GBBC Global Blockchain Business Council

OLIVER WYMAN
A MARSH BUSINESS

Proposed Risk Mitigation Framework for Non-Financial Risk of On-Chain Payments

Phase 2 Payments – November 2026

We extend our sincere gratitude to the working group members comprised of 54 institutions (including financial institutions, blockchain and market infrastructure, regulators, and more), who took part in RMF as contributors or observers. Your support and engagement are deeply appreciated.

Contact

Comments from financial industry stakeholders and regulators are actively encouraged to inform and refine future phases of this initiative. Please contact **RMF@gbbc.io** to share feedback and ask questions.

Frequently Asked Questions (FAQs)

Click here to access.

© GBBC Global Blockchain Business Council © Oliver Wyman

Contents

Executive summary **4**

Four key takeaways **5**

1. Stablecoins **6**

1.1. Value chain 7

1.2. Stakeholders across the value chain and risk mitigation strategies 9

1.3. Key risks and mitigation strategies 10

2. Tokenized deposits **13**

2.1. Value chain 14

2.2. Stakeholders across the value chain and risk mitigation strategies 16

2.3. Key risks and mitigation strategies 17

3. Consortium-based payments models **19**

4. Path forward **20**

© GBBC Global Blockchain Business Council © Oliver Wyman

Executive summary

The financial industry and regulators increasingly recognize the potential of blockchain technology to reshape financial products, payment flows, and market infrastructure. Prior phases of the Risk Mitigation Framework (RMF) established a foundation for assessing the non-financial risks of public blockchain infrastructure, including Layer 1 and Layer 2 systems. This chapter extends that work to the application layer, where risk is shaped not only by the underlying infrastructure, but also by the legal nature of the instrument, the operating model, and the allocation of responsibilities across participants.

The previous RMF chapters on *Non-Financial Risks of Blockchain Infrastructures (Layer 1 and Layer 2)* provide the methodological foundation for this chapter, including the common non-financial risk taxonomy and control approach for risks stemming from the underlying blockchain. Building on this foundation, the chapter identifies the additional or adapted non-financial risks associated with designing, operating, and integrating stablecoin and tokenized deposit capabilities. These risks should be assessed alongside the relevant infrastructure risks.

Stablecoins can support continuous, near real-time, and programmable transfers of value across wallets, payment applications, exchanges, and merchant networks. Tokenized deposits can extend commercial bank money onto digital rails while retaining a claim on the issuing institution and much of the existing banking control perimeter.

These models can reduce selected frictions associated with fragmented ledgers, sequential processing, reconciliation, and intermediary-dependent settlement. At the same time, they redistribute responsibilities across issuers, banks, custodians, wallet and signing providers, exchanges, payment processors, merchants, financial-market infrastructures, analytics providers, and blockchain ecosystems. Effective risk management therefore requires controls to be located where decisions are made and transactions are authorized, rather than assuming that the underlying network alone can manage application-level risk.

Application-layer controls and residual risk vary by deployment model. Permissioned networks enable controlled participation, identity, and governance but require concentration and common-mode dependencies to be managed; permissionless networks offer open participation and broad interoperability but rely more on institutional perimeter controls, analytics, signing and token controls, and exposure limits; and permissioned-public models combine public infrastructure with controlled wallets, token permissions, or identity credentials.

Many of the resulting risks remain familiar to financial institutions, but blockchain-based market structures can alter their causes, timing, and impact. Continuous operations, cryptographic authorization, smart-contract administration, transaction finality, cross-chain activity, public data visibility, infrastructure concentration, and multiparty governance can require targeted adaptations to established legal, compliance, operational resilience, information security, third-party, and transaction-risk frameworks. Robust controls can reduce these risks, but residual exposure remains due to the limits of monitoring and intervention mechanisms and continued reliance on underlying networks and shared infrastructure. The analysis also recognizes that blockchain-based models may remove or reduce certain risks. Shared records and atomic settlement can reduce reconciliation breaks, settlement-leg exposure, and selected intermediary dependencies.

Future phases of the RMF will extend this application-specific analysis to additional forms of tokenized money and digital assets, including central bank digital currencies (CBDCs), tokenized money market funds (MMFs), native cryptoassets, and decentralized finance (DeFi).

The RMF acknowledges the complexity of this multidisciplinary challenge and recognizes that further iteration and improvement are required. Therefore, the RMF is being published as a draft based on the practical experience and input from participating institutions. Comments from financial industry stakeholders and regulators are actively encouraged to inform and refine future phases of this initiative.

© GBBC Global Blockchain Business Council © Oliver Wyman

Stablecoins extend blockchain rails to payments but demand rigorous reserve, redemption, and financial-crime controls

Stablecoins offer significant advantages, including near real-time settlement, continuous (24/7) availability, and programmable transfers. Nevertheless, they present unique challenges such as reserve quality and transparency, redemption under stress, key and credential management, and financial-crime exposure across multiple blockchains. Emerging regimes, such as the GENIUS Act in the United States and MiCA in the European Union, are beginning to codify reserve and redemption requirements. Issuers need to demonstrate verifiable reserve backing and enforce controls directly at the token, policy, or signing layer.

Tokenized deposits preserve the protections of commercial bank money but introduce new operational dependencies

Tokenized deposits can preserve the legal and prudential characteristics of commercial bank deposits where the token continues to evidence a qualifying deposit claim under applicable law. They enable conditional payments, embedded compliance logic, and continuous settlement within existing banking relationships. Nevertheless, the operating model introduces new dependencies, such as synchronization between core ledgers and the blockchain, reliance on custody-technology and key-management vendors, and interoperability across banks and networks.

Tokenized assets and tokenized money are converging into a single settlement ecosystem

The benefits of tokenization compound when the asset leg and the cash leg of a transaction settle on shared rails. Security tokens settling against stablecoins or tokenized deposits enable atomic delivery-versus-payment, reducing counterparty risk, reconciliation breaks, and certain settlement-risk-related collateral and exposure requirements. These applications also share common dependencies, including Layer 1 and Layer 2 infrastructure, custody technology, oracles and data providers, and cross-chain bridges. Financial institutions should therefore manage tokenized assets and tokenized money within a single risk framework, applying consistent custody, key management, and monitoring standards across both.

Harmonized standards and sustained public-private collaboration are needed to move from pilots to scale

Jurisdictional treatment of tokenized assets and tokenized money remains fragmented, with deposit definitions, stablecoin regimes, and settlement-finality rules differing across markets. Regulators need to advance harmonized, technology-neutral standards that recognize blockchain records as authoritative books and records where appropriate. Market participants need to converge on common taxonomies, interoperability standards, and control expectations to enable integration into existing risk management frameworks. Continuous public-private collaboration remains essential to keep the framework current as the technology and its regulation evolve.

© GBBC Global Blockchain Business Council © Oliver Wyman

1. Stablecoins

Stablecoins are digital assets designed to maintain a stable value relative to a reference asset, typically a monetary unit such as the USD or Euro. They are issued or represented as transferable tokens on blockchain infrastructure and can be used across wallets, applications, exchanges, payment processors, merchants, and other market participants.

Two reserve-backed stablecoin archetypes are in scope: privately issued stablecoins and government-sector stablecoins. Privately issued stablecoins are money-like digital tokens that aim to maintain a stable value relative to a peg specified by one or more reference assets and are designed to minimize fluctuations relative to those assets[1]. They are not issued by a central bank and must be at least fully backed by one or more assets specified under the applicable regulatory framework (e.g., cash, treasury bills, or equivalent short-term sovereign debt)[2]. Government-sector stablecoins, such as the State of Wyoming's Frontier Stable Token, are similar instruments issued by a government or public-sector entity, intended to maintain a stable value relative to a reference asset, and supported by eligible assets under the applicable framework[3]. These taxonomy-based archetypes do not replace jurisdiction-specific legal classifications, which may impose different requirements relating to issuers, reserve composition and liquidity, redemption, disclosure, and conduct. Algorithmic stablecoins are not in scope for this analysis as they seek to maintain price stability primarily through protocol incentives or supply mechanisms rather than full reserve backing and are more commonly associated with DeFi use cases.

Key features of stablecoin market structures include:

- Reserve-backed: Issued tokens are supported by eligible reserve assets under the applicable framework. Reserve composition, custody, disclosure, and redemption arrangements vary by issuer and jurisdiction.
- Bearer-like instruments: Depending on the custody and control model, transfers may be authorized through private keys, distributed key shares, or hosted-account credentials, each with distinct risks. Institutional arrangements may enforce policy and transfer controls at the wallet, signer, or token layer.
- Continuous availability: Stablecoin networks may accept transfer instructions continuously, while operational support, liquidity access, and connected fiat systems may remain subject to service windows.
- Near real-time settlement: On-chain transfers may achieve finality near real time and support delivery-versus-payment or payment-versus-payment, reducing principal and settlement-leg risk. Finality timing and fiat conversion remain design- and system-dependent.
- Composability: Stablecoins can integrate with wallets, exchanges, merchant platforms, tokenized securities, and treasury workflows.
- Programmable transfers: Wallet eligibility (e.g., based on KYC/KYB), sanctions controls, transfer limits, approval rules, and freeze functions can be enforced at the token, signing, or application layer.
- Direct value transfer: Wallet-to-wallet transfers can reduce reliance on intermediaries for certain messaging and settlement functions, while acceptance, compliance, fiat conversion, and recourse may still rely on service providers.

1 CFTC GMAC Digital Asset Markets Subcommittee Recommendation – Digital Asset Taxonomy
2 Definitions follow the CFTC GMAC Digital Asset Markets Subcommittee taxonomy. Applicable frameworks include the U.S. GENIUS Act (permitted payment stablecoin issuers, with reserve and redemption requirements) and the EU's MiCA (e-money tokens).
3 Excludes CBDCs as they are direct liabilities of central banks and constitute a digital form of central bank money, rather than reserve-backed tokens designed to maintain a stable value relative to a reference asset.

© GBBC Global Blockchain Business Council © Oliver Wyman

Stablecoins face several challenges that may constrain broader adoption. Trust depends on robust reserve and redemption arrangements, supported by high-quality, segregated, and liquid reserve assets, transparent disclosures, and enforceable redemption rights. Issuers also generally rely on banks and other intermediaries for access to traditional payment, clearing, and settlement systems. Blockchain-based transfers raise specific considerations relating to financial crime and sanctions compliance, fraud prevention, key management, smart-contract administration, operational resilience, and user recourse. Differences in regulatory treatment across jurisdictions, together with the cross-border use of stablecoins, can further complicate supervision, disclosure, redemption, and settlement.

1.1. Value chain

Stablecoins can impact multiple stages of the payments value chain, including issuance, reserve management, distribution, custody, transfer, acceptance, fiat conversion, and record-keeping. Blockchain-based infrastructure may streamline selected payment and settlement functions while redistributing operational, financial, compliance, and legal responsibilities. Shared records and atomic settlement can reduce selected intermediary credit exposures, reconciliation breaks, settlement-reversal exposure, and principal risk; these benefits depend on design and do not remove off-chain dependencies. Understanding where responsibilities sit is important for identifying risks and designing appropriate control frameworks. The following table highlights key differences between traditional payment and blockchain stablecoin infrastructures:

Table 1: Comparison of traditional payment and blockchain stablecoin models across the value chain

Feature	Bank account / bank payment model	Blockchain stablecoin
Funding and issuance	Customers place funds with a bank upon completion of KYC, creating a deposit claim on the institution.	Tokens are minted against received funds or eligible reserve assets, subject to issuer governance, reserve management, and compliance controls.
Reserve and balance sheet management	Deposits are recorded on the bank balance sheet, subject to capital, liquidity, depositor-protection, and resolution frameworks.	Under applicable reserve-backed frameworks, outstanding tokens are backed by eligible reserve assets, with requirements for segregation, reconciliation, liquidity, and disclosure.
Access	Customers generally open a bank account and access payment services through that account.	Users access stablecoins through self-hosted or hosted wallets, exchanges, or payment apps, typically by exchanging fiat or other digital assets. In some models, the governed wallet serves as the primary control point for permissions, records, and audit.
Payments	Banks support cards, wires, automated clearing-house or equivalent account-to-account transfers, instant payments, and related fintech services.	Stablecoins move wallet-to-wallet, directly or through exchanges and payment service providers; acceptance remains use-case and market dependent.
Redemption	Bank account balances can generally be withdrawn or transferred on demand, subject to account terms, operating windows, and applicable fees.	Stablecoins may be sold on secondary markets or redeemed directly by eligible holders; eligibility, fees, and timing vary by issuer, law, and stress conditions.
Settlement	Payments settle on bank and central bank rails, often on a net basis across multiple ledgers.	Transfers may settle on-chain or within custodial or off-chain environments, including atomic delivery-versus-payment or payment-versus-payment where supported; fiat conversion still relies on banks and service providers.

© GBBC Global Blockchain Business Council © Oliver Wyman

Feature	Bank account / bank payment model	Blockchain stablecoin
Record-keeping	Multiple ledgers are updated and reconciled across banks, payment networks, and processors.	Blockchain provides a shared transaction ledger; customer, legal-ownership, reserve, and other off-chain records still require control and, where applicable, reconciliation.
Recourse and consumer protection	Chargebacks, reversals, dispute rights, and other customer protections are established through law, account terms, and payment-network rules, but can create fraud and settlement-reversal exposure.	Network settlement is generally irreversible, reducing settlement-reversal risk; recourse may be provided through issuer, token, wallet, application, or legal controls, including governed freezes, reissuance, or clawback where available.
Resolution and wind-down	Bank failure is handled through resolution and depositor-protection frameworks.	Stablecoin arrangements require legally effective reserve segregation, redemption priority, and wind-down procedures; legal treatment and operational workability in insolvency remain uncertain in many jurisdictions.

Exhibit 1: Illustrative stablecoin payment-token value chain

Step 1	Step 2	Step 3	Step 4	Step 5
Issuance and reserve management	Distribution, custody, and wallets	Transfer, settlement, and network operation	Merchant / processor acceptance	Fiat or digital asset conversion

These systems can consolidate traditionally separate messaging and settlement functions but introduce certain dependencies on smart contracts, wallet and signing infrastructure, blockchain networks, reserve-service providers, analytics and oracle services, and on/off-ramps. Effective risk management therefore depends on clearly defined governance, controls, and accountability across issuance, custody, transfer, acceptance, fiat conversion, and settlement.

© GBBC Global Blockchain Business Council © Oliver Wyman

1.2. Stakeholders across the value chain and risk mitigation strategies

Traditional payments rely on regulated banks and other account providers, payment networks, specialized intermediaries, internal controls, and legal frameworks governing settlement, recourse, and customer protection. Stablecoin arrangements can enable more direct and continuous movement of value while redistributing responsibilities across issuers, reserve providers, wallet and signing providers, exchanges, processors, merchants, and blockchain infrastructure. Accordingly, controls need to extend to token issuance, reserve management, redemption, wallet access, transaction signing, transaction monitoring, settlement, and conversion. The exact allocation depends on the operating model, but key participant groups include:

- **Stablecoin issuers and their program managers:** Own token design, issuance, redemption, disclosures, reserve policy, smart-contract administration, compliance, and lifecycle governance. They should ensure minting and burning remain authorized and reserve-backed; govern upgrades, permissions, freezes, reissuance, and wind-down; and distinguish KYC and customer due diligence at minting or redemption from ongoing ecosystem monitoring after tokens circulate. Intervention powers should be clearly disclosed, lawfully governed, and tested, including their practical limits once assets have been converted or moved.
- **Reserve custodians, trustees, and treasury service providers**: Hold or manage reserve assets and provide safeguarding, liquidity, settlement, reporting, and attestation. Key controls cover asset eligibility, segregation, legal ownership, bankruptcy remoteness where applicable, concentration, liquidity, redemption funding, reconciliation, and stressed operational continuity.
- **Exchanges and fintechs serving as on/off-ramps:** Provide access and fiat or crypto conversion, often as the primary customer interface. Responsibilities may include onboarding, KYC and AML controls, sanctions screening, transaction monitoring, redemption access, fraud controls, and customer support.
- **Wallet, custody, and transaction-signing providers:** Provide wallet access, asset safeguarding, transaction authorization, recovery, and policy enforcement. These functions may be performed by one provider or distributed across custodians, wallet platforms, and key-management or signing vendors; responsibilities should follow who controls keys, key shares, credentials, or approval policies and apply only where the provider exercises the relevant custody, authorization, policy, or market-access function. Controls should cover HSM, MPC, least privilege, backup and recovery, incident response, cryptographic agility, and tested migration to approved quantum-resistant schemes.
- **Payment processors, acquirers, and merchant service providers:** Enable acceptance, checkout, settlement into fiat or stablecoin balances, refunds, disputes, and reporting. They must manage wallet addresses, exchange-rate presentation, settlement rules, tax and accounting data, outages, and customer recourse where on-chain settlement may be irreversible.
- **Merchants:** Use stablecoins for acceptance, treasury, counterparty payments, or tokenized-asset settlement. For balances and wallets they control, key responsibilities include signer governance, reconciliation, refunds, sanctions controls, off-ramp selection, and treasury limits.
- **Analytics, identity, and compliance providers:** Support wallet screening, sanctions controls, fraud models, AML monitoring, and investigations. Data quality, source redundancy, availability, explainability, and fallback arrangements are material because failures can directly affect execution and compliance decisions.
- **Public blockchain ecosystems and infrastructure providers:** Provide network settlement, node and remote procedure call (RPC) or application programming interface (API) access, block explorers, indexing, bridges, cross-chain messaging, and monitoring. Their governance, code quality, validator distribution, finality, and incident response affect resilience; concentration among shared providers can create single points of failure even when the underlying network remains available.

© GBBC Global Blockchain Business Council © Oliver Wyman

- **Institutional end users (e.g., financial institutions and corporates):** Use stablecoins for treasury, payments, settlement, or tokenized-asset activity. Depending on the custody and access model, responsibilities may include wallet and signer governance, transaction verification, fraud controls, address accuracy, recovery procedures, and understanding applicable recourse and protections.

1.3. Key risks and mitigation strategies

Risks in stablecoin payments arise across issuance, transfer, custody, conversion, and settlement, with mitigation responsibilities distributed across the payment value chain. Many of these risks also exist in traditional payment systems, where controls have historically been embedded within regulated institutions, established payment networks, and defined legal frameworks. Stablecoin arrangements may allocate these functions and responsibilities differently. The following mitigation strategies focus on four participant groups with the clearest control accountabilities:

Table 2: Stablecoin key risks and mitigation strategies by participant group

	Mitigation strategies			
Risk	**Issuers**	**Reserve custodians / treasury providers**	**Wallet, custody, signing, and market-access providers**	**Payment processors and merchants**
Reserve shortfall / asset-quality failure: outstanding tokens are not fully or safely backed	Set eligible-asset and concentration policies; segregate reserves; gate minting on verified funding and approvals; reconcile supply to reserves; publish independent attestations and, where feasible, higher-frequency verifiable reserve reporting.	Safeguard reserves; monitor eligibility, concentration, liquidity, maturity, and credit exposure; provide independent reporting and real-time exception escalation.	Apply acceptance, listing and delisting criteria based on reserve transparency, liquidity, and redemption arrangements; set exposure limits and triggers.	Define accepted tokens and treasury limits; monitor reserve disclosures; convert or diversify balances when risk exceeds appetite.
Redemption and intraday liquidity stress: holders cannot redeem at par or participants lack funds for continuous gross settlement	Maintain clear redemption terms, liquidity buffers, stress playbooks, and automated treasury rebalancing; use netting or payment-versus-payment orchestration where appropriate; communicate status promptly.	Pre-position liquidity; test high-volume and off-hours redemptions; support cash movement within applicable operating windows.	Disclose eligibility, channels, fees, and timing; route users to approved off-ramps; apply documented throttles only when needed.	Avoid dependence on one off-ramp; set treasury buffers and contingency conversion and refund plans.
Peg instability / fragmented price discovery: stablecoin trades away from its reference value	Disclose the peg mechanism and reserve composition; monitor secondary markets; coordinate liquidity support within defined governance during stress.	Provide liquidity and settlement support within risk limits; escalate reserve or cash-settlement constraints.	Monitor venue-level prices and spreads; monitor contract events; provide freeze capabilities; apply margin, exposure, or suspension triggers.	Quote prices transparently; do not present secondary-market value as guaranteed par; apply defined conversion rules.

	Mitigation strategies			
Risk	**Issuers**	**Reserve custodians / treasury providers**	**Wallet, custody, signing, and market-access providers**	**Payment processors and merchants**
Unauthorized token administration: unauthorized mint, burn, freeze, transfer, upgrade, or administrative action	Use audited contracts; enforce role segregation, multiparty approvals, timelocks, and least privilege; govern upgrades and emergency actions; maintain freeze, reissuance, burn, and remediation procedures.	Release reserves only against validated, authorized mint, burn, or redemption events; block exceptions.	Monitor contract events and provenance; provide quarantine or freeze capability under issuer or regulated-entity instruction; preserve evidence.	Use approved contracts, wallets, and processors; notify providers of anomalies; retain records for claims and investigations.
Key management and account access: private keys, key shares, or hosted credentials are lost or compromised, or underlying signing schemes become vulnerable.	Prevent unilateral movement and policy bypass at signing; use HSM, MPC, multisig, least privilege, rotation, and tested recovery; inventory cryptographic dependencies; maintain re-keying and post-quantum migration plans.	Require dual authorization and policy-bound signing for reserve movements; segregate roles; use crypto-agile systems.	Enforce policy at signing; apply MFA, transaction limits, and anomaly detection; define liability across custody models; minimize public-key exposure; support cryptographic upgrades and post-quantum migration.	Set signer quorums and approval thresholds; secure devices and backups; test recovery.
Recourse and dispute gaps: limited recourse for irreversible transfers	Define and disclose freeze, reissuance, clawback, mistaken-transfer, and dispute rules; govern interventions lawfully and communicate limits.	Support freezes or reserve actions only under valid legal instructions and defined procedures.	Provide fraud reporting, evidence preservation, and issuer-directed intervention capabilities; allocate liability clearly.	Design refund and dispute processes; disclose acceptance terms; train staff and customers on address verification methodology and scams.
Compliance, KYC/AML, and sanctions control failure: prohibited activity enters stablecoin flows	Perform KYC and customer due diligence for minting and redemption customers; screen transactions and counterparties; continuously monitor circulation and cross-chain exposure; reject or freeze prohibited activity under lawful procedures; escalate and report.	Screen reserve counterparties and cash movements; monitor unusual funding and redemption patterns; act only under lawful instructions.	Perform KYC or KYB where required, wallet screening, transaction monitoring, and sanctions controls; enforce allowlists or pre-settlement checks where appropriate; quarantine and report suspicious activity.	Use approved wallets, routes, and processors; screen merchants and counterparties as required; reject prohibited payments; retain records.
Cross-chain and representation failure: native, bridged, or wrapped stablecoins are misidentified, duplicated, or disrupted across networks	Define canonical and issuer-supported representations by network; reconcile authorized supply across chains; govern burn-and-mint and bridge mechanisms; monitor route and bridge exposure.	Reconcile aggregate reserves to authorized supply across all networks; release assets only against validated burns or redemptions.	Support only approved contracts and routes; label native and bridged assets; monitor bridges; set exposure limits; suspend compromised pathways.	Accept only approved contracts and routes; verify token provenance; set route limits and contingency conversion procedures.

	Mitigation strategies			
Risk	**Issuers**	**Reserve custodians / treasury providers**	**Wallet, custody, signing, and market-access providers**	**Payment processors and merchants**
Continuous-operations failure: around-the-clock activity outpaces business-hours staffing for signing, monitoring, and response	Automate signing under enforced policy; staff 24/7 escalation; monitor network health.	Provide after-hours liquidity and settlement escalation within agreed limits.	Run continuous monitoring with on-call response; automate suspensions under documented triggers.	Define after-hours authorization backups and incident procedures.
Third-party and infrastructure dependency: provider outages or concentration disrupt processing even while the chain itself is available	Perform vendor due diligence; require uptime and exit terms; keep redundant RPC/data providers and fallback screening.	Assess provider concentration; contract contingency providers for critical services.	Aggregate multi-source data with deviation thresholds and circuit breakers; define degraded-mode procedures.	Avoid single-provider or single off-ramp dependence; document manual fallbacks.
Privacy and confidentiality leakage: public transaction data exposes counterparty, payroll, or supplier information	Minimize on-chain personal data; apply privacy-by-design and retention controls.	Keep confidential reserve and settlement details of public infrastructure.	Apply address management, metadata controls, and privacy-preserving compliance tooling.	Separate operational wallets; avoid embedding sensitive invoice or payroll data; choose configurations with adequate privacy controls.

2. Tokenized deposits

Tokenization of deposits involves representing bank-deposit claims using a blockchain solution and tokens as the carrier of deposit and payment information. These digital tokens incorporate the economic and legal characteristics of commercial bank money while largely preserving the regulatory controls that apply to bank deposits.

There are broadly two concepts relevant to deposit tokenization: tokenized deposits and deposit tokens. Tokenized deposits are digital tokens that represent an existing record of a traditional ownership claim for a bank deposit on the token-issuing bank or depository institution, for a fixed amount of commercial bank money denominated in a single currency4. They are typically recorded in a controlled ledger environment, such as a private blockchain and/or permissioned network, or approved wallets on public blockchain and public permissioned infrastructure. Existing market examples include single-bank institutional settlement tokens, bank token services, and multi-bank deposit networks. Relative to stablecoins, tokenized deposits generally have narrower transferability because they remain anchored to the issuing bank's account, customer, and compliance perimeter. Deposit tokens are transferable digital tokens issued by a licensed depository institution which evidence a deposit claim against the token-issuing bank or depository institution, for a fixed amount of commercial bank money or fiat cash denominated in a single currency5. The legal, regulatory, accounting, and operational treatment of deposit tokens remains an evolving area in many jurisdictions. This section therefore focuses on tokenized deposits.

Deposit insurance treatment depends on the underlying liability and applicable jurisdictional requirements. In the United States, proposed FDIC rules would clarify that deposit insurance treatment is technology-neutral: tokenized deposits that meet the statutory definition of a deposit would be treated like other bank deposits, regardless of the technology or record-keeping used to record the liability. Coverage would remain subject to ordinary deposit insurance rules, including ownership, account structure, coverage limits, and record-keeping requirements.[6] Outside of the United States, treatment depends on local definitions of deposits, depositor-protection schemes, and record-keeping requirements, which may complicate multi-bank or cross-border models. For example, in Europe, deposit definitions vary by member state and tokenized-deposit treatment remains under development.

Key features of tokenized deposits include:

- **Bank-issued claim:** The relevant liability is on the issuing bank or depository institution, without reference to a specific pool of reserve assets. Stability depends on prudential supervision, capital and liquidity requirements, risk management, central-bank liquidity facilities, depositor-protection schemes, and bank-resolution regimes where applicable.
- **Integration with core banking:** Tokenized balances must remain aligned with the bank's authoritative books and records, customer and ownership records, compliance controls, depositor-protection requirements, and prudential reporting.
- **Programmable bank money:** Transfers can embed policy logic, pre-settlement controls, conditional settlement, and integration with tokenized-asset delivery-versus-payment or payment-versus-payment flows.
- **Controlled participation:** KYC, wallet eligibility, account permissions, and transaction limits can be anchored in bank onboarding and account controls.

[4] GMAC Digital Asset Markets Subcommittee Recommendation – Digital Asset Taxonomy

5 GMAC Digital Asset Markets Subcommittee Recommendation – Digital Asset Taxonomy

6 GENIUS Act Requirements and Standards for FDIC-Supervised Permitted Payment Stablecoin Issuers and Insured Depository Institutions

- **Multi-bank interoperability and settlement challenges:** Transfers across banks require common data, compliance, legal, and operating standards, together with arrangements that preserve finality and the singleness of money (i.e., commercial bank money remains exchangeable at par across issuing banks). A common policy layer can normalize controls across supported networks, while settlement may use central-bank money, commercial-bank money, private clearing, or synchronized ledger movements.

Adoption of tokenized deposits will depend on resolving legal, regulatory, accounting, operational, and interoperability challenges across jurisdictions. Continuous token activity may strain processes, controls, liquidity management, and third-party dependencies that remain aligned to traditional banking schedules. Early use of on-chain monitoring and risk intelligence, even in closed-loop models, can build readiness for multi-bank and public-network interoperability.

2.1. Value chain

Tokenized deposits can alter stages of the bank-deposit and account-based payment value chain, from account opening and deposit origination through token issuance, wallet access, transfer, settlement, record-keeping, and conversion into conventional deposit balances. Depending on design, blockchain may serve as a synchronized sub-ledger, transaction layer, or authoritative books and records; in all cases, tokenized deposits remain bank liabilities subject to account, compliance, prudential, and resolution requirements. The following table compares traditional and tokenized-deposit models:

Table 3: Comparison of traditional deposit and tokenized deposit models across the value chain

Feature	Bank account / bank payment model	Blockchain tokenized deposit
Funding and issuance	Customers place funds with a bank upon completion of KYC, creating a deposit claim on the institution.	On-chain tokens record a fixed commercial-bank deposit claim; issuance may be customer-initiated or embedded in a payment workflow. Depending on design, the blockchain may serve as the bank's authoritative books and records, a synchronized sub-ledger, or a messaging layer.
Reserve and balance sheet management	Deposits are recorded on the bank balance sheet, subject to capital, liquidity, depositor-protection, and resolution frameworks.	Deposits remain bank liabilities on the balance sheet and remain subject to the same prudential and depositor-protection frameworks.
Access	Customers generally open a bank account and access payment services through that account.	Requires an existing or linked bank account and approved participant or wallet access; tokenization may be explicit or embedded in payment workflows.
Payments	Banks support cards, wires, automated clearing-house or equivalent account-to-account transfers, instant payments, and related fintech services.	Tokenized deposits may support wallet, account-to-account, or card-linked payment flows; on-chain transfers may execute near real time, while cross-bank reach depends on interoperability.
Redemption	Bank account balances can generally be withdrawn or transferred on demand, subject to account terms, operating windows, and applicable fees.	Holders may burn or convert tokenized balances into conventional deposits for withdrawal or transfer through traditional bank rails.
Settlement	Payments settle on bank and central bank rails, often on a net basis across multiple ledgers.	Transfers within a single bank settle on the issuing bank's books; multi-bank transfers require common rules and settlement in central-bank or agreed commercial-bank money.

Feature	Bank account / bank payment model	Blockchain tokenized deposit
Record-keeping	Multiple ledgers are updated and reconciled across banks, payment networks, and processors.	Today, many models use blockchain as a sub-ledger or synchronization layer; some use it as authoritative books and records, with core systems supporting reporting and controls.
Recourse and consumer protection	Chargebacks, reversals, dispute rights, and other customer protections are established through law, account terms, and payment-network rules, but can create fraud and settlement-reversal exposure.	Bank and payment-network rules continue to govern corrections, disputes, and reversals, subject to token-level design controls.
Resolution and wind-down	Bank failure is handled through resolution and depositor-protection frameworks.	Blockchain records should support resolution and depositor-protection processes; legal status and claims depend on applicable law, account ownership, and record integrity.

Exhibit 2: Illustrative tokenized deposit payment-token value chain

Step 1	Step 2	Step 3	Step 4	Step 5
Account opening and deposit origination	Token issuance and wallet access	Transfer, settlement, and network operation	Books-and-records synchronization	Conversion and redemption

Tokenized deposits can simplify selected payment, reconciliation, and settlement processes but create dependencies across blockchain infrastructure, wallet and signing controls, bank books and records, liquidity arrangements, and settlement venues. Effective risk management therefore depends on clearly defined governance, controls, decision rights, and accountability across issuing banks, vendors, wallet and signing providers, settlement venues, and other participants involved in issuance, access, transfer, settlement, record-keeping, and conversion.

© GBBC Global Blockchain Business Council © Oliver Wyman

2.2. Stakeholders across the value chain and risk mitigation strategies

Deposit and account-based payments rely on regulated banks, payment networks, clearing and settlement infrastructure, correspondent arrangements, core banking systems, and internal controls. Many supporting systems remain subject to operating windows, cut-off times, and business-day processes. Tokenized deposits can enable more continuous movement of bank-deposit value, requiring bank-grade controls to extend to token issuance, wallet and signing access, books-and-records integrity, settlement, and conversion. The exact allocation depends on the operating model, but key participant groups include:

- **Issuing banks and tokenized-deposit program owners:** Own onboarding, account terms, token issuance, books and records, compliance, and conversion. They must keep tokens aligned to authorized deposit balances and ownership records while preserving legal characterization, disclosures, depositor-protection treatment, and risk-appetite controls.
- **Correspondent and settlement banks:** Support cross-bank and cross-border settlement, liquidity movement, and interoperability. Prefunding may be used but is not inherent; requirements depend on settlement design, the settlement asset, and access to intraday liquidity or credit. Familiar risks around finality, liquidity, and concentration may arise faster and require more continuous monitoring.
- **Core banking vendors and ledger-reconciliation providers:** Support systems of record, posting, balance controls, synchronization, exceptions, reporting, and data feeds. They must maintain a consistent source of truth between on-chain records and the bank's official books, including models where the blockchain is authoritative.
- **Client interfaces and P2P applications:** Provide balance display, notifications, transaction initiation, device management, and recovery workflows. Where they do not control custody, authorization, or policy enforcement, responsibilities are limited to secure interface design, authentication, disclosures, and fraud prevention.
- **Payment network operators, settlement venues, and tokenized-deposit networks:** Provide routing, network rules, transfer standards, eligibility controls, interbank settlement models, and operating procedures. They define how tokenized deposits move across participants and how finality, corrections, disputes, outages, and network changes are handled.
- **Wallet, client-interface, and transaction-signing providers:** Provide access to tokenized-deposit balances, transaction authorization, balance display, recovery, and policy enforcement. The issuing bank remains responsible for the deposit liability and customer relationship, while providers operate under bank-approved policies and clearly allocated contractual responsibilities. Controls should cover HSM, MPC, least privilege, backup and recovery, incident response, cryptographic agility, and tested migration to approved quantum-resistant schemes.
- **Analytics, identity, and compliance providers:** Support wallet screening, sanctions controls, fraud models, transaction monitoring, and investigations. Banks remain accountable for outcomes, making coverage, explainability, resilience, and readiness for future interoperability critical.
- **Institutional end users (e.g., corporates and merchants):** Use tokenized deposits for payments, treasury, settlement, or tokenized-asset activity. Depending on the access and signing model, they need to understand legal claims, depositor-protection treatment, wallet responsibilities, refund procedures, finality, and controls over authorized users.

© GBBC Global Blockchain Business Council © Oliver Wyman

2.3. Key risks and mitigation strategies

Risks in tokenized deposits arise across issuance, wallet and signing access, transfer, settlement, record-keeping, conversion, and resolution, with mitigation responsibilities distributed across the deposit and payment value chain. Many of these risks also exist in traditional deposit and account-based payment systems, where controls have historically been embedded within regulated banks, payment networks, core banking systems, and established legal frameworks. Tokenized-deposit arrangements preserve much of this control perimeter but extend it to blockchain infrastructure, token administration, books-and-records synchronization, and continuous operations. The following mitigation strategies focus on four participant groups and their respective roles and control responsibilities:

Table 4: Tokenized-deposit key risks and mitigation strategies by participant group

	Mitigation strategies			
Risk	**Issuing banks**	**Correspondent / settlement banks**	**Wallet, signing, and application providers**	**Merchants and corporates**
Legal status ambiguity: token rights, deposit claims, account ownership, or insolvency treatment are unclear	Define the legal basis, account terms, ownership records, holder rights, deposit status, and depositor-protection treatment; obtain legal and regulatory review.	Define network rules, participant obligations, governing law, settlement finality, and dispute handling; align interbank contracts with tokenized-deposit flows.	Display issuer, claim, and legal status clearly; avoid implying protection, recourse, or transferability.	Review issuer, claim structure, terms, and recourse; reject unsupported tokenized-deposit representations or wrappers.
Mint/burn and books-and-records mismatch: tokenized supply diverges from the bank's authoritative deposit records	Restrict minting to verified balances; define the authoritative system of record; reconcile supply, burns, wallets, and postings near real time; escalate exceptions.	Set settlement windows and cut-offs that support synchronization; coordinate exception procedures across banks.	Provide reliable data feeds, event logs, and exception tooling; prevent stale balances; support correction workflows where legally available.	Reconcile receipts and payments; report discrepancies promptly; retain transaction identifiers.
Duplicate claims, over-issuance, and unauthorized transfer: balances are created or moved without valid backing or authority	Use audited contracts, supply caps, role segregation, multiparty approvals, and real-time anomaly detection; approve freeze or blocking decisions and maintain remediation processes.	Validate settlement before interbank release; monitor participant limits and prefunding arrangements.	Provide secure signing, event monitoring, and configurable controls; enforce bank-approved policies and quarantine or block only under authorized instruction.	Use bank-approved wallets, applications, and channels; apply internal approvals; notify the bank of unauthorized activity.
Financial crime and sanctions exposure: tokenized deposits are used for prohibited activity	Apply KYC and customer due diligence, transaction monitoring, sanctions, fraud, and regulatory reporting across issuance, transfers, and conversion; extend analytics to boundary and interoperability activity.	Set network eligibility and screening expectations; support information sharing and escalation across participating banks.	Provide wallet and counterparty screening, on-chain and off-chain monitoring, and configurable controls; block or freeze only under bank-approved policy or instruction.	Use approved counterparties, wallets, and channels; retain records for investigations and reporting.

© GBBC Global Blockchain Business Council © Oliver Wyman

	Mitigation strategies			
Privacy and confidentiality leakage: transaction data exposes personal, commercial, liquidity, or relationship information	Minimize on-chain sensitive data; use privacy-by-design and appropriate privacy-enabled or permissioned configurations; define retention, access, and disclosure controls.	Avoid placing confidential settlement or customer data on public infrastructure; preserve auditability without unnecessary disclosure.	Apply address and metadata controls, access permissions, and privacy-preserving compliance tools; support approved privacy configurations.	Separate operational wallets; avoid embedding invoice, payroll, or supplier data; use approved networks and configurations.
Key management and wallet access failure: customer, bank, or administrative keys are lost or compromised, or underlying signing schemes become vulnerable	Prevent unilateral movement and policy bypass at signing; use HSM, MPC, multisig, least privilege, rotation, recovery, and dual controls; inventory cryptographic dependencies; maintain re-keying and post-quantum migration plans.	Set participant key standards and policy-bound authorization; require incident notification; coordinate response, re-keying, and migration across banks.	Enforce bank-approved policy at signing; apply institutional key controls, device security, recovery workflows, limits, and anomaly monitoring; minimize public-key exposure; support cryptographic upgrades and post-quantum migration.	Maintain secure wallets, backups, signer governance, and approval thresholds; train operators.
Interoperability failure: tokenized deposits cannot move or settle consistently across banks, networks, or representations	Adopt common token, data, and legal standards; define canonical representations; normalize controls across supported networks through a common policy layer; limit support based on risk.	Use common settlement and messaging standards; monitor route and shared-provider dependencies; define how interbank exposures settle in central-bank or other agreed money.	Support approved standards and policy abstraction; reconcile across systems and routes; manage upgrades and compatibility.	Use approved routes and token contracts; monitor settlement confirmations; reject unsupported representations.
Conversion, redemption, and dispute failure: holders cannot convert balances or resolve exceptions	Define conversion, correction, complaint, and dispute procedures; support burns and conversion to conventional deposits under clear rules.	Coordinate interbank dispute and settlement-correction procedures; define finality and exception handling.	Provide clear workflows, preserve evidence, and maintain escalation channels; execute corrections under bank instruction.	Understand finality and recourse; retain transaction records; initiate claims or disputes promptly.
Critical vendor and infrastructure dependency: failure of shared core, wallet, network-access, identity, or analytics services disrupts operations	Map dependencies by criticality; set resilience, audit, and service expectations where feasible; diversify providers; test exit, replacement, and fallback plans.	Identify shared infrastructure across participating banks; set contingency arrangements and test alternate settlement or communication paths; conduct resiliency testing.	Disclose material dependencies; provide service-health telemetry; support independent failover, recovery, and portable records or configurations.	Maintain alternative bank channels and operating procedures; test degraded-mode reconciliation, approvals, and customer communication.

3. Consortium-based payments models

Consortium-based models are emerging across both stablecoins and tokenized deposits, bringing multiple institutions together to sponsor, govern, distribute, or operate a common token or network. By pooling investment and aligning participants around common rules, technical standards, and shared infrastructure, consortia can reduce duplicative development, improve interoperability, broaden distribution, drive harmonized operating practices across participating institutions, and accelerate adoption.

These benefits depend on a clear and durable operating model. Where functions are distributed across consortium members and shared service providers, effective arrangements require defined decision rights, control ownership, accountability, and escalation across normal operations, technology changes, incidents, member entry and exit, and wind-down. Key risk-management considerations include:

1. Governance and decision rights: Define voting rights, reserved matters, approval thresholds, conflicts-management procedures, change governance, emergency powers, escalation paths, and deadlock resolution.
2. Legal structure and regulatory perimeter: Establish an appropriate legal entity or contractual framework; identify the regulated issuer or issuing banks; define governing law, liability, enforceability, and ownership of shared assets, data, and intellectual property.
3. Accountability and control ownership: Allocate responsibility for issuance, reserve or balance-sheet management, compliance, technology, signing, customer protection, incident response, reporting, and regulatory engagement. Define who may authorize minting, burning, or changes to supply; apply role segregation, multiparty approvals, issuance limits, and reconciliation to verified reserves or authorized deposit balances and books and records, as applicable.
4. Participation and operating standards: Set requirements for member admission, due diligence, technical and compliance standards, data sharing, service levels, suspension, and exit. Define arrangements for member default, insolvency, or operational failure, including suspension of access or issuance, continuity of critical services, treatment of outstanding obligations, transfer of responsibilities, and orderly replacement or exit.
5. Settlement architecture and external interoperability: Define the settlement asset, timing, finality, and liquidity model for transfers between members, including prefunding, netting, and member-default arrangements; establish technical, legal, and operational standards for connectivity to external payment systems, token networks, and fiat rails.
6. Operational resilience and wind-down: Assess concentration in shared infrastructure and service providers; define liquidity and settlement arrangements, business-continuity procedures, portability of records and credentials, recovery from member or service-provider failure, and orderly migration or wind-down plans.

Consortium governance should complement, rather than dilute, each participant's legal, regulatory, and risk-management responsibilities. Members should therefore align consortium rules with their own risk appetite, control frameworks, and obligations in each jurisdiction in which the arrangement operates.

© GBBC Global Blockchain Business Council © Oliver Wyman

4. Path forward

The public consultation period for this chapter of RMF remains open until February 26, 2027. Please submit any comments to RMF@gbbc.io.

RMF in the Real World

The RMF aims to provide a foundational step towards enabling the safe adoption of public blockchains within regulated financial services, providing supervisors and regulatory bodies with an overview of how the industry has adopted active risk management practices for blockchain infrastructures and the applications built on them.

2026 Use Cases to be released in Q4 2026

To further develop the RMF, a dedicated community initiative is planned to expand and analyze real-world examples, case studies, and best practices related to blockchain risk management. Central to these efforts is an ongoing commitment to foster continuous public-private sector collaboration, integrating market feedback to ensure that the RMF remains up to date.

Looking ahead, future phases of the RMF may extend this application-specific framework to additional forms of tokenized money and digital assets, including CBDCs, tokenized MMFs, native cryptoassets, and decentralized finance (DeFi). Each phase will follow the approach established here, combining consistent value-chain analysis, clear stakeholder accountabilities, and risk mitigations designed for integration into existing frameworks. We will continue to invite market participants, regulators, policymakers, technology providers, and infrastructure operators to provide comments based on their practical experience and insights regarding effective blockchain risk management practices.

If you are a financial institution and would like to apply to join the RMF core working group, please contact RMF@gbbc.io.

© GBBC Global Blockchain Business Council © Oliver Wyman

About Global Blockchain Business Council

Global Blockchain Business Council (GBBC) is the largest leading non-profit association for the blockchain, digital assets, and emerging technologies community. Founded in 2017 in Davos, Switzerland, GBBC comprises more than 500 institutional members and 251 Ambassadors across 119 jurisdictions and disciplines.

GBBC furthers adoption of digital technologies by engaging regulators, business leaders, and global changemakers to harness these transformative tools for more secure and functional societies.

GBBC industry verticals: Financial Services, Global Commerce/Supply Chains, and Commodities, underpinned by AI, digital identity, governance, hardware, infrastructure, policy, regulation, and security.

GBBC initiatives: BITA Standards Council (BITA), GBBC Digital Media, Global Standards Mapping Initiative (GSMI), International Journal of Blockchain Law (IJBL), InterWork Alliance (IWA), and U.S. Blockchain Coalition (USBC).

For more information, visit https://www.gbbc.io/

About Oliver Wyman

Global leader in management consulting. With offices in more than 70 cities across 30 countries, Oliver Wyman combines deep industry knowledge with specialized expertise in strategy, operations, risk management, and organization transformation. The firm has more than 6,000 professionals around the world who work with clients to optimize their business, improve their operations and risk profile, and accelerate their organizational performance to seize the most attractive opportunities.

Oliver Wyman has a dedicated Digital Assets platform that supports industry powerhouses including i) regulators and public policy makers who are setting transformative requirements and norms, ii) traditional finance companies that are pioneering the digital asset landscape with blockchain-driven products and services, iii) trailblazing crypto natives that have established themselves as leaders in crypto and digital assets, and iv) investors. The team's unparalleled industry experiences have also positioned us as thought leaders, evidenced by a series of publications on digital assets including centerpieces in collaboration with leading institutions in the domain.

For more information, visit https://www.oliverwyman.com/our-expertise/hubs/digital assets.html

Copyright ©2026 Oliver Wyman, and GBBC
Oliver Wyman was commissioned by GBBC to curate the RMF. All rights reserved. This publication may not be reproduced or redistributed, in whole or in part, without the written permission of Oliver Wyman, and GBBC. Oliver Wyman, and GBBC accept no liability whatsoever for the actions of third parties in this respect. The information and opinions in this publication were prepared by Oliver Wyman, and GBBC. This publication is not investment advice and should not be relied on for such advice or as a substitute for consultation with professional accountants, tax, legal or financial advisors. Oliver Wyman, and GBBC have made every effort to use reliable, up-to-date and comprehensive information and analysis, but all information is provided without warranty of any kind, express or implied. Oliver Wyman, and GBBC disclaim any responsibility to update the information or conclusions in this publication. Oliver Wyman, and GBBC accept no liability for any loss arising from any action taken or refrained from as a result of information contained in this publication or any publication or sources of information referred to herein, or for any consequential, special or similar damage even if advised of the possibility of such damages. The publication is not an offer to buy or sell securities or a solicitation of an offer to buy or sell securities. This publication may not be sold without the written consent of Oliver Wyman, and GBBC.