Fystack

Crypto Custody and Compliance

Guide

Practical insights for secure digital asset custody and regulatory compliance in **Asia Pacific (APAC).**





Secure Custody

Institutional-grade asset protection

Regulatory Compliance

Stay aligned with evolving regulations

Cross-Border Readiness

Navigate regional standards with confidence

Risk Management & Governance

Build robust controls and operational resilience

Secure Today. Compliant Tomorrow. Trusted Everywhere.

Fystack

About This Guide

Every regulator in this guide evaluates custody infrastructure across the same five dimensions. But the thresholds, enforcement mechanisms, and acceptable architectures vary significantly by jurisdiction.

1

Key Control

Who holds signing authority? Single vs. multi-party (MPC threshold).

2

Cold Storage

% of customer assets offline. Ranges from 80% (South Korea) to 95%+ (Japan); ~98% in practice (Hong Kong per SFC VATP Guidelines Part 10.8).

3

Asset Segregation

Customer funds technically and legally separated from operator funds.

4

Data Residency

Where are keys, signing logs, and transaction records stored?

5

Audit Obligations

Who verifies your infrastructure? Frequency and independence.

80-98%

Cold Storage Range

Across APAC (ex-SEA) markets

$4.3B+

Enforcement Penalties

Total across major crypto entities 2022–2023

$320B+

Global Stablecoin Cap

Mid-2026; USDT & USDC share 84%

4

Markets Covered

Hong Kong, Japan, South Korea, Australia

Fystack

Regional Framework: Four Markets. Four Compliance Realities.

A comprehensive side-by-side comparison of cryptocurrency custody regulations, infrastructure expectations, and licensing barriers across major Asia-Pacific markets outside Southeast Asia.

Market	Framework	Cold Storage	Key Requirements	Market Status
Hong Kong	SFC VASP Regime + Stablecoins Ordinance (effective 1 Aug 2025)	Principles- based custody framework; ~98% typical industry practice	SFC VASP license mandatory; client asset segregation; annual audit; stablecoin issuers require separate HKMA license (Stablecoins Ordinance effective Aug 1, 2025; first licenses issued 2026)	Active. Fastest-growing institutional hub in APAC
Japan	FSA Payment Services Act (PSA) + FIEA	At least 95% cold wallet or equivalent secure custody	CAESP registration with FSA; segregated customer wallets; annual independent audit; JVCEA membership	Mature. Most established licensing regime in region
South Korea	VAUPA (Jul 2024) + FTVA VASP Registration	Approximately 80% cold storage expected under prevailing supervisory standards	KoFIU registration; ISMS certification; real-name bank account; liability insurance ≥ 5% hot wallet value	Active. Strong consumer protection focus
Australia	AML/CTF Amendment Act 2024 + Digital Assets Framework Bill 2025	Risk-based; no fixed percentage mandate	AUSTRAC registration mandatory; AFSL requirements depend on service type and Digital Assets Framework finalization; Travel Rule obligations being progressively implemented under Australia's AML/CTF reforms	Transitioning. Major regulatory overhaul underway.

Note on Market Access: Mainland China continues to maintain a restrictive stance toward cryptocurrency trading and virtual-asset business activities - new market entry remains blocked. Taiwan (FSC VASP registration, effective from 2025) and India (PMLA VASP registration) are emerging compliance markets not covered in depth here but worth monitoring.

Fystack

Compliance Cost: The Price of Non- Compliance

Legal compliance and secure asset custody are not just regulatory check-marks:they are existential requirements that protect businesses from devastating financial penalties and permanent operational shutdown.

$4.3B+

Total Enforcement Penalties

Across major crypto entities 2022–2023 (Source: DOJ, NYDFS, OFAC public records)

$320B+

Global Stablecoin Cap

Mid-2026; subject to daily fluctuation. USDT & USDC share: 84%. Core risk: infrastructure non- compliance.

Entity / Year	Penalty	Regulator	Primary Violations
Binance (2023)	$4.3 Billion	DOJ, FinCEN, OFAC, CFTC	Systemic AML/sanctions violations (over 100,000 transaction alerts ignored)
Coinbase (2023)	$100 Million	NYDFS (New York)	AML/KYC backlog and immature transaction monitoring controls
Robinhood (2022)	$30 Million	NYDFS (New York)	Inadequate compliance staffing and manual transaction monitoring failures
Kraken (2022)	$362,158	OFAC (US Treasury)	Iran sanctions violations: lacked post-onboarding IP geolocation controls

Fystack

The Binance Lesson: How to Avoid Crippling Penalties?

By processing billions in prohibited transactions, Binance triggered a catastrophic $4.3B global settlement. This was due to systemic AML/KYC failures, willful evasion of sanctions, and a complete lack of compliance oversight, leading to the forced resignation and imprisonment of its CEO. A proactive, unyielding compliance program is the ultimate shield against absolute corporate ruin.

What Binance Did Right

- Systemic AML and KYC compliance failures
- Willful evasion of global sanctions programs
- Complete lack of proactive transaction monitoring

The Takeaway for APAC Operators

Ignoring compliance is no longer a viable business strategy. Building robust compliance infrastructure proactively - including real-time sanctions screening, automated transaction monitoring, and documented AML/KYC frameworks - is far less costly than facing billions in fines, forced executive restructuring, and immediate reputational ruin.

Fystack

Hong Kong: SFC VASP Regime + Stablecoin Ordinance

Hong Kong has emerged as the most active institutional digital asset hub in APAC,operating a dual-regulator model between the Securities and Futures Commission (SFC) and the Hong Kong Monetary Authority (HKMA).



Fystack

The Clearest Institutional Path in APAC

The SFC's VASP licensing regime became effective June 1, 2023 under the Anti-Money Laundering and Counter-Terrorist Financing Ordinance (AMLO). The Stablecoins Ordinance came into effect on August 1, 2025 (enacted May 2025). The HKMA began issuing the first stablecoin issuer licenses in 2026. Organizations strictly providing standalone custody services must align with the specialized VA Custodian licensing framework introduced under the AMLO updates.

Key Requirements

- An SFC VASP license is mandatory for all exchanges and custodians serving Hong Kong investors.
- Licensed platforms are generally expected to maintain approximately 98% of client assets in cold storage in line with SFC custody expectations. While this is not a statutory requirement, it is effectively expected in practice. The SFC is also exploring a more holistic framework that combines asset monitoring and insurance coverage.
- Client assets must be maintained in segregated accounts, with strict separation between customer funds and operator funds.
- Licensed platforms may serve both retail and professional investors, subject to SFC-imposed restrictions and token eligibility requirements.
- An annual independent audit of custody infrastructure is required.
- Stablecoin issuers must obtain separate licensing from the HKMA under the Stablecoins Ordinance, which took effect on August 1, 2025.
- AML and KYC controls must follow a risk-based framework aligned with FATF standards.
- Travel Rule compliance is required for transfers between VASPs.

Why Hong Kong Sets the Institutional Standard

- Hong Kong operates one of the most mature digital asset licensing regimes in APAC outside of Japan.
- Its dual-regulator framework assigns oversight of trading platforms to the SFC and payments and stablecoins to the HKMA, creating a clear separation between custody and issuance functions.
- Organizations that build and operate in accordance with Hong Kong regulatory standards can gain access to institutional capital flows across the Greater China region.

Fystack

Hong Kong Custody Checklist

01

Obtain SFC VASP license before serving HK investors

02

Target approximately 98% cold storage in line with prevailing SFC custody expectations

03

Implement client asset segregation with separate blockchain addresses

04

Establish AML/KYC framework aligned with HKMA/FATF standards

05

Deploy MPC threshold signing (2-of-3)

06

Integrate Travel Rule tooling for VASP-to-VASP transfers

07

Engage independent auditor pre-licensing

08

For stablecoin operations: register with HKMA under the Stablecoins Ordinance (effective Aug 1, 2025) separately

Fystack

Hong Kong: AML & Travel Rule Mandates

In addition to the SFC custody framework, VASP operators must adhere to rigorous AML/CFT requirements and information transfer protocols aligned with FATF standards.

Regulatory Notice: AMLO (Anti-Money Laundering and Counter-Terrorist Financing Ordinance) | **Verify VASP Networks:** TRUST, Verify VASP | **Implementation Date:** June 2023 (VASP regime); August 1, 2025 (Stablecoins Ordinance effective)

Mandatory Travel Rule

Every digital asset transfer between VASP entities must be accompanied by verified sender and recipient KYC details in real time

Network Integration

Operators must integrate secure messaging networks such as TRUST or VerifyVASP to transmit required transaction metadata

Sanctions Screening

Real-time screening against OFAC, UN, and local lists before transaction signing

Local Compliance Presence

A compliance officer based in Hong Kong is required for licensed operators

Fystack

Japan: FSA CAESP Licensing

Japan has the world's most established crypto regulatory regime, with a framework that predates Europe's MiCA regulation by several years. Its Payment Services Act (PSA) framework provides the clearest template for mature market operations in APAC.



Fystack

The Most Mature Framework in APAC

The FSA requires all Crypto-Asset Exchange Service Providers (CAESPs) to register and comply with stringent custody, segregation, and audit requirements. Japan was the first jurisdiction globally to formally regulate crypto-asset transactions.

Key Requirements

- CAESP registration with the Financial Services Agency (FSA) mandatory
- **At least 95% of customer crypto assets** must be safeguarded using cold-wallet or equivalent secure custody arrangements — the most stringent cold custody standard in APAC
- User assets audited annually by independent auditors
- Customer assets segregated from operator funds; separate management required
- AML/KYC compliance and full transaction monitoring
- Security tokens (equity/bond-type) governed separately under FIEA, requiring Type I financial instruments license
- JVCEA (Japan Virtual and Crypto Assets Exchange Association) membership is typically required for full licensing
- Travel Rule compliance applies to VASP-to-VASP transfers

Why Japan Sets the Technical Custody Standard

Japan's requirement that at least 95% of customer crypto assets be held in cold-wallet or equivalent secure custody is the most stringent cold custody standard in the APAC region. Its annual independent audit obligation and JVCEA self-regulatory framework create a mature compliance ecosystem. Operators who build to Japan's standards exceed the requirements of every other market in this guide. With the latest Payment Services Act (PSA) amendments coming into full effect in June 2026, operators must also navigate newly defined intermediary registration categories and stricter cross-border enforcement protocols by the FSA.

Fystack

Japan Custody Checklist

01

Register as CAESP with FSA before operating

02

Implement at least 95% cold wallet or equivalent secure custody by design

03

Deploy multi-party threshold signing (2-of-3 or 3-of-5 MPC)

04

Establish complete customer asset segregation

05

Set up annual independent audit engagement pre-licensing

06

Join JVCEA for self-regulatory framework participation

07

Implement Travel Rule tooling for all VASP transfers

08

Maintain full AML/KYC with transaction monitoring system

Japan: AML & Travel Rule Mandates

Japan's FSA enforces comprehensive AML/CFT requirements on all registered CAESPs, aligned with FATF Recommendations 15 and 16.

Regulatory Authority: FSA (Financial Services Agency) | **Self-Regulatory Body:** JVCEA (Japan Virtual and Crypto Assets Exchange Association) | **Cold Storage Mandate:** 95%+

CAESP Registration

All operators must be registered with the FSA. Unregistered operation is a criminal offense

Transaction Monitoring

Automated systems required to detect suspicious patterns; STRs filed with the FSA

Travel Rule

Mandatory for transfers between CAESPs; originator and beneficiary KYC data must be transmitted

Annual Audit

infrastructure, customer asset holdings, and compliance controls required every year

Fystack

South Korea: VAUPA + KoFIU Requirements

South Korea's regulatory framework is driven by two primary instruments: the Act on Protection of Virtual Asset Users (VAUPA, effective July 2024) and the FTRA VASP registration requirement via KoFIU.



Fystack

Active Market. Consumer Protection Focus.

South Korea has one of the most active retail crypto markets globally, with strict consumer protection built into its regulatory architecture. The VAUPA significantly raised operational standards for all VASPs in 2024.

Key Requirements

- **KoFIU (Korea Financial Intelligence Unit) registration** mandatory for all VASPs
- **ISMS (Information Security Management System) certification** from KISA required — operators cannot launch without it
- **Korean regulations generally require the majority of customer virtual assets to be maintained in cold storage, commonly interpreted as approximately 80% under current supervisory standards.**
- **Real-name bank account required:** VASPs must partner with a licensed Korean bank; anonymous fiat rails are not permitted
- **Liability insurance or reserves:** Minimum 5% of hot wallet asset value; floor of KRW 3 billion for major exchanges
- **Customer fund segregation:** Deposits held separately from operator funds in a designated bank account
- **Travel Rule:** Transfers of KRW 1 million (~$880) and above require Travel Rule compliance; FSC oversight

Why South Korea's Framework Matters for Fintechs

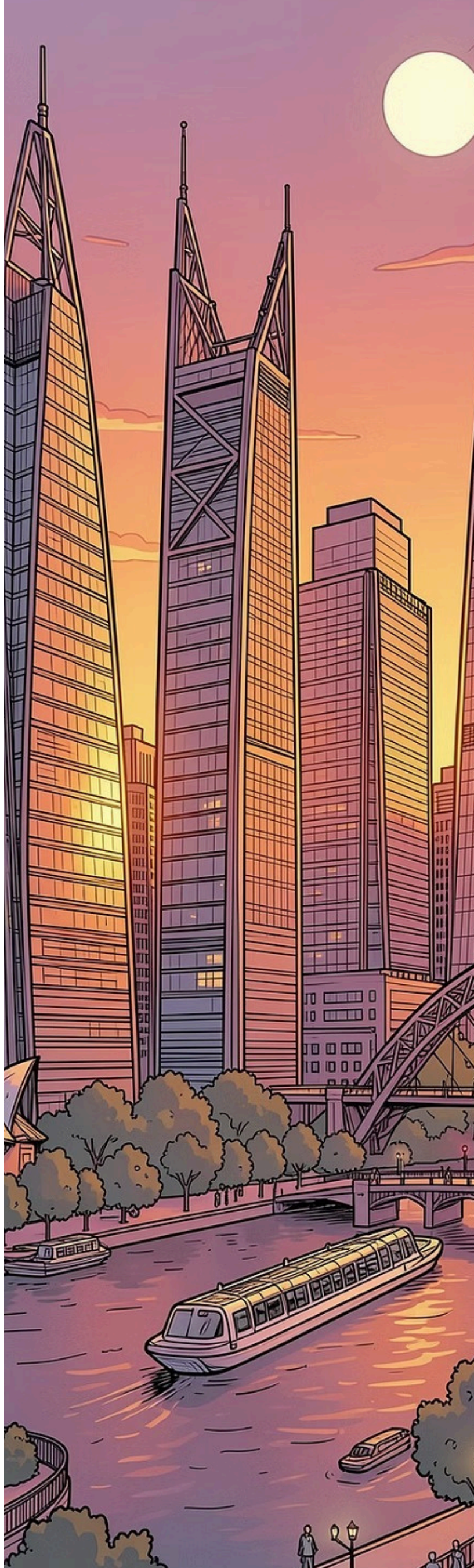
Korea's real-name bank account requirement creates a significant market access barrier-operators must establish a formal banking relationship before launch, not after. The ISMS certification requirement means technical compliance must be independently verified before licensing approval. The cold storage requirement (commonly interpreted as approximately 80%) is lower than Japan's but is explicitly enforced through liability insurance requirements covering the remaining hot wallet exposure.

Under recent regulatory tightening, KoFIU directly vets the criminal records and financial credibility of major shareholders, substantially raising the governance threshold for market entry.

Fystack

Australia: The Risk-Based Compliance Model

Australia's regulatory regime is anchored by the landmark Corporations Amendment (Digital Assets Framework) Act 2026, which formally integrates digital asset platforms into the AFSL framework under ASIC oversight. This is tightly coupled with rigorous anti-money laundering obligations and Travel Rule enforcement administered by AUSTRAC.



Fystack

Australia: Key Regulatory Pillars

ASIC's Role in Digital Assets

- **Licensing:** ASIC licensesandoversees financial service providers, which may include digital asset exchanges if their offerings constitute financial products (e.g., derivatives, managed investment schemes)
- **Market Integrity:** Ensures fair and orderly markets for crypto-related financial products, protecting investors from misconduct and deceptive practices
- **Custody Standards:** Provides guidance on the secure handling and segregation of client crypto assets, emphasizing robust risk management and operational resilience

AUSTRAC & AML/CTF Act

- **DesignatedServices:** Digital Currency Exchanges (DCEs) are designated as 'reporting entities' under the Anti- Money Laundering and Counter- Terrorism Financing (AML/CTF) Act 2006
- **Registration:** All DCEs must register with AUSTRAC before offering services in Australia
- **AML/CTF Program:** Required to develop and implement a comprehensive AML/CTF program, including KYC, transaction monitoring, and suspicious matter reporting
- **Travel Rule:** Implements the FATF Travel Rule for transfers, requiring collecting and sharing originator and beneficiary information for transactions above specific thresholds

Fystack

Australia: Compliance Checklist

Primary Regulators: ASIC (financialservices), AUSTRAC (AML/CTF) | Key Legislation: AML/CTF Act 2006, Corporations Act 2001

01

AUSTRAC Registration - Register as a Digital Currency Exchange (DCE) with AUSTRAC

02

AML/CTF Program Implementation - Develop and maintain a robust AML/CTF program, including risk assessments, customer identification (KYC), and ongoing transaction monitoring

03

ASIC Licensing Assessment - Determine if your digital asset offerings require an Australian Financial Services (AFS) Licence from ASIC and apply if necessary

04

Custody & Security Standards - Implement secure custody solutions for client digital assets, adhering to ASIC's guidance and industry best practices for segregation and risk management

05

Travel Rule Compliance - Ensure systems are in place to comply with the Travel Rule for crypto transfers, collecting and transmitting required information

06

Regular Reporting - Submit suspicious matter reports (SMRs) and threshold transaction reports (TTRs) to AUSTRAC as required

Fystack

New Zealand: Flexible Framework. Strong AML Oversight.

Unlike Japan, Hong Kong, or South Korea, New Zealand does not operate a dedicated crypto licensing regime. Businesses remain subject to AML/CFT obligations and broader financial services laws, creating a more flexible pathway for market entry.



FMA's Role & Financial Products

- **Financial Markets Authority (FMA):** The FMA regulates digital assets classified as financial products (e.g., equity tokens, debt tokens, or units in collective investment schemes)
- **FSP Registration:** Entities providing financial services related to crypto assets must register on the Financial Service Providers Register (FSPR) and comply with relevant market conduct rules
- **Disclosure & Fair Dealing:** Providers are obligated to provide clear, concise, and effective disclosure to investors and adhere to fair dealing requirements under the Financial Markets Conduct Act (FMC Act)

RBNZ's Oversight & Financial Stability

- **Reserve Bank of NewZealand (RBNZ):** The RBNZ maintains oversight of the financial system's stability, monitoring risks posed by crypto assets, especially those used as money substitutes
- **Stablecoins & Payments:** The RBNZ has indicated its interest in regulating stablecoins to ensure they do not undermine monetary policy or financial stability
- **Banking Sector Engagement:** Banks and other RBNZ-regulated entities engaging with crypto are subject to RBNZ's prudential supervision to manage associated risks

AML/CFT Requirements

- **AML/CFT Act 2009:**All crypto asset service providers (CASPs), including exchanges and custodians, are designated reporting entities under the Anti-Money Laundering and Countering Financing of Terrorism Act
- **KYC/CDD:** Strict Know Your Customer (KYC) and Customer Due Diligence (CDD) procedures are mandatory, including identity verification and ongoing monitoring of transactions
- **Suspicious Activity Reporting:** CASPs must report suspicious transactions to the Financial Intelligence Unit (FIU) to combat money laundering and terrorism financing

Custody Standards & Investor Protection

- **AssetSegregation:** Although not explicitly mandated by crypto-specific law, general financial services principles dictate that client assets should be segregated from operational funds
- **Security Practices:** Custodians are expected to employ robust cybersecurity measures and best practices for secure storage of digital assets to protect against theft and loss
- **Complaints & Dispute Resolution:** Financial service providers, including those dealing with crypto, are typically required to have internal and external dispute resolution processes for customer complaints

Fystack

New Zealand: Compliance Checklist

Primary Regulators: Financial Markets Authority (FMA), Reserve Bank of New Zealand (RBNZ) | Key Legislation: Financial Markets Conduct Act 2013, Anti-Money Laundering and Countering Financing of Terrorism Act 2009

01

FSP Registration & Disclosure

Register on the FSPR where offering regulated crypto-related financial products and comply with FMC Act disclosure requirements..

02

Robust AML/CFT Program

Implement and maintain a comprehensive AML/CFT program, including rigorous KYC/CDD, transaction monitoring, and suspicious activity reporting

03

Cybersecurity & Data Protection

Establish and enforce strong cybersecurity protocols and data protection measures to safeguard client information and digital assets

04

Secure Custody Solutions

Ensure secure storage and management of client digital assets, employing best practices for cold storage and segregation of funds

05

Consumer Protection & Fair Dealing

Provide transparent information to consumers regarding risks, fees, and terms, and establish effective internal and external dispute resolution mechanisms

06

Regulatory Reporting

Comply with all required reporting obligations to the FMA, RBNZ, and FIU, including annual AML/CFT reports and any specific financial product-related disclosures

Fystack

APAC Custody Standards: Side-by- Side

A comparative overview of key crypto asset custody requirements across APAC jurisdictions excluding Southeast Asia, highlighting regional regulatory trends.

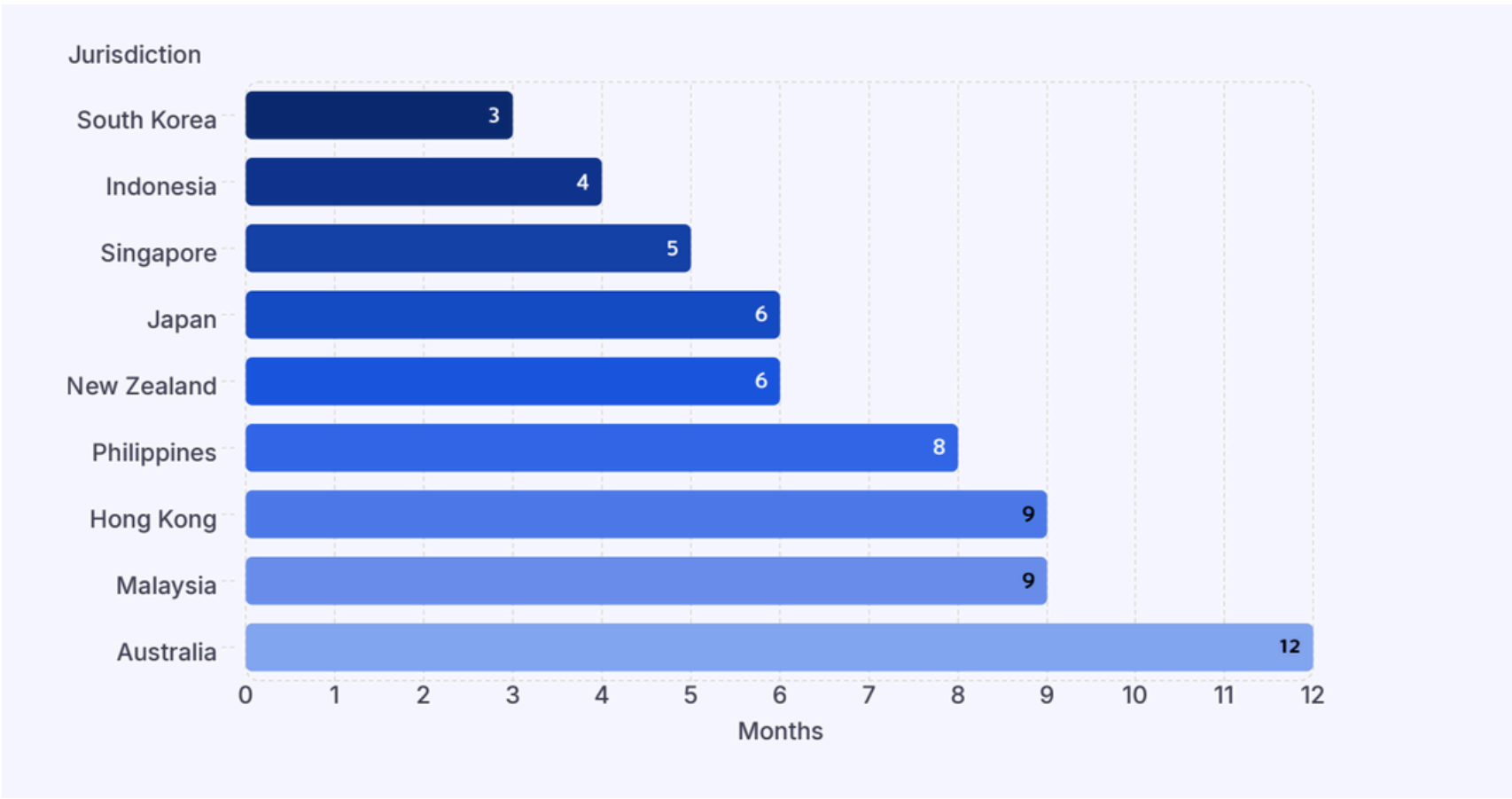
Jurisdiction	Cold Custody Approach	Segregation Mandate	Annual Audit Required	Travel Rule Compliance
Hong Kong	~98% (principles-based)	Yes	Yes	Yes
Japan	95%	Yes	Yes	Yes
South Korea	80%	Yes	Yes	Yes
Australia	Risk-based (no fixed %)	Yes	Yes	Yes
New Zealand	Best practice benchmark	Yes	Yes	Yes

Note: *This table focuses on APAC jurisdictions excluding Southeast Asia. Percentages shown reflect either statutory requirements (Japan, South Korea) or typical industry custody benchmarks and supervisory expectations. Hong Kong and Australia use principles-based frameworks without fixed percentage mandates. Custody standards are subject to ongoing regulatory evolution.*

Fystack

Licensing Timeline: From Application to Operations

Navigating the crypto asset regulatory landscape requires a clear understanding of the relevant timeframes involved in obtaining necessary licenses. The duration from initial application to full operational approval can vary significantly across APAC jurisdictions, impacting strategic planning and market entry.

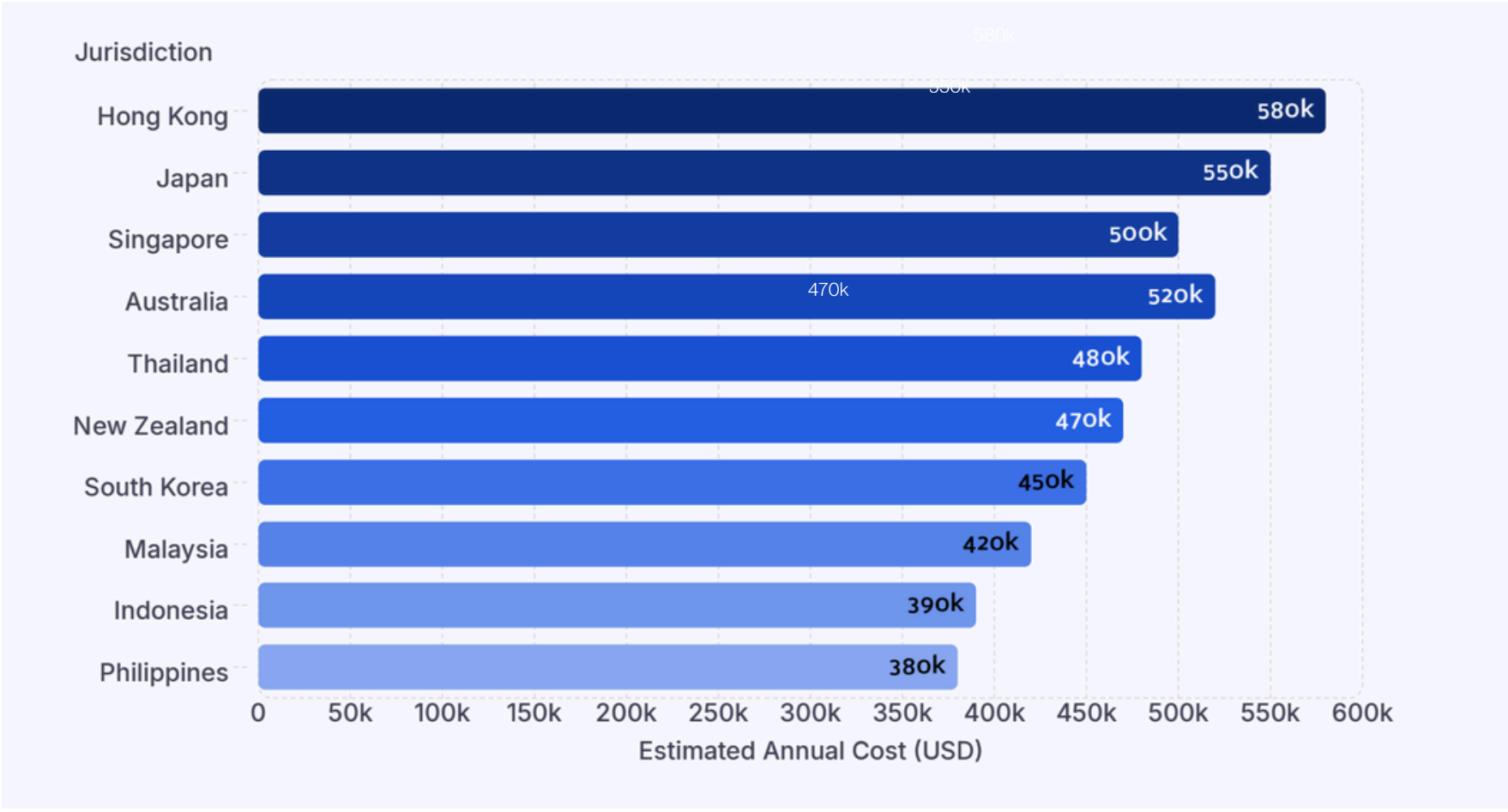


The bar chart above illustrates typical maximum durations for crypto asset licensing across key APAC markets (excluding Southeast Asia). These timelines are illustrative estimates based on industry observations and can vary significantly depending on application completeness, regulatory feedback cycles, and specific service offerings. South Korea often presents a faster path, while Australia's comprehensive framework typically requires longer review periods. Actual timelines should be confirmed with relevant regulatory authorities.

Fystack

Compliance Cost Breakdown by Market

Understanding the financial implications of regulatory adherence is crucial for crypto asset service providers. This breakdown provides estimated annual compliance costs for a mid-sized crypto exchange across key APAC markets, covering essential categories.



The chart illustrates estimated annual compliance expenditures for a mid-sized crypto exchange. These are illustrative estimates based on legal, audit, technology, and staffing assumptions and should not be considered definitive. Actual costs vary significantly based on operational scale, business model, service scope, and specific regulatory requirements. Consult with local compliance experts for precise cost projections.

Fystack

Market Entry Strategy: Which Market First?

Selecting the optimal entry point into the diverse APAC crypto market requires careful consideration of regulatory landscapes, operational costs, and strategic objectives. Three primary pathways emerge for crypto asset service providers (CASPs).

Fast Track: Agility & Speed

Prioritize markets like **South Korea**, **Indonesia**, and **Singapore**. These jurisdictions offer potentially quicker licensing processes and lower initial compliance costs, ideal for rapid market entry and testing new services.

Institutional Grade: Robust Foundations

Target **Hong Kong** and **Japan** to establish a strong, highly compliant presence. These markets demand the highest standards for custody, auditing, and AML/CFT, attracting sophisticated institutional investors.

Phased Regional Expansion

Begin with a single, well-understood market to build expertise and a robust compliance framework. Then, leverage this foundation to strategically expand into neighboring APAC countries, adapting to local nuances.

Regulatory Harmonization Trends: While each market has unique rules, there's a growing trend towards regulatory convergence in APAC, driven by global standards from bodies like FATF. This may simplify multi-jurisdictional compliance over time.

Fystack

Common Compliance Pitfalls: What NOT to Do

⚠ Underestimating Cold Custody Requirements

Failing to meet stringent cold custody percentages, often set between 80% to 95%+ in leading APAC jurisdictions, exposes client assets to unnecessary risk and leads to direct non-compliance.

⚠ Delaying AML/KYC Implementation

Procrastinating on robust Anti-Money Laundering (AML) and Know Your Customer (KYC) processes can result in severe penalties, reputational damage, and inadvertently facilitate illicit financial activities.

⚠ Ignoring Travel Rule Compliance

Overlooking the Financial Action Task Force (FATF) Travel Rule for virtual asset transfers will inevitably draw regulatory scrutiny and can lead to operational restrictions or fines for non-compliant transactions.

⚠ Inadequate Cybersecurity Measures

Weak cybersecurity protocols endanger client digital assets and sensitive data, making firms vulnerable to breaches, regulatory fines, and a significant loss of market trust.

⚠ Poor Asset Segregation Practices

Failing to properly segregate client funds from operational capital is a major red flag for regulators, leading to severe penalties and compromising consumer protection.

⚠ Failing to Maintain Comprehensive Audit Trails

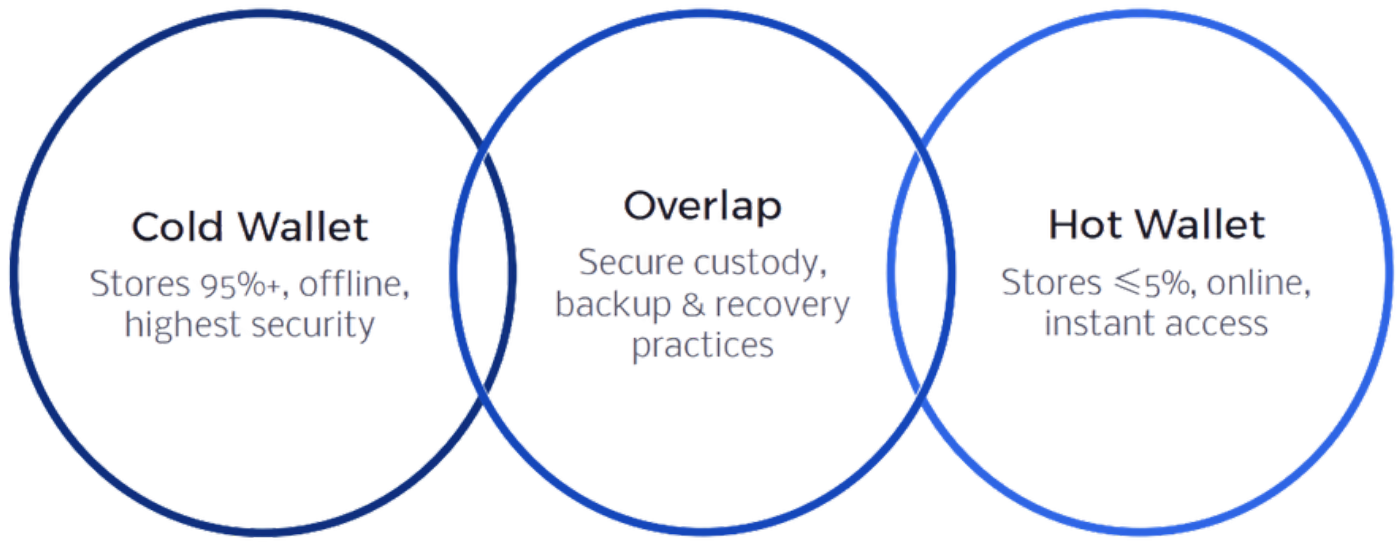
A lack of detailed, immutable audit trails for transactions, custody events, and compliance activities hinders regulatory oversight and can prevent effective incident response.

ⓘ **Regulatory Enforcement Trends:** Regulators across APAC are increasingly moving from guidance to enforcement, with a heightened focus on proactive compliance. Firms demonstrating a clear commitment to best practices will be better positioned to thrive.

Fystack

Custody Infrastructure: Cold vs Hot Wallet Strategy

Effectively managing crypto assets requires a strategic balance between security and accessibility. This involves a dual approach utilizing both cold (offline) and hot (online) wallets, each serving distinct purposes in asset protection and operational liquidity. Striking the right balance is crucial for both regulatory compliance and optimal user experience.



The diagram highlights the core trade-offs: Cold Wallets prioritize maximum security for the vast majority of assets, while Hot Wallets enable agile transactions. Best practices include implementing multi-signature requirements for cold storage, conducting regular security audits, and establishing clear operational policies for managing hot wallet funds, ensuring robust protection against theft and unauthorized access.

Fystack

AML/KYC Best Practices Across APAC

Effective Anti-Money Laundering (AML) and Know Your Customer (KYC) practices are fundamental to maintaining integrity and preventing illicit financial activities within the crypto ecosystem. For crypto asset service providers (CASPs) in the APAC region, a robust four-step process is essential for compliance and safeguarding operations.

Customer ID



Risk Assessment

Regulatory Reporting

Ongoing Monitoring

This structured approach ensures comprehensive oversight throughout the customer lifecycle, from initial onboarding to continuous transaction analysis. Adhering to these best practices helps CASPs mitigate financial crime risks and comply with stringent regulatory requirements across diverse APAC jurisdictions.

Crucial Note on Travel Rule: Beyond these core steps, CASPs must also comply with the FATF Travel Rule, requiring the collection and exchange of originator and beneficiary information for crypto asset transfers above a certain threshold. Implementing solutions for this data sharing is a non-negotiable component of compliance in many APAC markets.

Fystack

Regulatory Reporting Requirements by Jurisdiction

Understanding and adhering to diverse regulatory reporting mandates is critical for crypto asset service providers (CASPs) operating across the APAC region. These requirements ensure transparency, mitigate financial crime risks, and maintain regulatory compliance. Below is a summary of key reporting obligations in various jurisdictions

Jurisdiction	Key Reporting Requirements
Hong Kong	Quarterly operational and compliance reports to the Securities and Futures Commission (SFC).
Japan	Annual audits and detailed monthly transaction/operational reports to the Financial Services Agency (FSA).
Singapore	Ongoing disclosure obligations and periodic reports to the Monetary Authority of Singapore (MAS), covering financials and operations.
South Korea	Monthly transaction and suspicious activity reports to the Korea Financial Intelligence Unit (KoFIU).
Australia	Quarterly transaction reports (Threshold Transaction Reports, International Funds Transfer Instructions) to AUSTRAC.
Thailand	Annual financial statements and operational reports to the Securities and Exchange Commission (SEC).
Philippines	Regular reports to the Bangko Sentral ng Pilipinas (BSP) and/or Securities and Exchange Commission (SEC) on transactions and compliance.
Malaysia	Periodic reports to the Securities Commission (SC) on operational activities, security measures, and client protection frameworks.
Indonesia	Monthly and annual activity reports to Bappebti, including transaction volumes and customer data.
New Zealand	Ongoing reporting to the Financial Markets Authority (FMA) and Reserve Bank of New Zealand (RBNZ) on anti-money laundering and counter-terrorism financing (AML/CFT) compliance.

Fystack

Stablecoin Regulations: A Growing Focus

Stablecoins, due to their potential for widespread adoption in payments and financial services, are increasingly being carved out from broader crypto regulations and subjected to dedicated frameworks. This reflects a global effort to balance innovation with financial stability and consumer protection.

Jurisdiction	Key Regulatory Framework/Status
Hong Kong	Stablecoin Ordinance requires licensing for issuers, mandating robust reserve backing and operational standards.
Japan	Pioneering law (2023) mandates stablecoins be backed by fiat currency and issued by licensed banks or trust companies, enhancing investor protection.
South Korea	Under review with a focus on comprehensive consumer protection and financial stability, likely leading to dedicated legislation soon.
Australia	Emerging discussions and consultations, with a view to integrate stablecoins into existing payments and financial services regulation.
New Zealand	Currently relies on broader financial services, AML/CFT, and payments-related regulation while monitoring the market for any need for more dedicated stablecoin rules.

Why Stablecoins Matter: Stablecoins are pivotal for bridging traditional finance with the crypto ecosystem, enabling efficient cross-border payments and facilitating decentralized finance (DeFi). Robust regulation is crucial to prevent systemic risks, ensure market integrity, and build user confidence, making them a central component of future compliance efforts.

Note: *Stablecoin regulatory frameworks are rapidly evolving. This overview reflects the status as of mid-2026 and should be verified against the latest regulatory guidance from each jurisdiction's primary regulator.*

Fystack

Future Regulatory Trends in APAC (2024-2026)

The regulatory landscape for crypto assets in the Asia-Pacific (APAC) region is set for dynamic evolution. Over the next few years, key themes will emerge, driving greater harmonization, increased scrutiny on new sectors, and a deeper integration with broader financial and societal objectives. Staying informed and agile will be crucial for compliance and competitive advantage.

1

Convergence Towards FATF Standards

Jurisdictions will increasingly align with Financial Action Task Force (FATF) recommendations, standardizing AML/CFT frameworks for virtual assets across the region.

2

Focus on DeFi and Self-Custody Risks

Regulators will intensify efforts to understand and govern decentralized finance (DeFi) protocols and self-custody solutions, addressing associated risks like market integrity and consumer protection.

3

Central Bank Digital Currencies (CBDCs) Integration

Expect greater development and pilot programs for CBDCs, leading to new frameworks for their issuance, distribution, and interoperability with existing payment systems.

4

Environmental/ESG Compliance Requirements

The environmental impact of crypto mining and the broader ESG (Environmental, Social, Governance) considerations will gain regulatory attention, potentially leading to disclosure mandates and sustainability requirements.

5

Cross-Border Regulatory Cooperation

Enhanced collaboration among APAC regulators will facilitate consistent enforcement and information sharing, crucial for managing the inherently global nature of crypto transactions.

Fystack

Technology Stack for Compliance: Essential Tools

Navigating the complex crypto regulatory landscape requires a robust technological foundation. Building an effective compliance tech stack is crucial for automating processes, ensuring data integrity, and staying ahead of evolving requirements. Here are the essential software and systems vital for a comprehensive compliance program:

01

KYC/AML Platform

Automates identity verification, due diligence, transaction monitoring, and suspicious activity reporting to prevent financial crime.

02

Custody Management System

Ensures the secure storage, tracking, and management of digital assets, including support for hot and cold wallets, and multi-signature security.

03

Compliance Management Software

Centralizes policy management, tracks regulatory changes, manages audit trails, and streamlines internal compliance workflows.

04

Travel Rule Solution

Enables secure and compliant VASP-to-VASP data sharing for transactions exceeding specified thresholds, adhering to FATF guidelines.

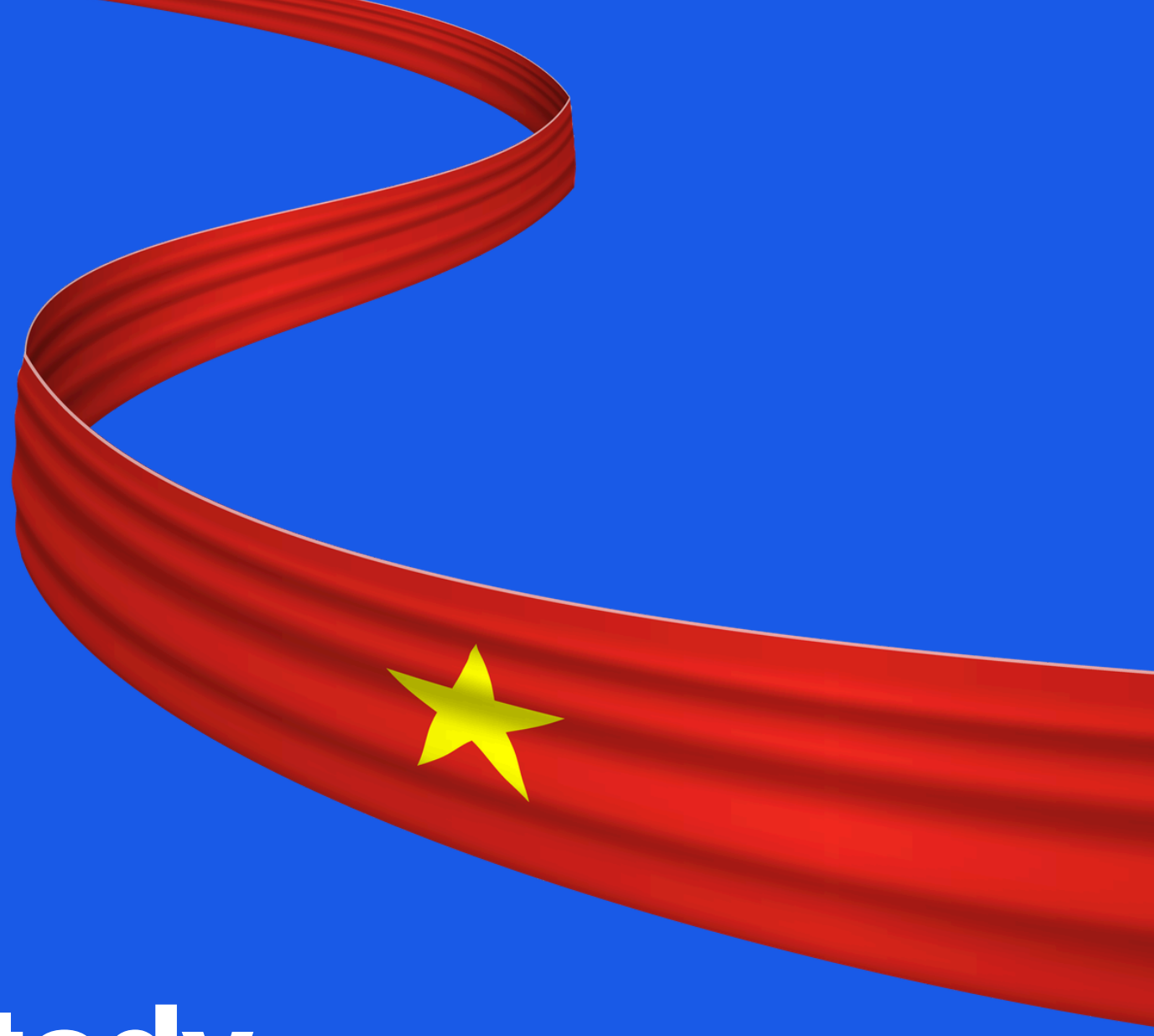
05

Reporting & Analytics Tools

Automates the generation of regulatory reports, provides insights into compliance performance, and supports data-driven decision-making.

Integration & Scalability: The effectiveness of this tech stack hinges on seamless integration between systems and the ability to scale with business growth and regulatory changes. Prioritize solutions with open APIs and modular designs.

Fystack



Your custody infrastructure partner in APAC

Fystack provides self-hosted custody infrastructure for enterprise teams. We enable financial institutions, CEXs, and OTC desks to deploy compliant, robust, and sovereign cryptographic custody systems fully localized onshore in Vietnam.

12+ Chains
MULTICHAIN INDEXING

< 1ms
ADDRESS LOOKUP SPEED

Flat Rate
FIXED PRICING MODEL

Fystack

ENTERPRISE PARTNER

Why Choose Fystack in Vietnam

We solve the core operational and compliance challenges faced by local and international businesses expanding transaction volumes in Vietnam.

100%
ONSHORE DATA COMPLIANCE

Zero
SINGLE POINTS OF FAILURE

Open
SOURCE CUSTODY CORE

1. 100% Onshore Data Residency Compliance

- **Decree 53 & Level 4 Security:** Fystack is designed to run self-hosted on your private servers or domestic cloud facilities (such as Viettel IDC or FPT). All key shares, signing logs, and user metadata remain onshore, satisfying local laws.

2. Enterprise-Grade MPC Cryptography

- **Threshold Signature Schemes:** Eliminate single points of failure with multi-party signature protocols (2-of-3 or 3-of-5). Private keys are never assembled in a single location, rendering remote key extraction impossible.

3. Auditability & Compliance Tooling

- **Open-Source Transparency:** Built on our vetted open-source libraries `mpcium` and `multichain-indexer` for clear local IT audit reviews.
- **Webacy-Powered Screening:** Features a compliance address analysis dashboard integrating Webacy's risk API to automatically isolate illicit wallets.

Fystack

Self-Hosted Control vs. SaaS Lock-In

A head-to-head comparison of self-hosted infrastructure ownership against standard vendor-managed cloud custody.

FEATURE / STANDARD	FYSTACK (SELF-HOSTED)	TRADITIONAL SAAS CUSTODY
Data Residency	**100% Onshore Compliance**	Offshore Cloud Storage (Violates Decree 53)
Cryptographic Control	**Full Cryptography Ownership**	Vendor Lock-In (Proprietary SaaS)
Pricing Structure	**Flat Subscription Rate**	Volume-based Fees (Charges rise with usage)
Local Auditing	**Onshore Logs & Raw Database**	API-Only Logs (No physical database access)

The Ultimate Decision: Sovereign Ownership

- **Freedom of Cryptography:** Fystack ensures you retain the keys, the database, and the infrastructure. Your business is never exposed to service halts or sudden fee increases by overseas third-party SaaS vendors.

Fystack

Custody infrastructure built for regulated markets?

Fystack provides self-hosted custody infrastructure — MPC key management deployed on your own servers, across 12+ chains. Built for fintechs, payment companies, and neobanks across APAC and emerging market

www.fystack.io

contact@fystack.io

https://github.com/fystack/