APEX | ISOGONAL

Understanding and mitigating stablecoin risks for financial institutions

Contents

Foreword

Digital assets are reshaping how finance operates, offering new ways to move, record, and manage value. Among these, stablecoins have drawn particular interest for their ability to combine the reliability of traditional currencies with the efficiency of blockchain settlement.

As institutions explore these instruments, careful evaluation becomes critical. Each stablecoin differs in how it is issued, governed, and backed, and these distinctions have direct consequences for stability, liquidity, and trust. Events in recent years have shown how weaknesses in reserve design, governance, or technology can lead to lasting disruption.

This eBook offers a structured approach to assessing stablecoins for institutional use. It reviews the major categories of risk and explains how sound oversight, transparency, and operational discipline can reduce exposure. It also highlights the role of trusted intermediaries that help financial firms manage digital assets responsibly.

Stablecoins represent a bridge between established financial systems and emerging digital networks. With clear frameworks and careful implementation, they can support efficiency and confidence across markets. This guide has been developed to assist professionals in evaluating these opportunities with clarity and caution.

Daniel Coheur
Global Head of Digital Assets
Apex Group

Angie Walker
Commercial Head of Apex Digital
Apex Group

Jasmine Burgess
CEO / CIO
Isogonal Ltd

Executive summary

Stablecoins, tokenised deposits, and tokenised money market funds are gaining traction as digital settlement tools. They provide instant movement of value and continuous availability, but they introduce risks that differ from traditional systems. Institutions need a clear assessment framework before using any form of tokenised cash.

Key exposures

- **Issuer and reserve strength:** Stability depends on the credibility of the issuer, the structure and quality of reserves, and the ability to meet redemptions during periods of stress.
- **Operational accuracy:** Errors involving networks, addresses, or key management result in immediate and permanent loss. Processes need the same level of discipline as high-value payments.
- **Cyber and smart-contract security:** Wallet compromise, phishing, and contract weaknesses remain leading causes of digital-asset failures. Strong custody controls and independent audits are vital.
- **Blockchain reliability:** Network outages, congestion, and slow finality can interrupt settlement or restrict access to funds at critical moments.
- **Governance and transparency:** Weak oversight, limited reporting, and unclear administrative privileges create hidden exposure that may surface only during market stress.

Regulatory direction

- MiCA in the EU, the FSRA in Abu Dhabi, the BMA in Bermuda, and new US proposals are introducing clearer requirements for reserves, reporting, redemption rights, and internal control.
- Tokens issued within these frameworks generally offer more predictable protections for institutions.

Practical entry point

- Permissioned tokenised money market funds provide a familiar structure with regulated oversight.
- They allow institutions to gain operational experience with on-chain settlement while reducing issuer-related uncertainty.

Institutions need a structured review that covers regulatory alignment, reserve strength, operational discipline, technical controls, governance, and chain performance.

Bottom line: Digital settlement is viable for institutions when it is supported by clear governance, strong controls, and continuous supervision.

Introduction

Stablecoins, tokenised deposits, and central bank digital currencies (“CBDCs”) are attracting attention for their ability to enable faster, programmable financial transactions. As expected, but less frequently highlighted, digital payments also introduce new categories of risk. These risks can be managed: years of stablecoin use and refinement within crypto markets have already created a number of operational best practices.

The risk profiles of institutions such as banks, asset managers, and investment firms differ markedly from those of typical users in crypto markets. It is therefore timely to highlight where the deeper risks lie. Not all digital tokens are equal in legal status, regulatory treatment, or risk exposure. Minor errors, such as confusing a wallet’s blockchain network, can expose enterprises to severe and irreversible losses.

The aim of this eBook is to equip finance professionals with frameworks to evaluate and compare stablecoins for institutional use, covering issuer, operational, protocol, cyber, and governance risks.

Digital payments improve transaction speed but introduce new risks.

Institutions must apply the same care to issuer, operational, and governance assessments as they do in traditional finance.

We also outline the work being done by trusted intermediaries, including stablecoin rating services such as Moody’s, cybersecurity auditors such as Halborn, regulated digital custodians, and newer entities such as stablecoin clearing houses. These intermediaries are helping to mitigate systemic risks that sit outside an institution’s control or tolerance.

Finally, we discuss why permissioned digital payments and tokenised money market funds (“MMFs”) can serve as a safer training ground for institutions. These instruments carry materially lower operational, cyber, and compliance risks and do not affect how new instruments are treated for regulatory capital or reporting purposes.

Not all stablecoins are created equal

Stablecoins, tokenised deposits, and tokenised MMFs differ in both structure and regulatory standing. At a high level, stablecoins are typically fiat-backed tokens issued by non-banks, such as USDC by Circle or USDT by Tether, and are pegged one-to-one with a currency. Tokenised bank deposits are digital tokens that represent a claim on an actual bank deposit, recorded as a bank's liability on a distributed ledger. Tokenised MMF shares, by contrast, are tokens representing ownership in a regulated MMF.

These instruments vary significantly in legal protection and oversight. A USD stablecoin issued by a fintech company is not a bank deposit and carries no government insurance. Holders depend on the issuer's contractual promise and reserve quality. Tokenised bank deposits, however, provide direct recourse to the issuing bank and may benefit from existing regulatory frameworks and deposit insurance, although they are typically limited to that bank's network.

Tokenised MMFs are regulated securities backed by high-quality assets and subject to oversight by fund custodians, administrators, and regulated investment managers. This structure reduces the likelihood that any single party could misstate reserve values. In return, these funds may impose redemption limits during periods of market stress and may not always serve as practical instruments for payments.

Stablecoins, tokenised deposits, and tokenised MMFs differ in risk, regulation, and reliability.

Institutions should assess each structure carefully before adoption.

Implication: Because of these differences, risk profiles vary widely. A tokenised deposit from a regulated bank or a government-backed MMF usually carries lower credit and transparency risk than a stablecoin issued by an opaque offshore entity. Even among stablecoins, reserve practices differ. Some hold only cash and short-term US Treasuries with monthly audits, while others hold riskier or less transparent assets. Not all stablecoins offer the same standards of safety, liquidity, or disclosure, so institutions must select with care.

Institutions new to blockchain may find it prudent to begin with permissioned tokenised MMF shares. These are effectively on-chain shares of conservative MMFs. They combine regulated, familiar assets with blockchain-based settlement, allowing teams to gain operational experience in a lower-risk environment before expanding to privately issued stablecoins.

Issuer and reserve risk

One of the most fundamental considerations is the creditworthiness and integrity of the stablecoin's issuer and its reserves. This includes the risk of issuer default, insolvency, or reserve inadequacy, which directly affects the token's ability to hold its peg.

Issuer insolvency and credit risk

Stablecoin holders have a claim on the issuer's reserves. Those reserves can be held intact and isolated from the issuer, but as history has shown, if the issuer faces financial trouble or misconduct, the coin's value can unravel. Past examples include allegations that some issuers printed tokens without full backing. Similar issues have occurred even with MMF issuers, such as during the Lehman collapse in 2008. Without proper oversight, an issuer's failure could freeze redemptions or break the one-to-one peg. Unlike bank deposits, stablecoin holders are usually unsecured creditors in an insolvency scenario. While they may rank high in claims on reserve pools, most issuers do not have insurance to backstop losses. The risk is higher for issuers operating in loosely regulated environments.

Mitigations: Use stablecoins issued by well-capitalised firms under regulatory supervision in established jurisdictions. Regulatory frameworks are increasingly requiring stablecoin issuers to be licensed entities such as bank subsidiaries or trust companies. Diversify exposure and avoid relying on a single issuer, regardless of convenience. Dependence on one issuer concentrates risk. If that issuer fails, the payment chain can stall, which supports the case for diversified options and contingency plans such as the ability to switch to an alternative stablecoin or payment network.

Reserve quality and liquidity

A stablecoin's stability depends on the assets backing it. Risk increases if reserves are of poor quality or not fully backed. If reserves are invested in illiquid or high-risk instruments to chase yield, redemption reliability suffers. Liquidity mismatch remains the largest real risk in a reserve pool.

Stablecoins have liabilities that must be met on demand, often within minutes. Some reserve pools invest in assets that can **only be accessed during banking hours,** which provides no help if there is a run on the stablecoin at night or over a weekend. Fiat assets held in bank accounts are difficult to sell quickly, especially outside banking hours, creating a liquidity crunch if many users redeem at once. For example, a stablecoin backed by two-month Treasury bills may struggle to liquidate those assets quickly enough to meet redemptions in a panic.

Mitigations: Select stablecoins that can hold 24/7 versions of high-quality assets, such as tokenised MMFs that have repo facilities, other stablecoins (yield-bearing or otherwise), or trusts that have been able to build 24/7 solutions for liquidation. Examine the reserve composition and reporting frequency. High-quality, short-duration assets such as cash and US Treasuries are still sound.

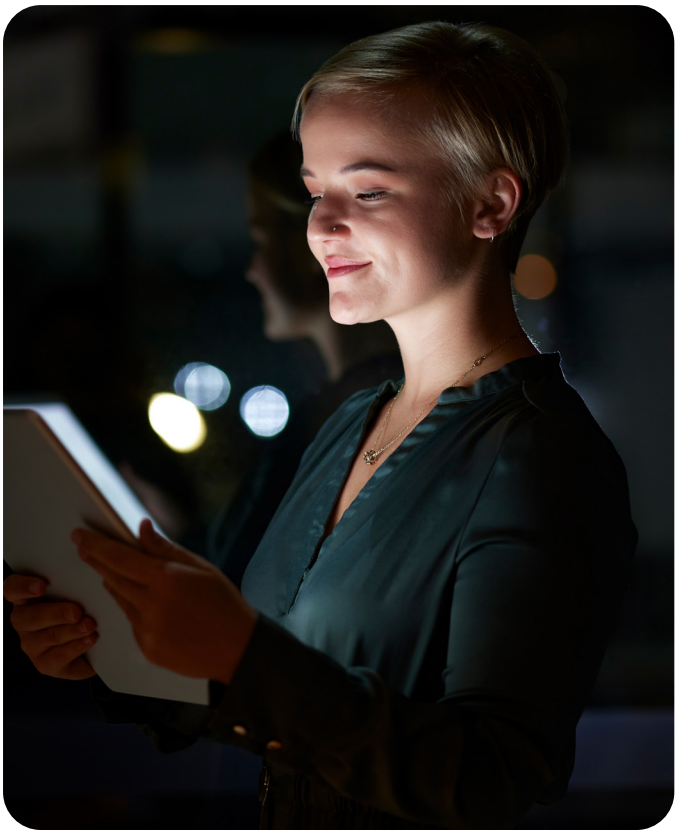
Transparency is critical, but understanding the operational mechanics that might temporarily affect the peg is equally important. Limited visibility can unsettle institutions. Delayed redemptions when assets are still being processed can do so as well.

Opt for issuers that provide frequent, independent reserve attestations, ideally real-time verification of backing assets, and clear redemption processes. Users can rely on exchanges to convert out of their stablecoin, but without the due diligence underneath, this liquidity may be mistaken for comfort that the asset will always be worth a unit of fiat.

Issuer and reserve risk

Redemption and legal structure

Investigate the legal rights attached to the reserves. Are they segregated and protected if the issuer becomes insolvent? If not, holders may find themselves behind other creditors in a recovery process. For example, if reserves are co-mingled or pledged elsewhere, redemption could become uncertain during insolvency. A sound structure will hold reserves in ring-fenced accounts or trusts for the benefit of token holders, reducing legal risk. Also review the redemption process. Is redemption direct with the issuer or through intermediaries? Are there thresholds or fees? Institutions should favour those offering same-day redemption at par for authorised holders. In the US, state based Trust structures are common bankruptcy remote vehicles to use. Each state has different rules. For example, the NYDFS does not allow 24/7 assets to be held as part of the reserves (which runs counter to the risk mitigant above), whereas other states, such as Delaware, do permit this through trust structures. These details are important when selecting a reliable stablecoin.



Concentration and systemic considerations

The more your operations rely on a single stablecoin, the more counterparty risk you assume. Many firms now set internal limits on exposure to any one issuer. They also monitor market indicators, such as price deviations or negative news, to reduce exposure early if required. Some maintain contingency plans to switch to an alternative stablecoin or fiat when signs of distress appear. This agility is critical, as stablecoin holdings are exposed directly to issuer risk.

Credit rating agencies such as Moody's are developing scoring systems for stablecoins based on reserve quality and reliability. These independent reviews, together with bank credit ratings for tokenised deposits or fund sponsor ratings for MMFs, can support institutional decision-making. Stablecoin clearing houses and custodial networks are also helping institutions hold diversified balances across issuers, protocols, and jurisdictions, improving operational resilience.

Issuer and reserve risks demand a credit-style approach. Scrutinise the issuer as carefully as any counterparty. Transparency, strong asset backing, and clear legal structures are essential. If information is incomplete or unclear, the stablecoin may be unsuitable for institutional use. Encouragingly, best practices such as monthly audits, proof-of-reserves, and regulated issuer frameworks are helping to improve stability and comparability.

> *"Treat digital assets with the same discipline applied to traditional finance."*
>
> **Jasmine Burgess**

Operational risk

Operational risk covers failures of internal processes, systems, or human error when integrating stablecoins into enterprise operations. Even though the technology is new, long-established operational principles still apply: mistakes or control lapses can lead to losses. Key operational challenges include:

The chain of the wallet is critical

If a stablecoin is sent on the wrong chain, for example moving an EVM-based token to a Solana address, or any wallet–token chain mismatch, the assets will be permanently lost. There is no recovery mechanism on public chains, and this can cause instant, irreversible loss. Training the operations team can alleviate this risk. Until you have that experience in-house, using permissioned or controlled networks helps mitigate this risk, as catastrophic mis-routes can be identified and reversed by design.

Settlement finality and irreversibility

Blockchain transactions settle quickly and irreversibly. There is no option to call the bank to reverse that wire. If you send 1,000 tokens to the wrong address, they are likely gone forever. This raises the stakes for accuracy in payment operations. Institutions must adapt procedures, for instance, by implementing standard operating procedure for wallet addresses (copy-paste checks or checksum tools) and requiring multi-person approval for large transfers.

A common best practice is using a test transaction for new payees: sending a small amount first, confirming receipt, then sending the rest. Some enterprises use whitelisted address books that only allow transfers to pre-approved addresses to prevent costly mistakes. The overarching goal is fail-safe processes: every transaction should undergo at least dual control (maker-checker) before irreversibly hitting the blockchain.

Key management and custody

Owning stablecoins means controlling private keys, which are essentially the passwords that grant access to funds. Lost or compromised keys mean lost funds, with no recourse. This is perhaps the biggest operational change compared to traditional banking. Firms must decide whether to self-custody or use an external custodian. Self-custody gives control but places full responsibility on your team to secure keys (through hardware wallets, multisignature, backups, and similar methods).

Custodial solutions such as regulated crypto custodians or bank digital asset custody services can hold keys on your behalf, often with insurance and professional key management in place. Many institutions adopt a hybrid approach: keeping a working amount in secure hot wallets for liquidity, while storing the bulk in cold storage or with a custodian. Using multisignature wallets or multi-party computation can ensure that no single person can move funds unilaterally. This guards against both internal fraud and external theft. Regular audits of wallet procedures and backup recovery drills are essential. A number of incidents have occurred where poor key management led to permanent loss, such as an exchange losing access to a backup or an employee misplacing a seed phrase.

Treat private keys as you would physical cash in a vault: restrict access, use strong authentication, and audit regularly.

System integration and reconciliation

Stablecoin flows occur on a blockchain ledger that may be external to your core systems. This can lead to reconciliation risks and discrepancies between on-chain balances and internal records. For instance, your treasury may initiate a token payment on Saturday, but your accounting system or ERP might not automatically capture that off-hours movement. Firms need to extend their technology infrastructure, integrating blockchain wallet monitoring into treasury management systems or using middleware that updates internal ledgers in near real time.

Daily (or more frequent) reconciliation of on-chain wallet balances to internal books is essential. Many firms set up dashboards that track all pending and confirmed transactions on the relevant blockchains, providing operations teams with visibility into settlement status. It is also wise to adjust cut-off times and procedures, for example by adding an end-of-day process to record any token transactions that happened outside normal business hours. Essentially, real-time financial operations need to match the 24/7 nature of digital assets.

Third-party dependencies

Few institutions run their own blockchain nodes or manage every function in-house. You might rely on a custody platform, a crypto exchange for conversions, a node or API service for blockchain connectivity (such as Infura or Alchemy), or a settlement network provided by a fintech or consortium. These third parties introduce vendor risk: if they go down, your operations could halt. There have been cases where a major custodian's outage froze clients' ability to move funds for hours.

Mitigation includes carefully vetting vendors (SLA uptime, security certifications) and maintaining contingency plans. For example, keep backup access through a secondary wallet provider or maintain the ability to connect a self-hosted node if your primary provider fails. Business continuity plans should include scenarios such as network congestion or service provider outages. Running regular drills for these scenarios will ensure your team can respond effectively.

> *"Stablecoins still require the same level of industrialisation and resiliency that we have within our global payment systems today. Becoming a regulated issuer brings a world of complexity.*
>
> **Angie Walker**

24/7 operational readiness

Unlike traditional payment cycles, stablecoin transactions can occur at any time. This means your organisation may need to provide round-the-clock support. If a problem or urgent need arises on a Sunday morning, is there an on-call procedure? Even if you do not staff 24/7, you might still need a protocol for off-hours emergencies such as a key compromise or an unexpected large incoming transfer.

Many firms adopting digital assets have implemented follow-the-sun support models or duty rotations for their operations and IT teams. Stablecoin processes should be included in your wider operational risk framework. Documentation and training should ensure continuity if a key person is unavailable. Regular stress testing, such as simulating a high volume of token transactions, helps assess capacity and readiness.

In essence, stablecoin operational risk is about combining new technology with established process discipline. Controls that banks apply to wire transfers, including dual approvals, tested procedures, and audit trails, should apply equally to blockchain transactions. By investing in training, clear roles, and automated safeguards, institutions can significantly reduce the chance of an operational mishap causing financial loss or reputational damage.

Cybersecurity and smart contract risk

Where there is money, there are hackers, and with digital tokens, the attack surface can be broad. Cyber risk in the stablecoin context includes the threat of theft (of keys or tokens) and vulnerabilities in the smart contracts or platforms supporting the tokens.

Wallet security and cyber attacks

Holding stablecoins makes an organisation a potential target for cybercriminals. Attackers may attempt to compromise computers or devices that store private keys or trick employees into revealing credentials or signing unauthorised transactions. Unlike bank accounts, where fraudulent transactions might be detected, reversed, or insured, crypto transfers, once executed, are final and often pseudonymous, making recovery difficult. There have been high-profile thefts via phishing, such as an employee being tricked into signing a transaction that drains a wallet, and malware that searches for private keys on compromised machines.

Best practices start with locking down the environment: use dedicated hardware wallets or Hardware Security Modules for signing transactions. These devices keep private keys isolated from internet-connected systems. Implement strong multi-factor authentication and physical security for any system that can initiate transfers. Segment duties, for example, one machine (offline) prepares transactions, while another (online) broadcasts them, to minimise exposure. Regular penetration testing and red team exercises can help identify weaknesses.

It is also critical to configure whitelisting on custodial solutions or smart contracts. Set up wallets so they only send to pre-approved addresses. This way, even if an attacker tricks someone, they cannot redirect funds to an unauthorised address.

In short, apply a defence-in-depth cybersecurity posture: assume any single layer, such as an employee's PC or an API key, could be breached and design multiple checkpoints that an attacker would have to defeat.

Until an organisation is confident managing these risks, it is safer to work with permissioned stablecoins, tokenised deposits, or tokenised MMFs, as these are almost always permissioned. In the event of a hack or cyber breach, the issuer in a permissioned environment can freeze stolen assets and reissue them to the rightful owner.

This feature provides valuable protection and serves as one of the best "training wheels" for institutions entering the space.

Smart contract vulnerabilities

Stablecoins are typically implemented as smart contracts on a blockchain, such as ERC-20 tokens. If an institution uses more complex functionality, for example locking stablecoins in a decentralised finance ("DeFi") lending protocol or a multisignature contract, it inherits the risk of bugs in that code. Even major stablecoins have experienced smart contract upgrades or integrations that went wrong, although the largest, such as USDC, are professionally audited and tested. If an organisation issues or uses an in-house stablecoin or tokenised deposit on a programmable ledger, bugs in the logic or permission settings could have severe consequences. The Parity multisig bug that froze Ethereum funds in 2017 remains a cautionary example.

Mitigations: Use only well-audited smart contracts and platforms. Before deploying any contract, even a simple custody or escrow contract, have it reviewed by reputable security firms. Companies such as Halborn specialise in auditing blockchain code for vulnerabilities. Many institutional-grade protocols undergo multiple audits and formal verification. Stay on supported releases and keep contract libraries and node software up to date to include security patches. For third-party DeFi platforms, monitor their community and news channels to receive early warnings of vulnerabilities or governance changes. Some institutions also purchase crime or crypto-theft insurance to offset financial loss in case of a hack. While insurance does not prevent incidents, it can help mitigate impact.

Case study: The Parity multisig bug (2017)

In 2017, a flaw in Parity Technologies' Ethereum wallet software caused one of the most significant smart contract failures in blockchain history. The vulnerability affected multi-signature wallets that many projects and ICOs used to manage pooled funds securely.

A user inadvertently triggered a bug in the wallet's underlying smart contract library, became its temporary owner, and then accidentally deleted the code. This action permanently froze more than $150 million in Ether, making the funds inaccessible.

Public blockchain risks and private networks

A well-established public blockchain such as Ethereum has a large amount of computational power or staked value securing it, making direct attacks on the network difficult. In contrast, a small private or permissioned blockchain, such as one used for a bank's tokenised deposit system, might have only a few validating nodes that could be more easily compromised or suffer downtime due to software errors.

Paradoxically, public chains can offer stronger technical security guarantees due to decentralisation and continuous community scrutiny, while private chains provide greater access control.

Many enterprises now blend these approaches, for example using permissioned layers or consortium networks built on top of public chains. This provides the security of a public chain while maintaining transaction privacy and access control through smart contracts.

The key is to assess the security of the ledger that a stablecoin operates on. If a smaller network is chosen for reasons such as privacy or transaction speed, institutions should demand robust testing and operational security from its operators, as it will not have the same level of public scrutiny as a major chain.

Real incidents highlight this trade-off: Solana, a high-speed public chain, has suffered outages due to overload, and Ethereum Classic has experienced 51% attacks. No blockchain is entirely risk-free, but some have proven more resilient than others.

Using mature, widely adopted chains for critical transactions is advisable, especially at early stages. If a newer chain is used, have a fallback plan, such as the ability to pause or migrate assets to another network if a major issue occurs. Multi-asset chains can help mitigate such risks.

If a protocol fails or is frozen, the issuer may be able to make holders whole on a new network. Multi-chain stablecoins also require attention to network compatibility, as wallets must match the correct chain to receive assets safely.

Cross-chain and bridge risks

Moving stablecoins across blockchains introduces additional risks. Many stablecoins exist on multiple networks, and third-party bridge services enable transfers between them. Unfortunately, bridges have become frequent targets for hackers.

More than $2 billion was stolen from cross-chain bridges in 2022 alone. Bridges typically lock tokens on one chain and mint equivalents on another. If the bridge's smart contract is compromised, the locked tokens can be stolen, leaving the newly minted tokens unbacked.

Furthermore, if stablecoins are sent to an address on the wrong network, such as sending to an Ethereum address instead of a Solana address, those funds may be irretrievably lost.

Mitigations: Avoid unnecessary cross-chain transfers and try to keep transactions on a single network or within unified platforms when possible. When bridging is necessary, use only established bridges that have undergone thorough audits and have insurance or recovery funds in place. Limit exposure by avoiding large sums on bridges for extended periods. New interoperability technologies, such as hashed timelock contracts, aim to reduce reliance on bridges. Always double-check destination networks and test with small transfers before using new routes. Treat cross-chain transfers as high-risk operations requiring extra oversight.

In summary, cyber and technical risks demand traditional IT security discipline applied with blockchain-specific awareness. Cybersecurity teams should be involved from the start, reviewing key storage methods, audit reports, and network resilience. Everyone handling digital assets should be trained to think critically, verify addresses, and identify phishing attempts. One wrong action can have immediate financial consequences. The lesson remains clear: **if you hold the keys, protect them like the crown jewels.**

Blockchain protocol and infrastructure risk

Blockchain protocol and infrastructure risk overlaps with cyber risk but focuses on the underlying blockchain infrastructure and how its performance or design can introduce risk. For institutions, the blockchain is effectively part of the payment and settlement infrastructure, and it comes with its own reliability and efficiency considerations.

Network downtime or performance issues

Major public blockchains aim for near-constant uptime, but some have experienced outages or slowdowns. Solana, known for high throughput, has had notable outages, such as a 17-hour halt in September 2021 caused by bot traffic, and others in 2022. If you were relying on Solana stablecoin transfers at those times, you would not have been able to move funds until the network was restored. Even Bitcoin and Ethereum have had brief incidents such as temporary chain splits or congestion issues. During peak congestion, transaction fees can spike and confirmations slow down. This unpredictability is a risk: a time-sensitive payment might get stuck in a backlog, or costs might exceed expectations, for instance, an overnight spike turning a $1 transfer into a $50 one.

Mitigations: For mission-critical use, favour blockchains with a strong track record of stability and sufficient capacity for your needs. If using a newer or less tested network, stress-test it by simulating heavy loads and observing performance. Architect processes to handle delays, such as a queue system to retry transactions when issues clear. Some institutions maintain redundancy by using multiple networks, for example, holding stablecoins on Ethereum and another chain, so if one network is unavailable, the other can serve as a backup. Keeping some liquidity off-chain or on a secondary network is similar to maintaining a disaster recovery site. Monitor network health and subscribe to alerts so that any issues can trigger contingency plans.

Case study: Solana network outages (2021–2022)

Between 2021 and 2022, Solana, a high-speed blockchain, suffered several major outages that halted network activity for hours. The most severe, in September 2021, lasted 17 hours after a flood of automated transactions overwhelmed validators.

Subsequent incidents revealed weaknesses in consensus coordination and software stability. For institutions, these outages highlighted that performance and scale can compromise reliability. The key takeaway is to rely on well-tested networks for critical operations and maintain contingency procedures for transaction continuity.

Blockchain protocol and infrastructure risk

Finality and consensus risks

Different blockchain designs define finality differently. Proof-of-work chains such as Bitcoin or Ethereum (before the Merge) provide probabilistic finality, where each subsequent block increases security. Other chains, such as many proof-of-stake networks, offer near-instant finality. However, attacks such as 51% attacks or consensus bugs can still compromise finality. Ethereum Classic's 51% attacks showed that smaller networks can experience reversals of transactions that were thought to be settled. Institutions must understand these nuances. For high-value transfers, it may be prudent to wait for a defined number of confirmations or even require additional assurances before considering settlement final.

Mitigations: Define internal policies for confirmation thresholds by transaction size, for example, waiting for six blocks on Ethereum for transfers above $1 million. Consider additional safeguards such as checkpointing, which records transaction states externally to detect reorganisation.

The key is not to treat blockchain settlement as infallible. While rare, reversals or disruptions can occur, so risk tolerance should align with confirmation depth and monitoring procedures.

Interoperability and integration:

When different systems must interact, such as in delivery-versus-payment ("DvP") where a tokenised asset on one ledger trades for a stablecoin on another, settlement risk can arise from timing or integration mismatches. Atomic DvP is most reliable when both legs occur on the same chain or on tightly integrated networks. If not, one leg may settle without the other. Similarly, corporate systems that interface with blockchain networks via APIs and middleware may encounter operational mismatches.

Mitigations: Whenever possible, execute DvP transactions on a single platform where a smart contract can enforce simultaneity. If cross-chain settlement is necessary, use specialised atomic swap protocols or trusted intermediaries that assume the interim risk. Test integration points thoroughly. For instance, if your treasury management system triggers a blockchain transfer through an API, determine how it behaves if the API call fails or the network is slow. Build error handling and manual override procedures. Stay informed on interoperability developments and on Chainlink CCIP, which are designed to improve the reliability of transactions that move across different chains.

Overall, protocol and infrastructure risks serve as a reminder that when using stablecoins, part of the payments infrastructure is outsourced to networks beyond your direct control.

Due diligence on these networks is as important as due diligence on the issuer. Assess network governance, including how upgrades are decided, whether changes could affect your use case, the level of decentralisation, and the existence of backstops. Some permissioned systems have administrative keys to pause or fix issues, which introduces both risk and a degree of control. Engaging in industry forums or consortia can give institutions influence in the governance of the networks they depend on. For example, banks involved in permissioned chain governance can advocate for features or standards that enhance reliability.

However, the true potential of stablecoins lies in open DeFi applications that are built in public blockchains. When issued on permissioned blockchains, their use becomes limited, restricting access to open DeFi ecosystem and applications. To enforce compliance and maintain control on public blockchains, issuers can leverage ERC-3643 permissioned token smart contracts. This approach enables ownership tracking, controls, and interoperability with DeFi.

In summary, enterprise risk management should encompass blockchain technology risks. Treat the blockchain like a key vendor or service provider: require reliability standards, implement monitoring and incident response plans, and diversify or insure against potential failures.

Governance and transparency risk

This category covers weaknesses in how stablecoins are governed, both in the internal governance of the issuer or project and in the broader regulatory oversight surrounding them. In short, it concerns who makes the rules, who oversees operations, and how transparent those processes are.

Issuer governance and controls

An often underappreciated risk is the possibility of mismanagement or malfeasance due to poor governance at the issuer. For instance, if a stablecoin's leadership can unilaterally decide to lend out reserves to affiliated parties, or if there's no independent board or oversight, the risk of something going wrong (without users knowing until it's too late) is higher.

Transparency gaps, like delayed or no audits, or opaque corporate structures, go hand in hand with governance risk. When evaluating a stablecoin, scrutinise the organisation behind it.

Do they have a reputable management team and a board with proper risk and audit committees? Are their reserve management policies published and monitored?

Technical governance also matters: many stablecoins have admin keys or the ability to freeze accounts or mint new tokens. You need to know who holds those powers and under what conditions they're used. If a single Chief Technology Officer can print new tokens or blacklist your address without notice, that's a risk.

On the other hand, if an issuer has too little control (as in some decentralised stablecoins governed by token holders), one must assess that governance process: is it slow? Prone to hacks (e.g. governance token attacks)? For example, decentralised stablecoin projects like MakerDAO (issuer of DAI) have had governance challenges and are only as robust as the community's decision-making.

Mitigations: Favour stablecoins with strong governance frameworks. This might include regulated oversight (e.g. a New York trust company issuing a stablecoin under New York State Department of Financial Services regulation, which ensures certain governance standards), or issuers that voluntarily publish governance reports. Check if the smart contract has been audited for governance-related functions (like emergency shutdown or freeze functions) and whether those have multisignature control or regulatory oversight. Some stablecoins even have independent trustees or reserve managers to provide checks and balances. In short, governance risk is mitigated by transparency and accountability - the more an issuer operates like a prudent financial institution (with independent audits, clear policies, separation of duties), the better. If instead you find secrecy or a "move fast and break things" culture, be wary.

Governance and transparency risk

Decentralised governance vulnerabilities

For stablecoins that are algorithmic or crypto-collateralised (like DAI, which is governed by MKR token holders, or the ill-fated Terra which had a governance token), there are unique risks. For one, governance decisions (like adjusting reserve ratios or monetary policy of the coin) might be influenced by large token holders who don't have your interests at heart. There have been cases in DeFi where governance was attacked (someone buys a majority of governance tokens to push a malicious proposal). Additionally, changes can happen that you, as a user, have no control over, e.g. a decision to support a hard fork or to wind down a project.

Mitigations: If using such stablecoins, you may need to actively participate in or monitor their governance forums. However, many institutions for now avoid purely decentralised stablecoins for core uses due to these uncertainties, sticking instead to fiat-backed coins or tokenised deposits where governance is more traditional.

Transparency as a tool

One advantage of many stablecoins is on-chain transparency of transactions. But transparency must extend to off-chain operations (reserves, corporate actions) to be meaningful. Insist on a level of reporting from issuers, for example, monthly reserve attestations by a reputable audit firm are becoming an industry norm.

Some issuers provide real-time dashboards of backing assets or publish the addresses holding their reserves. Use that information. Additionally, examine the history: have there been incidents (like freezes or hacks), and did the issuer communicate promptly and thoroughly? A good partner will be open about challenges and how they handled them. If you encounter an issuer that is evasive or inconsistent in disclosures, that's a governance red flag.

Regulatory inconsistencies and uncertainty

This is governance in a broader sense, the external governance by laws and regulators. The stablecoin landscape globally is still patchy: some jurisdictions have clear rules (e.g. the EU's MiCA, which establishes a framework for stablecoin issuers; some countries treat certain stablecoins as e-money), while others are in flux. Regulatory arbitrage is a risk: an issuer might choose the laxest jurisdiction, which could leave you exposed. Conversely, a crackdown in one country could impact your usage even if you're elsewhere (e.g. if the US bans a stablecoin, its global liquidity and support may drop).

There's also the question of classification: is a given token considered a security, a deposit, a "stored value," etc.? Classification changes can impose new compliance requirements suddenly. For example, if a regulator later deems a stablecoin to actually be a money market security, an institution using it might suddenly need to consider securities law compliance.

Mitigations: Stay informed and agile. This means having your compliance/legal teams actively track developments in all jurisdictions you operate in. Engage with regulators where possible, as many regulators appreciate when industry participants proactively share their plans and concerns ("ask permission, not forgiveness" after the lessons of Facebook's Libra). Work within regulated frameworks when available; for instance, if you can use a stablecoin that's issued under a strong regulatory regime (like one overseen by a central bank or a major jurisdiction's law), that reduces uncertainty. If you venture into grey areas (say, using an algorithmic stablecoin or a DeFi platform for yield on stablecoins), be prepared for possible sudden changes in legality or guidance. Always have an exit strategy: what would you do if tomorrow a law banned the stablecoin you use, or required all holdings to be disclosed? Planning these scenarios (like an emergency risk management exercise of "regulatory risk scenario analysis") is prudent.

Governance and transparency risk

KYC/AML and financial crime compliance

Governance also means making sure the stablecoin usage aligns with financial crime laws. Public stablecoins move on pseudonymous blockchains, raising concerns about illicit use. Regulators expect that institutions treat stablecoin flows just like traditional funds from an AML perspective. If you accept stablecoins from a client, you'd better know who that client is and whether the source of funds is clean. There's also the Travel Rule, requirements to pass sender/receiver information for crypto transactions above certain thresholds, which now apply in jurisdictions like the EU.

Mitigations: Implement blockchain address screening (using tools like Chainalysis, TRM, etc.) to flag sanctioned or high-risk addresses. Only use stablecoin services that have KYC, for example, when redeeming or onboarding into stablecoins, go through platforms that perform KYC checks so you aren't dealing with anonymous counterparties. Maintain internal policies restricting use of privacy coins or mixers; while on-chain privacy techniques exist (and may be needed for business confidentiality), they can trigger red flags, so tread carefully and with legal advice.

Essentially, treat stablecoin transactions as bank transactions: document them, screen them, and be prepared to provide rationale and reports to regulators/auditors.

The compliance burden is not removed by the tech, if anything, it's under more scrutiny due to high-profile crypto-related enforcement actions.

Governance and transparency risks underscore that stablecoins straddle the line between technology and trust. These risks can be mitigated by selecting trustworthy issuers or protocols with strong governance, operating transparently and in compliance, and remaining adaptable to regulatory change.

When the risks in this area exceed your institution's comfort level, it may be better to choose a different stablecoin, ideally one designed to be regulator friendly, or to work through intermediaries who assume some governance responsibility, such as a custodian ensuring compliance. We'll explore some of these intermediary roles next.

Framework	What it regulates	Why it matters for institutions
MiCA (EU)	Issuance, reserve quality, redemption rights, governance, disclosure	Creates the most comprehensive global standard for fiat-backed stablecoins
FSRA (ADGM)	Stablecoin reserve segregation, PoR, operational controls, technology risk	Strong operational and reserve rules; clear supervisory expectations
BMA (Bermuda)	Digital asset business licensing, governance, audit, risk management	Provides a robust framework for custody and issuance under one regulator
US (proposed)	Bank-grade issuance, classification, prudential supervision	Would impose the strictest issuer standards once finalised

Framework for evaluating stablecoins (due diligence checklist)

Having explored the major risk categories, how can an institution systematically evaluate a stablecoin's risk before using it? It is helpful to adopt a checklist or matrix covering key factors. Below is a condensed framework of questions to ask, essentially a due diligence checklist grounded in the risk areas already covered (issuer, reserves, technology, and related considerations).

Issuer and regulation

Who is the issuer and what is their regulatory status? Prefer stablecoins from regulated entities such as a bank or a licensed trust company, or those operating under clear regulations such as e-money rules or stablecoin-specific laws. Verify if the issuer is subject to routine supervision, such as bank examinations. If it is a non-bank fintech, check for money transmitter licences or similar oversight. An unlicensed offshore issuer introduces significant legal and credit risk. For example, the US is considering legislation such as the GENIUS Act to restrict issuance to permitted, regulated entities, and using such an issuer would be wiser than one operating in a regulatory void.

Redemption process

Can you redeem the stablecoin easily for fiat? Identify who can redeem (retail or institutional holders) and the speed and cost of redemption. A reliable stablecoin provides 1:1 redemption, often through an account portal, on a predictable schedule such as same-day or next-day. If redemptions are limited (for example, only for large holders or subject to long delays), you may have to rely on secondary markets, which is less direct. Review whether there have been redemption suspensions or if terms allow them, as many issuers retain such clauses for extreme conditions. For institutional use, you want confidence that under normal circumstances you can always redeem at par promptly.

Reserve quality and security

What assets back the stablecoin, and where are they held? Look for high-quality, liquid reserves: cash in insured banks and short-term government securities remain the gold standard. If reserves include riskier instruments such as corporate debt, loans, or other crypto assets, understand that these increase default or liquidity risk. Ensure reserves are held with trusted custodians and ideally segregated from the issuer's own assets. If possible, confirm that reserves are legally protected (for example, held in trust accounts). A red flag arises if an issuer will not fully disclose reserve composition, uses vague descriptions such as "may include loans," or holds most reserves with one institution. Proceed with caution in such cases.

Transparency and reporting

Does the issuer provide independent reporting on reserves and operations? Regular audits or attestations (monthly is ideal) by reputable firms build confidence. Transparency also means publishing details such as reserve asset breakdowns and, if possible, the on-chain reserve addresses for verification. Some top-tier stablecoins and tokenised deposits now provide daily or real-time reserve updates. Also consider how transparent the smart contract operations are. Are functions such as freeze or mint documented? Has the code been open-sourced or reviewed? If an issuer is evasive about these aspects, it is a governance concern. In short, demand transparency, as it is your best window into the risk.

Framework for evaluating stablecoins (due diligence checklist)

Governance and controls

What governance framework does the stablecoin operate under? Look for evidence of strong internal controls: audited smart contracts, documented decision-making processes, and, ideally, third-party or regulatory oversight of critical actions. For instance, if an issuer can freeze tokens, under what conditions will this be exercised (law enforcement request or internal discretion)? If it is a DAO-governed stablecoin, examine its governance history: are upgrades reviewed and tested, and is there a risk of governance capture? For institutional use, prefer issuers with formal governance policies and, where applicable, oversight by a board or regulator.

Underlying blockchain (protocol)

Which blockchain or blockchains does the stablecoin operate on, and are these networks reliable and widely adopted? A stablecoin on a major chain such as Ethereum is easier to integrate and typically more liquid but may come with higher transaction fees. Smaller chains may offer lower fees but greater operational risk. If a stablecoin exists on multiple chains, verify that each version is fully backed and redeemable. Some issuers treat tokens on all chains equally, while others distinguish between primary and wrapped versions. Consider interoperability. Will the stablecoin be usable on the platforms and with the counterparties you require? A niche or proprietary ledger may limit utility. Also assess network security, as highly decentralised chains are more resilient, while newer ones may trade safety for speed. Align your stablecoin choice with your institution's technology risk appetite. For example, use a slower but highly secure chain for large settlements and a faster chain for smaller payments.

Privacy features

Does using the stablecoin expose transaction details that could compromise confidentiality? On public blockchains, transactions are visible to all participants, even if pseudonymous. Frequent institutional transfers could allow observers to infer business relationships or cash flows. Some enterprise-oriented stablecoin solutions offer privacy layers or permissioned networks to protect sensitive data. If confidentiality is a priority, for example when paying vendors or making internal transfers, consider stablecoins that support built-in privacy or allow address rotation. At minimum, use new addresses for different transactions, split large transfers, or time them strategically. Always ensure that privacy measures do not conflict with compliance obligations, as some tools, such as mixers, may be prohibited for regulated entities. The key question is whether using this stablecoin will expose data that violates confidentiality needs, and if so, how this can be mitigated.

Operational support

Consider practical integration factors. Does the stablecoin issuer or its partners provide integration assistance, APIs, or customer service? For enterprise adoption, a responsive support channel or service layer is valuable. Some banks and fintechs offer "stablecoin as a service," managing the technical complexity on behalf of clients. If operating directly, ensure your institution has the internal capability to manage it end to end. Also, clarify escalation procedures. If a transaction fails, funds are sent to a blocked address, or a technical issue occurs, can the issuer intervene or advise? While many stablecoin systems are self-service, a cooperative issuer able to assist or freeze funds in legitimate circumstances can reduce operational risk.

This checklist is a tool to filter and compare options. For example, if Stablecoin A has audited reserves, a banking licence, and operates on a reliable network, but Stablecoin B has opaque reserves and no regulatory oversight, a risk-conscious institution would favour A even if B is more widely used in crypto markets. The objective is to align the stablecoin choice with your institution's risk appetite and control framework. Thorough due diligence at the outset can prevent costly complications later.

Risk mitigation strategies and best practices

After selecting a stablecoin (or deciding among tokenised deposit or MMF options), institutions should implement strategies to continuously manage and mitigate risk. Many of these practices mirror traditional risk management, adapted for the digital asset context.

Employee training and roles

People are often the weakest link, so invest in structured and ongoing training to ensure teams understand how these instruments work in practice. Hiring staff with direct, hands-on experience in digital assets is invaluable, not those who only understand the legal or theoretical aspects, but those who have operationally handled digital assets, bridged protocols with the same token, whitelisted wallets, and recycled API keys to manage transfers and permissions securely.

The operations team should understand blockchain explorers, transaction hashes, and gas fees (where applicable), and have the authority to pause activity during periods of high network congestion.

The security and operations teams should remain vigilant against social engineering threats specific to crypto, such as fake wallet applications or malicious signature requests.

Roles and responsibilities must be clearly defined: who is responsible for initiating transfers, who approves them, who manages custody technology, and who monitors incoming funds. Some firms appoint a "Digital Asset Controller," equivalent to a cash manager, to oversee all stablecoin movements and custody arrangements.

Regular drills or simulations are also valuable. For example, teams can practise large-value transfers or simulate a lost key scenario to ensure everyone follows the playbook precisely. With clearly defined roles, rehearsed processes, and trained personnel, the likelihood of errors or panic in unfamiliar situations is greatly reduced.

Automation with safeguards

Where possible, use automation to reduce manual intervention and error risk, but always balance it with strong oversight and safety mechanisms. For instance, automated triggers can sweep excess stablecoin balances above a defined threshold back to a base account or convert them into fiat currency weekly to limit exposure. Smart contracts can also automate delivery versus payment settlements, reducing manual steps and operational delays.

However, human oversight and circuit breakers remain critical. Incidents such as the DeversiFi fee error demonstrate that even code can fail. Implement multi-signature approvals on all automated processes, and maintain detailed activity logs for audit purposes.

Automation should eliminate common errors such as entering an incorrect wallet format or sending tokens to exchange deposit addresses, while human reviewers should assess anomalies such as unusually large transactions flagged by automated rules before final approval.

A well-designed automation layer should combine efficiency with accountability, ensuring that technological tools support human judgment rather than replace it.

Internal policies and limits

Institutions should update treasury and investment policies to explicitly cover digital assets. For example, set a maximum exposure limit to stablecoins as a percentage of total liquidity, and diversify across at least two issuers to prevent concentration risk.

Specify which stablecoins are approved by name, allowing only those that have passed rigorous due diligence. Policies should also define authorised use cases, such as:

> *"Stablecoins may be used for settlement with approved counterparties or short-term yield parking, but not for long-term speculation."*

Clear guidance helps prevent unapproved or ad hoc activities. Incorporate compliance checkpoints, for instance:

> *"Any stablecoin transaction above $X must undergo compliance screening and CFO approval."*

By treating stablecoins as a distinct asset class with well-defined controls, institutions can align digital asset activity with existing risk and governance frameworks. Regular policy reviews should ensure that approved issuers, thresholds, and use cases remain up to date with market developments and regulatory expectations.

Continuous monitoring and alerts

In the digital asset environment, conditions can change within minutes rather than days. Establish real-time monitoring of all on-chain positions, associated wallets, and relevant market indicators. Blockchain analytics tools can detect unusual movements, such as unapproved outgoing transfers or access from unknown IP addresses, which may indicate compromise.

Monitor the stablecoin's market price across exchanges and DeFi pools. Any deviation from its peg, even by a few cents, should trigger attention and predefined actions. In parallel, track news about the issuer, such as regulatory investigations, reserve audits, or changes in banking partners, as these can directly impact confidence and liquidity.

Stablecoin exposures should be treated as risk positions requiring dashboards, alerts, and defined limits. Integrating blockchain data feeds into existing risk management systems can provide a single, consolidated view of liquidity and exposure. The objective is to know immediately when intervention is required, whether to withdraw funds, rebalance holdings, or escalate alerts to management.

Incident response plans

Despite best efforts, incidents can and will occur, including hacks, service outages, or sudden regulatory actions. A predefined and tested incident response plan ensures swift and coordinated action when problems arise.

If a wallet theft or compromise is detected, the team must know who to notify, both internally and externally. Maintain updated contact details for law enforcement, cyber insurers, and stablecoin issuers who may be able to blacklist stolen funds if informed promptly.

If a major depeg occurs, operations should pause transactions involving the affected stablecoin and immediately notify internal stakeholders and counterparties. In the event that a blockchain network experiences an outage, teams should be prepared to delay settlements or revert temporarily to traditional payment methods.

Response plans should be documented, regularly updated, and tested through tabletop exercises. Speed of execution is often the deciding factor in mitigating losses. During the 2023 USDC depeg, institutions that acted quickly to redeem avoided temporary valuation losses, while others had to wait for recovery.

Define clear criteria for escalation, for example:

> *"If stablecoin X trades below $0.98 for more than four consecutive hours, the risk committee must convene to decide next steps."*

Testing, rehearsal, and clarity of responsibility are essential to ensure confidence and resilience during high-stress events.

Use of trusted intermediaries

If the operational or cybersecurity risks of direct management are too great, consider outsourcing to regulated intermediaries. Using a licensed custodian to hold stablecoins can reduce exposure, as custodians often provide insurance coverage, regulatory oversight, and operational continuity.

If evaluating stablecoin quality proves complex, rely on third-party research or ratings from credible providers such as Moody's, which assess reserve composition and issuer transparency. Similarly, cybersecurity firms like Halborn or Trail of Bits can conduct penetration testing or smart contract audits to uncover weaknesses before they become critical vulnerabilities. In the future, a stablecoin clearing house may emerge, establishing common standards for collateral, netting, and settlement under regulatory supervision. Until then, institutions can replicate some of these benefits internally by using multiple issuers and managing them through a centralised operational hub, effectively creating an in-house clearing function that standardises settlement and reporting.

This approach balances autonomy with oversight, ensuring the institution benefits from technological innovation without bearing all the operational risk directly.

Diversification and incremental adoption

A phased approach is prudent. Start small with limited amounts and lower-risk use cases. As experience grows, expand gradually. Diversify across both issuers and forms of tokenised money. For example, use stablecoins for fast settlements while keeping most liquidity in tokenised MMFs with a more comfortable risk profile. This balances blockchain settlement benefits with limited exposure to any single risk source.

Treat digital assets with the same discipline applied to traditional finance. Training, automation, policies, and continuous monitoring build resilience. Start small, diversify exposure, and maintain a tested response plan to ensure control and continuity.

Tokenised MMFs: a safe sandbox for starters

For institutions new to digital assets, permissioned tokenised MMFs present an attractive training ground to build confidence and test risk controls. These are essentially shares in ultra-low-risk funds, such as funds holding treasury bills or insured bank paper, that have been tokenised on a blockchain. They are typically offered on private or permissioned networks to KYC-verified investors.

Sophisticated market participants are leveraging permissioned tokens, such as ERC-3643, to issue tokenised MMFs on public blockchains. This approach ensures regulatory compliance while giving issuers control over who can invest and when tokens can be transferred. Additionally, in cases of token loss, these tokens can be recovered, adding an extra layer of security.

Familiar underlying asset

A tokenised MMF is still an MMF, a regulated product with a stable net asset value objective (often one dollar per share) and high-quality assets. The risk of sudden loss is very low, barring extreme market events that could impose redemption gates or minor net asset value fluctuations. There is no new issuer credit risk beyond what already exists in traditional MMFs. This means your downside from a value perspective is limited compared to holding a purely crypto-backed or algorithmic stablecoin, which could theoretically lose all value.

Operational exposure to blockchain

Using a tokenised MMF involves many of the same operational steps as using a stablecoin, including setting up wallets, managing private keys or custody arrangements, and integrating with blockchain networks for transfers. Teams gain experience through activities such as handling 24/7 redemptions via blockchain. A digital transfer agent and fund administrator with on-chain capabilities like Apex Group can support 24/7 services required, helping issuers reduce operational and compliance risks.

Regulatory oversight

These funds are subject to securities regulation and ongoing supervision. They have regulated asset managers, independent custodians, and regulated administrators overseeing every trade and asset movement. They must also meet rules on liquidity buffers, maturity limits, and reporting, often providing daily transparency on holdings. This three-party oversight reduces the potential for fraud or error in any reserve pool. Regardless of what occurs on-chain, relying on well-established fund processes provides assurance to risk committees that the instrument follows established rules. It effectively wraps new technology in a familiar regulatory structure.

Integration with existing systems

Many tokenised MMF offerings include integration support from large custodians. For example, BNY Mellon and other institutions have developed platforms that allow clients to buy tokenised fund shares through familiar interfaces such as portals or APIs, with settlement occurring on a blockchain in the background. This allows organisations to test treasury integration indirectly while the custodian bridges the gap. Over time, institutions can choose to engage more directly as confidence grows. It provides a smoother on-ramp to blockchain participation.

Tokenised MMFs: a safe sandbox for starters

Yield and opportunity cost mitigation

Unlike cash stablecoins, which typically yield nothing, MMF shares generate interest, often at competitive rates. One risk of holding stablecoins is the opportunity cost of idle funds. Tokenised MMFs address this by offering returns similar to other short-term investments. Finance departments may therefore be more comfortable allocating liquidity to these products, as they can gain blockchain exposure without sacrificing yield. Some firms use tokenised MMFs for short-term cash management, earning a return while gaining operational familiarity with digital assets, and later extend usage to settlements or payments.

Psychological and compliance comfort

From a compliance standpoint, dealing with a known asset manager and a product governed by a prospectus can ease internal approvals. It is simpler to explain to a risk committee that the institution is investing in a US government MMF managed by a regulated entity, in token form, than to justify using a new coin operated by a startup. This builds internal confidence. Furthermore, if an operational issue occurred, such as a wallet error, regulators would likely view a loss during a controlled, regulated trial more favourably than losses from speculative crypto exposure. It demonstrates responsible innovation.

In practice, many institutions are starting here. They often begin with small tokenised MMF holdings for liquidity management. Risk teams observe the process over a quarter or two, then gradually expand or extend usage to settlement use cases.

It serves as a sandbox with training wheels, offering practical experience with blockchain operations, such as wallet infrastructure or custodian-managed private keys, while maintaining minimal asset value risk. Over time, both compliance and treasury teams build confidence with on-chain assets, making the transition to stablecoins or other digital instruments smoother.

Bottom line: For institutions cautious about entering the stablecoin market, permissioned tokenised MMFs offer a safer first step.

They provide hands-on exposure to blockchain technology in a regulated environment. Lessons learned in control design, technology integration, and liquidity management directly apply to stablecoins and other forms of tokenised money. Many view tokenised MMFs as the safest training environment for finance professionals entering the digital asset space.

The role of a stablecoin clearing house and other intermediaries

Throughout this guide, we have highlighted how risk can be mitigated through disciplined practices and the support of trusted partners. It is worth considering how the financial industry might collectively manage stablecoin risk at scale. One concept being explored is a **stablecoin clearing house.**

This would serve as a trusted intermediary for stablecoin transactions among institutions, similar in function to clearing houses in traditional financial markets. While still theoretical, such a structure could reduce systemic and counterparty risks in several ways.

Standardised risk management

A clearing house could set consistent standards for all stablecoins it accepts, requiring issuers to meet strict criteria for reserve quality, transparency, and legal structure. For instance, it could mandate real-time reserve verification and impose limits on asset risk, effectively weeding out weaker issuers.

By only handling approved stablecoins, it would protect participants from transacting in tokens with uncertain or insufficient backing. It might also mutualise reserves or establish an emergency fund for contingencies.

Multi-issuer diversification

Rather than the market relying heavily on one or two dominant stablecoins, a clearing house could enable interoperability among multiple issuers. If one issuer failed or was temporarily unable to redeem, the clearing house could reroute liquidity by swapping balances into another stablecoin or guaranteeing short-term funding. This would address the single-issuer dependency issue, insulating participants from an outage or failure. The system would ensure continuity of settlement in much the same way a power grid reroutes supply when a plant goes offline.

Liquidity backstop and netting

A clearing house could operate as a central counterparty that nets transactions, reducing the need for constant redemptions. For example, if two banks transact stablecoins with one another, the clearing house could settle only the net difference, lowering on-chain transaction volumes and liquidity demands. It could also coordinate with central banks to access temporary liquidity in times of stress, acting as a stabilising backstop similar to a lender of last resort. Although stablecoins lack such a mechanism today, a clearing entity could absorb shocks by pooling resources or pausing redemptions in an orderly, pre-agreed manner.

24/7 oversight and incident response

A centralised utility could monitor stablecoin flows in real time, identifying emerging systemic issues such as reserve depletion or unusual activity. It could coordinate responses and impose circuit breakers in extreme scenarios, pausing withdrawals or settlements to prevent a wider collapse. While this introduces moral hazard and governance challenges, collective contingency protocols developed with regulators could improve stability compared with uncoordinated institutional responses.

The role of a stablecoin clearing house and other intermediaries

Unified compliance and legal clarity

A clearing house could enforce consistent KYC and AML standards across participants, eliminating weak links. It could also operate under a clear rulebook, defining the legal status of stablecoin balances held within the system. This would simplify cross-border transactions and reduce uncertainty over regulatory classification. By serving as a focal point, it could liaise with multiple regulators to align oversight, avoiding the fragmented global landscape where stablecoins are classified differently across jurisdictions.

Protocol switching

If a blockchain protocol suffers an upgrade failure or severe congestion, the clearing house could move stuck tokens to a functioning network, maintaining liquidity continuity. This would address interoperability challenges by transferring the token or liability to another supported network. Such flexibility would be more robust than relying solely on automated interoperability protocols, which can introduce additional technical risks.

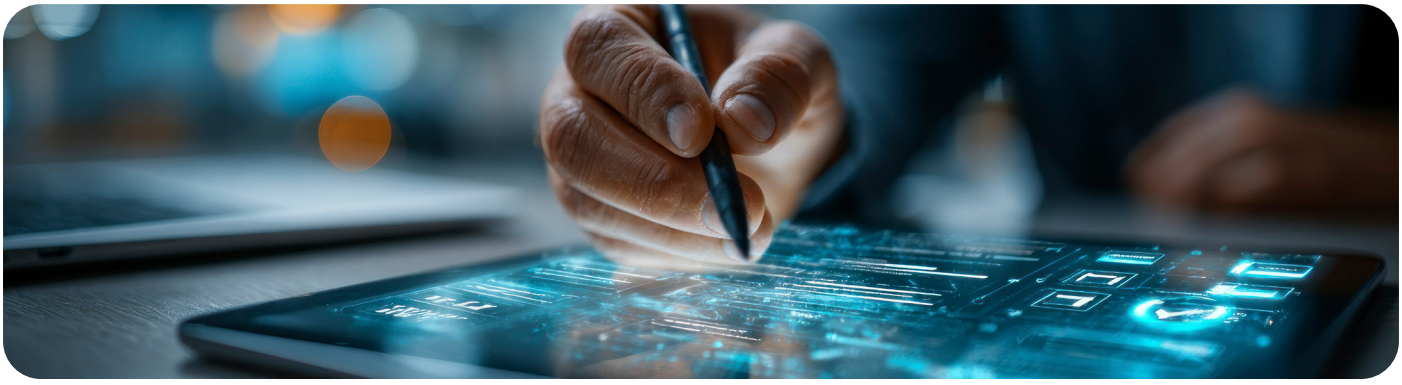
A communication layer independent of issuers

In the event of operational or reputational issues at the issuer level, a clearing house holding pooled reserves could act as an independent information source. It could provide timely updates on issuer conditions and market developments, reducing speculation and misinformation. Participants would benefit from a central point of contact with reliable visibility into the ecosystem.

Of course, a clearing house introduces centralisation and becomes a potential single point of failure if not properly governed. It would require robust oversight and resilience comparable to systemically important financial market infrastructures. The same risk categories outlined earlier would apply: governance, technology, and operational risk must be carefully managed to sustain trust and reliability.

In the meantime, while such industry-wide structures are still conceptual, trusted intermediaries are already filling some of these roles. Rating agencies such as Moody's are scoring stablecoins to improve transparency and discipline. Audit firms provide attestations on reserves, custodians offer secure storage and even issuance capabilities, and cybersecurity firms such as Halborn and Trail of Bits ensure smart contracts are robust. Institutions should make use of these partners where appropriate; there is no need to manage every risk in isolation when reliable providers can share the load.

Ultimately, whether through a formal clearing house or a network of trusted intermediaries, the institutional stablecoin ecosystem is likely to evolve into a structured, interconnected system resembling traditional finance, complete with standards, backstops, and coordinated oversight to contain risk.



Take-aways

The rise of stablecoins and other tokenised cash instruments offers a compelling vision of instant, always-on finance. Yet adopting these technologies in an institutional setting brings real challenges. By understanding issuer credit risks, operational pitfalls, technological vulnerabilities, governance weaknesses, and regulatory uncertainty, financial professionals can make informed decisions that balance innovation with prudence. The central message is clear: due diligence and sound risk management remain the best tools for safeguarding institutional integrity, just as they are with any other financial product.

When evaluating stablecoins for enterprise use, take a holistic approach. Examine the issuer's strength and transparency, scrutinise the reserves, assess the blockchain infrastructure, and account for the human factors such as training and process. Use frameworks and checklists to compare options and engage credible partners where possible. These may include rating agencies, cybersecurity auditors, or regulated custodians who can supplement internal expertise. If a stablecoin's risk exceeds your institution's tolerance, do not accept it unmitigated; either choose a safer option or apply controls such as hedging, insurance, or shifting exposure to a trusted intermediary.

> *"Due diligence and sound risk management remain the best tools for safeguarding institutional integrity.*
>
> **Jasmine Burgess**

It is important to acknowledge that not all stablecoins are equal. Some are as robust as a blue-chip financial institution, while others are fragile and opaque. The goal of this guide is to help identify which is which, and to ensure appropriate guardrails are in place. Tools such as tokenised MMF can provide a gentler starting point, allowing teams to gain experience with digital assets at minimal risk. These can serve as a stepping stone toward wider adoption of stablecoins or CBDCs when they become available.

Integrating stablecoins into mainstream finance will be a gradual process of collaboration between industry participants and regulators, and of learning from early missteps. There will likely be further teachable moments, including periods of market stress or failure, but each will contribute to better standards and more resilient frameworks, much as early banking crises led to modern risk management practices. By addressing risks proactively and engaging reliable partners, financial institutions can confidently explore this new terrain. The promise of faster, more efficient money is significant, and with vigilance and proper governance, it can be achieved without compromising stability or trust.

Stablecoin adoption must be grounded in rigorous due diligence, strong governance, and continuous risk oversight. When approached methodically, digital assets can strengthen rather than threaten institutional finance.

Note: Risk management in the digital asset space is a continuous process. Start cautiously, remain informed and prepared, and foster a culture of compliance and prudence as innovation advances.

With this mindset, stablecoins and related instruments can become valuable tools in the institutional financial toolkit, promoting efficiency and opportunity securely and responsibly.

> *"A stablecoin isn't just a means of value within one jurisdiction. It is a potential global payment mechanism and supporting that operation 24/7 is essential.*
>
> **Angie Walker**

How can we help?

Apex Digital 3.0 empowers the financial ecosystem with institutional-grade digital infrastructure for the current and future generations of digital fund lifecycle management. Built on trust, powered by AI, and designed for scale, it enables our clients to transition into digital fund representation and DeFi with confidence. It brings mobility, accessibility, democratisation, and transparency at a time when investor expectations centre on diversification, composability, and 24/7 market access.

We provide a comprehensive range of institutional-grade services to wealth and asset managers, covering the full digital asset value chain from fund tokenisation and digital treasury to liquidity and stablecoin infrastructure. These capabilities enable end-to-end support for issuers, managers, and intermediaries seeking to engage securely in the tokenised economy.

Our modular service suite includes:

- **Licensing and regulatory advisory**
  Support for jurisdiction selection, licence application, and regulatory compliance across leading markets.
- **Corporate services**
  Entity incorporation, company secretarial, and directorship services to establish and maintain regulated structures.
- **Middle-office and reserve management**
  Trade lifecycle support, reserve asset reconciliation, and independent risk and liquidity reporting.
- **PoR and transparency**
  Chainlink-integrated reporting and real-time, immutable verification of reserve assets for enhanced market confidence.
- **Tokenisation and secure minting**
  ERC-20 or ERC-3643 token issuance, identity-linked minting and burning, and 24/7 operational support.
- **Custody and asset segregation**
  Bankruptcy-remote structures and regulated custody through partners such as EDB, Citi, or other approved custodians.

Apex Digital 3.0 is the bridge between traditional finance and programmable digital money.

We provide the compliance, governance, and operational trust layer that enables institutional adoption of stablecoins to scale securely and sustainably.

Glossary

Term	Definition and institutional relevance
Algorithmic stablecoin	A stablecoin that maintains its peg through algorithmic supply controls rather than full reserve backing. These models carry higher failure risk and are generally unsuitable for institutional use.
Blockchain bridge	A mechanism that allows assets to move between different blockchain networks. Bridges introduce counterparty and cyber risks and should be vetted for audits and insurance.
Chainlink	A decentralised oracle network providing verified external data to smart contracts, often used for PoR. Enables real-time transparency for institutional users.
Custodian	A regulated entity that securely stores digital assets and private keys. Custodians reduce operational and key management risks and are essential for compliance-grade asset segregation.
Depeg	A loss of a stablecoin's one-to-one value relative to its reference currency. Monitoring for depegs is critical for treasury and liquidity management.
Fiat-backed stablecoin	A token backed by fiat currency and short-term liquid assets, such as cash and Treasuries. Considered the most institutionally acceptable stablecoin type due to clear asset backing.
Multisignature	A wallet configuration that requires multiple authorised signatures to approve transactions. Strengthens internal controls and reduces single-point fraud or error.
Private key	A cryptographic credential granting access to blockchain assets. Institutional policies must define secure storage, recovery, and access protocols.
Proof of Reserve	Verification process ensuring that token reserves match issued supply, often automated using oracles like Chainlink. Builds transparency and investor confidence.
Smart contract	Code on a blockchain that executes automatically when conditions are met. Requires rigorous security auditing before institutional deployment.
Tokenisation	The conversion of financial or real-world assets into digital tokens on a blockchain. Enables efficiency, fractionalisation, and 24/7 transferability.
Tokenised money market fund	Digital shares of regulated MMFs that combine blockchain settlement with conservative yield instruments. Provide a low-risk entry point for institutions exploring digital assets.
U.S. Treasury bills	Short-term government securities often used as stablecoin reserve assets. Their liquidity and credit quality underpin peg stability.

apexgroup.com

Contact us | Disclaimer

7015_011225