Continuum

INSURING STABLECOINS IN APAC

RISK INSIGHT SERIES

JUNE 2026

Contents

Legal Disclaimer

The information, opinions, and materials provided on this platform are for general informational purposes only and do not constitute legal, financial, or professional advice. While every effort is made to ensure accuracy and timeliness, no guarantee is given that the content is free from errors or omissions. The publisher assumes no liability for any loss, damage, or inconvenience arising from reliance on this content. All content is provided "as is" without warranties of any kind.

Where third-party materials, references, or links are included, they are provided for convenience and do not imply endorsement. All intellectual property rights remain with their respective owners. Unauthorized reproduction, distribution, or modification of this content is prohibited

AI Disclosure: This article was created with the assistance of AI tools for research and drafting. It was reviewed, edited, and fact-checked by our human editorial team before publication.

Introduction

Stablecoins have crossed from speculative instrument to financial plumbing. The total market value of fiat-referenced stablecoins surpassed USD 323 billion in mid-2026, with USDT at roughly USD 187 billion and USDC at around USD 77 billion in circulation.[1] The growth has been driven by two forces in parallel: institutional payment use cases that need a settlement asset with the speed of crypto and the predictability of fiat, and a wave of new regulatory regimes that have given supervised counterparties the comfort to engage.[2]

Across APAC, the regulatory shift is now real. Hong Kong's Stablecoins Ordinance came into effect on 1 August 2025, with the HKMA granting the first two issuer licences in April 2026 to HSBC and Anchorpoint Financial.[3] The Monetary Authority of Singapore finalised its single-currency stablecoin framework in 2023, with the regime moving into force in 2026.[5] Japan's Financial Services Agency has backed a joint stablecoin pilot by MUFG, SMBC, and Mizuho, with a target launch in March 2027 under the country's existing electronic payment instrument framework.[67]

What has not kept pace with the regulatory clarity is the insurance picture sitting behind it. Licensed issuers, reserve custodians, infrastructure providers, corporate users, and on-chain protocols each face a distinct set of exposures, and the insurance market response is fragmented and inconsistent. Standard wordings written for traditional banks, payments firms, or technology businesses do not always respond cleanly to stablecoin-specific loss scenarios.

The consequence is a coverage gap that is rarely visible in the abstract but becomes immediate the moment a depeg, a reserve loss, an issuer failure, or a smart contract exploit happens. Treasury holders find their general PI excludes digital asset positions. Issuers discover their D&O does not contemplate the new category of regulatory action. Infrastructure providers learn that their tech PI excludes sanctions-related loss. On-chain users learn that their parametric cover is undercapitalised at exactly the moment a major loss event tests it.

This report maps the insurance question across five categories: licensed issuers, reserve custody, holders and users, infrastructure providers, and decentralised stablecoin protocols. For each, it sets out what the regulatory framework now demands, where the insurance market currently responds, and where the gaps sit.

Background

From Speculative Asset to Regulated Financial Plumbing

The stablecoin market in 2026 looks very different from the stablecoin market of 2021. The asset class has moved from a tool for crypto-native traders to a recognised settlement and payment instrument used by corporate treasuries, B2B payment platforms, and licensed financial institutions. Three regulatory developments across APAC have done most of the work to make that shift legitimate.

In Hong Kong, the Stablecoins Ordinance brought the issuance, offering, and marketing of fiat-referenced stablecoins inside the HKMA's supervisory remit from August 2025.[4] The HKMA received 36 applications in the first batch and granted licences to only two: HSBC and Anchorpoint Financial Limited, a joint venture between Standard Chartered Bank Hong Kong, HKT, and Animoca Brands.[3] The five-percent approval rate signals the supervisory bar, and the licensees are required to maintain 100 percent backing of outstanding stablecoins with reserves held in custody and segregated from issuer assets.[8]

In Singapore, the Monetary Authority finalised its single-currency stablecoin framework in August 2023.[5] The regime applies to stablecoins pegged to the Singapore dollar or a G10 currency that are issued from Singapore. To carry the MAS-regulated label, an issuer must hold 100 percent reserves in cash, equivalents, or short-dated government debt, segregate reserve accounts, publish monthly attestations, undergo annual audits, and meet prescribed redemption timelines, typically at par within five business days.

In Japan, the framework treats stablecoins as electronic payment instruments under the 2023 Payment Services Act amendments, with issuance restricted to banks, licensed money-transfer agents, and trust companies. The FSA has actively supported the MUFG, SMBC, and Mizuho consortium developing a yen-referenced stablecoin under a trust bank structure, with a target launch by the end of Japan's fiscal year on 31 March 2027.[6][7]

Each of these frameworks does substantial work on the regulatory side. None of them does the equivalent work on the insurance side. The HKMA expects supervised issuers to manage operational, custody, and cyber risk to bank standards; it does not specify what insurance must respond to those risks. The MAS framework requires segregated reserves and monthly attestations; it does not specify what cover must sit behind those reserves. The Japanese trust bank model uses the existing banker insurance market; it does not yet have a clear answer for the stablecoin-specific exposures that will arise.

The Bank for International Settlements has flagged the broader systemic concern. Major stablecoin issuers now hold reserves primarily in fiat-denominated short-term assets such as US Treasuries, repurchase agreements, and bank deposits.[10] The Basel Committee has issued guidance on the maturity profile of reserve assets, recommending limits on individual reserve assets and on portfolio-weighted average maturity.[11] The combined effect is that reserve composition is now within a relatively narrow band, but the insurance question of what covers those reserves if something goes wrong in custody remains open.

Five sets of insurance buyers have emerged: licensed issuers, reserve custodians, corporate treasuries and B2B payment users, infrastructure providers, and decentralised stablecoin protocols. Each carries its own risk profile and coverage question.

Insurance for Licensed Issuers

The Five Lines a Supervised Stablecoin Issuer Now Needs

A licensed stablecoin issuer is a new type of regulated entity. It is not quite a bank, not quite a payment institution, not quite a fintech, and not quite a custodian. The insurance market response to this hybrid status is to assemble cover from multiple existing lines, each of which addresses a slice of the issuer's actual exposure. For a firm holding an HKMA licence or operating under the MAS or JFSA equivalents, five lines should be in place.

Directors and Officers Cover for the Issuance Entity

Stablecoin issuance is now a regulated activity, and the directors carry the personal liability that comes with running a supervised business. D&O responds to regulatory inquiries, oversight failure allegations, disclosure breaches, and shareholder actions following a material loss event. The HKMA expects fitness and propriety standards from senior management of licensed issuers, which makes the D&O position load-bearing rather than nominal.[4]

Professional Indemnity for Issuance Services

Issuing, redeeming, and managing a stablecoin is a professional service in the eyes of the regulator.[8] PI responds to errors in issuance, redemption, or settlement: delayed redemptions, misallocation between holders, reconciliation failures. Standard fintech PI wordings rarely contemplate these scenarios and need to be specifically negotiated.

Cyber Cover for Technology and Smart Contract Risk

A licensed issuer typically runs a smart contract on a public blockchain, manages reserves and minting and burning operations off-chain, and connects the two through custody and treasury systems. Each layer carries cyber exposure. Cyber cover needs to respond to network compromise, social engineering, ransomware, and smart contract failure on the on-chain contract itself.[16]

Crime and Specie for Reserves in Custody

Reserve assets sit with custodian banks, money market fund providers, or qualified asset managers.[10] Crime cover responds to internal dishonesty or social engineering targeting the custody arrangement; specie cover responds to the underlying assets. Limits rarely match the size of a stablecoin in circulation, leaving most reserves exposed to custody loss.

Regulatory Liability Cover:

Regulatory liability is the newest line to attach. HKMA, MAS, and JFSA investigations carry defence costs even where the issuer prevails.[5] Where an investigation escalates to enforcement, the financial exposure can be material. Cover responds to defence costs and certain penalties arising from supervisory action. Older D&O policies were not drafted for the new stablecoin licensing regimes.

Insuring the Reserves

The 1:1 Backing Question No One Has Fully Answered

The defining characteristic of a fiat-referenced stablecoin is that every token in circulation should be backed by an equivalent value of reserve assets. The licensing frameworks in Hong Kong, Singapore, and Japan all require it. The question that the insurance market has not standardised an answer to is what happens to that reserve if something goes wrong in the custody chain.

Where the Reserves Actually Sit

For the largest stablecoins, reserve composition is now well-documented. Tether reported total reserves of USD 181.2 billion as of Q3 2025, with approximately USD 135 billion in direct and indirect US Treasury exposure, USD 12.9 billion in gold, USD 9.9 billion in Bitcoin, and the balance in secured loans and other investments.[9] USDC's reserves sit primarily in short-dated US Treasuries held in a BlackRock-managed fund, with the remainder in cash deposits at regulated banks.

The Bank for International Settlements has noted that major stablecoin issuers back their tokens primarily with fiat-denominated short-term assets, and the Basel Committee has provided guidance on maturity limits for reserve portfolios.[10][11] The result is a reserve profile that is relatively concentrated in short-dated government debt, money market instruments, and bank deposits with custodian counterparties.

The Custody Chain and Its Loss Scenarios

Reserve assets sit with three types of holder: banks (for cash deposits), custodian banks (for treasuries and securities), and money market fund providers (for the fund-wrapped portion of the reserves). Each carries its own loss scenarios. Cash deposits beyond deposit insurance limits are unsecured claims on the bank. Custodied securities can be lost through fraud at the custodian, although bankers' liability insurance and custodian indemnities typically respond. Money market fund holdings are subject to fund-level risk and to the fund manager's own controls.

The USDC depeg in March 2023 is the clearest available case study. Circle held approximately USD 3.3 billion of its USD 40 billion in reserves at Silicon Valley Bank when the bank failed.[12] The exposure was eight percent of the reserve total but enough to trigger a depeg event that saw USDC fall to USD 0.87 within hours.[13] The peg restored within 72 hours after the FDIC guaranteed all SVB deposits, but the broader DeFi market experienced significant contagion, with DAI losing its peg shortly after because it held USDC as a stable reserve asset.[14]

What Specie and Crime Cover Actually Respond To

Specie insurance covers high-value items in storage and in transit. For stablecoin reserves, the relevant categories are physical cash, precious metals (where issuers hold gold reserves), and certain physical security instruments. Crime insurance responds to losses arising from dishonest acts: theft by an employee at the custodian, social engineering of the issuer's treasury team, fraudulent transfer instructions intercepted in the settlement chain.

What neither line responds to cleanly is the broader category of custodian failure, where the custodian itself becomes insolvent or where the legal mechanism for segregating customer assets fails under stress. For that exposure, the issuer's protection depends largely on the custodian's own bankers' liability cover, on the legal

status of the custody arrangement under the relevant jurisdiction's insolvency law, and on the issuer's choice of custodian counterparty in the first place. The variation across APAC jurisdictions in how custody is treated is significant, and the resulting insurance picture is correspondingly uneven.

Limits Rarely Match the Size in Circulation

The mismatch most commonly missed is between the insured limits and the size of the stablecoin in circulation. A specie or crime policy with a limit of, say, USD 200 million is meaningful cover for a small issuer but represents less than 0.2 percent of USDT's circulating supply. For institutional users relying on a stablecoin as a settlement asset, the question of how much of the reserve is actually insured against custody loss versus how much is exposed to the underlying credit risk of the custodian network deserves direct disclosure. At present, issuer disclosure on reserve insurance is inconsistent across APAC licensees, and the differences between licensees are not always apparent without reading the audit and attestation documents in detail.

For APAC fund managers, the valuation question has additional dimensions. Currency exposure, less liquid local markets, and the rising prevalence of cross-border deals all introduce judgment calls into the marking process. A robust valuation policy, documented and consistently applied, is both a compliance discipline and a precondition for insurers to underwrite the IMI programme with confidence.

Tokenised Reserves Add a New Risk

A growing share of stablecoin reserves is now held in tokenised form. BlackRock's BUIDL fund, Franklin Templeton's BENJI, and similar tokenised money market funds offer stablecoin issuers a way to hold short-dated treasuries on-chain. The benefit is operational efficiency and improved reserve transparency. The cost is that the reserves now carry smart contract risk in addition to the underlying credit and market risk of the treasuries themselves. Insurance for tokenised reserves needs to address both the conventional custody question and the on-chain failure modes that the underlying funds were not previously exposed to.

Insurance for Stablecoin Holders and Users

Three Risks Treasury Holders Are Carrying Uninsured

The insurance picture for the firms holding and using stablecoins is markedly thinner than the picture for the issuers themselves. Corporate treasuries holding stablecoins for working capital, B2B payment platforms routing settlement through stablecoin rails, and fintechs using stablecoins as a cross-border value transfer mechanism all face exposures that traditional treasury policies, payment institution PI, and standard cyber wordings were not built to absorb.

Depeg Risk

A stablecoin holder bears the risk that the peg breaks. The 2023 USDC episode showed how quickly that risk can materialise: a fully-collateralised, regulated stablecoin can lose 13 percent of its value in hours on the basis of news about a single banking counterparty.[12] For a corporate treasurer holding USDC as a cash equivalent, the practical question is what happens when the peg breaks and remains broken. Treasury policies treat stablecoins as cash; loss triggers treat them as something else.[13]

Direct insurance against depeg events is almost non-existent in the conventional insurance market. The exposure is too systemic and too correlated for traditional underwriting to absorb at meaningful scale. On-chain parametric cover for depeg risk exists in limited form, but capacity is small and pricing is volatile. For most treasury holders, the practical answer is concentration limits and active monitoring rather than insurance.

Issuer Failure Cover

Beyond depeg, the deeper exposure is issuer failure. A licensed issuer can fail. The reserve arrangements can fail to deliver the expected recovery. Holders can find themselves as unsecured creditors of an entity that does not have ready cash to redeem at par. Insurance against this scenario is effectively unavailable in the conventional market. The closest analogue is deposit insurance for bank deposits, which by design does not extend to stablecoin holdings.

For institutional holders, the practical mitigation is jurisdictional choice (licensed issuers in supervised regimes), counterparty diversification, and active monitoring of reserve attestations. For B2B payment users, the exposure window is typically narrow enough that a single-day issuer failure does not produce a catastrophic loss, but the scenario where a payment is in flight when the issuer becomes unable to honour redemptions remains uncovered.

> “The exposure is too systemic and too correlated for traditional underwriting to absorb at meaningful scale. “

Counterparty Risk When the Rail Fails Mid-Transaction

A stablecoin payment that fails mid-transaction creates a different exposure to the depeg or issuer failure scenarios. The funds may be in transit, locked in a smart contract, or sitting in a bridging arrangement at the moment of failure. For high-value B2B payments, the financial exposure can be material, and the recovery process can be slow and contested. Cyber and PI policies for the payment originator may respond to internal failures but typically do not respond to failures in the third-party rail.

Freezing and Blacklisting Risk

A feature of centralised stablecoins that holders often underestimate is the issuer's ability to freeze tokens at addresses on its blacklist. Both USDT and USDC contracts contain administrative functions that allow the issuer to render tokens unusable at any wallet, typically in response to legal process, sanctions enforcement, or fraud claims. The practice is now routine, with issuers freezing thousands of addresses per year, often in coordination with law enforcement or in response to OFAC designations.[16]

For institutional holders, the exposure is twofold. An upstream counterparty may be blacklisted, leaving tokens stranded mid-transaction. Or a treasury holding stablecoins routed through previously-compromised wallets can have assets frozen as part of an enforcement action regardless of the holder's own conduct. Standard treasury and PI policies do not contemplate this scenario, and recovery through legal process is slow and uncertain.

Sanctions and AML Exposure on Every Transaction

Every cross-border stablecoin transaction carries sanctions and AML exposure. The FATF travel rule, updated in 2025, expanded the information requirements for cross-border virtual asset transfers above USD or EUR 1,000 and explicitly included fraud prevention and proliferation financing alongside the existing money laundering and terrorist financing objectives.[15] Eighty-five jurisdictions have passed implementing legislation, but supervision and enforcement remain uneven, creating a compliance environment where the rules are clear but the supervisory expectations are still developing.

For corporate users, the practical exposure is twofold. First, an inadvertent transaction with a sanctioned counterparty can trigger regulatory action even where the originator had no knowledge of the recipient's status. Second, an AML compliance failure in the firm's stablecoin handling process can lead to enforcement consequences that ordinary tech PI and cyber wordings typically exclude.

Audit and Disclosure Pressure

The auditing profession has begun to engage with stablecoin holdings on corporate balance sheets, with implications for how those positions need to be disclosed and how the underlying risk needs to be characterised. For a treasury holding meaningful stablecoin positions, the disclosure question is moving from optional to required, and the disclosure typically needs to address insurance and risk transfer arrangements. Firms with no specific cover in place are increasingly being asked to explain the absence rather than the presence.

The Infrastructure Layer

Custody Platforms, On and Off Ramps, and the Sanctions Exposure Tech PI Excludes

The plumbing of the stablecoin economy carries the same regulatory weight as the issuer itself, often with a thinner insurance response. Custody platforms, on-ramp and off-ramp providers, wallet providers, and payment processors each sit at points in the value chain where loss events concentrate. Each is exposed to a category of regulatory and operational risk that standard tech PI and cyber wordings were not written to cover.

Custody Platforms

Custody platforms hold customer assets for issuers, exchanges, and corporate treasuries. Exposure concentrates in private key management.[16] Cyber cover responds to network compromise and ransomware; crime cover to internal dishonesty and social engineering; specie cover to the underlying assets.

Harder to place is operational risk short of a cyber attack: a transfer authorised in error, an authentication failure, a smart contract integration producing an unexpected result. Cover for these scenarios is unsettled and varies materially between providers.

On-Ramp and Off-Ramp Providers

On-ramp providers convert fiat into stablecoins; off-ramp providers do the reverse. Both carry sanctions and AML exposure on every transaction, with the FATF travel rule adding cross-border information requirements on each transfer.[15]

The most-missed gap is the exclusion in standard tech PI wordings for regulatory fines, AML penalties, and sanctions-related loss. The exclusion is rarely contested at placement, and firms typically discover it only when an enforcement action arrives.

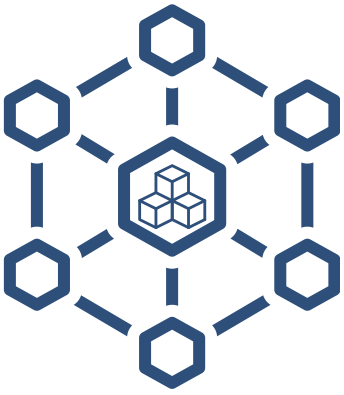
Wallet Providers

Wallet providers split into custodial (provider holds user keys) and non-custodial (user holds own keys). Custodial wallets face the same exposures as institutional custodians, scaled down to retail.[16] Non-custodial wallets face product liability and PI claims when software fails, when smart contract integrations produce unexpected losses, or when user interface design contributes to a user error.

Standard software PI wordings do not always extend to on-chain interactions, and the line between defective software and user error compounded by design is increasingly contested in wallet provider claims.

Payment Processors

Payment processors using stablecoins for B2B or cross-border settlement sit at the centre of overlapping regulatory expectations from multiple jurisdictions.[15] Tech PI typically excludes regulatory fines, AML penalties, and sanctions-related losses. Cyber responds to network events but not compliance failures. The combination leaves a meaningful regulatory exposure often sitting outside the firm's insurance arrangements.



Algorithmic Stablecoins and On-Chain Cover

When Smart Contracts Replace Underwriters

Algorithmic and crypto-collateralised stablecoins sit outside the licensed issuer regimes. DAI, the largest of the category, is governed by MakerDAO governance and backed by a mix of crypto collateral and real-world assets. The risk profile is different from a fiat-referenced stablecoin in a critical way: there is no regulated entity to hold to account, no balance sheet to look to for redemption, and no traditional custody chain to insure. The risk lives in the code, in the oracle that feeds the code, and in the governance that controls the code.

Where the Losses Actually Come From

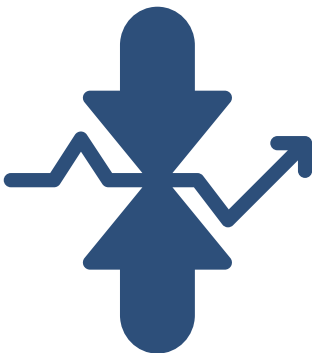
Smart contract failure has been the dominant loss event for decentralised protocols. Across DeFi, approximately USD 2.2 billion in funds were stolen in 2024, with smart contract-specific incidents accounting for several hundred million of that total.[17] Logic errors, reentrancy bugs, inadequate access controls, and stolen private keys remain the most common attack vectors.[16]

Oracle manipulation has emerged as a distinct and growing category. The reliance of decentralised stablecoins on price oracles to maintain their pegs creates an attack surface where manipulation of the oracle data can trigger liquidations, mispriced collateral, and cascading losses across the protocol.[16] Single-source oracles remain prevalent in DeFi deployments despite the availability of decentralised alternatives.

Governance attacks introduce a class of risk that traditional D&O does not contemplate. A governance vote that produces a harmful protocol upgrade, a coordinated voting bloc that pushes through a change against the interest of token holders, or a flash loan attack that temporarily acquires voting power can all destabilise an algorithmic stablecoin without any traditional cyber breach occurring. The losses are real but the legal pathway to recovery is unclear.

On-Chain Insurance Protocols

The insurance response to these risks lives mostly on-chain. Nexus Mutual is the largest of the protocols, operating as a member-owned mutual that pools capital from members and pays out claims based on a community-validated assessment process. Its capital pool has grown materially, reaching approximately USD 400 million in assets by late 2025, and the cover offered now extends across smart contract risk, custody risk, and certain depeg scenarios.[18]



Sherlock combines smart contract auditing with insurance cover. After completing an audit, Sherlock offers up to USD 10 million in cover per protocol, with Nexus Mutual providing excess cover for 25 percent of the underlying limit through a partnership arrangement.[19] The combination creates a layered response: the audit catches the issues that would otherwise become claims, and the cover responds when something escapes the audit. Nexus Mutual has also integrated with restaking infrastructure to expand its capital base through 2025 and into 2026.[20]

Parametric cover for depeg, for oracle failure, and for specific smart contract failure modes has become available on a small scale. The capacity remains limited relative to the size of the underlying market, and the pricing remains volatile. Institutional buyers increasingly want a traditional carrier behind the on-chain wrapper, both for capacity reasons and for the comfort of a regulated counterparty. The hybrid model, on-chain primary cover with traditional reinsurance, is the most likely structural answer but is still in early development.

Where the Continuum View Sits

The Continuum position on this space is that the right answer for institutional buyers is rarely a pure on-chain solution and rarely a pure traditional solution. For stablecoin holders and infrastructure providers operating across APAC, the practical response is to combine traditional cover where the carriers will engage (D&O, PI, Cyber, Crime, Specie) with specialist on-chain or parametric cover where the traditional market does not respond at meaningful capacity. Treating the two as separate is the single most common source of unintended gaps. Treating them as a coordinated response, with consistent triggers and complementary limits, is the work the market is still learning how to do well.

Where Regulators Stand

Algorithmic and crypto-collateralised stablecoins sit outside the HKMA, MAS, and JFSA frameworks by design. Each of those regimes is built around fiat-referenced stablecoins with identified issuers and segregated reserves, neither of which fits the algorithmic model.[4] The May 2022 collapse of Terra and its UST stablecoin, which wiped approximately USD 45 billion in market value in a matter of days, sharpened the regulatory caution. The Basel Committee's standards specifically distinguish fiat-referenced stablecoins from other cryptoassets, with the latter facing materially higher capital treatment for any bank exposure.[11]

For market participants, the practical consequence is that algorithmic stablecoins will likely remain outside the supervised regimes for the foreseeable future. The insurance question stays on-chain rather than migrating to traditional carriers. For institutional buyers considering exposure, the absence of a regulated issuer changes both the risk profile and the available coverage response in ways that traditional cover does not address.

Summary

The peg is regulated. The insurance behind it is not standardised.

Stablecoins have moved into the regulated mainstream across APAC. Hong Kong's Stablecoins Ordinance has granted its first two licences.[3] Singapore's single-currency stablecoin framework is now in force.[5] Japan's largest banks have agreed a joint stablecoin pilot under FSA supervision, with a target launch in early 2027.[6] The asset class has crossed USD 323 billion in market value, and the institutional buyer base is widening month by month.[1]

What has not standardised is the insurance behind any of it. Licensed issuers face a five-line cover requirement that the market has only recently begun to assemble in a coordinated way. Reserve custody arrangements rely on a mix of specie, crime, and bankers' liability cover that rarely matches the size of a stablecoin in circulation. Treasury holders and B2B users carry depeg, issuer failure, counterparty, sanctions, and AML exposures that most existing policies do not specifically contemplate. Infrastructure providers operate inside tech PI wordings that typically exclude the regulatory fines and sanctions-related losses they are most exposed to. Decentralised stablecoin protocols rely on on-chain cover from Nexus Mutual, Sherlock, and similar mutuals, with capacity that remains limited relative to the underlying risk.[18][19]

The 2023 USDC depeg remains the clearest stress test the market has run. A regulated stablecoin with 100 percent backing lost 13 percent of its value within hours because 8 percent of its reserves were trapped at a failing bank.[12] The peg recovered within 72 hours, but the contagion effects through DeFi were significant and the lesson for insurance buyers was specific: reserve attestations are not the same as insurance, and the gap between the two becomes visible only when a custody event occurs.[14]

For licensed issuers, the immediate action is to ensure each of the five cover lines (D&O for the issuance entity, PI for issuance services, Cyber for technology and smart contract risk, Crime and Specie for reserves, and Regulatory Liability for supervisory action) is in place with limits and wordings appropriate to the scale and jurisdiction of operations. For reserve custodians, the work is to disclose the insurance position behind the custody arrangement with the same rigour applied to the reserve attestation itself. For treasury holders and B2B users, the action is to map stablecoin holdings against existing PI, cyber, and crime wordings and to identify where digital asset exclusions or silent gaps create unhedged exposure.

For infrastructure providers, particularly on-ramp and off-ramp operators, the focus is on negotiating tech PI wordings that respond to the regulatory and sanctions exposures the firm actually faces, rather than accepting standard exclusions. For decentralised protocols, the practical answer is the hybrid model: on-chain primary cover supported by traditional reinsurance where available, with active management of the capacity question as the protocol scales.

For insurers, the underwriting opportunity is real and growing. Those that build stablecoin-specific capability around reserve composition, custody, smart contract audits, and cross-border compliance will write differentiated business. Those that default to broad digital asset exclusions will cede ground to specialists already in the space.

Regulators have brought the peg inside the supervised system. The insurance behind it still hasn't caught up.

References

1. DeFiLlama, "Stablecoin Market Cap, Supply and Peg Data," 2026. https://defillama.com/stablecoins

2. CoinDesk, "Circle's USDC Outpaces Growth of Tether's USDT for Second Year Running," January 2026. https://www.coindesk.com/markets/2026/01/06/circle-s-usdc-outpaces-growth-of-tether-s-usdt-for-second-year-running

3. Hong Kong Monetary Authority, "Granting of Stablecoin Issuer Licences," April 2026. https://www.hkma.gov.hk/eng/news-and-media/press-releases/2026/04/20260410-4/

4. Hong Kong Monetary Authority, "Regulatory Regime for Stablecoin Issuers," 2026. https://www.hkma.gov.hk/eng/key-functions/international-financial-centre/stablecoin-issuers/

5. Monetary Authority of Singapore, "MAS Finalises Stablecoin Regulatory Framework," August 2023. https://www.mas.gov.sg/news/media-releases/2023/mas-finalises-stablecoin-regulatory-framework

6. The Defiant, "Japan Megabanks MUFG, Mizuho, and SMBC Establish Joint Stablecoin Council," 2026. https://thedefiant.io/converge/tradfi-and-fintech/japan-megabanks-mufg-mizuho-and-smbc-establish-joint-stablecoin-council

7. CoinDesk, "Japan's FSA to Support Country's 3 Largest Banks in Stablecoin Issuance," November 2025. https://www.coindesk.com/policy/2025/11/07/japan-regulator-to-support-country-s-3-largest-banks-in-stablecoin-issuance

8. Davis Polk, "Hong Kong's Licensing and Regulatory Framework for Stablecoins is Now in Effect," 2025. https://www.davispolk.com/insights/client-update/hong-kong-s-licensing-and-regulatory-framework-stablecoins-now-effect

9. Tether, "Q3 2025 Attestation Report: Profit Surpassing $10B, Record Levels in U.S. Treasuries Exposure," Q3 2025. https://tether.io/news/tether-attestation-reports-q1-q3-2025-profit-surpassing-10b-record-levels-in-us-treasuries-exposure-accelerating-usdt-supply-amidst-worlds-macroeconomic-uncertainty/

10. Bank for International Settlements, "Stablecoin Growth: Policy Challenges Approaches (BIS Bulletin No 108)," 2024. https://www.bis.org/publ/bisbull108.pdf

11. Basel Committee on Banking Supervision, "Consultative Document on Cryptoasset Standards," 2024. https://www.bis.org/bcbs/publ/d567.pdf

12. CNBC, "Stablecoin USDC Breaks Dollar Peg After Firm Reveals It Has $3.3 Billion in SVB Exposure," March 2023. https://www.cnbc.com/2023/03/11/stablecoin-usdc-breaks-dollar-peg-after-firm-reveals-it-has-3point3-billion-in-svb-exposure.html

13. Chainalysis, "Crypto Market Reaction to Silicon Valley Bank and USDC Depeg," 2023. https://www.chainalysis.com/blog/crypto-market-usdc-silicon-valley-bank/

14. Financial Action Task Force, "Targeted Update on Implementation of the FATF Standards on Virtual Assets and Virtual Asset Service Providers," 2025. https://www.fatf-gafi.org/en/publications/Fatfrecommendations/targeted-update-virtual-assets-vasps-2025.html

15. Chainalysis, "Security Risks of Stablecoins," 2025. https://www.chainalysis.com/blog/stablecoin-security-risks/

16. Chainalysis, "Crypto Hacking Stolen Funds Update," 2024. https://www.chainalysis.com/blog/crypto-hacking-stolen-funds-2024/

17. Nexus Mutual, "Nexus Mutual v3: A Year of Progress in Onchain Risk Infrastructure," 2025. https://nexusmutual.io/blog/nexus-mutual-v3-a-year-of-progress-in-onchain-risk-infrastructure

18. CoinDesk, "DeFi Insurance Alternative Nexus Mutual Integrates Restaking Specialist Symbiotic," November 2025. https://www.coindesk.com/business/2025/11/19/defi-insurance-alternative-nexus-mutual-integrates-restaking-specialist-symbiotic

Continuum

Risk. Insurance. Technology.

hello@continuuminsure.com

www.continuuminsure.com

Continuum Risk Advisory Pte Ltd ("Continuum") registered in Singapore, UEN 202316352E is an independent risk advisory consultancy and technology provider. Continuum provides general risk advice and insurance product information through our website and other online means. Continuum is not an insurance company, insurance agency or insurance brokerage company and does not provide financial advice.