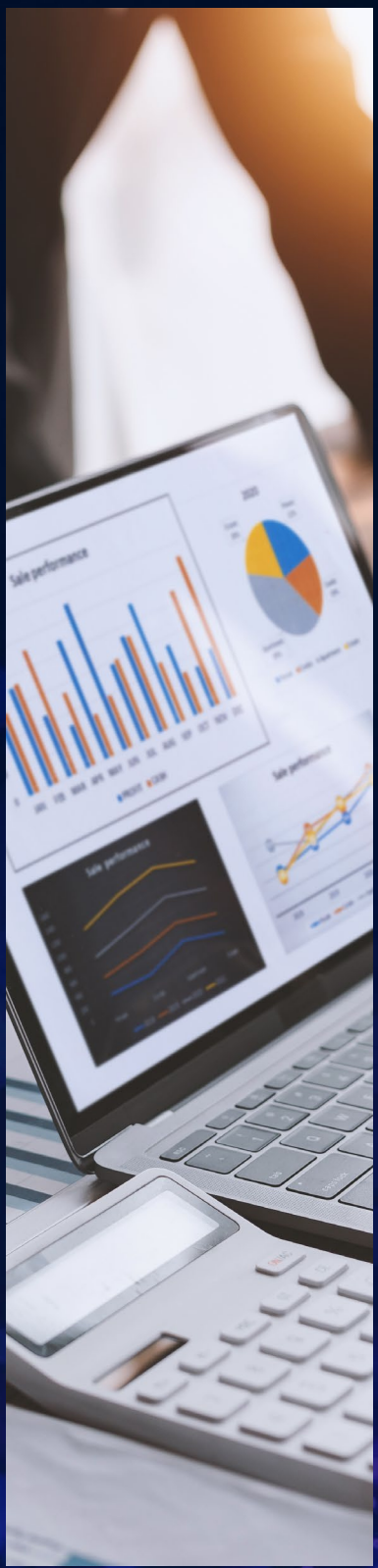
Stablecoins

The bridge between traditional finance and digital assets

Opportunities and challenges

Agenda

Introduction



Digital assets have once again taken center stage, ignited by recent US executive orders, a shift in regulatory guidance from federal agencies, and the enactment of stablecoin legislation via the Guiding and Establishing National Innovation for US Stablecoins (GENIUS) Act, signed into law on July 18, 2025. Banks, and financial institutions more broadly, now have the green light to offer digital asset products and services, including transactions involving stablecoins.

Stablecoins have the potential to significantly disrupt traditional payment rails. They transact on public, permissionless blockchains like Ethereum, Solana, and Tron that operate 24x7x365 and offer near-real-time settlement across the globe with minimal transaction fees. Imagine being able to send an international payment for less than a penny that settles in a matter of seconds.

Stablecoins are governed through smart contracts, which are stored on public blockchains, developed and controlled by the issuer. They do not have the traditional volatility of digital assets like Bitcoin as they are pegged 1-to-1 to sovereign currencies like the US dollar.

Now, the GENIUS Act is further driving market adoption. The bipartisan GENIUS Act will help provide regulatory clarity for stablecoin issuers and create consumer protections by requiring audited reserves, enforced Know Your Customer/Anti-Money Laundering (KYC/AML) requirements, and prioritized insolvency claims for stablecoin holders.

Stablecoin use cases continue to grow. Whether they're being used for cross-border payments and remittances or for collateral and funding, companies are taking a close look at how they can incorporate stablecoins into their existing business models.

In this paper, we'll explore how stablecoins are disrupting existing payment rails, the benefits they provide, and the risk considerations companies must address when designing and implementing stablecoin solutions.

Foundation for change : GENIUS Act

In a landmark moment marking the first crypto legislation passed in US history, the GENIUS Act was signed into law in July 2025, providing a comprehensive US regulatory framework for “payment stablecoins.” This bipartisan legislation aims to provide clarity, consumer protection, and consistency for the fast-growing approximately $260 billion stablecoin market.

Permitted issuers: In broad strokes, the GENIUS Act restricts stablecoin issuance to regulated “permitted” issuers, such as subsidiaries of insured banks or newly chartered nonbank stablecoin companies, that are subject to federal or state supervision. These issuers must back their stablecoins 1-to-1 with US dollars or similarly liquid assets (e.g., short-term Treasuries) and maintain full reserves at all times. These issuers also face strict transparency and compliance obligations, including monthly disclosures of reserve holdings and redemption policies, and routine auditing of reserves. Consistent with bank requirements, issuers will be subject to AML rules similar to those under the Bank Secrecy Act (BSA).

Holders: Notably, the GENIUS Act protects stablecoin holders by giving them first priority to claim the reserve assets if an issuer becomes insolvent. It further clarifies that properly regulated stablecoins will not be treated as securities under US law, removing a major legal uncertainty for the industry. By establishing these guardrails, the legislation seeks to legitimize “digital dollars” as a secure part of the financial system, even directing the Federal Reserve to coordinate with foreign regulators to ensure stablecoins operate smoothly across borders. Holders of stablecoins will not be permitted to earn any form of interest or yield on their holdings paid by the issuer, and their holdings are not backed by deposit insurance issued by the Federal Deposit Insurance Corporation (FDIC).

Impact: Under this new regulatory framework, stablecoin issuers will need to obtain new licenses and maintain bank-like reserve standards, raising the bar for market entry. Banks and traditional financial institutions may see new opportunities in offering stablecoin services, potentially enabling faster payment networks. Major corporations in payments have been exploring stablecoins to reduce transaction costs and settlement time, and they stand to benefit from the GENIUS Act’s legal clarity and consumer protections that now make adoption less risky.

Asset managers and corporate treasurers could also feel ripple effects as regulated stablecoins might increasingly be treated like traditional liquid funds on balance sheets. Meanwhile, finance, accounting, and risk departments should be prepared for stablecoin transactions to fall under familiar compliance regimes, such as rigorous AML monitoring and audits, much like any other financial product.

The passage of the GENIUS Act marks a turning point in the United States, elevating stablecoins from a niche crypto tool to a mainstream financial instrument, as it provides for the first time the regulatory framework that banks and financial institutions have been looking for. As the world of digital finance continues to evolve, finance professionals across banking, investment, and corporate sectors will be closely watching the impact of this landmark legislation.

Foundation for change : GENIUS Act (continued)

Tax treatment

While the GENIUS Act did not contain any explicit tax changes, there are some important tax considerations to be understood when using stablecoins. First, the issuance of a stablecoin for fiat should not be treated as a taxable transaction. The issuance is more properly treated as issuing debt for tax purposes.

Second, stablecoins are not money for tax purposes but rather property, and this has several consequences. Upon disposition, there may be very small amounts of taxable gain or loss, as the value can fluctuate away from $1 by tiny amounts. Gains and losses will sometimes trigger Form 1099-DA reporting. And any "interest" one receives for the loan of stablecoins will be treated as ordinary fee income and not interest for tax (Interest can only come from true debt, which requires the loan of fiat currency as opposed to property.)

Accounting and disclosure treatment

Stablecoin holder considerations. The accounting evaluation of digital assets such as stablecoins is important for determining the initial classification and measurement, as well as the financial statement presentation and related disclosures.

The GENIUS Act defines a "payment stablecoin" as a digital asset issued for payment or settlement purposes, redeemable at a predetermined fixed amount, backed by reserve assets that can only be liquidated to redeem the stablecoins. Issuers must maintain at least $1 of permissible high-liquid reserves, such as US dollars or short-term Treasury bills, for each dollar of the stablecoin issued. Stablecoins that meet the GENIUS Act's definition of a payment stablecoin may qualify as financial assets under US generally accepted accounting principles (GAAP) because the GENIUS Act requires payment stablecoins to be redeemable at a predetermined fixed amount.

However, a careful analysis of a stablecoin’s terms and conditions should be performed to determine its appropriate accounting classification.

Stablecoin issuer considerations. The GENIUS Act mandates how the interest earned on the stablecoin reserves should be managed by the stablecoin issuer. This may impact the accounting analysis of whether the customer cash should be reflected on the stablecoin issuer’s balance sheet. In addition, the GENIUS Act also mandates disclosure requirements for permitted payment stablecoin issuers, including the disclosure of stablecoin redemption procedures and the issuance of monthly reports detailing outstanding stablecoins and reserve composition. These reports must be certified by executives and examined by registered public accounting firms.

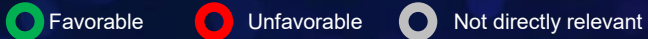
Furthermore, issuers with reserves exceeding $50 billion are required to provide audited annual financial statements in compliance with US GAAP. Companies that hold or are planning to hold stablecoins that would qualify as payment stablecoins should consider their capabilities in meeting the disclosure and audit requirements imposed by the GENIUS Act.

Drivers of opportunity

The GENIUS Act has boosted market confidence in digital assets, which have reached a critical turning point with a $4 trillion market cap. It has extended the engagement of major players who were already preparing for the uptake of stablecoins, as well as captured the attention of those on the sidelines. For many, the legislation introduces various benefits that will stimulate its adoption; for others, it may pose a challenge.

Selected impacts	Stablecoin issuers	Market Makers	*Counterparties*	*Asset managers*	*Correspondent banks*	*Clearing*	Retail	Fintechs
Disintermediation: Through use of public blockchain, roles previously filled by market participants will be displaced as a result of automation.								
Generates yield: Given reserves with US dollars, creates additional revenue streams.								
Efficient operations: Stablecoin transactions can often be performed more cheaply than conventional payments given the application of smart contracts.								
Instant cross-border payments: Facilitates real-time instant cross-border payments and quicker clearing and settlement for commercial transactions.								
Increased capital and liquidity in trading: Using stablecoins allows for near-real-time clearing and settlement in trading, which will enhance liquidity.								
Market demand: Retail and institutional users seek to adopt stablecoin for convenience and cost.								
New market entrants: Given the regulators' desire to diversify and promote new market entrants, stablecoins will create opportunity and challenge legacy financial institutions.								

Banks, counterparties, asset managers, etc.



Use cases: Cross-border payments

Why it matters for cross-border payments

Cross-border payments represent a clear near-term opportunity for banks to realize value from digital assets as banks look to move to instant cross-border payments. The current correspondent banking system processes $150 trillion annually[1] through networks that typically take 2–5 days for settlement, requires multiple intermediaries, and costs $25–$35 per transaction. Banks maintain substantial balances in nostro/vostro accounts globally to facilitate these flows, and digital asset solutions can address fundamental inefficiencies, including:

- **Settlement time:** Reduced from days to minutes or seconds (depending on specific blockchain used)
- **Cost:** Significant fee reductions have been observed, in some cases exceeding 99 percent compared to legacy payment rails
- **Capital efficiency:** Meaningful reductions in trapped liquidity as prefunding requirements are lowered
- **Transparency:** Real-time tracking and auditability versus opaque, "black box" processing.

Initial steps have been taken by some leading banks, who are processing transactions over blockchain rails. JPMorgan, for example, moves $2 billion daily[2] via its blockchain platform and PayPal launched their own proprietary stablecoin in 2023, which now boasts a $1.17 billion market cap.[3] These examples highlight the market demand for expansion into stablecoins.

[1] McKinsey, Global Payments Report, September 2023

[2] J.P. Morgan, Introducing Kinexys, November 2024

[3] www.coingecko.com

Use cases: Cross-border payments (continued)

Digital asset rails transform traditional cross-border processes by shortening the settlement time from several days to in most cases seconds (seconds or minutes depending on the chain), all while substantially reducing costs.

Correspondent bank

Initiation and processing

- Payment initiated, funds check, compliance checks, beneficiary bank validation
- Correspondent bank routing
- SWIFT MT103 / Pacs.008 message
- Holds in nostro account
- Next-day processing

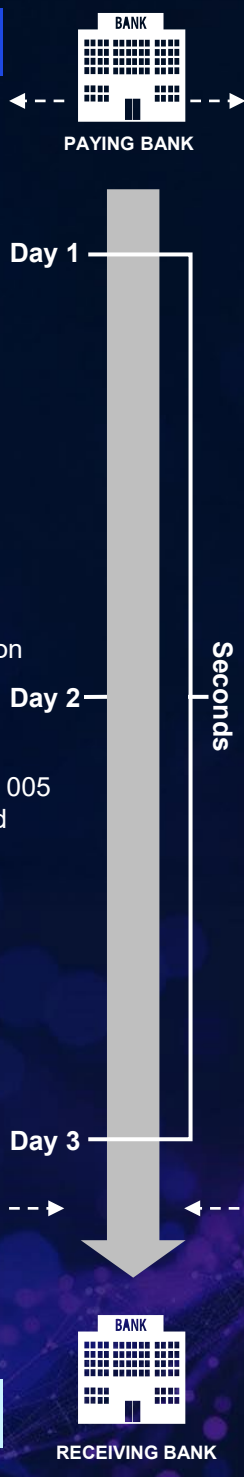
Correspondent hop
(multiple hops may be required)

- Message validation
- Compliance recheck
- Liquidity check
- Forward to next bank
- Nostro / Vostro Settlement
- Rate negotiation
- USD → EUR conversion executed
- .003 percent – 005 percent spread applied

Final settlement

- Beneficiary bank receives
- Final validation
- Credit to customer account
- Send confirmations
- Reconciliation complete

Settlement can happen on an average of two to three days



Digital assets

Initiation and processing

- Payment request: User initiates payment request with payment details (e.g., amount, currency, destination)
- Smart routing selects optimal path (public chain, cost, speed, liquidity optimized)
- Payment initiated (same compliance checks) via digital wallet

Blockchain network settlement

- Transfer and settlement performed on public blockchains
- No intermediary banks or institutions
- Currency conversion (off-chain), as needed

Completion

- Receiving partner credited
- Instant finality
- Confirmations sent
- Full transparency
- Immutable record
- Instant reconciliation

Settlement in under one minute (often a few seconds)

Use cases: Cross-border payments (continued)

The significant scale of this change will require coordinated changes across multiple major systems. A high-level representative view of the impacts to a bank's broader payments ecosystem as they incorporate stablecoins as an offering is provided below. First, an impact assessment should be conducted by banks looking to enter the stablecoin space to determine the specific risks/impacts across their payments ecosystem.

High-level cross-border payments technology architecture impact heat map

Front office layer

- Online banking
- Mobile banking
- Branch systems
- Corporate portal
- API gateway
- ATM

Core processing layer

- **Core banking platform**
  - *New digital asset account types*
  - *Balance management for multiple asset types*
  - *New transaction codes/workflows*
- **Treasury management system**
  - *Digital asset position management*
  - *Real-time liquidity monitoring*
  - *New asset class integration*
- **Payment hub**
  - *Support for underlying blockchain technology*
  - *Smart routing logic*
  - *New message formats*
- **Wallet infrastructure**
  - *Custody (hot and cold)*
  - *Integration with existing technology stack*
  - *On-chain connectivity*

Data and analytics

- **Data warehouse**
  - *New data structures*
  - *Blockchain event ingestion*
- **Analytics platform**
  - *New dashboards and reports*
- **Integration platform**
  - *Integration of external and internal data sources*
  - *Need for additional blockchain technology infrastructure*

Back office

- **General ledger**
  - *New account codes*
- **Settlement systems**
  - *New settlement instructions*
  - *Updates needed to ensure 1:1 ratio with stablecoin supply*
- **Reconciliation**
  - *Automated matching with internal accounting systems and blockchain ledger*

Risk and compliance

- **KYC/AML system**
  - *Blockchain analytics tools and integration*
  - *New transaction monitoring rules*
- **Risk management platform**
  - *New asset class parameters*
  - *Counterparty risk for liquidity providers*
- **Regulatory reporting**
  - *New report formats*
  - *Real-time reporting capability*

High-priority changes

- ***Payment hub*** *would require updates to add support for underlying blockchain (e.g., Ethereum) in addition to the existing payment rails*
- ***Core banking*** *needs new account structures for digital asset holdings*
- ***Treasury*** *must track positions across traditional and digital assets*
- ***Wallet infrastructure*** *needs to be developed/implemented to authorize and approve on-chain transactions*

Key integration points

- ***API gateway*** *becomes critical for partner connectivity*
- ***Real-time data feeds*** *required between systems*
- ***New compliance integrations*** *with blockchain analytics providers*

- *Low impact: Minor updates or reporting only (Months 1–6)*
- *Medium impact: Integration and configuration changes (Months 7–12)*
- *High impact: Significant changes to core functionality (Months 13—18)*

Use cases: Trading

Why it matters for trading

With the potential for real-time settlement, stablecoins and underlying blockchain capabilities will accelerate migration to T+0 for qualified asset classes, impacting multiple phases of the trading lifecycle. This acceleration, coupled with the emergence of innovative technology, will have far-reaching impacts across the trading lifecycle. From onboarding to regulatory reporting, firms need to address these impacts and the potential for increased efficiency and reduced costs.

	Onboarding	Transaction qualification and execution	Transaction monitoring	Clearing	Settlement	Reporting
Challenges	New client types such as Web3 and crypto native players	Recency of market data in real time for digital and tokenized asset classes		Real-time application of post-trade confirmation reconciliation	Real-time estimation of liquidity and capital consumption	Real-time capability for digital asset and regulator requirements for T+0 or T+1
Focus areas – Phase	• Modified standards for credit and margin demands reflected in credit support annex (CSA) • Treatment of collateral types for margin • Application of liquidation bots and instant termination in CSA	• Total participant exposure • Model risk management • Qualified market risk and validity of value at risk	• Real-time reporting on exposures and market position against limit standards • Responsive stop-loss triggers • Robust application of margin requirements and liquidation	• Tokenization of asset types and speed of clearing • Reduction of reconciliation steps and time • Opportunities for new central counterparty clearinghouses to evolve as digital asset custodians • Potential to pre-fund transactions, reducing risk	• Netting of liquidity consumption in real time • Payments accuracy and speed	• Blending all to regulator requirements or different timing requirements for digital assets than others • Alignment of systems and governance oversight
Focus areas – Enterprise	Capital allocation and strategy by product type Treasury and funding strategy Liquidity estimation and planning Enabling technologies, workflow, and ecosystem partnerships Evolution of standards for governing stablecoin clearing (ISO, ERC-20, etc.)					

Market timing: Imminent | Future

Benefits

- Lower-cost automated operations
- Enhanced liquidity management
- Liberated capital
- Potential to remove FX barriers
- Increased settlement timing and reduction in capital tie-up

Use cases: Trading (continued)

Stablecoins represent both a challenge and an opportunity in trading. They necessitate comprehensive upgrades across system architecture for blockchain integration, enhanced compliance, and market expansion, which will demand significant investment in interoperable, scalable solutions to maintain a competitive advantage.

High-level trading technology architecture impact heat map

Front office layer

Retail customer execution	Institutional execution	Prime broker and securities lending
EMS/OMS	Onboarding	Market data

Trades processing

Enrichment/risk management
- *Blockchain transactions and associated controls*
- *Support for both fiat-collateralized and crypto-collateralized stablecoins*

Allocation/affirmation/confirmation
- *Dynamic allocation adjustments*
- *Event-driven systems for efficient alerts*
- *Links to new confirmation systems*

Asset servicing
- *Integration into multiple blockchains and vendors*
- *Transparent reporting of holdings for processing corporate actions*

Clearing and settlement

Central depositories/custody
- *Secure stablecoin handling*
- *Enhanced custody processing*
- *Wallet integration*

Clearing
- *Secure management of transaction disputes and failures*
- *Resilient fail system ensures scalability*

Settlement
- *Streamline operational processes*
- *Implement blockchain settlement*

Data and analytics platforms

Trade data
- *Transaction records*
- *New data pipelines*

Client data
- *Enhancements to customer data platform for specific attributes*

Account data
- *Enhancement of accounts structure*

Back office book and records

Margin/collateral
- *Inventory management*
- *Reserve management*

Treasury/funding
- *Enhanced data integration*
- *Fees/network costs*

Reconciliation
- *Utilize blockchain transparency*
- *Ensure transaction finality and accuracy*

Risk and compliance

Compliance and supervision
- *Rule interpretation*
- *Adherence to new rules*
- *Real-time reporting*

Risk management
- *Real-time stability monitoring*
- *Stress-test algorithmic stablecoins*
- *Enhance governance*

NFRR
- *Enhance transactional scrutiny*
- *Report generation quality control*

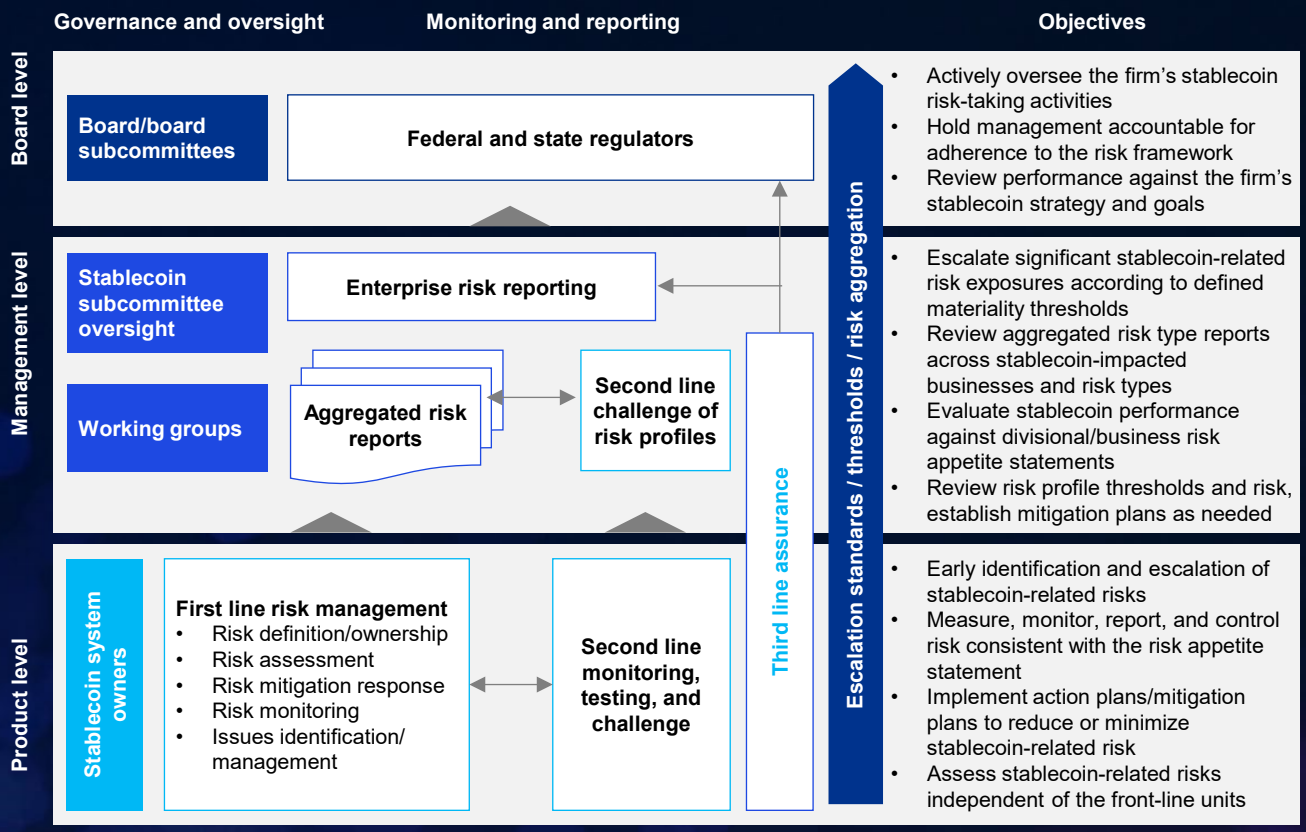
Architectural changes
- Required integration of blockchain APIs
- Upgraded trading systems
- Enhanced user interfaces
- Inclusion of blockchain analytics
- Updates to risk models
- Automated compliance workflows
- Real-time data monitoring
- Incorporation of blockchain nodes
- Hybrid data architectures
- Upgraded settlement frameworks
- Development of middleware layers
- API gateways updates
- Enhanced cybersecurity protocol

Impact	Impact detail and timeline
High	• Core infrastructure changes • Phase 1 (Months 1–6)
Medium	• Integration and configuration changes • Phase 2 (Months 7–12)
Low	• Minor updates or reporting only • Phase 3 (Months 13–18)

Trust and adoption: Governance

Establishing stablecoin governance

When incorporating payment stablecoins into your business model, governance will be paramount to help ensure that all relevant risks are identified and subsequently mitigated. Given that stablecoins transact on public blockchains, they will introduce new inherent risks to an organization that must be incorporated into existing risk taxonomies.



Refine policies and controls

Any new product launch requires a thorough assessment of inherent risks and corresponding mitigation strategies through policies, procedures, and governance. After establishing initial stablecoin risk management standards, organizations must enhance existing payment controls to accommodate stablecoin operations. Updates should address blockchain and digital asset considerations, including those around custody, business strategy, operations, continuity planning, compliance, and monitoring. Regular policy reviews and audits are essential to building organizational and customer trust, with ongoing updates to align with evolving regulations.

Trust and adoption: Regulatory and compliance

As stablecoins and other digital assets evolve, issuers, exchanges, and service providers must continuously adapt their AML strategies. Organizations should focus on the following foundational components to establish compliant operations across the digital asset ecosystem, including decentralized finance (DeFi) platforms, centralized exchanges, and stablecoin payment networks.

Focus areas	KYC	CIP/CDD /EDD	Red flags program	Transaction monitoring	Dynamic risk assessment	Strategic partnerships and tools
Why it matters	• Enhances security and compliance by verifying identities, reducing fraud, and aligning with regulatory requirements	• Customer identification programs (CIP)/ customer due diligence (CDD) verify customer identities and assesses risk profiles; enhanced due diligence (EDD) requires more in-depth investigation for higher-risk customers	• Identifies and monitors suspicious activity for early intervention to prevent fraudulent activities and help ensure compliance with financial regulations	• Automates scrutiny of financial transactions to detect anomalies or suspicious patterns, helping to prevent fraud and money laundering, and helps ensure adherence to regulatory standards	• Establishes a flexible risk assessment framework that can adapt to both internal and external changes, including new regulatory requirements	• Leverages external expertise and technological solutions to strengthen monitoring capabilities beyond internal resources
Key actions	• Require detailed documentation of funds origin, especially for transactions involving crypto exchanges • Schedule periodic reverifications of customer identities using advanced methods like biometrics; this will play a key role in onboarding processes that are fully online	• Categorize and continually monitor customers based on risk profile with varied levels of scrutiny, especially for those exposed to crypto-related transactions • Establish clear transaction purposes and scrutinize business relationships, particularly involving significant funds or high-risk regions	• Enhance red flag indicators targeting non-monetary alerts, such as IP correlation to online activity, inconsistent identification information, and reluctance to provide information	• Update models to detect unusual transaction patterns and relationships, such as rapid money movement • Tailor risk indicators to specific cryptocurrency activities, such as frequent small transactions to exchanges or sudden spikes in account activity	• Continuously adjust risk parameters to cover a broad spectrum of potential threats • Schedule periodic risk model reviews to incorporate new data and insights • Engage cross-departmental teams to ensure risk assessment reflects comprehensive insights and covers all potential vectors of exposure	• Access cutting-edge tools and platforms for blockchain forensics and expertise • Participate in cooperative information sharing under Section 314(b) with other financial institutions to enhance detection capabilities

Next steps

1) Begin with a comprehensive risk assessment to identify vulnerabilities across customer types, products, and geographies.
2) Implement core controls—such as KYC, due diligence, and transaction monitoring—tailored to the institution's risk profile. Integrate red flag indicators into these processes.
3) Leverage automation, data analytics, and regular program reviews to ensure the AML framework remains efficient, scalable, and aligned with evolving regulatory expectations.

Trust and adoption: Cybersecurity

Stablecoins promise to compress settlement times from days to seconds for cross-border payments, but without disciplined governance and cybersecurity measures, they can just as quickly lead to compromise and catastrophic loss. Executives who embed these five pillars will be positioned to capture the efficiencies of digital dollars—while regulators, boards, and customers see a program that is audit-ready, resilient, and "safe and sound" by design.

Focus areas

	Institutional-grade custody	Smart-contract security	On-chain system security	Off-chain system security	APIs and infrastructure security
Why it matters	• Private keys enable mint, burn, and transfer functions; where compromise of keys can result in loss of funds as crypto transactions are irreversible	• Bugs in issuance, redemption, or bridge code can lead to unlimited minting of stablecoins and result in loss/theft of funds	• The speed and pseudonymity of stablecoins enable poisoning scams, ransomware attacks, and sanctions evasion if flows go undetected	• Full backing is only as strong as the bank accounts, cash-equivalent assets, and enterprise resource planning (ERP) interfaces behind the token	• APIs are often required to bridge legacy systems with public blockchains and create a security risk if not properly controlled and managed
Key actions	• Use hardware security modules (HSMs), multi-signature and/or multiparty computation (MPC) custody • Enforce granular, role-based policy engines with approval thresholds • Segregate wallets for treasury vs. client flows	• Commission prelaunch formal verification, continuous bug-bounty programs, and orchestrated "chaos testing" in lower environments • Require third-party audits for any on-chain upgrades	• Deploy on-chain analytics and risk-scoring tools that flag zero-value transfers, mixer exposure, and high-risk jurisdictions • Automate Travel Rule data exchange where applicable	• Segregate reserves in bankruptcy-remote accounts and monitor them in real time • Integrate proof-of-reserve feeds with internal reconciliation dashboards • Engage a public accounting firm to conduct periodic proof-of-reserve attestations as required by the GENIUS Act	• Implement secure authentication protocols, such as Oauth2, JSON web tokens (JWT), or mutual TLS (mTLS) • Design APIs with rate-limiting restrictions to help prevent brute force attacks, DoS attacks, etc • Harden APIs against credential stuffing and session hijacking

Next steps

1) Run a joint CISO–Treasury workshop to map proposed payment flows, identify key-pair custodians and relevant systems, and agree on segregation-of-duties principles.
2) Refresh your cyber-risk appetite statement to cover stablecoins, token issuance, cross-chain bridges, and exposure thresholds to third-party stablecoins.
3) Perform a comprehensive risk assessment to identify inherent crypto-related risks, incorporating these risks into your risk taxonomy, and design and implement relevant controls to mitigate these risks.
4) Integrate blockchain analytics into your SIEM so on-chain anomaly alerts flow into the same 24/7 SOC queues as traditional threat intel.
5) Map critical dependencies (bridges, node providers), design hot-/warm-standby infrastructure, and test end-to-end incident response procedures.
6) Coordinate with regulators early as supervisors increasingly expect prenotification and evidence of robust controls.

Enablement

Enabling stablecoin transactions in a traditional bank or financial organization requires new architecture and integrations, but it can be accomplished with a high-level, modular approach using the following key components:

Digital wallet and custody infrastructure: Institutions need to securely hold and manage stablecoins on behalf of the business and/or their customers. Many banks may start with a custodial model—outsourcing storage and management of private keys to regulated third-party custodians—and gradually build in-house capabilities as they gain expertise over time. Robust digital wallet controls, including access management and transaction approval workflows, are essential for asset protection as stablecoins are bearer assets. Qualified custodians and providers of MPC or HSM key management solutions help alleviate the direct management of private keys by offering secure, automated private key solutions. These providers operate within audited control environments—such as those with SOC reports, insurance coverage, and enforced segregation of duties—helping to ensure strong operational and regulatory safeguards. Meanwhile, blockchain analytics firms offer address risk scoring, travel rule facilitation, sanctions and fraud monitoring, and case management tooling. Partnering with a third-party custodian can shift certain specialist functions outward. However, organizations can't outsource ultimate BSA/AML accountability, suspicious activity decisioning, and customer remediation processes. Institutions must still integrate alerts into existing operations, tune false positive rates, document risks and controls, and demonstrate controls effectiveness to regulators and internal audit functions.

Blockchain network connectivity: Stablecoin transactions require financial institutions to seamlessly integrate with public blockchain networks, either through direct node operation or service provider APIs. Companies can select networks based on speed, cost, and market acceptance (for example, USD-pegged stablecoins on Ethereum, Solana, etc.). In practice, companies can use middleware platforms that handle the blockchain interaction layer, eliminating the complexity of signing transactions and paying gas fees that would otherwise require deep blockchain coding in the institution's core systems.

API integration with core banking/ERP: The key to making stablecoins practical for everyday payments lies in integrating with the familiar interfaces and workflows of existing banking applications and corporate systems. Typically, APIs can bridge traditional banking platforms and corporate ERPs with public blockchain networks. For example, a bank could integrate a stablecoin transfer API into its online banking platform, enabling stablecoin transfers to feel as familiar to the user as a traditional payment operation. A well-implemented stablecoin integration will also support instant settlement capabilities, including automatic fiat-stablecoin conversions in the user's account, and embedded compliance checks for KYC/AML requirements as payments move on crypto rails.

The goal is to incorporate stablecoins without having to overhaul the entire IT landscape. By using APIs and platforms that extend existing systems to interact with blockchain networks, organizations can create an architecture where stablecoins flow through the organization much like any other currency—integrated with ledgers, payment operations, and customer touchpoints. For example, a corporate treasury could trigger a stablecoin payment to a vendor abroad directly from its ERP system once the stablecoin API is integrated, with the transaction recorded and reconciled in both the on-chain ledger and the internal accounting system.

Enablement (continued)

Stablecoin issuance platforms

"Stablecoin-as-a-service" platforms offer end-to-end support, including smart contract development, reserve administration workflow, attestation data feeds, mint/burn controls, and regulatory compliance reviews. Even so, an issuing company retains multiple responsibilities: smart contract ownership, reserve asset strategy (cash, T-bills, concentration limits), liquidity stress scenarios, legal opinions on token structure (stablecoins versus tokenized deposits), financial reporting treatment, tax/accounting mapping, operational resilience (incident, key compromise, chain outage), and customer disclosures (redemption rights, cutoff times). Platform support can increase speed around time to market, but internal ownership of risk, disclosures, and supervisory engagement cannot be fully outsourced. Institutions may prudently start by leveraging established third-party stablecoins (e.g., USDC) while building the governance scaffolding required before issuing their own proprietary stablecoin.

Internal readiness: Technology, processes, and people

Enabling stablecoins not only is a tech integration project, but also involves preparing the organization's processes and people for a new asset class that operates on decentralized, public blockchains. Institutions should consider the following internal readiness steps as they build out their strategy:

- **Policy and compliance training**: Update internal policies to include stablecoin handling, such as guidelines for employees on transferring or custodying stablecoins and procedures for reporting any security incidents. Train compliance officers and customer service teams on the nature of stablecoin transactions. For example, staff should understand that while a stablecoin is pegged to US dollars, it isn't FDIC-insured—and stablecoins cannot pay interest by the issuers or be classified as "deposits" as spelled out in the GENIUS Act. Employees will need to confidently explain to customers how stablecoin payments work, what risks they present, and how the company is ensuring that transactions are safe and compliant.
- **Dedicated cross-functional team**: Many banks are appointing digital asset teams or task forces that span the IT, risk, operations, and legal business units to oversee stablecoin initiatives. This team would coordinate the rollout, ensuring that technology integration aligns with regulatory guidelines and that robust risk management procedures are in place. Having a cross-functional group also helps in tackling change management aspects: updating standard operating procedures, accounting treatments, and audit controls for this new asset class.
- **Risk management and security**: Companies should extend existing risk management frameworks to cover stablecoin activities. This includes liquidity risk, ensuring the chosen stablecoin has reliable 1:1 redemption (helped by GENIUS Act compliance mandating full reserves); cybersecurity, including secure handling of private keys and protection against hacks; and third-party risk if relying on external providers. Operational risk protocols must be updated because, unlike a mistaken automated clearinghouse (ACH) transfer that can be reversed with bank intervention, on-chain transactions are irreversible. Therefore, internal processes might include pretransaction verification steps for large stablecoin payments.

Customer experience and education: Finally, introducing stablecoin services requires a strong focus on customer experience. Banks should make using stablecoins as simple and intuitive as any traditional payment method—offering clear in-app options, transparent fees, and reliable customer support. This may involve updating user interfaces to display stablecoin balances alongside traditional accounts, as well as providing educational content that explains the benefits, risks, and disclosures in plain language. It will be important to communicate that GENIUS Act-compliant stablecoins are essentially digital dollars operating on faster, modern payment rails that allow for instant transfers and 24/7 availability. Ultimately, building trust is essential: customers are more likely to adopt stablecoin services if they're confident the bank has made them safe, easy to use, and valuable for real-world needs like lower-cost cross-border payments or faster vendor settlements.

How KPMG can help

KPMG has provided services around digital assets and blockchain technology for nearly a decade. Our cross-functional team of digital asset subject matter professionals offer wide-ranging support for companies to evaluate digital asset strategies, design and implement an appropriate operating model, create governance frameworks and underlying controls, and enable technology and operations.

Strategic advisory services

KPMG helps to identify digital asset opportunities and market entry points. We conduct extensive market landscape analyses to help identify competitive positioning and strategic advantages for specific digital asset products and services, as well as detailed financial impact assessments and ROI calculations for potential investments.

Integration and operations

We help develop operating models and design system architectures for efficient integration with existing technologies that can align digital asset initiatives with corporate strategies. This includes build vs. buy assessments for third-party custody solutions based on the strategic objectives, risk appetite, and in-house expertise of the company.

Governance, risk, and controls

KPMG advises companies on their most pressing governance, risk, and regulatory challenges. We have deep experience assisting our clients navigate complex transactions and applications (e.g., bank charters, money transmitter licenses, etc.), as well as experience in developing and enhancing risk management programs, including those for financial crimes, cybersecurity, and third-party vendor management. Our clients have found that robust internal control programs are key to offering scalable and regulatory compliant stablecoin services.

Payments

KPMG conducts impact assessments and can create a strategic roadmap across a company's broader payments ecosystem (as with any new payment type/chance such as instant payments or ISO 20022).

Compliance and forensics

KPMG has deep, extensive experience with digital asset compliance, enabling us to assist institutions with managing KYC, transaction monitoring, regulatory, and reputational risk. We have helped institutions establish policies and procedures; design monitoring controls that are tailored to an institution's customer type, products, and services; and perform independent assessments to evaluate the institution's overall compliance function against regulatory requirements and industry-leading practices. KPMG can assist with providing surge support for specific AML-related operational tasks and has extensive experience delivering tailored trainings to targeted audiences within the institution.

Our team stands ready to provide tailored solutions to meet your company's unique needs. We look forward to speaking with you about your digital asset strategy and working together to drive success.

Contact us

Brian Consolvo
Cyber & Tech Risk
E: bconsolvo@kpmg.com

Eamonn Maguire
FS Ops
E: emaguire@kpmg.com

Contributing authors

Dallas Bray
Director
FS Ops

Greg Genega
Manager
Digital Assets & Innovation

Michael Martinen
Managing Director
Capital Markets

Robert Sledge
Partner
Audit

Jason Bui
Managing Director
Accounting Advisory Services

Alex Jaramillo
Senior Associate
FS Ops

Turgay Mehmet
Managing Director
C&O Financial Services

Courtney H. Trimble
Principal
Payments

Steve D'Antuono
Principal
Forensics

Chris Konecny
Managing Director
Banking & Payments Technology

Ihsan Siddiqui
KPMG
FS Ops

Tony Tuths
Principal
Tax

For more digital assets and stablecoins insights: visit.kpmg.us/DigitalAssets

KPMG

kpmg.com

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities.

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act upon such information without appropriate professional advice after a thorough examination of the particular situation.

MADE | MDE200791 (September 2025)