ripple | BLOCKCHAIN ASSOCIATION SINGAPORE

Best Practices for Custody and Security for Institutional Stablecoin Users

2025

Stablecoins are becoming a critical component of institutional finance, providing efficiency, liquidity, and stability for payments, settlements, and treasury management.

However, as their adoption increases, ensuring the security and integrity of stablecoin holdings requires robust custody solutions.

This report, developed by the Blockchain Association of Singapore (BAS)'s Stablecoin & CBDC, and Cybersecurity Sub-Committees, outlines key principles for safeguarding stablecoins, incorporating global best practices tailored for institutional users.

Institutional Custody Models for Stablecoins

Custody solutions for stablecoins generally align with broader digital asset custody models but differ in their emphasis on compliance, operational security, institutional-grade risk management and the regulatory landscape around stablecoin adoption. The primary custody models include self-custody, third-party custody, and hybrid solutions, each catering to different institutional needs.

Licensed Digital Asset Custodians

(Third-Party Custody Providers)

Third-party custodians manage stablecoins on behalf of institutions requiring regulatory compliance and secure storage solutions. Digital asset custodians, such as Archax and BDACs, provide institutional-grade security, including multi-signature authentication, key recovery mechanisms, and compliance oversight. Many of these custodians are insured, offering protection against cyber threats and operational risks. Financial institutions also turn to bank-grade custody solutions, with firms like BNY Mellon and Standard Chartered's Zodia Custody providing regulated custody services integrated with traditional banking infrastructure.

Self-Custody Models

Institutions that require full control over their stablecoin holdings may opt for self-custody solutions. This approach eliminates counterparty risk but demands rigorous security practices to prevent unauthorised access or asset loss. Hardware wallets provide offline security for long-term holdings, while multi-signature wallets allow enterprises and DAOs to implement governance structures requiring multiple approvals for transactions. Some institutions also use distributed security models, which reduce single points of failure and enhance private key protection.

Hybrid Custody Models

Depending on the needs of institutions, they may opt for a hybrid approach, which combines various elements of self-custody and third-party custody. This model allows institutions to retain control over certain assets while leveraging the security and compliance benefits of a third-party custodian for others.

Tailoring Custody to Institutional Needs

Selecting the right custody model depends on an institution's specific risk tolerance, operational requirements, and regulatory obligations. Institutions engaging in high-frequency transactions may prefer centralised custody solutions for efficiency, while those focused on long-term holdings or decentralised governance structures may opt for hybrid or self-custody models.

Key Differences Between Custodians and Custody Technology Providers

Unlike custodians, custody technology providers offer infrastructure and software solutions that help institutions manage digital asset security without directly holding the assets. These providers enable organisations to implement advanced security features such as multi-signature wallets, hardware security modules (HSMs), and real-time transaction monitoring while maintaining operational control over their stablecoins.

Access and Control

- Custodians directly manage client assets, providing regulated security solutions.
- Custody technology providers enable institutions to manage their assets independently, offering enhanced security tools without taking custody.

Insurance Coverage

- Custodians provide insurance policies to mitigate risks such as cyberattacks, fraud, or operational failures.
- Custody technology providers do not typically offer direct insurance for client assets but provide security measures to minimise risks.

Backup and Recovery

- Custodians are responsible for full asset recovery in case of loss, system failure, or cyber incidents.
- Custody technology providers offer backup solutions but place the responsibility for key management on the institution.

Regulatory Protection

- Custodians operate under financial regulations that ensure compliance with AML/CFT standards, capital requirements, and investor protection rules.
- Custody technology providers are generally not subject to the same regulatory requirements since they do not hold client assets.

A Security-First and Compliance-Driven Approach to Stablecoin Custody

A security-first and compliance-driven approach is essential for institutions managing stablecoin custody. As global regulators increasingly focus on digital asset custody, institutions must implement best-in-class security frameworks while maintaining oversight of evolving regulatory developments. Establishing credibility, navigating regulatory uncertainty, and fostering user trust require institutions to proactively align their custody practices with emerging compliance standards while ensuring robust security measures remain at the core of their operations.

Robust Private Key Management and Cybersecurity Measures

Private key security is a critical component of institutional stablecoin custody. Institutions must deploy advanced cryptographic solutions to prevent unauthorised access and reduce single points of failure. Strong encryption protocols, multi-factor authentication (MFA), and continuous security monitoring must be enforced across all storage and transaction layers. Cold storage solutions should be mandated for large reserves, while operational wallets should implement real-time fraud detection and anomaly tracking.

Given the increasing sophistication of cyber threats, regulators may introduce mandatory security assessments, such as penetration testing, incident response planning, and cybersecurity audits. Custodians and institutions must remain agile in updating security protocols, ensuring that governance frameworks evolve alongside technological advancements.

Asset Segregation and Regulatory Oversight

Custodians should implement strict segregation of client assets from proprietary funds to ensure that institutional holdings remain protected in the event of financial distress, fraud, or operational failures.

As regulatory standards evolve, there is growing recognition of the need for custodians to maintain both on-chain (tokenised) and off-chain (real-world asset-backed) segregated accounts, supporting full auditability and verifiability of backing reserves.

Independent third-party audits should be conducted periodically to validate asset backing and ensure that stablecoin reserves remain unencumbered. These practices are increasingly seen as foundational to trust, transparency, and regulatory alignment.

Incident Response and Recovery Plans

Regardless of the custody model used, institutions must establish a comprehensive incident response and disaster recovery framework. Contingency plans should account for key loss, cyber breaches, and operational failures, incorporating real-time monitoring and emergency access procedures. For third-party custodians, clear recovery mechanisms and liability frameworks must be in place, ensuring that clients retain access to their assets even in the event of custodian failure or security compromise.

Implementing a Risk-Based Custody Framework

Institutions must assess custody solutions based on their security needs, operational requirements, and regulatory obligations. A diversified strategy incorporating elements of self-custody, third-party custodianship, and custody technology providers allows organisations to manage risk effectively. The choice of custody model should be dictated by the institution's use case—for example trading, treasury management, or settlement functions—ensuring that security measures are tailored to the specific risks associated with each function.

1

Security Risks

Exposure to cyber threats, insider risks, and operational vulnerabilities.

2

Regulatory Risks

Compliance with jurisdictional requirements, AML/CFT obligations, and asset segregation rules.

3

Operational Risks

Resilience in transaction execution, recovery mechanisms, and business continuity planning.

4

Counterparty Risks

Due diligence on custodians, service providers, and key counterparties to mitigate insolvency risks.

Investor Protection and Insurance Frameworks

A well-regulated custody framework should not overlook the importance of implementing measures for investor protection. Custodians should be required to maintain adequate insurance coverage against cyberattacks, fraud, and operational failures. Institutions should also ensure that custody agreements include strong legal protections, minimising exposure to counterparty risks, and custodial insolvencies.

Licensing and Compliance Requirements

Institutional users engaging with stablecoin custody providers should be mindful of the regulatory status and compliance standards that underpin these services. Working with licensed providers that are subject to regulatory oversight helps ensure financial soundness, operational integrity, and appropriate risk safeguards. It is important to consider whether the provider's compliance approach aligns with the risk profile of the user. For example, institutional clients may require higher levels of transparency, asset segregation, and regulatory reporting compared to retail-focused services. Robust Anti-Money Laundering (AML) and Counter-Terrorism Financing (CFT) measures are also critical. These include adherence to the Financial Action Task Force (FATF) Travel Rule, effective transaction monitoring, and processes for identifying and reporting suspicious activity. Given the global nature of stablecoin transactions, a point for consideration would be whether stablecoin custody providers support cross-border AML/CFT compliance to help mitigate regulatory and operational risks across jurisdictions. As regulatory expectations continue to evolve, there is increasing recognition that compliance obligations may need to be calibrated based on the types of users being served. Differentiating between institutional and retail custody models can help ensure proportionate and risk-based oversight. This alignment strengthens institutional risk management and supports broader efforts to maintain market integrity and regulatory confidence.

Financial Stability Considerations

As stablecoins become more integrated into traditional financial systems, custody arrangements will increasingly play a role in supporting financial stability. Custodians should maintain adequate liquidity reserves to cover operational risks, security incidents, and client withdrawals. For larger custodians, periodic stress testing is important to assess resilience against market disruptions, cyber incidents, or systemic risks.

To maintain market confidence, business continuity and disaster recovery frameworks should be established for major custodians to ensure uninterrupted access to stablecoin holdings even in extreme scenarios. Regulatory coordination across jurisdictions is also critical in promoting the resilience of the broader financial ecosystem, particularly given the cross-border nature of stablecoin markets.

As regulatory bodies move toward establishing global standards for stablecoin custody, institutions must take a leadership role in shaping best practices that balance compliance with operational resilience.

Institutions that actively engage with regulators, industry consortiums, and policymakers will be better positioned to influence regulatory developments while ensuring their custody models remain adaptable to future compliance requirements.

By embedding security-first principles into a compliance-driven custody framework, institutions can enhance trust in stablecoins as a reliable settlement and liquidity instrument while ensuring financial stability and long-term resilience in digital asset markets.

About the Blockchain Association of Singapore (BAS)

The Blockchain Association Singapore (BAS) envisions being the leading industry platform for advocacy, collaboration, and fair use of blockchain and scalable technologies in Singapore and beyond. The association strives to empower its members and the broader community by fostering engagement with the latest trends, issues, and developments in these technologies. BAS facilitates collaborations and knowledge-sharing between regional and international stakeholders, promotes best practices and co-develops standards for blockchain governance, and provides education and training to build industry capabilities. BAS aims to empower the community and build industry capabilities, promoting best practices and co-developing standards for blockchain technologies. BAS is committed to driving digital transformation and cultivating a strong talent pipeline for the digital economy in Singapore. Learn more at singaporeblockchain.org

Members of the BAS Stablecoin and CBDC as well as the Cybersecurity Sub-Committees who contributed to this report include representatives from Ripple, Rakkar, StraitsX and CT Advisory Ltd.

About Ripple

Ripple is the leading provider of digital asset infrastructure for financial institutions—delivering simple, compliant, reliable software that unlocks efficiencies, reduces friction, and enhances innovation in global finance. Ripple's solutions leverage the XRP Ledger and its native digital asset, XRP, which was purpose-built to enable fast, low-cost, highly scalable transactions across developer and financial use cases. With a proven track record working with regulators and policymakers around the world, Ripple's payments, custody and stablecoin solutions are pioneering the digital asset economy—building credibility and trust in enterprise blockchain. Together with customers, partners and the developer community, we are transforming the way the world tokenizes, stores, exchanges, and moves value. Learn more at ripple.com

About Rakkar

Rakkar Digital Group stands as Asia's leading qualified digital asset custodian, offering unparalleled asset security to financial institutions. Fortified by our strategic backing from SCB 10X, the investment arm of the SCBX Group, Rakkar empowers institutions with secure and compliant custodial solutions with unmatched efficiency. Founded in 2022 and belting esteemed certifications and attestations in security excellence such as ISO27001, SOC 1 and SOC 2, Rakkar remains unwavering in its mission to offer the most secure, institutional-grade custodian services across Asia. Learn more at rakkardigital.com

About StraitsX

StraitsX is the stablecoin-native settlement layer driving global finance, and a Major Payment Institution licensed by the Monetary Authority of Singapore. As the issuer of XUSD and XSGD stablecoins, StraitsX leverages the power of blockchain and stablecoin technology to drive payments interoperability while offering innovative tools for liquidity management, stablecoin integration, and cross-border transactions. Partnering with leading financial institutions, global liquidity providers and payment technology partners. StraitsX delivers cutting-edge payment solutions in a highly regulated and reliable environment, bridging the gap between traditional finance and the digital economy. Learn more at straitsx.com

CT Advisory Ltd

CT Advisory Ltd is a boutique consultancy that specialises in Fintech, Web3, and Financial Services. Incorporated in Hong Kong, CT Advisory connects corporates, startups and investors, advancing digital innovation and technology exchange between Asia, Europe, and beyond.

With a sound track record around Web3-based transformation, digital currencies, finance and regulation, CT Advisory helps clients build strong use cases, solve real-world problems, and scale across continents. Actively contributing to major industry and government initiatives, CT Advisory conjoins a network of global innovation leaders and industry experts.

DISCLAIMER

This document is provided for general informational purposes only. Every effort has been made to ensure the accuracy of the information contained herein; however, neither the Blockchain Association of Singapore (BAS), Ripple, Rakkar, StraitsX and CT Advisory Ltd, nor any of their past, present, or future members or affiliates, makes any representations or warranties, express or implied, as to the accuracy, completeness, or suitability of the information. Neither BAS, Ripple, Rakkar, StraitsX and CT Advisory Ltd, nor their members or affiliates, shall be liable for any errors, omissions, or any outcomes arising from the use of this information, whether foreseeable or unforeseeable, and hereby disclaim all liability in respect of such use. The recipient acknowledges and agrees that any use of this document is at their own risk and constitutes acceptance of these terms. The recipient is responsible for informing any subsequent recipient of these terms and conditions. The information contained in this document does not constitute, and should not be construed as, an offer, recommendation, or solicitation to buy or sell securities or any other financial instruments. This document is a summary presented for informational purposes only and is not intended to be, and should not be relied upon as, legal or professional advice.

ripple