GBBC
Global Blockchain
Business Council

OliverWyman

Proposed Risk Mitigation Framework for Non-Financial Risks of Blockchain Infrastructures

Phase 1– July 2025

Core Industry-Leading Working Group Contributors

Ava Labs

Cardano Foundation

Clearstream

Euroclear Group

Global Blockchain Business Council (GBBC)

Hedera Foundation

Ripple

Oliver Wyman

The Depository Trust & Clearing Corporation (DTCC)

Observers

The World Bank

We would like to extend our sincere gratitude to the financial institutions that are not named yet participated in RMF – Phase 1. Your contributions are greatly appreciated.

Contact

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

Frequently Asked Questions (FAQs)

Click here to access.

Contents

Executive Summary

The financial industry and regulators recognize the transformational potential of blockchain technology to reshape legacy operations and business models within the financial services sector. Indeed, over the past decade, leading institutions and central banks across the world have worked on a broad set of experiments and initiatives which have demonstrated the profound benefits blockchain technology can bring to the financial system. The following work focuses on public permissionless and public permissioned blockchain infrastructures ("public blockchains") as their associated risks are not adequately addressed by existing risk management frameworks.

Public blockchains need to be seen within the context of ever-increasing levels of technology-infrastructure externalization by financial institutions—a continuation of a trend that has already given rise to the communication infrastructure of the internet and cloud-based services. At the same time, open-source software development models have gained acceptance and have proven to be not only resilient, but in some cases superior to traditional closed software development models.

Public blockchains represent a natural extension of these broader macro trends. A critical gap impeding the wider adoption of blockchain infrastructure is the absence of recognized risk management frameworks and corresponding regulatory acceptance, particularly by financial institutions. A clear Risk Mitigation Framework (RMF) addressing public blockchains can be established by expanding and adapting existing risk management frameworks designed for externalized infrastructure, such as cloud, and open-source software development. Significant advancements in the resilience and security of public blockchains suggest these infrastructures can now offer reliable solutions suitable for institutional use.

Yet, despite blockchain's maturity, broad institutional adoption of public blockchains still faces challenges. Unlike modern traditional technologies where Service Level Agreements (SLAs) can clarify operational responsibilities and liability, public blockchains typically implement intrinsically more complex operating and governance models. Conversely, the decentralized structure of public blockchains mitigates certain traditional digital infrastructure risks, such as single points of failure or single-operator dependence.

Financial institutions seeking to use public blockchains must adapt their risk frameworks to identify, assess, and mitigate these new risks. Additionally, public blockchain communities should support these efforts to enable adoption at scale. Recognizing these challenges, the RMF proposal presents a structured, actionable approach to integrate the non-financial risks of public blockchains into established risk management standards and tools, such as the Operational Risk Reference Taxonomy introduced by the Operational Riskdata eXchange Association (ORX). The RMF aims to advance public blockchain infrastructure by providing a concise and adaptable standard for integration into existing frameworks, facilitate regulatory endorsement to advance harmonized policy development, and remove institutional obstacles to adoption.

Finally, the last section of this RMF examines the specific risk management challenges of security tokens, one of the most prominent use cases for public blockchains. Security tokens, whether natively issued or structured as token wrappers, have significant potential to streamline complex multi-infrastructure processes and deliver operational efficiencies through instantaneous settlement and fractional ownership. Despite this potential, security tokens on public blockchains face notable adoption hurdles due to the lack of a unified risk syntax.

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.

Five key takeaways

Blockchain introduces specific novel risks requiring targeted risk frameworks

Blockchain technology offers significant advantages—such as decentralized network with built-in redundancies, immutable records, and continuous (24/7) operations—that enhance transparency, operational efficiency, and resilience. However, these same features introduce novel risks that do not fit neatly into traditional risk management frameworks. A clearly defined categorization into three categories where 1) novel risk mitigation strategies need to be defined, 2) risks requiring adaptation to existing standards, and 3) where standard risk mitigation strategies are sufficient is important to enable financial institutions and regulators to prioritize their risk management efforts, while maximizing the benefits that blockchains bring to the financial system.

Public blockchain governance differs fundamentally from traditional operating models

Unlike traditional digital infrastructure services that are centrally governed and where risks are contractually distributed, public blockchains leverage various decentralized governance models and rely significantly on open-source quality assurance mechanisms. Public blockchain ecosystems should endeavor to clearly define such governance structures, including their risks and challenges. Simultaneously, financial institutions must adapt their own internal governance and decision-making processes to their public blockchains of choice, ensuring governance visibility and adequate reaction capability.

Public blockchain adoption demands new resiliency strategies

Financial institutions should consider public blockchain adoption in conjunction with complementary support services (e.g., third-party node operators, failover systems to traditional service providers, etc.) to achieve resilience. Furthermore, financial institutions must move from being passive users of software services to actively participating in public blockchain ecosystems. Institutions can further strengthen public blockchain robustness and resilience by directly or indirectly participating in their operations (e.g., running nodes) and contributing to underlying codebases (e.g., participating in open-source development).

Security tokens present compelling benefits but require new risk management approaches and an adapted market structure

Security tokens provide clear benefits, including enhanced transparency, fractional ownership, potentially improved liquidity, operational efficiencies, and automated compliance. Nevertheless, they present unique challenges such as interoperability, settlement finality, and specialized custody requirements. Effective management of the associated risks demands coordinated efforts from both regulators and market participants. Regulators need to establish clear regulatory standards for a market structure that requires fewer intermediaries. Market participants need to develop and implement robust blockchain-specific risk management frameworks.

A structured approach to risk analysis of blockchains

Institutional blockchain adoption should be accompanied by empirical validation processes, adversarial network, and load tests to ensure operational resilience and continuous improvement. Ongoing public-private collaboration, leveraging community-driven and open-source mechanisms, is essential. Financial institutions should actively participate in and provide resources for such work. Continuous improvements to existing open-source risk frameworks and standards should be pursued to ensure relevance and responsiveness.

1. Context and scope

1.1. Overview

The RMF is an industry-led effort, facilitated by Global Blockchain Business Council (GBBC) and Oliver Wyman, to give financial institutions guidelines to analyze and control for the non-financial risks that arise when they use public blockchain infrastructure. A cross-sector working group—comprising financial-market infrastructures, global systemically important banks, multilateral development banks, and leading Layer-1 protocol teams—has collaborated to provide a common reference that is rooted in their practical experience of managing risks or blockchain implementations and provide an overview of how the new technology can be incorporated into established risk management frameworks.

While blockchain, akin to the internet, is inherently use-case agnostic and supports numerous non-financial applications, the cross-sector working group identifies its transformative potential to drive a new wave of financial innovation with a potential to fundamentally reshape financial services. The Bank for International Settlements (BIS) believes tokenization will enhance the capabilities of the monetary and financial system by enabling new ways to serve end users and by removing the traditional separation of messaging, reconciliation, and settlement[1]. Similarly, the Executive Order issued by the President of the United States 'Ensuring Responsible Development of Digital Assets' recognizes that advances in technology and the rapid growth of digital asset markets are shaping the future of finance[2].

Public blockchains extend these potential benefits beyond traditional financial services, offering new infrastructure rails for exchanging information and value over a shared database layer. This expansion requires the adaptation and evolution of existing risk management practices. Just as cloud services and the internet have become foundational for financial institutions, blockchain technology represents the next step in the evolution of the infrastructure. Financial institutions must therefore engage with these technologies, contribute to their development and governance, and adopt new responsibilities essential to managing shared public infrastructures.

Financial institutions have an opportunity to leverage blockchain technology to offer integrated financial services, improve financial inclusion, modernize legacy systems, and reduce risks associated with interconnected infrastructures and processes. Blockchain's potential has gained widespread recognition, with regulated institutions accumulating considerable experience designing and operating public and private blockchain systems. However, to move from proof-of-concept stages to scaled production-level deployments, clearer regulatory guidance and industry standardization is necessary. Financial institutions must also systematically integrate these emergent infrastructures into established risk management practices.

This first version of the RMF addresses two archetypes of public blockchains: public permissionless and public permissioned. These two types present distinct characteristics and risk profiles, necessitating tailored approaches to identify, assess, and mitigate risks effectively. The RMF deliberately deprioritizes private permissioned blockchains from its scope, as their governance typically resembles conventional outsourced IT, which is adequately covered by existing cloud, outsourcing, and third-party risk management standards. The RMF focuses primarily on public blockchains, characterized by shared and open infrastructure maintained by a global community rather than bilaterally contracted vendors.

The RMF leverages established globally recognized financial industry standards, frameworks, and taxonomies[3] to ensure seamless and appropriate mitigations for public blockchain use into existing non-financial risk management frameworks.

[1] BIS, The next-generation monetary and financial system

[2] The White House, Strengthening American Leadership in Digital Financial Technology

[3] Frameworks, standards, and taxonomies leveraged include: Committee of Sponsoring Organisations (COSO) of the Treadway Commission, NIST Cybersecurity Framework, Cloud Controls Matrix, Digital Asset Securities Control Principles, Digital Operational Resilience Act,, Markets in Crypto-Assets Regulation, Basel BCBS44, Identity and Access Management, Principles for Financial Market Infrastructure

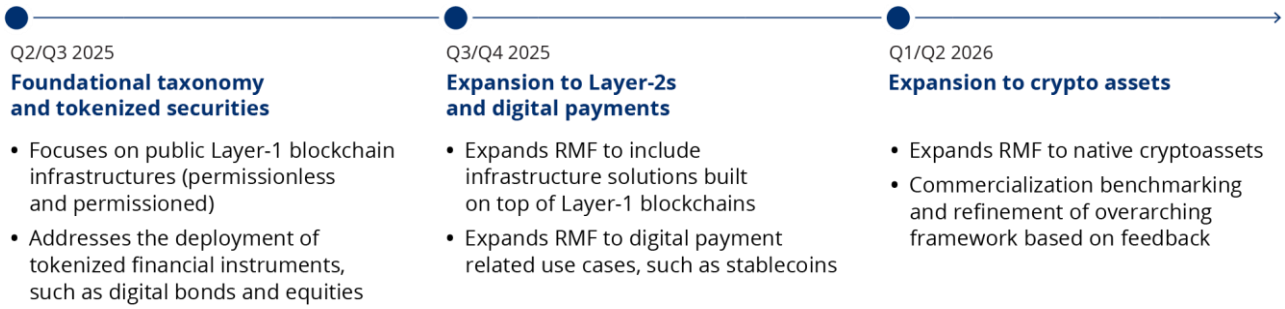
1.2. Objective

The RMF targets three key objectives to advancing public blockchain infrastructure adoption:

- Provide a concise, adaptable, baseline standard by designing seamless integration into existing risk management frameworks. The RMF should accommodate financial institutions at any stage of public blockchain adoption.
- Facilitate regulatory feedback through active dialogue with policymakers and regulators to support harmonized policy development and rulemaking.
- Remove institutional obstacles by addressing operational uncertainties and regulatory ambiguities with mitigants and controls, enabling confident and risk-aware interactions with public blockchains.

The RMF will be developed in phases, progressively expanding its risk-based mitigation focus across asset classes and use cases.

Exhibit 1: Risk mitigation framework phases



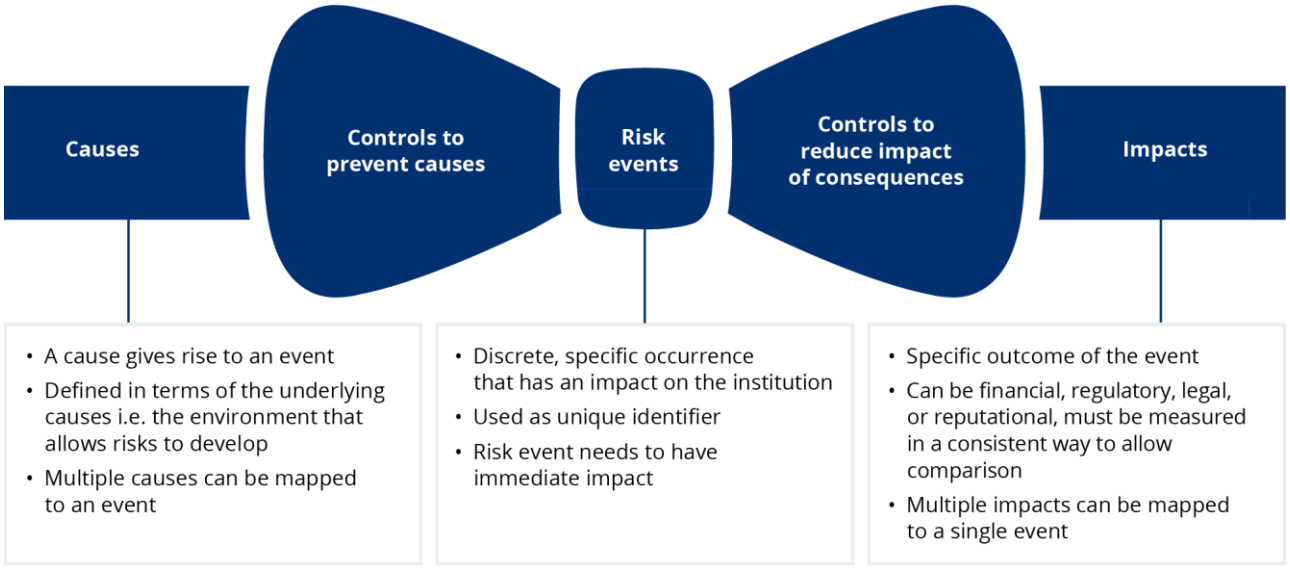
2. Reference methodology for managing non-financial risks

The ORX Reference Taxonomy, developed by the Operational Riskdata eXchange Association, was first introduced in the early 2000s and has evolved over the past two decades into a globally recognized framework for classifying non-financial risks. It provides a structured, hierarchical model that organizes risk types into consistent categories. Since its launch, the taxonomy has been refined to incorporate risks from new and emerging technologies, such as cloud computing and the internet. Several regulators, like the European Banking Authority (EBA), explicitly reference or align their guidance broadly with ORX taxonomy principles.

While the ORX framework's taxonomy remains broadly applicable to blockchain technologies, certain blockchain-specific characteristics alter the nature and impact of underlying risks. Consequently, tailored mitigation strategies are necessary to effectively manage these risks within institutional risk appetite. Therefore, this RMF uses the ORX taxonomy as its foundational structure, adapting it to address blockchain-specific risk scenarios and mitigation strategies.

The ORX taxonomy is based on an event-driven structure that draws from the bow-tie method. This method maps risk scenarios across three core dimensions: causes (the underlying drivers or conditions that make risk events possible), events (the actual incidents), and impacts (the resulting consequences)[4]. It also emphasizes the importance of linking these dimensions to mitigation strategies presented through preventive, detective, and corrective actions. This structure supports a dynamic approach to non-financial risk management and is widely used by financial institutions.

Exhibit 2: Bow-tie methodology



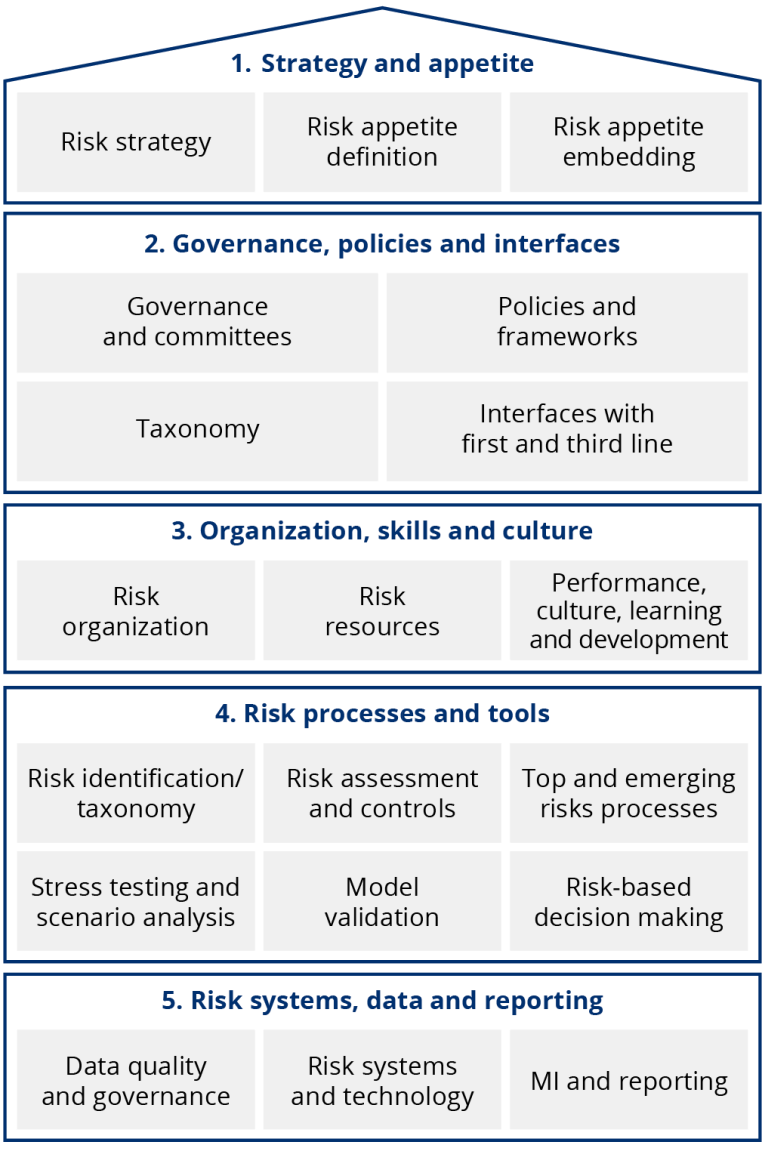
[4] Oliver Wyman, ORX Reference Taxonomy for operational and non-financial risk - Causes & Impacts (Summary Report – November 2020)

3. Adapting non-financial risk management frameworks to incorporate public blockchain risks

3.1. Risk framework

The RMF focuses on the successful incorporation of non-financial risks and mitigations into standard risk taxonomy and strategies. Financial institutions typically have existing Enterprise Risk Management (ERM) and Non-Financial Risk (NFR) frameworks. It is crucial that blockchain-related risks are managed in an integrated rather than isolated manner; thus, this RMF is intentionally designed to align seamlessly with standard ERM and NFR structures used by financial institutions, facilitating straightforward adoption and integration.

Exhibit 3: Standard risk management framework structure



While not falling directly under the rubric of this RMF, for the purpose of completeness we have outlined how a financial institution could incorporate public blockchain-related risk management practices:

1. **Strategy and appetite:** Financial institutions must clearly articulate how the usage of public blockchains align with their overall risk strategy. As public blockchains becomes integrated into core business processes, the risk appetite must explicitly reflect this shift, ensuring clear thresholds, tolerances, and escalation criteria for blockchain-related risks. Risk appetite should be network-specific and evidence-based with results from technical and governance due diligence (e.g., code quality, sustainability, validator concentration, upgrade history, bug-bounty scope, oracle dependencies).
2. **Governance, policies, and interfaces:** Financial institution governance structures must explicitly recognize and incorporate public blockchain-related activities, especially if they become strategically significant. Public blockchains operate 24/7 and are often highly automated. Therefore, they require mechanisms that are more in line with trading-related governance processes. Policies and procedures should be reviewed and updated to clearly define public blockchain-specific roles, responsibilities, and escalation paths, ensuring effective oversight and integration with existing governance processes.
3. **Organizational skills and culture:** Public blockchain as a modern technology necessitates specialized expertise. Institutions should proactively embed knowledge into their risk functions through dedicated training and targeted augmentation of the skill set. The transparent nature of public blockchain data may also require adaptation of the internal code of conduct to ensure teams understand and effectively address the unique challenges. Software risk-control mechanisms need to be systematically embedded in business processes that use smart contracts, requiring that the respective team's skills are adequate.
4. **Risk processes and tools:** Represents the primary area of focus and adaptation. Central to effective non-financial risk management is the development of a structured risk taxonomy that explicitly incorporates public blockchain-related risks. This taxonomy should be built upon and integrate with standard industry frameworks, ensuring consistency and comprehensive oversight. This includes identifying unique public blockchain risks, assessing their specific nature, and implementing robust blockchain-specific mitigation strategies.
5. **Risk systems, data, and reporting:** Must accommodate blockchain's continuous (24/7) operating environment. Systems should seamlessly integrate blockchain data streams, ensuring real-time risk detection, monitoring, and timely reporting. Enhancing infrastructure to manage continuous data flows and providing effective, real-time management information reporting will be essential to maintaining operational resilience and robust risk oversight.

3.2. Approach

As outlined above, public blockchains differ in several significant ways from traditional digital infrastructures, particularly within the financial market domain. Many of these differences stem from the distributed, multi-party operational and governance models that public blockchains adopt. While select non-financial risks can be addressed through conventional governance and controls, a subset of threats calls for broader structural changes in institutions' risk mitigation strategies and appropriate governance mechanisms that reflect the shared responsibility among network participants. These challenges are intrinsic to how blockchain systems operate—for instance, vulnerabilities in consensus mechanisms or governance shortfalls in decentralized networks—which no single institution can mitigate on its own.

The RMF analyzes known public blockchain risks and compares them with existing ORX risk types and established risk management positions, identifying three distinct categories: novel risks requiring entirely new mitigation strategies, risks requiring adaptations of existing standards, and standard risks manageable using established frameworks. The RMF acknowledges the complexity and multidisciplinary nature of this challenge, requiring further iteration and improvement. Consequently, we invite industry participants and regulatory stakeholders to provide feedback and input for the future development and detailing of the framework.

Table 1: Risks assessed

Risk type	Relevant ORX Risk	Specific risks assessed	
Novel risks	**Technology risk**	Hardware risk	• Third-party dependencies • Limited node diversity
		Software risk	• Data corruption due to software or configuration errors • Code vulnerabilities
		Network risk	• Protocol governance risk • Weakness in consensus design • Scalability constraints • Protocol upgrade and hard fork risk • Finality lag and transaction rollback risk
	Information security risk	Risk of data loss	• Compromised data integrity • Private key loss and inadequate key management practices
		Cyber risk events	• Cryptographic vulnerabilities • Smart contract errors and exploits • Consensus attacks • Denial of service (DoS)
		Risk of data privacy breach / confidentiality mismanagement	• De-anonymization through public transaction data analysis • On-chain exposure of sensitive or confidential data
		Risk of improper data access	• Privilege misconfiguration • Misuse of data transparency and roles
	Financial crime risk	Risk of money laundering and terrorism financing	• Illicit fund integration • Terrorist financing • Obfuscation of transaction origin through complex multi-step activity
		Risk of sanctions violation	• Insufficient screening of on-chain transactions and counterparties • Sanctions evasion risk
		Bribery and corruption	
		KYC / KYT / Transaction monitoring control failure	
	Business continuity risk	Inadequate business continuity planning / event management	
		Dependency on external governance for network recovery	
	Third party risk	Reliance on public blockchains	
		Inability to effectively manage providers	
Adapted risks	**Legal risks**	Lack of attributable counterparty (ORX Level-2 risk category - mishandling of legal processes)	
		Risks that arise from contractual rights / obligations failure	
	Transaction and process execution	Processing/execution failure relating to clients and products	
	Data management	Inadequate data architecture/IT infrastructure	
Standard risks	**Security and safety**	*Out of scope as traditional frameworks sufficiently cover these risks.*	
	People		
	Conduct		
	Internal fraud		
	External fraud		
	Regulatory compliance		
	Model		
	Statutory reporting and tax		

3.3. Risk mitigation capabilities

For effective management of non-financial risks in public blockchains, financial institutions should consider adopting and integrating comprehensive risk mitigation capabilities across the following three dimensions:

- **Technological risk mitigation:** Financial institutions have made substantial advances in developing sophisticated mitigants, most recently for cloud-based services—implementing real-time monitoring, automated alerts, redundancy strategies, and cyber-resilient infrastructures. Significant progress has also been made regarding open-source code risks, including automated vulnerability scanning, vulnerability databases, strategies for immediate patching, pinning specific code versions, and software composition analysis (SCA) tooling. Public blockchains represent an evolution of this trend, and these existing technological solutions and approaches can be leveraged as part of an institution's evolving blockchain risk management practices.
- **Process-oriented mitigation:** Financial institutions typically invest substantial efforts in defining rigorous internal processes, including formalized policies and operating procedures. However, the inherently distributed operational model and multi-stakeholder environment of public blockchains challenge the traditional internally focused approaches. Institutions considering public blockchains may need to contemplate modification of their process environments, to ensure alignment with blockchain-specific operational dynamics. These adaptations might include processes such as asset-freezing mechanisms, on-chain contingency procedures, and rapid response protocols for incidents.
- **Governance mitigation:** Traditional outsourcing arrangements alleviate governance-related risks, such as change management and escalation processes, through contractual agreements incorporating clearly defined SLAs. In contrast, public blockchains typically rely on decentralized governance mechanisms that often involve community-based structures, such as decentralized autonomous organizations (DAOs), and collective decision-making among asset holders, node operators, or users. Governance decisions in these decentralized settings are usually guided by community consensus or majority vote rather than explicit contractual obligations, which provide transparency and collective oversight but rely heavily on voluntary coordination and alignment among stakeholders rather than binding mandates. Financial institutions can analyze decentralized blockchain governance structures and their coordination dynamics and decide whether those fall within their stated risk appetite and, if they choose to engage, participate in these governance frameworks to shape them to better suit their needs.

The proposed mitigation strategies are presented from two distinct perspectives: the public blockchain ecosystems and the financial institutions. The ecosystem perspective reflects actions that can be taken collectively by protocol developers, node operators, governance participants, and other involved actors through open standards, voluntary coordination, and protocol design. This perspective aims to capture the diverse and distributed group of actors and stakeholders involved in the development, maintenance, and operation of a public blockchain infrastructure. In contrast, the financial institution perspective focuses on what regulated entities can do independently—such as technical integration, monitoring, and fallback planning—to manage their exposure to public blockchains. This dual view enables a realistic and comprehensive approach to risk mitigation by aligning controls with where agency and accountability reside and provide supportive delimitations.

4. Novel risks

Risks in this category encompass novel risks introduced by public blockchains and decentralized architectures, requiring expansion or enhancement of existing controls and governance frameworks. These risks oblige institutions to rethink their control frameworks.

4.1. Technology risk

As with any digital infrastructure, the integrity and availability of public blockchains determines whether data can be processed reliably and safely. One key category impacting this is technology risk. The architecture and operating model of public blockchains can reduce certain traditional technology risks (such as data redundancy and system availability). At the same time, though, this also can introduce novel risks. Public blockchains are interconnected infrastructures—meaning that, even more so than in the traditional financial infrastructures space, a vulnerability in a blockchain could affect a large user base. Robust technology risk management by financial institutions is therefore essential.

An important mitigation strategy, unique to blockchain, is the governance mechanisms that support and maintain the network. Financial institutions should determine where they can directly participate in blockchain protocol operations and governance. Institutions may proactively contribute to codebase development and directly operate or sponsor key blockchain utilities (such as APIs, node infrastructures, and block explorers), thereby enhancing security and operational resilience across the ecosystem.

4.1.1. Public blockchain risks and mitigation strategies

See Appendix for detailed matrix: **Table 5**

Hardware risk

Limited node diversity: Public blockchains rely on distributed nodes for data validation and redundancy. Potentially, some node operators can be concentrated with a few hosting providers or in geographic regions based on community origins and operational efficiencies. Such concentration increases the risk that provider outages, regional failures, or natural disasters could simultaneously impact a critical number of nodes, causing processing degradation or, at worst, network downtime.

Mitigation strategies

- For public blockchain ecosystems: incentivizing diversified node hosting, concentration monitoring and disclosure, and providing tools and guidance to lower the cost of hosting.
- For financial institutions: prioritizing blockchains with demonstrated node distribution, continuously monitoring node metrics, running a set of their own distributed nodes, and maintaining documented failover plans.

Third-party dependencies: Public blockchain networks may rely on external infrastructure providers such as Remote Procedure Call (RPC) endpoints, node gateways, and indexing services, which can create centralization risks and potentially unexpected single points of failure. Outages, degradation or cyberattacks on such providers could significantly disrupt data processing and access.

Mitigation strategies

- For public blockchain ecosystems: encouraging diversification of infrastructure providers, striving towards more decentralized architectures, supporting and incentivizing self-hosting, monitoring third-party providers' health, and implementing robust failover mechanisms.
- For financial institutions: employing multiple independent providers for redundancy, assessing provider resilience during due diligence, continuously monitoring service availability, and maintaining documented failover plans.

Software risk

Code vulnerabilities: Public blockchain networks rely on complex decentralized consensus protocols and node code, which can introduce undiscovered vulnerabilities. Such flaws may be exploited by attackers to disrupt node operations, compromise consensus mechanisms, or gain unauthorized access, leading to operational failures or security breaches. Exploitation of these vulnerabilities can lead to reduced network integrity, transaction errors, and unintended forks.

Mitigation strategies

- For public blockchain ecosystems: rigorous code reviews, formal verification, continuous static and dynamic analysis, real-time anomaly monitoring, adversarial testing infrastructures, multiple competing node implementations, third-party or community audits, rapid patching teams, and coordinated disclosure processes.
- For financial institutions: selecting networks with secure coding practices and third-party audits, continuously monitoring vulnerability disclosures and network performance, testing preproduction environments prior to integration, documented plans for suspending transactions, and documented failover plans to backup infrastructure.

Data corruption: Public blockchains rely on consistent software implementations and correct configuration of sufficient nodes to ensure expected blockchain infrastructure behavior. Software bugs, version mismatches, or misconfigurations can cause degraded performance, delayed transactions, and, at worst, involuntary operational disruptions such as temporary forks.

Mitigation strategies

- For public blockchain ecosystems: standardizing node implementations, incentivizing configuration compatibility checks, providing node operators with automated deployment tools, real-time monitoring for divergence, and providing rapid node recovery and emergency configuration updates.
- For financial institutions: using validated node software, rigorous configuration management, continuous node monitoring, promptly reinitializing nodes from trusted snapshots, verifying ledger integrity, and coordinating with protocol maintainers.

Network risk

Protocol upgrade and hard fork risk: Public blockchains can require network-wide upgrades, often in the form of hard forks, to introduce new features, enhance security, or address vulnerabilities. If poorly coordinated or communicated across the validator pool, these changes can cause operational misalignment or inconsistent network behavior. For financial institutions, insufficient visibility or preparation for upgrades may result in incompatible systems, node failures, service disruptions, and transaction discrepancies.

Mitigation strategies

- For public blockchain ecosystems: establishing transparent upgrade governance, advanced communication, monitoring upgrade adoption, and providing emergency patches.
- For financial institutions: active monitoring of governance forums, testing upgrades and their interaction with their own systems in preproduction environments, maintaining communication with development teams, auditing post-upgrade transactions, preparing fallback infrastructure, and delaying critical transactions during upgrade uncertainties.

Finality lag and transaction rollback risk: Public blockchains may rely on probabilistic finality, meaning transaction irreversibility becomes less likely with the amount of data validated after the transaction in question. During periods of network degradation, this can lead to delayed finality or, at worst, blockchain reorganizations, reversing confirmed transactions.

Mitigation strategies

- For public blockchain ecosystems: modifying consensus mechanisms for deterministic finality, transparently communicating finality thresholds and risks, monitoring network forks, implementing checkpointing solutions, and enabling rapid node reconciliation.
- For financial institutions: selecting blockchains with appropriate finality models, adopting conservative probabilistic thresholds for critical transactions, real-time monitoring of blockchain stability, designing resilient internal systems to handle reorganizations, and maintaining documented plans to promptly reconcile or pause affected transactions during reorganization events.

Protocol governance risk: Public permissionless blockchains, in particular, can rely on governance mechanisms that are determined by community decisions. These governance processes can be slow, result in stakeholder disputes, create unexpected outcomes, and in rare cases, end in a community split with two competing infrastructure versions (e.g., Ethereum and Ethereum Classic). Such events may trigger operational disruptions, increased integration complexity, diminished predictability, and higher maintenance costs.

Mitigation strategies

- For public blockchain ecosystems: establishing transparent and technically enforceable governance frameworks, structured proposal and voting processes, pre-voting and other intent-signaling methods, and proactive governance monitoring.
- For financial institutions: active monitoring of governance proposals and voting, participation or partnership with ecosystem contributors, governance robustness assessment during infrastructure selection, operational buffers for protocol-driven changes, and documented failover plans.

Weakness in consensus design: Public blockchain networks rely on consensus protocols designed to decentralize validation power. However, economic incentives or technical constraints can unintentionally encourage centralization of such activities, creating structural vulnerabilities such as lower-than-expected fault or collusion tolerance or, at worst, consensus instability. This can disrupt transaction processing and weaken network resilience.

Mitigation strategies

- For public blockchain ecosystems: designing incentive structures that promote validator diversity, implementing safeguards against concentration (e.g., staking caps, validator rotation, slashing mechanisms), continuously monitoring validator concentration, and enabling governance-driven validator rebalancing.
- For financial institutions: continuously monitoring validator decentralization, participating in validation, and maintaining documented failover plans.

Scalability constraints: Public blockchain networks inherently face scalability constraints due to design choices prioritizing decentralization and security over throughput. Protocol limitations on block sizes, transaction speeds, or finality can cause network congestion during periods of high transaction demand. Resulting transaction delays, increased fees, and backlogged workflows to disrupt dependence on timely settlements.

Mitigation strategies

- For public blockchain ecosystems: protocol upgrades to enhance throughput, support for Layer-2 scaling solutions (such as rollups and sharding), optimization of block propagation, transaction compression, and dynamic fee mechanisms.
- For financial institutions: evaluating network scalability and transaction performance during due diligence, continuous real-time monitoring of transaction latency and fee volatility, designing workflows with fallback or batching capabilities, and preparing contingency measures for migrating workflows during sustained network congestion.

Key Differences for Public Permissioned Blockchains

The mitigation strategies operate slightly differently for public permissioned blockchains, where validator roles are often centrally administered and controlled. Such blockchain networks, typically governed by consortia, member associations, or trusted entities, can explicitly mandate and typically also contractually enforce deployments aligned with financial institution regulatory standards. Furthermore, permissioned participation enables stricter orchestration and can include legally binding service level commitments. It can, however, reintroduce degrees of concentration risk when oversight rests with a single or a coordinated set of organizations.

4.2. Information security risk

Blockchain introduces security challenges with specific operational, legal, and reputational implications. Blockchains are connected data domains, and it is therefore important to not only secure the data and information shared on-chain, but also to ensure that sensitive information is not shared in the first place to avoid potential leakage to third parties. In addition, public blockchains are permanently exposed to potential malicious actors, and while encryption and blockchain architecture provide safeguards, specific elements related to interoperability (such as bridges) remain vulnerable and need to be carefully protected and utilized with due care.

Blockchains are permanently interconnected; vulnerability in one area can have cascading effects across others. A holistic network-wide approach is therefore required to manage these risks.

4.2.1. Public blockchain risks and mitigation strategies

See Appendix for detailed matrix: **Table 6**

Risk of data loss

Private key loss and inadequate key management practices: Public blockchains require the use of cryptographic keys to authorize transactions and other uses. The responsibility of safely administering and utilizing these keys falls on users or their custodians. Inadequate management or loss of these keys can permanently prevent access to and usability of the associated data, causing financial loss, operational disruptions, and reputational damage.

Mitigation strategies

- For public blockchain ecosystems: promoting secure key-management standards, enabling multi-signature or threshold schemes, encouraging robust backup practices, and supporting protocol-level key recovery solutions.
- For financial institutions: adopting institutional-grade custody solutions incorporating hardware security modules (HSMs), enforcing dual-control access policies, monitoring key usage in real-time for anomalies, establishing clear procedures for key revocation, and maintaining structured key recovery processes.

Compromised data integrity: Data on public blockchains depends on secure peer-to-peer communications and consensus among distributed nodes. Malicious nodes or network-level attacks such as message tampering or relay hijacking could inject corrupted data, disrupt consensus, or cause temporary ledger forks, leading to operational disruption and delayed or rejected transactions.

Mitigation strategies

- For public blockchain ecosystems: enforcing secure peer communication protocols, promoting node diversity, conducting regular protocol hardening, and continuous monitoring for fork anomalies and ledger inconsistencies.
- For financial institutions: maintaining redundant validation infrastructure, performing off-chain reconciliations, continuously monitoring ledger consistency and node performance, automated node shutdown, and documented failover plans when ledger integrity is impacted.

Cyber risk events

Consensus attack: Public blockchain networks depend on decentralized validator sets to ensure secure and accurate transaction processing. Excessive concentration of mining or staking power amongst a coordinated set of validators could enable malicious actors to achieve majority control (51% attack), potentially allowing them to manipulate transaction ordering, censor legitimate transactions, or reorganize the blockchain. Such attacks compromise transaction integrity and disrupt network reliability.

Mitigation strategies

- For public blockchain ecosystems: incentivizing decentralized validator participation, implementing staking caps and slashing or other incentive mechanisms, continuous monitoring of validator distribution and consensus behavior, and rapidly activating governance-driven interventions.
- For financial institutions: selecting networks with robust decentralization and active governance, continuously monitoring validator concentration and consensus health, diversifying exposures across blockchain networks, pausing transactions during consensus instability, and maintaining plans for migration in cases of compromise.

Denial of service (DoS) attacks: Public blockchain nodes are inherently susceptible to DoS attacks, which overwhelm them with excessive traffic or transaction requests, causing network congestion, latency, and operational disruption.

Mitigation strategies

- For public blockchain ecosystems: implementing protocol-level rate limiting, spam protection, and DoS mitigation solutions, continuously monitoring transaction and traffic volumes, and providing emergency rerouting or prioritization capabilities.
- For financial institutions: evaluating network resilience during infrastructure selection, monitoring real-time memory pool (mempool), congestion, transaction delays, and fee volatility, establishing operational buffers, postponing or rerouting critical transactions, and maintaining alternative processing pathways and response protocols.

Cryptographic vulnerabilities: Public blockchain networks rely heavily on cryptographic algorithms such as ECDSA or EdDSA, which may become vulnerable to future quantum computing advancements or cryptanalytic breakthroughs. Exploitation of these vulnerabilities could compromise private keys, enabling unauthorized transactions, theft, or network-wide loss of trust.

Mitigation strategies

- For public blockchain ecosystems: integrating quantum-resistant cryptographic schemes into future protocol upgrades, reducing public key exposure through transaction design, continuous monitoring of cryptographic research, and rapid emergency upgrade pathways.
- For financial institutions: adopting quantum-resilient key management practices, minimizing public key reuse and exposure, actively monitoring for unusual wallet activity, and maintaining contingency procedures for rapid key rotation or asset quarantining in case of suspected compromise.

Smart contract errors and exploits: Due to their complexity and immutability upon deployment, blockchain smart contracts and core protocol code carry inherent risks of irreversible logical errors or vulnerabilities that could cause permanent adverse consequences. Errors discovered post-deployment could result in permanent transaction failures, unauthorized asset transfers, or severe operational disruptions.

Mitigation strategies

- For public blockchain ecosystems: rigorous coding standards, comprehensive pre-deployment audits and formal verification, supporting upgradable contract frameworks, real-time anomaly detection, and emergency contract upgrade or halt mechanisms activated via community governance.
- For financial institutions: relying on strictly audited libraries and upgradable designs for critical contracts, implementing multiparty authorization processes, real-time monitoring for execution anomalies, and rapid activation of predefined emergency patches or migration to secure contract versions upon detection of vulnerabilities.

Risk of data privacy breach/confidentiality mismanagement

On-chain exposure of sensitive or confidential data: Public blockchains create inherent risks of permanently exposing sensitive, personal, or confidential data if inadvertently recorded directly or via metadata leakage due to their immutable and transparent nature. Such exposure can cause irreversible privacy violations, regulatory breaches, and misuse risks.

Mitigation strategies

- For public blockchain ecosystems: promoting off-chain data handling, supporting privacy-enhancing architectures, scanning for improper data uploads, and facilitating smart contract proxy mappings.
- For financial institutions: strict internal controls against on-chain transmission of sensitive data, employing privacy technologies, continuous monitoring of transaction metadata, regular privacy audits, promptly migrating business logic away from affected contracts.

De-anonymization through public data analysis: Public blockchain transparency enables advanced analytics, potentially linking pseudonymous addresses to identifiable individuals or institutions, exposing sensitive financial activities and operational details. Such de-anonymization can compromise privacy, lead to regulatory scrutiny, and erode institutional trust.

Mitigation strategies

- For public blockchain ecosystems: integrating privacy-enhancing mechanisms like zero-knowledge proofs and stealth addresses, actively monitoring analytics tools for de-anonymization attempts, and supporting robust pseudonymity features.
- For financial institutions: using privacy-focused wallets and transaction methods, avoiding address reuse, auditing transaction patterns regularly, monitoring public analytics platforms, updating address management policies proactively, and considering transitions to networks with stronger privacy provisions if needed.

Risk of improper data access

Misuse of data transparency and roles: The inherent data transparency of public blockchains can allow actors that have an information advantage or that have an operator role (e.g., relayer of transaction data) that influences transaction ordering to extract value from third party transactions. Sometimes referred to as "maximal extractable value" (MEV), this encompasses various forms of front-running, sandwich attacks transaction diversion before settlement, which can cause losses to users.

Mitigation strategies

- For public blockchain ecosystems: privacy-preserving and fair-ordering features such as commit-reveal or encrypted mempool designs, alternatives to account-based data architectures, protocol-level sequencing protections, and real-time analytics to flag ordering anomalies and isolate offending relayers.
- For financial institutions: thorough due diligence on MEV mitigations of public blockchains, submitting orders through private relays or batched channels, restricting internal access to client order flow, continuously monitoring execution timing and slippage for front-running signatures, and triggering immediate investigations, account freezes, and client notifications when anomalies surface.

Privilege misconfiguration: Improperly configured smart contract permissions or decentralized application roles can enable unapproved actions, resulting in unauthorized transactions, asset mismanagement, or operational disruptions. Such misconfigurations arise from overly permissive settings, incorrect role assignments, or inadequate decentralized governance controls.

Mitigation strategies

- For public blockchain ecosystems: integrating automated privilege-linting in deployment processes, clearly defining permission standards, and enforcing best coding practices in smart contracting languages.
- For financial institutions: internal privilege audits adhering to least-privilege principles, continuous real-time monitoring of privilege usage, periodic access log reviews, immediate revocation of compromised privileges, and prompt reconfiguration and stakeholder communication after incidents.

Key Differences for Public Permissioned Blockchains

Validator selection in public permissioned environments typically allows for more tightly controlled patch rollouts and contractual uptime guarantees but concentrates trust in a finite operator set. To balance security and transparency, consortium charters embed validator-rotation schedules, independent code-audit obligations, mandatory incident disclosures, and performance dashboards, while members still operate geographically distributed nodes and independent threat monitoring.

4.3. Financial crime risk

Financial crime risk presents distinct challenges within the blockchain ecosystem due to the global and immediate nature of blockchain-based settlements. While financial crime risks exist on all rails and can manifest differently on blockchain infrastructures compared to traditional systems, the transparent nature of public blockchains can enhance detection and mitigation when supported by adequate controls.

Transactions executed on public blockchains are instantaneous, borderless, and irreversible, introducing specific vulnerabilities related to money laundering, terrorist financing, sanctions evasion, and corruption. While public blockchains offer transaction-level transparency due to their openly accessible ledgers, the pseudonymous nature of users complicates identity verification and transaction attribution.

To address these challenges, financial institutions can consider supplementary solutions designed to incorporate advanced anti-money laundering (AML) analytics, digital identity verification, and enhanced transaction monitoring capabilities.

This section consolidates mitigation strategies for financial crime risks due to the substantial overlap in control measures, focusing on shared preventive, detective, and corrective practices for both public blockchain ecosystems and financial institutions.

4.3.1. Public blockchain risks and mitigation strategies

See Appendix for detailed matrix: **Table 7**

Risk of money laundering and terrorism financing

Obfuscation via complex multistep transfers: Public blockchain networks enable complex transaction flows involving multiple wallets, decentralized exchanges, bridges, mixers, and smart contracts without consistent identity linkage. These features significantly enhance layering, allowing rapid asset movement that obscures transaction origins, complicating transaction monitoring and AML compliance.

Illicit-fund(s) integration: Weaknesses in customer due diligence and inconsistent transaction monitoring during asset issuance, token trading, or use of on/off-ramps allow illicit actors to introduce funds into legitimate financial systems through blockchain assets. This undermines AML effectiveness, hampers traceability of illicit funds, and increases regulatory exposure.

Terrorist financing: Public blockchains offer pseudonymous participation and privacy-enhancing mechanisms, such as mixers, privacy coins, and stealth addresses, potentially enabling covert financial transfers. These features complicate the detection and monitoring of illicit fund flows, heightening the risk of regulatory breaches and exposure to terrorist financing.

Mitigation strategies

- For public blockchain ecosystems: promoting open transaction transparency standards, encouraging ecosystem wide integration of optional compliance tooling, and enabling blockchain data accessibility to support analytics and community-driven anomaly detection. Public blockchain ecosystems can also provide mechanisms for optional tagging and rapid isolation of suspicious assets, facilitating responsive governance interventions and community-based response frameworks.
- For financial institutions: strict implementations of robust KYC and KYT procedures, restricting interactions primarily to pre-vetted or whitelisted counterparties, and leveraging transaction profiling tools. Institutions should conduct real-time analytics monitoring to swiftly detect suspicious transaction patterns and anomalous fund flows. When suspicious activity is identified, financial institutions may freeze implicated assets, initiate forensic investigations, escalate incidents internally, and fulfill regulatory reporting obligations without delay.

Risk of sanctions violations

Sanctions evasion risk: Public blockchain networks can enable sanctioned individuals or entities to bypass international financial restrictions more easily through pseudonymous transactions, privacy-enhancing tools, and decentralized exchanges. This lack of embedded identity verification complicates traditional sanctions screening, increasing regulatory risk and the potential for enforcement actions against institutions.

Insufficient screening of on-chain transactions and counterparties: The pseudonymous nature and global accessibility of blockchain transactions complicate effective sanctions and compliance screening, allowing sanctioned actors to interact undetected with institutional or client-controlled assets. Limited integration of analytics and screening mechanisms into financial market applications using public blockchain exacerbates the challenge, increasing the risk of prohibited transactions.

Mitigation strategies

- For public blockchain ecosystems include promoting standardized address-screening mechanisms for financial market use cases, transaction metadata standards, and integrations with third-party compliance providers. Public blockchain ecosystems could also assist detection efforts and enable community-driven identification and flagging of suspicious transactions for rapid intervention.
- For financial institutions, critical mitigations involve performing rigorous, real-time sanctions screening during onboarding and transaction processing, inclusive of wallets, restricting interactions to pre-screened wallets and counterparties, screening of jurisdictions watchlists, and continuously leveraging blockchain analytics and internal watchlists. Institutions should swiftly freeze implicated assets, halt prohibited transactions, escalate incidents internally, and ensure prompt reporting to relevant regulatory authorities.

Risk of bribery and corruption

Crypto-facilitated bribery: Pseudonymous blockchain transactions can facilitate covert cross-border transfers, enabling bribery payments to public officials or corporate insiders. The inherent anonymity and global accessibility make detecting these illicit payments challenging, making it easier for allowing such transactions to bypass traditional financial controls and anti-corruption oversight.

Mitigation strategies

- For public blockchain ecosystems: providing infrastructure to integrate analytical tools to detect unusual patterns and enabling community-based flagging.
- For financial institutions: implementing multiparty authorizations and enhanced transaction due diligence, politically exposed person scans; using specialized analytics tools for real-time monitoring of payment flows, freezing suspicious transactions, initiating internal investigations, and reporting incidents to regulatory authorities.

Risk of KYC/transaction monitoring control failure

Absence of KYC and adequate monitoring: The accessible nature of public blockchains allows transactions without formal identity checks, which can lead to illicit activities like money laundering, fraud, and sanctions evasion. The absence of embedded identity verification and transaction monitoring can allow illicit transactions to enter financial institutional systems if not addressed.

Mitigation strategies

- For public blockchain ecosystems: promoting optional identity verification standards, facilitating integration of transaction monitoring solutions, and enabling community-driven reporting mechanisms for suspicious activities.
- For financial institutions: strict KYC/KYT onboarding processes, robust real-time transaction monitoring and analytics-driven auditing, immediate suspension of suspicious transactions, account isolation, and prompt regulatory reporting.

Key Differences for Public Permissioned Blockchains

In public permissioned environments, validator admission and/or user onboarding are often curated, enabling networks to hard-code KYC, sanctions list, and governance-approved oracles directly into the infrastructure, and enforce legal recourse through consortium contracts. The tighter gatekeeping eases monitoring but creates single-point dependencies; consortium charters should mandate independent list management, third-party analytics reviews, and transparent incident reporting, while each user still runs its own compliance stack to catch residual risk

4.4. Business continuity risk

Public blockchains are the ultimate source of transaction and ownership truth for asset ownership and transaction settlement—any outage, attack, or fork can freeze transaction activity and cast doubt on asset records. Ensuring continuity under stress is therefore critical to protect users and maintain market confidence. Robust Business Continuity Planning (“BCP”) can mitigate such risks, providing actionable mitigation strategies at both the level of financial institutions and public blockchain ecosystems.

It is vital to set impact tolerances for disruptions, defining how long and under what conditions individual participants can tolerate outages or errors.

4.4.1. Public blockchain risks and mitigation strategies

See Appendix for detailed matrix: **Table 8**Table 8:

Inadequate business continuity planning/event management

Inadequate business continuity and recovery planning: Financial institutions face significant risks if unable to promptly recover critical operations following public blockchain disruptions, due to inadequate business continuity and disaster recovery plans. Limited integration of blockchain-specific disruptions into existing frameworks, coupled with unclear recovery protocols and dependencies on infrastructures without robust fallbacks, can severely impact transaction processing, settlements, compliance, and reputation.

Mitigation strategies

- For public blockchain ecosystems: advanced communication of upgrade schedules, promotion of modular node architectures, diversity of node implementation, proactive and freely available blockchain monitoring, development of community-driven disaster recovery plans, incentivization of associated node operator responsibilities, and tools for rapid node redeployment.
- For financial institutions: incorporating blockchain scenarios into business continuity plans, maintaining fallback systems and documented plans, operating own nodes, continuous monitoring of network dependencies, transaction rerouting, and joining community-driven disaster recovery efforts.

Dependency on external governance for network recovery: Financial institutions face risks when relying on decentralized blockchain governance structures without formal escalation or recovery procedures. Distributed community governance processes can delay decision-making during critical incidents like protocol bugs, security breaches, or operational failures, leading to potentially extended network downtime and transactional disruptions.

Mitigation strategies

- For public blockchain ecosystems: implementing transparent and proactive governance frameworks, clear emergency protocols, regular incident responsiveness monitoring, development of community-driven disaster recovery plans, incentivization of associated node operator responsibilities, expedited patch distribution, and coordinated recovery tools.
- For financial institutions: conducting due diligence on governance maturity, maintaining active participation or relationships within governance communities, closely tracking governance activities for delays, and establishing robust internal fallback infrastructure and contingency processes for managing extended disruptions.

Key Differences for Public Permissioned Blockchains

Public permissioned blockchains leverage controlled validator and node management to establish continuity strategies. By embedding defined governance roles, formalized recovery frameworks, and proactive monitoring protocols, these environments may be able to minimize downtime and maintain operational stability. Furthermore, public permissioned blockchains can enforce stringent business continuity standards, such as hybrid deployment models (combining on-premises, private cloud, and regulated public cloud infrastructure), and real time monitoring. Consortium-led governance provides the ability to establish clear SLAs between participants and providers, dedicated secure network connections, and clearly defined impact tolerances and recovery processes.

4.5. Third party risk

The question of whether public blockchains should be categorized as third parties within existing risk management frameworks remains subject to ongoing debate, primarily due to their decentralized nature and lack of clearly identifiable operators. This section includes considerations for financial institutions and regulators seeking to apply traditional third-party risk management standards to mitigate risks associated with public blockchains. Additionally, the use of public blockchains commonly involves interactions with more traditional third parties, including data oracles and custodial service providers, which institutions must also factor into their risk management approaches.

4.5.1. Public blockchain risks and mitigation strategies

See Appendix for detailed matrix: **Table 9**

Public blockchain brings about new, systemic third-party risks requiring redesign of operating models and mitigation strategies, particularly across two critical categories

Reliance on public blockchains: While the decentralized operational model of public blockchains inherently provides a degree of resilience, and many public blockchains have a strong performance track record, it simultaneously limits control and direct accountability over infrastructure performance through traditional means such as contracting. Traditional third-party risks such as operational disruption, which also apply to public blockchains, therefore cannot be mitigated in the traditional ways.

Mitigation strategies

- For public blockchain ecosystems: promoting validator decentralization and diversity, transparent governance processes, continuous performance monitoring, and publication.
- For financial institutions: proactively developing or deploying multi-chain architectures with failover systems, continuously monitoring performance and availability, and maintaining documented failover plans.

Inability to effectively manage providers: Financial institutions utilizing public blockchains often rely on specialized third-party providers (e.g., oracle data providers, node-filtering solutions, and wallet providers), whose operational failures or compliance issues could create significant risks. While some of these vendors are traditionally organized and governed, others may operate in a partially or wholly decentralized manner, leveraging techniques similar to those used by public blockchains (e.g., a network of data providers for an oracle), thus limiting the deployment of traditional third-party risk management approaches.

Mitigation strategies

- For public blockchain ecosystems: encouraging or incentivizing standardized operational transparency for ecosystem builders and defining own or leveraging existing best practices for providers in the ecosystem.
- For financial institutions: rigorous upfront due diligence assessments of third-party blockchain service providers, establish appropriate SLAs where possible, diversifying engagements across multiple providers to reduce single points of failure, continuously monitoring provider compliance and performance metrics, and developing documented contingency and provider-replacement strategies.

Key Differences for Public Permissioned Blockchains

Public permissioned blockchain environments may blend decentralized and traditional third-party management approaches by combining structured contractual agreements with decentralized validator and governance frameworks. Institutions should seek strong contractual terms where feasible (such as Layer-1 service providers) while embedding decentralized redundancy strategies into operational designs. Regular resilience testing, continuous monitoring, and detailed contingency plans aligned with community-defined standards further bolster third-party risk mitigation and resilience.

5. Adapted risks

Risks in this category require targeted adaptations of traditional non-financial risk management practices to address specific blockchain complexities like decentralization, irreversibility of transactions, immutability of records, 24/7 operations, and cross-jurisdictional global nature of blockchains.

5.1. Legal risks

Legal risks when utilizing public blockchains are driven primarily by uncertainties in how laws, regulations, and contractual obligations are enforced. These uncertainties arise from regulatory ambiguity across jurisdictions and the inherently borderless nature of blockchain, complicating the determination of applicable laws and jurisdictional authority.

Consequently, mitigating against legal risks continues to require proactive governance, clear roles and responsibilities, and a current understanding of the evolving legal landscape.

5.1.1. Public blockchain risks and mitigation strategies

See Appendix for detailed matrix: **Table 10**

Legal risk management control failure

Lack of attributable counterparty (ORX Level-2 risk category - Mishandling of legal processes): Public blockchains' operational and governance models can make it infeasible to derive or enforce obligations and resolve disputes resulting from unexpected public blockchain behavior.

Mitigation strategies

- For public blockchain ecosystems: publishing clear governance charter frameworks, exploring community governance escalation mechanisms, and providing monitoring logs.
- For financial institutions: thorough legal risk and governance due diligence, identifying and utilizing contractable counterparties for ancillary services where possible, and assessing the views of prudential regulators where applicable.

Risks that arise from contractual rights / obligations failure: Smart contracts can act as an execution tool for contractual rights and obligations means of algorithmic code executable on a blockchain. Blockchain's immutability can cause challenges in correcting errors or bugs when using such tools, limiting the ability to implement traditional legal remedies.

Mitigation strategies

- For public blockchain ecosystems: encouraging development of standardized audited smart contract templates, promoting pre-deployment audits, and maintaining agile, community-driven governance processes that facilitate rapid response to misalignments.
- For financial institutions: conducting rigorous pre-deployment legal reviews, employing continuous real-time monitoring of smart contract executions, and maintaining clearly defined contingency plans for rapid migration or replacement of compromised or misaligned contracts.

Key Differences for Public Permissioned Blockchains

Public permissioned blockchain networks may offer flexibility in managing legal risks due to their structured governance and validator control. These networks should establish explicit dispute resolution mechanisms, jurisdictional guidelines, and legally binding frameworks that govern network operations. Participants operating within these environments should leverage their existing internal governance processes that ensure consistent alignment with changing legal standards and regulatory changes.

5.2. Transaction and process execution

Transaction processing and execution risk involves failures or delays in the accurate handling of transactions, arising from system errors, misconfigured smart contracts, procedural breakdowns, or inadequate operational oversight. In the context of public blockchains, these risks can be heightened due to the irreversible nature of transactions and the complexity and comparative novelty of underlying technology (including 24/7 operation). Managing these risks demands control mechanisms across client interactions, transaction execution logic, and internal operational processes.

5.2.1. Public blockchain risks and mitigation strategies

See Appendix for detailed matrix: **Table 11**

Transaction and process execution risk control failure

Processing/execution failure relating to clients and products: Public blockchain transactions and asset transfers are typically irreversible, significantly amplifying the impact of errors made through client-facing interfaces or validation misconfigurations. Unlike traditional financial systems, there is no operator that can provide remediation, significantly amplifying the impact of user or technical errors.

Mitigation strategies

- For public blockchain ecosystems: establishing clearly defined transaction formats and standards, developing and encouraging best practices for data checks, and providing real-time monitoring to enable financial institutions to promptly identify transaction anomalies or errors.
- For financial institutions: implementing dual-authorization controls for transaction submissions, rigorous user training and interface validations, and developing off-chain correction procedures and immediate client-notification processes to address errors.

Key Differences for Public Permissioned Blockchains

Public permissioned networks may blend decentralized redundancy with accountable and transparent governance structures. They can deploy structured escalation protocols, clearly defined validator roles, and automated operational controls to mitigate execution risks. Participants within these networks should similarly leverage structured monitoring frameworks, standardized transaction-validation practices, and transparent incident-response procedures to maintain operational stability and regulatory alignment.

5.3. Data management

Data management risk involves ensuring data—such as transaction records, asset ownership, compliance documentation, and other sensitive information—is accurate, secure, well-structured, and compliant. Public blockchains improve certain risks, such as data quality through consensus-driven accuracy, real-time 24/7 availability, and immutable records. However, public blockchains can also introduce distinct challenges related to integration with existing IT infrastructures, interoperability across different infrastructures, and compliance with data retention, destruction, and privacy regulations. Financial institutions adopting public blockchain need to reconsider and likely adapt their data management practices and governance frameworks.

5.3.1. Public blockchain risks and mitigation strategies

See Appendix for detailed matrix: **Table 12**

Data management risk control failure.

Inadequate data architecture/IT infrastructure: The transparent nature of public blockchains creates new challenges for how financial institutions typically think about data risks. If not duly considered and addressed, it can result in inadvertent leaking of personal data, data subject to banking secrecy or similar confidentiality, or contractually confidential data, including trade secrets.

Mitigation strategies

- For public blockchain ecosystems: best practices and guidelines for data risk management, tooling and standards for safe anonymization and other privacy tools (e.g., hashing, zero-knowledge proofs), and development of private batch-processing solutions.
- For financial institutions: analysis of data risks in public blockchain use cases, due diligence on specific data risks of public blockchains, use of private batch-processing solutions, and documented failover plans.

Key Differences for Public Permissioned Blockchains

Public permissioned blockchains can similarly address these risks by combining standardized governance practices, interoperability and data management frameworks, and off-chain compliance strategies. Participants operating within these environments should emphasize structured integration solutions, continuous performance monitoring, and comprehensive off-chain storage and privacy management to maintain compliance, operational resilience, and trust.

6. Standard risks

Risks in this category closely resemble those associated with traditional infrastructure, and existing risk management frameworks—such as cybersecurity standards and audit controls—remain effective without significant adjustments. This section summarizes key risk categories, highlighting limited blockchain-specific considerations that institutions may evaluate as deemed necessary.

- **Security and safety:** Involves protecting critical infrastructure, assets, personnel, and transactions from compromise or loss. For public blockchains, this can encompass securing nodes, managing cryptographic keys, and ensuring system integrity. Established IT security frameworks (such as ISO 27000, NIST Cybersecurity Framework) remain relevant, though institutions may require incremental adjustments, such as cryptographic key management protocols. Additionally, this risk category is addressed in the Technology and Information Security Risk sections of this framework, which include detailed mitigation strategies for novel risks.
- **People risk:** Concerns human error, negligence, or unethical behavior adversely impacting operations. For public blockchain environments, examples include mismanagement of private keys or erroneous transaction execution by employees. Standard controls such as role-based access controls, dual authorizations, comprehensive training, background checks, and defined roles remain effective.
- **Conduct risk:** Relates to behaviors by employees or institutions causing harm to clients or undermining market integrity (for example, mis-selling, insider trading, and market manipulation). Traditional conduct frameworks—such as codes of ethics, surveillance systems, conflict-of-interest management, whistleblower policies, and compliance oversight—remain applicable. However, institutions may benefit from enhanced transaction monitoring and, potentially, oversight of employee-controlled wallets to ensure alignment with established conduct standards.
- **Internal fraud:** Concerns deliberate misconduct by employees or insiders resulting in asset theft, unauthorized transactions, or manipulation of blockchain-based systems. Controls such as segregation of duties, multi-party authorization, rigorous monitoring, background checks, and strong internal governance remain fully effective. Established internal fraud frameworks require minimal adjustments, primarily enhanced monitoring of private-key usage and employee-controlled digital wallets, aligning with measures already used in traditional financial infrastructures.
- **External fraud:** Involves malicious acts by external entities, including cyberattacks, phishing, theft of cryptographic keys, and fraudulent impersonations. Established cybersecurity measures (such as multi-factor authentication, network segmentation, and endpoint security) combined with continuous monitoring and anti-fraud processes (such as fraud analytics and real-time alerts) effectively address these threats. Furthermore, external fraud risks are addressed in both the Third-Party, and Information Security risk sections, reinforcing comprehensive controls, vendor assessments, and secure system architectures.
- **Regulatory compliance:** Covers risks from violations or non-conformance with applicable laws and regulations governing financial markets. Regulatory authorities typically adopt technology-neutral approaches; thus, blockchain remains subject to existing regulatory frameworks (such as AML/KYC, investor disclosures, and securities laws). Established compliance frameworks, governance processes, and audit mechanisms apply directly with minimal additional measures, such as integrating blockchain analytics for enhanced regulatory reporting. Institutions should also remain attentive to evolving blockchain-related regulations, proactively updating policies to sustain compliance.

- **Model risk:** Primarily addresses risks arising from incorrect outcomes or inaccuracies due to flawed analytical models and valuation methodologies. These risks are not inherently blockchain-specific, and existing model risk management frameworks—covering governance, independent validation, testing, and documentation—continue to comprehensively address such concerns without significant blockchain-related adjustments.
- **Statutory reporting and tax:** Encompasses risks related to errors or non-compliance in financial, regulatory, and tax reporting obligations. Blockchain platforms largely fit into established reporting frameworks, utilizing existing controls like internal control over financial reporting, reconciliations, audit trails, and established accounting standards (although some may be under development in select jurisdictions). Institutions may require minor enhancements, such as integrating blockchain-derived transactional data and providing additional training on digital asset-specific taxation or reporting obligations.

7. Private permissioned blockchains

In exploring blockchain technology, most regulated financial institutions have historically implemented private permissioned blockchains, which are characterized by centralized governance, defined accountability, purpose-built operations, and closed-loop compliance and risk management.

The risks of private blockchain applications can be managed using traditional enterprise risk management frameworks—including robust cybersecurity controls (for example, ISO 27001 and NIST standards), formal business continuity plans, and established third-party risk management procedures. Defined roles, structured governance models, and enforceable contractual arrangements help to ensure effective incident response, legal recourse, and management of data privacy, transaction validation, and compliance obligations. Financial institutions should remain cognizant of new expressions of certain risks, such as smart contract-specific risks, which may require enhanced mitigations or tailored monitoring.

Due to their centralized nature, private permissioned networks benefit from reduced exposure to public blockchain-related risks as detailed in this RMF. However, the practical challenge for such solutions remains clarifying their value proposition compared to traditional infrastructures. Additionally, institutions should consider well-known operational challenges related to scalability at mass-production levels and the ongoing costs associated with maintaining private permissioned distributed ledgers.

8. Security Tokens

Tokenization involves representing traditional financial assets, such as bonds, equities, or funds, using a blockchain solution and tokens as the carrier of asset information. These digital tokens incorporate the economic and legal characteristics of conventional securities. One advantage of such solutions is the programmatic representation of the entire asset lifecycle, including corporate actions, on-chain. Additionally, blockchains enable composability and programmability. Programmability allows for the creation of self-executing code, typically in the form of smart contracts, on the blockchain, automating agreements and logic. Composability enables these smart contracts and decentralized applications to seamlessly connect and build upon one another, fostering an ecosystem of interconnected functionalities. This structure enables the potential for faster, more secure, and cost and capital efficient processes.

There are broadly two approaches to securities tokenization—issuance of the digital security in traditional format represented by a digital twin (tokenized security), or directly as a blockchain-native instrument (security token). This paper will focus on security tokens as blockchain-native instruments. While acknowledging that both approaches may coexist during a transitional period, the focus here is primarily on the potentially more efficient native instruments.

Key features of security token market structures include:

- Cost efficiency: Eliminating intermediaries, automating settlement, and clearing processes can substantially reduce transaction and servicing costs through programmability, with estimates suggesting annual infrastructure savings of $15–$20 billion[5].
- Enhanced transparency and auditability: Immutable blockchain records provide secure, tamper-proof transaction histories, significantly enhancing transparency.
- Automated compliance: Smart contracts automatically enforce compliance and regulatory obligations (such as KYC/AML), streamlining legal and operational processes.
- Improved risk management: Instantaneous (atomic) settlements significantly reduce counterparty, bankruptcy, and non-financial risks, freeing up substantial amounts of collateral—potentially over $100 billion annually in global capital markets[5].
- Fractionalization: Investors can purchase smaller portions of high-value or illiquid assets, enhancing market accessibility.

Despite these benefits, security tokens face adoption hurdles. Inconsistent global frameworks create complexity and uncertainties for issuers and investors alike. There are also market structure design challenges for security tokens concerning scalability, security, and recovery, which in some cases may need to be addressed at a design level by public blockchain ecosystems. Resolving these challenges will be essential to achieve widespread adoption.

[5] DASCP Framework Whitepaper, The Financial Stability Implications of Tokenisation

8.1. Value chains

Tokenization can alter individual stages of the capital markets value chain, from issuance through trading, settlement, custody, and record-keeping. The following exhibit highlights differences between traditional and blockchain market structures:

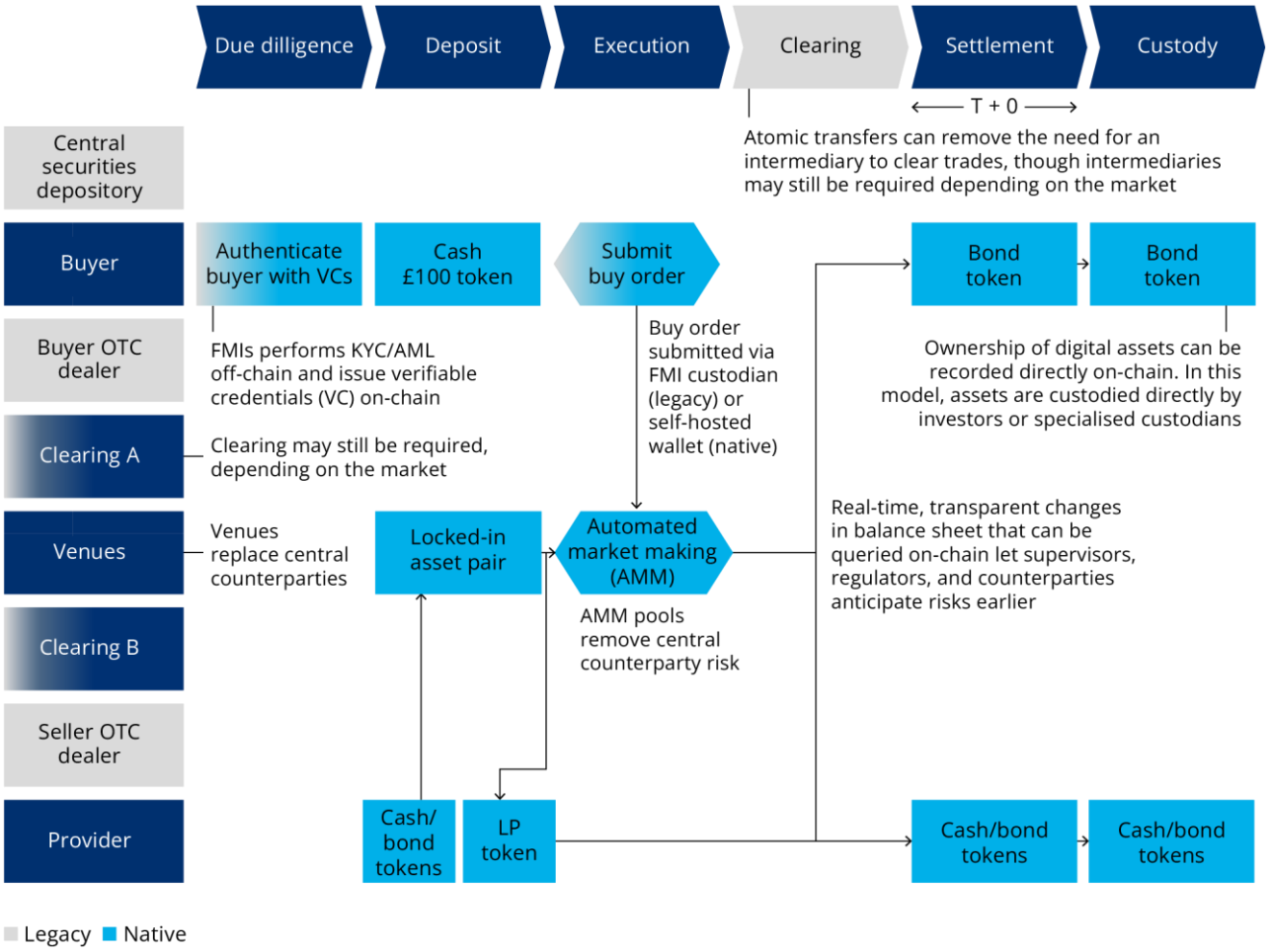
Table 2: Comparison of traditional markets and blockchain markets across the value chain

Feature	Traditional markets	Blockchain markets
Issuance	Manual, intermediated process (underwriters, IPOs)	Digital issuance (STOs, automated compliance via smart contracts)
Trading	Broker-mediated, centralized exchanges, hours limited to market and business hours	Digital exchanges, peer-to-peer capabilities, 24/7 continuous trading available
Settlement	T+1 or 2 settlement cycles via clearinghouses, delayed finality	Instantaneous or T+0 on-chain settlement, automated delivery-vs-payment
Custody	Centralized custodians, omnibus accounts, asset segregation complexity	Digital wallets, direct private-key management, possible self-custody
Record-keeping	Centralized ledgers, manual reconciliation among multiple entities	Immutable, real-time synchronized blockchain
Intermediaries	Numerous (such as brokers, clearinghouses, custodians, funds administrators, trading agents)	Reduced number of intermediaries (fewer reconciliation steps required)
Accessibility	Restricted investor base, high entry barriers, limited fractionalization	Enhanced global access, fractional ownership, possible low-entry thresholds
Transparency	Limited transparency, delayed reporting	Real-time transaction visibility possible, immutable audit trail
Cost	Higher due to manual processes, intermediary fees, reconciliation processes	Lower through automation, disintermediation, simplified workflows, single source of truth eliminates reconciliation
Liquidity	Certain markets can be illiquid, limited secondary market access for select segments	Potential to be enhanced due to fractionalization, and streamlined secondary markets access

Traditional secondary trading relies on complex web of intermediaries—brokers/dealers, exchanges, clearing houses, depositories, and transfer agents—each adding complexity, potential delays, and additional costs. Blockchain reconfigures this flow by enabling direct transactions through smart contracts.

These systems can consolidate traditionally separate functions into streamlined processes, reducing operational dependencies and costs by enabling direct issuer-to-investor and investor-to-investor connectivity. Decentralized Finance (DeFi) applications have also begun to enable tokenized asset trading and lending through decentralized marketplaces and liquidity pools with respective challenges and risks. Detailed considerations of DeFi-based tokenization structures are beyond the scope of RMF.

Exhibit 4: Illustrative process flow for a potential native (tokenized) bond purchase



Various jurisdictions have adopted distinct regulatory frameworks to govern tokenized securities, reflecting their unique legal environments and market needs. Approaches differ in their scope, underlying philosophies, and institutional arrangements, with broadly three different approaches: (1) specific legislation to support digital securities and tokenization (Luxembourg and Switzerland); (2) amendment of security rules to accommodate security tokens (Japan); or (3) mandating parallel processes for securities tokens and the underlying security (USA).

8.2. Stakeholders across the value chain and risk mitigation strategies

Historically, risk management in capital markets has been achieved through a combination of internal controls, specialized intermediaries, and utilities. Specific regulatory frameworks have been developed to control and mitigate financial and operational risks on a market and individual firm level. As we have seen in the previous section, security tokens allow for more direct interactions of market participants, which in turn leads to new responsibilities among the different participants in security token markets:

- **Issuers and their advisors**: Responsible for structuring instruments and placing them with investors in a manner that can ensure compliance throughout the token lifecycle is maintained, including the choice blockchain and smart contract structures. New duties for Issuers and their advisors include the need to guarantee that all necessary regulatory compliance can be incorporated into the smart contracts of the issued tokens, thus ensuring adherence to market rules such as KYC, AML, and suitability. Issuers must coordinate closely with control agents to manage token governance, including emergency freezes or reissuances in the case of theft or loss. Beyond embedding rules into tokens, issuers can leverage composability to integrate financial products and services to provide investors with tailored and innovative opportunities. Furthermore, issuers should embed clearly defined settlement finality standards in token documentation and adopt widely recognized interoperability standards to facilitate consistent price transparency and cross-chain compatibility.
  In markets where maintenance of a traditional security registrar such as a transfer agent is required, issuers need to coordinate closely with the registrars, who retain responsibilities for maintaining ownership records, ensuring synchronization between on-chain and off-chain data, and managing compliance obligations through smart contracts.
- **Venue operators (such as ECNs [electronic communication networks] and MTFs [multilateral trading facilities]):** Assume broader responsibilities due to the absence of a need to centrally clear and settle transactions. Direct market access for investors is also more prevalent in security token markets, and venue operators often facilitate atomic delivery-versus-payment (DvP) transaction settlement. Decentralized exchanges (DEX) are a new concept for venue operators; they resemble dark pool OTC trading platforms but differ in that they provide open access (rather than closed traditional dark pools). To ensure AML and KYC compliance, they rely on embedded smart contract compliance protocols and external identity verification mechanisms. Demonstration of transaction transparency and fair market practices to protect participants from market manipulation and operational disruptions is an additional challenge in this environment as instruments can be issued and traded on different blockchains. For DEXs, specifically, venues must implement oracles or incentivize liquidity pools to ensure robust and fair price discovery, and defined token listing requirements must be in place to support transparent pricing across fragmented blockchain environments.
- **Digital registrars (control agents):** Digital registrars serve as the blockchain-era equivalent of traditional transfer agents, maintaining official ownership records of security tokens. They ensure on-chain token balances align with authorized issuance quantities and enforce compliance measures (for example, whitelisting eligible investors or implementing transfer restrictions via smart contracts). Some regulatory frameworks explicitly include this role—for instance, Luxembourg's new "control agent" is responsible for overseeing digital securities issuance and tracking who owns what, similar to a crypto-securities registrar in Germany. By bridging on-chain activity with off-chain regulatory oversight, digital registrars add a crucial layer of trust and risk mitigation to security token markets.
- **Custodians:** Provide critical services for investors who are required to engage in third-party custody rather than self-manage custody of their assets. They face novel risks stemming from blockchain interoperability and cross-chain asset transfer reconciliations. All of which require a detailed understanding of the non-financial risks associated with the activities and sophisticated approaches to managing the risks and ensuring the residual risks either with own or third-party capital. As an additional layer of protection, custodians must clearly delineate their responsibilities vs. that of the client's—such as managing secure key access to assets held on-chain. Additionally, custodians need to coordinate tightly with issuers and control agents to ensure

seamless execution of reissuances or emergency governance actions, as well as ensuring clear accountability around compliance actions such as KYT.

- **Investors**: Enjoy increased autonomy in a security token environment but assume greater direct responsibility. They must manage cryptographic keys securely (either directly via self-custody or indirectly through trusted custodians). Investors need to conduct thorough due diligence on tokens and blockchain platforms, including risk assessment of the technologies. Over time as the environment matures, industry standard technology ratings may emerge as a third-party service, but fiduciary responsibilities will always require a significant degree of in-house technology assessment capability. A clear understanding of the rights and recourse mechanisms that are contained within the tokens and smart contracts investors acquire is needed. Protection against new scams and frauds (such as malicious smart contracts and fake tokens) requires the same approach.

DASCP framework

In May 2024, the Digital Asset Securities Control Principles (DASCP) whitepaper was released, providing a taxonomy of risks and controls for digital asset securities (see GBBC DASCP fact card). The DASCP framework provides essential guidance and best practices, aligning closely with the established Principles for Financial Market Infrastructure (PFMI) by BIS and IOSCO. The framework is based on the premise that defined responsibilities aligned to practical controls will support robust, compliant, and secure tokenized market structures.
The framework consists of six core principles, each addressing critical facets relevant to stakeholders involved in the value chain:

1	**Legal certainty**	Ensures digital asset operations comply with existing laws and regulations, supporting market integrity and investor confidence
2	**Regulatory compliance**	Advocates for consistent alignment with evolving regulatory frameworks, reinforcing trust and security across the digital asset ecosystem
3	**Resilience and security**	Emphasizes building robust technological infrastructures capable of resisting disruptions and maintaining the integrity and confidentiality of sensitive data
4	**Safeguarding customer assets**	Prioritizes implementing stringent governance and operational protocols over smart contracts to securely manage and protect customer assets
5	**Connectivity and interoperability**	Supports seamless transactions and flexible settlements across diverse blockchain platforms and traditional financial systems
6	**Operational scalability**	Aims for efficiency and cost-effectiveness through standardized processes and smart contract automation to accommodate market growth

The DASCP identified 36 risks and 57 controls across four categories (Legal, Smart Contract Governance, Resilience and Data Protection, and Network Settlement) that could be leveraged to mitigate these risks. While the DASCP was originally conceived as a blockchain-agnostic framework that did not distinguish between public and private blockchain risks, we have mapped the DASCP principles against the risk mitigation strategies presented in the RMF. This reconciliation enables a comprehensive and context-sensitive mapping between the two approaches. The comprehensive mapping is outlined below:

Table 3: DASCP principles relevance to mitigation strategies across framework

DASCP Principle	Risk mitigation strategies
Legal certainty	• Stakeholder communication and transparency: Clarifying rights, obligations, and mechanisms for dispute resolution across relevant jurisdictions, with standardized disclosures and updates to reflect evolving legal interpretations. • Jurisdictional and legal compliance: Ensuring contracts and operations align with applicable laws and regulatory frameworks, supported by jurisdiction-specific legal assessments and enforceability reviews. • Contract adaptation and migration: Clearly defined processes for updating or migrating contractual obligations to reflect changing laws or regulatory requirements. • Defined dispute resolution frameworks: Clearly structured processes to handle disputes effectively through community or consensus-based approaches.
Regulatory compliance	• Governance, oversight, and change management: Continuous monitoring and rapid implementation of regulatory requirements, supported by structured change-management protocols and regulatory horizon scanning. • Transaction monitoring, blocking, and screening: Effective AML, KYC, and KYT practices embedded into blockchain operations, with adaptive rule sets and real-time alerting to respond to emerging typologies and jurisdictional requirements. • Incident reporting and regulatory escalation: Immediate and transparent responses to compliance incidents, ensuring proactive engagement with regulators, with predefined escalation paths and proactive engagement with relevant regulatory bodies. • Privacy and data protection: Adherence to evolving global and jurisdiction-specific data protection regulations (such as GDPR), with embedded privacy-by-design principles and auditable data handling practices.
Resilience and security	• Node and infrastructure resilience: Diversified and geographically distributed infrastructure. • Decentralization and validator management: Broad, incentivized validator participation with governance safeguards to mitigate concentration risk and single points of failure. • Participation in governance: Transparent contribution to network code and validation practices, with auditable change logs. • Operational monitoring and anomaly detection: Real-time detection with automated alerts and proactive and predefined response protocols. • Code, smart contract, and security audits: Regular independent security audits of smart contracts and system code with public disclosure of findings and remediation timelines. • Oracle security and data redundancy: Robust external data sources with contingency mechanisms. • Key management and cryptography: Strong cryptographic controls, multi-signature authorization, and secure key handling. • Backup, rollback, and recovery: Immediate recovery strategies and failover plans to maintain operational integrity. • Multiparty approvals for sensitive controls: Requiring consensus-driven control procedures for critical operations. • Performance benchmarking and regular load-testing: Ongoing structured stress-testing and scenario-based benchmarking to ensure blockchain performance under varying loads. • Automated failover and redundancy solutions: Clearly defined processes and technical configurations to instantly activate backup nodes, systems, and infrastructure components in the event of failure.
Safeguarding customer assets	• Key management and custody: Secure and auditable custody infrastructure, with clearly defined roles, responsibilities, and liability frameworks for all custodial parties. • Key rotation and emergency asset recovery plans: Defined standards and practices for rapid key rotation and secure asset recovery or reissuance, including contingency protocols for compromised or lost keys. • Access controls and privilege management: Strong operational governance with tiered access controls and role-based permissions to ensure secure asset handling and transaction authorization. • Transaction freezes and circuit-breakers: Clearly defined and transparent intervention mechanisms to protect assets under exceptional circumstances, with predefined criteria and governance oversight. • Comprehensive due diligence and vendor assessments: Conduct thorough initial and ongoing assessments of third-party providers and vendors, including evaluations of operational resilience and cybersecurity posture.
Connectivity and interoperability	• Validator decentralization and incentives: Encouraging diverse and geographically distributed validator participations to enhance network resilience and support blockchain interoperability. • Multi-chain contingency planning: Establish preparedness protocol for asset migration or cross-chain activities, including contingency procedures to maintain continuity in the event of blockchain interoperability failures. • Blockchain interoperability solutions: Leveraging standardized, well-tested cross-platform communication and settlement protocols to ensure seamless and cohesive market operations, with clear governance over protocol updates. • Continuous monitoring of cross-chain asset integrity: Implement real-time validation and reconciliation mechanism to detect and resolve potential duplication, reconciliation errors, or blockchain interoperability issues, with automated alerts and resolution workflows.
Operational scalability	• Scalability and performance solutions: Employ high-throughput processing capabilities and modular scalable infrastructure solutions that dynamically adjust to increasing transaction volumes. • Performance monitoring and benchmarking: Continuously monitor system performance and conduct structured benchmarking to ensure transaction throughput and response times meet evolving market demands. • Transaction prioritization and automation: Deploy efficient, automation for transaction processing and settlement, with prioritization mechanisms to maintain performance under high load conditions. • Migration and redeployment: Maintain rapid response protocols and infrastructure flexibility to enable seamless redeployment or migration of blockchain operations in the event of system stress. • Off-chain reconciliation and record-keeping: Combining blockchain transparency with robust off-chain record-keeping solutions to ensure data accuracy, auditability, and regulatory compliance.

8.3. Key risks and mitigation strategies

While we have covered blockchain-related risks in the previous chapter, we draw upon DASCP principles to inform and underpin the key risks across the value chain and to cover additional risks of security tokens that need to be mitigated on the market or individual firm level:

Table 4: Additional risks and mitigations of security tokens

	Mitigation strategies			
Risk	**Issuers and their advisors**	**Exchanges and venue operators**	**Custodians**	**Investors**
Token corruption/ theft: Unauthorized token transfers or asset theft	Embed emergency freeze/reissuance mechanisms into token smart contracts; appoint and adequately instruct control agents authorized to intervene in security incidents.	Actively monitor transaction flows; rapidly execute token freezes when notified by issuers or authorities; reissue tokens as necessary; maintain clear incident response processes.	Immediately isolate and freeze compromised tokens upon issuer or regulatory instruction; maintain clearly defined procedures for asset recovery or reissuance.	Secure tokens using approved wallets; closely monitor holdings; immediately notify custodians or issuers if unauthorized activity occurs.
Key management: Loss or compromise of cryptographic keys	Require advanced key-security standards (multi-signature, multi-party computation, HSM) in token offerings; provide explicit guidelines and best practices for participants regarding key management.	Implement rigorous key management policies including multi-signature approvals and cold storage solutions; conduct regular security audits; educate users about credential management.	Maintain advanced cryptographic custody infrastructure; enforce multiparty authorization processes; carry robust insurance against key-loss events.	Select adequately secure and capitalized custodians or use secure self-custody (hardware wallets, backups); rigorously follow recommended security practices, including two-factor authentication.
24/7 Operational readiness: Adapting tokenized market structures	Select resilient issuance platforms; establish explicit coordination procedures with custodians and exchanges for rapid incident management and crisis response; perform regular stress and recovery play book tests.	Maintain continuous operational infrastructure (24/7) with redundant systems and real-time monitoring; establish clear escalation and rapid response protocols to manage outages.	Operate robust and redundant 24/7 infrastructure; define clear escalation pathways; continuously monitor operations for anomalies to swiftly respond to incidents.	Prioritize exchanges and custodians with proven continuous availability; participate in and test emergency procedures and escalation processes for rapid incident response.
Interoperability: Asset duplication, theft, or reconciliation errors	Adhere to established token interoperability standards; actively participate in industry standard-setting initiatives.	Develop secure cross-chain trading and settlement functionalities; regularly perform cross-chain reconciliation and maintain strict audit trails to promptly identify discrepancies.	Offer custody services compatible with multiple blockchain standards; systematically audit and reconcile cross-chain asset transfers; defined procedures and controls for technical or custodial interoperability –	Select trading venues and custodians aligned with interoperability standards; actively monitor asset transfers and report anomalies.

Risk	Mitigation strategies			
	Issuers and their advisors	**Exchanges and venue operators**	**Custodians**	**Investors**
			including smart contract wrapping.	
Settlement finality: Ambiguity around transaction finality due to varying blockchain conventions	Clearly define and communicate transaction finality standards at issuance; align token design and issuance platforms with market-established finality conventions.	Ensure immediate and irrevocable trade settlements; monitor blockchains proactively for potential reorganizations or finality disruptions.	Align custody practices with clearly defined market-wide settlement finality standards; maintain authoritative transaction records to quickly resolve settlement ambiguities.	Conduct due diligence and select networks / custodians / exchanges and venue operators with clearly defined and compliant market-wide standards
Price transparency and discovery: Fragmented reporting of pricing data	None in addition to current issuance standards and requirements.	Implement mechanisms to ensure reliable price discovery, incentivized liquidity provisions; establish compliant token listing procedures to publish security token prices across the chains they were issued on, work with control agents to ensure all issuance chains are captured for any specific token traded on the venue.	Provide clients with clear, transparent, and independently verifiable asset crypto valuation tools; facilitate regular reconciliation of pricing data across different market venues.	Prioritize exchanges and issuers providing comprehensive and transparent price disclosures; actively verify transaction data to ensure compliance with best-execution standards.

9. Path forward

The RMF aims to provide a foundational step towards enabling the safe adoption of public blockchains within regulated financial services. We invite market participants, technology providers, and infrastructure operators to provide comments based on their practical experiences and insights regarding effective blockchain risk management practices. The RMF also aims to provide supervisors and regulatory bodies with an overview of how the industry has adopted active risk management practices for blockchain infrastructures.

To further develop the RMF, a dedicated community initiative is planned to curate 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:

- Phase 2 (anticipated in Q3/Q4 2025): Expands the framework to include infrastructure solutions built on top of Layer-1 blockchains, and addresses on-chain digital payment use case, such as stablecoins, related novel risks and mitigants.
- Phase 3 (anticipated in Q1/Q2 2026): Further extends the RMF to incorporate native cryptoasset use cases, commercialization benchmarking, and refines the overarching framework through feedback and iterations via RMF working group and participants.

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

Appendix

Risk and mitigation matrices

Technology risks and mitigations approaches

Table 5:

		Mitigation strategies	
Risk	**Description**	**Public blockchain ecosystems**	**Financial institutions**
Hardware risk			
Limited node diversity	**Description:** Risk that reliance on a public blockchain network with limited node diversity exposes the financial institution to service disruption, degraded performance, or operational failure due to infrastructure centralization. **Driver:** The public blockchain network is operationally dependent on nodes concentrated in a few cloud providers or geographic regions, often due to cost-efficiency, technical maturity, or lack of enforced decentralization standards. **Event:** A major cloud provider outage, regional power failure, or natural disaster leads to simultaneous node failures across the network. **Impact:** Transaction delays, reduced network availability or reliability, inability to settle or validate transactions in a timely manner, and—in severe cases—temporary disconnection from the blockchain or full protocol halt, with potential downstream effects on institutional operations and customer obligations.	**Preventive:** Incentivize diverse node hosting through protocol incentive economics; enforce decentralization thresholds via governance; support multi-platform node deployments; enable and promote non-cloud self-hosting with accessible tooling. **Detective:** Support monitoring node distribution by region and provider; track decentralization metrics and issue alerts on threshold breaches; perform regular resilience and concentration audits. **Corrective:** Provide tools for automated node migration; enable protocol-level failover mechanisms; publish fallback configurations; support fast resynchronization after outages.	**Preventive:** Select blockchains with proven infrastructure decentralization and node distribution; require hosting diversity in vendor and blockchain due diligence; run own nodes in diverse regions or providers. **Detective:** Continuously monitor node health and distribution in supported blockchains; assess validator and infrastructure concentration risks; review decentralization reports and community metrics. **Corrective:** Switch to alternative RPC or data providers during outages; failover plans, including failover to backup nodes or internal infrastructure; adjust exposure or pause transactions until network stability is restored.

		Mitigation strategies	
Risk	**Description**	**Public blockchain ecosystems**	**Financial institutions**
Third-party dependencies	**Description:** Risk that institutional reliance on specific third-party infrastructure components—such as RPC endpoints, node gateways, or indexing services—creates centralized points of technical failure, undermining the resilience of otherwise decentralized blockchain networks. **Driver:** Dependence on a limited set of external infrastructure providers (such as public RPC nodes, API services, block explorers) without redundancy or internal alternatives; lack of direct control over uptime and service configuration. **Event:** A critical provider suffers an outage, degradation, or targeted attack, resulting in the unavailability or malfunctioning of core blockchain connectivity or data services. **Impact:** Inability to submit or verify transactions, halted application workflows, degraded user or system performance, and potential financial or reputational harm due to service-level disruptions.	**Preventive:** Encourage ecosystem diversity in RPC and indexing providers; promote open-source reference implementations and incentivize self-hosting; design protocols to minimize reliance on centralized access points. **Detective:** Monitor usage concentration across third-party infrastructure; track service health and latency patterns; conduct dependency mapping across core services. **Corrective:** Provide fallback endpoints and client failover logic; support emergency relay or data source switching; coordinate with providers to restore critical infrastructure rapidly.	**Preventive:** Use multiple, independent RPC and data providers; evaluate provider risk during vendor onboarding; where no direct counterparty exists, apply architectural and open-source assessments in place of legal assurances; evaluate decentralization as a resilience feature during due diligence; maintain critical components internally or establish partnerships with anchor contributors (such as reliable node operators, indexers); initiate risk-based fallback actions where feasible. **Detective:** Continuously monitor provider uptime, latency, and data consistency; implement service-level alerting; review provider audits and status feeds. **Corrective:** Failover plans including failover to alternate providers or internal nodes; pause transaction flows if data integrity is compromised; reprocess delayed or missed submissions once service is restored.
Software risk			
Code Vulnerabilities	**Description:** Risk that undiscovered flaws in the public blockchain protocol or node software code are exploited, leading to unintended network behavior, security breaches, or operational failures. **Driver:** High complexity of decentralized consensus protocols and networking logic; insufficient test coverage across diverse runtime conditions. **Event:** An attacker exploits a code vulnerability to disrupt node operations, alter consensus behavior, or gain unauthorized access to protocol functions. **Impact:** Loss of network integrity or availability, transaction processing errors, unanticipated forks, or reputational and legal consequences.	**Preventive:** Adopt rigorous code review and testing standards; implement formal verification and fuzzing for critical components; promote modular and well-documented architecture; support multiple competing node implementations. **Detective:** Conduct continuous static and dynamic code analysis; monitor for abnormal network behavior or node crashes; support third-party or community-led vulnerability disclosure programs and audits. **Corrective:** Develop rapid patching and coordinated disclosure processes; maintain emergency release channels and upgrade paths; provide tooling and documentation for safe node recovery or resynchronization.	**Preventive:** Select networks with a strong track record of secure development practices; require evidence of third-party audits and testing; testing components in sandbox / preproduction. environments before integration. **Detective:** Monitor upstream code changes, Common Vulnerabilities and Exposures (CVEs), and protocol disclosures; run infrastructure observability tools to detect irregular performance or behaviors; maintain watchlists of security advisories. **Corrective:** Suspend transaction submission during exploit windows; failover plans including switch to alternative infrastructure if needed; validate ledger state post-incident and implement compensating controls for affected workflows.

		Mitigation strategies	
Risk	**Description**	**Public blockchain ecosystems**	**Financial institutions**
Data corruption	**Description:** Risk that defects in node software or misconfigurations lead to inconsistent interpretation of public blockchain data, resulting in divergent ledger states across the network and requiring recovery through resynchronization or rollback. **Driver:** Bugs in client implementations, version mismatches, or incorrect node configuration parameters affecting block validation or state transitions. **Event:** Nodes process blocks differently due to software or configuration errors, leading to data inconsistencies, temporary forks, or invalid local state. **Impact:** Operational uncertainty, degraded network performance, delayed transaction processing, and the need for corrective actions such as node resynchronization or emergency patches, with potential disruption to dependent services.	**Preventive:** Standardize and document supported node implementations and configurations; incentivize compatibility checks for protocol upgrades; promote use of automated deployment and validation tools. **Detective:** Monitor node behavior and ledger state divergence across nodes; implement network-level consistency checks and telemetry; detect version drift and configuration anomalies in real time. **Corrective:** Support fast node resynchronization and snapshot recovery; release emergency patches or configuration overrides; coordinate network-wide responses to restore consensus and correct state.	**Preventive:** Use only validated node software from trusted sources; maintain configuration management and change control procedures; run test environments for upgrade and configuration validation. **Detective:** Monitor node performance, state alignment, and peer behavior; track logs for signs of desynchronization or state errors; alert on configuration drift or unexpected runtime conditions. **Corrective:** Reinitialize affected nodes using trusted snapshots; verify ledger integrity before resuming operations; escalate and coordinate with protocol maintainers.
Network risk			
Protocol upgrade and hard fork risk	**Description:** Risk that changes to the public blockchain protocol—such as hard forks or scheduled upgrades—are insufficiently coordinated or communicated, leading to operational misalignment, service disruption, or inconsistent network behavior from an institutional perspective. **Driver**: Lack of formal coordination or institutional involvement in upgrading governance; insufficient lead time or visibility into changes. **Event:** Upgrade proceeds without synchronized institutional readiness, causing incompatibility across systems or node failures. **Impact:** Operational disruption; failed or delayed transactions; misaligned ledger views; service outages or reconciliation issues	**Preventive:** Establish transparent upgrade governance and communication processes; provide upgrade timelines and testing resources in advance; support backward-compatible transitions where feasible. **Detective:** Monitor upgrade adoption rates and client version diversity; track ecosystem readiness and relay stakeholder feedback; simulate upgrade conditions on testnets. **Corrective:** Offer emergency client patches and rollback options; coordinate through governance to pause or delay upgrades if needed; maintain compatibility tools and documentation	**Preventive:** Monitor protocol governance forums and roadmaps; test upcoming changes in sandbox / preproduction environments; maintain relationships with protocol teams for early insight and participate in development process (e.g., providing feedback). **Detective:** Track client version status across infrastructure; audit transactions and ledger behavior post-upgrade; assess divergence risk indicators; monitor open-source repositories. **Corrective:** Activate fallback infrastructure aligned with last-known stable state; delay high-value transactions during uncertainty; engage with providers to re-align services and data feeds.

		Mitigation strategies	
Risk	**Description**	**Public blockchain ecosystems**	**Financial institutions**
Finality lag and transaction rollback risk	**Description:** Risk that assumptions regarding the finality of blockchain transactions are invalidated due to delayed block confirmations, temporary forks, or consensus instability—resulting in the reversal or omission of previously confirmed transactions. **Driver:** Public blockchains often rely on probabilistic or delayed finality mechanisms; confirmation depth may be insufficient to guarantee immutability during periods of network latency, congestion, or validator misbehavior. **Event:** A chain reorganization or delayed finalization replaces blocks previously believed to be settled, causing legitimate transactions to be dropped, reordered, or duplicated in dependent systems. **Impact:** Breakdown in transactional consistency, failed or incorrect settlements, operational risk in downstream processes (e.g., reconciliation, custody, trade execution), and potential financial exposure or reputational damage for institutions relying on timely and irreversible ledger updates.	**Preventive:** Implement consensus mechanisms with robust finality models; introduce upgradable finality thresholds; improve propagation speed and fork-choice rules to minimize reorg depth. **Detective:** Monitor block finalization times and fork frequency; track reorg events and near-finality reversals; alert ecosystem participants to prolonged finality delays. **Corrective:** Implement checkpointing or delayed finality confirmation mechanisms; coordinate community response to deep reorgs; support tools to resync or reconcile impacted nodes.	**Preventive:** Use conservative finality thresholds before processing critical transactions; select networks with robust finality models; include reorg tolerance in integration design; implement contractual framework or rulebook addressing finality. **Detective:** Track network finality status and reorg indicators in real time; validate transaction finality depth before downstream processing; monitor for signs of consensus instability. **Corrective:** Flag and reconcile affected transactions after rollbacks; pause settlement operations during instability; coordinate with service providers to restore consistent state.
Protocol governance risk	**Description:** Risk that the governance processes of a public blockchain result in uncoordinated, delayed, or contentious decision-making, leading to protocol fragmentation, unanticipated technical changes, or misalignment with institutional requirements. **Driver:** Decentralized or informal governance mechanisms lacking clear accountability, coordination structures, or consistent upgrade planning; competing stakeholder interests and token-holder voting dynamics. **Event:** A governance dispute, unclear proposal outcome, or abrupt protocol change leads to hard forks, incompatible client behavior, or delayed implementation of necessary technical upgrades. **Impact:** Operational disruption, version fragmentation, diminished predictability of protocol evolution, and elevated integration and maintenance costs.	**Preventive:** Define transparent, inclusive, and technically enforceable governance processes; implement structured proposal and voting systems with clear thresholds; provide timelines and specifications for planned changes. **Detective:** Track governance participation, proposal activity, and voting trends (e.g., pre-voting and other intent signaling methods); monitor signals of contention or low stakeholder engagement; assess upgrade coordination maturity. **Corrective:** Facilitate community interventions to de-escalate governance disputes; support rollback or override mechanisms for unstable upgrade proposals; publish guidance to help nodes maintain network compatibility.	**Preventive:** Engage with governance forums, protocol stewards and key stakeholders to stay informed; participate in governance processes or partner with ecosystem contributors; include governance risk in blockchain selection; plan operational buffers for governance-driven changes. **Detective:** Monitor upcoming governance proposals, voting, and stakeholder alignment; assess likelihood and impact of contentious decisions; subscribe to alerts and governance analytics tools. **Corrective:** Delay system upgrades until proposals stabilize; coordinate internally to adapt to protocol changes; switch or reduce exposure to networks with unstable governance if required; documented failover plan.

		Mitigation strategies	
Risk	**Description**	**Public blockchain ecosystems**	**Financial institutions**
Weakness in consensus design	**Description:** Risk that technical and economic design features of a public blockchain's consensus protocol led to unintended centralization of validation power, undermining the intended distributed infrastructure and creating potential exposure to consensus instability. **Driver:** Protocol-level incentive models or operational constraints that encourage aggregation of mining or staking resources (e.g., economies of scale, yield optimization, low hardware diversity); lack of decentralization safeguards such as staking caps, validator rotation, or slashing mechanisms. **Event:** Consensus power becomes concentrated in a small set of actors due to structural protocol dynamics or implementation design, raising the risk of unintentional dominance or enabling collusion without malicious exploitation. **Impact:** Reduced fault tolerance, systemic reliance on a small subset of validators, potential for network governance capture or transaction processing disruption, and diminished infrastructure resilience for institutions relying on the network.	**Preventive:** Design staking or mining incentives to promote validator diversity; implement safeguards against concentration such as staking caps, validator rotation, or slashing; encourage light node support and diverse node operation. **Detective:** Continuously monitor validator concentration and dominance metrics; track validator behavior for signs of coordination or collusion; audit consensus participation and performance across network epochs. **Corrective:** Enable governance-driven removal or rebalancing of dominant validators; trigger emergency changes to consensus parameters; introduce structural reforms to incentivize broader participation.	**Preventive:** Evaluate decentralization posture and validator distribution during blockchain selection; prefer blockchains with active governance and decentralization incentives; factor validator incentives into risk assessments. **Detective:** Track validator set composition and governance participation trends; monitor network health dashboards and decentralization indices; engage service providers for infrastructure exposure reports. **Corrective:** Reduce reliance on affected networks if validator dominance becomes material; failover plans; escalate governance concerns through formal channels.

		Mitigation strategies	
Risk	**Description**	**Public blockchain ecosystems**	**Financial institutions**
Scalability constraints	**Description:** Risk that a public blockchain cannot efficiently scale under increased transaction demand, resulting in processing delays and performance bottlenecks during periods of high activity. **Driver:** Design trade-offs prioritizing decentralization and security over throughput; protocol limitations on block size, transaction speed, or finality time; lack of dynamic resource allocation mechanisms. **Event:** A spike in transaction volume exceeds the network's capacity to process and confirm transactions within expected timeframes, leading to congestion and reduced service quality. **Impact:** Delayed transaction settlements, increased transaction fees, backlogs in business processes dependent on timely confirmations, and operational disruptions for institutions relying on the network for critical workflows.	**Preventive:** Implement protocol upgrades that improve throughput and finality; support alternative scaling solutions (e.g., rollups, sharding); optimize block propagation and transaction compression techniques; support Layer-2 implementations[6]. **Detective:** Continuously monitor transaction backlog, block utilization, and fee volatility; perform stress testing and benchmarking under simulated high-load conditions; assess network responsiveness to congestion; simulate transaction prices for different scenarios. **Corrective:** Enable dynamic fee adjustment or transaction prioritization mechanisms; activate additional infrastructure capacity or alternate processing layers; coordinate community interventions to mitigate systemic congestion.	**Preventive:** Assess blockchain scalability roadmap and capacity during infrastructure selection and due diligence; select networks with proven transaction throughput under load; design transaction workflows with fallback or batching capabilities. **Detective:** Monitor transaction latency and fee volatility in real time; assess backlog metrics and confirmation delays; use analytics providers to forecast potential congestion events. **Corrective:** Delay non-critical transaction flows during congestion; reroute activity to less congested time windows or alternative networks; initiate migration of workflows if long-term capacity limits are reached.

[6] Layer-2s to be included in next stage of analysis

Information security risks and mitigations approaches

Table 6:

		Mitigation strategies	
Risk	**Description**	**Public blockchain ecosystems**	**Financial institutions**
Risk of data loss			
Private key loss and inadequate key management practices	**Description:** Risk of losing access to public blockchain data (such as digital assets) due to the loss, mismanagement, or destruction of cryptographic keys required to authorize blockchain transactions, with limited or no recovery mechanisms. **Driver:** Direct control of private keys by end users or internal custodians without robust recovery protocols; insufficient key backup strategies; inadequate user training or technical safeguards; lack of custodial redundancy. **Event:** Private keys are accidentally deleted, lost, or compromised, resulting in permanent loss of access to wallets, assets, or smart contract functions. **Impact:** Irrecoverable financial loss; operational disruption; client impact; increased legal and reputational risk, particularly if institutions are unable to safeguard or recover client-controlled digital assets.	**Preventive:** Encourage adoption of secure key management standards; promote use of multi-signature, threshold schemes, or hardware security modules; provide guidance for custodial integrations and backup architecture. **Detective:** Monitor for abnormal signing patterns or transaction behavior; support for tooling for anomaly detection and address tracking. **Corrective:** Support key rotation or revocation mechanisms where feasible; incentivize recovery solutions via social or custodial recovery; coordinate with ecosystem participants.	**Preventive:** Use institutional-grade custody solutions with secure enclave or HSM support; define clear key access roles, responsibilities, and separation of duties; implement encrypted key backups and dual control mechanisms. **Detective:** Continuously monitor for unauthorized access attempts or unusual transaction flows; validate key usage against policy thresholds; audit logs of key interactions and access patterns. **Corrective:** Revoke or isolate compromised keys; restore access through recovery protocols and backup keys; notify affected clients and execute incident response procedures.
Compromised data integrity	**Description:** Risk that an attacker manipulates or injects invalid data into the public blockchain, compromising the integrity of the ledger view across nodes and potentially disrupting consensus or transaction finality. **Driver:** Malicious node behavior, exploitation of protocol vulnerabilities, or network-level attacks (e.g., message tampering, relay hijacking) that alter or desynchronize data propagation across participants. **Event:** Corrupted or manipulated blocks or state data are propagated through the network, leading to inconsistent ledger views, rejection of valid transactions, or the formation of temporary forks.	**Preventive:** Enforce secure peer communication protocols and message validation; promote node diversity; conduct ongoing protocol hardening and upgrade cycles. **Detective:** Monitor for propagation delays, fork anomalies, and ledger inconsistencies; implement consensus integrity alerts; validate incoming block and state data against protocol expectations. **Corrective:** Enable re-synchronization from trusted checkpoints or unaffected peers; isolate and disconnect malicious nodes; coordinate rollback or corrective consensus actions as needed.	**Preventive:** Use off-chain reconciliation processes to verify on-chain state; maintain redundant validation infrastructure; select blockchains with resilient consensus and peer authentication. **Detective:** Continuously monitor ledger consistency across connected nodes; review anomaly alerts from service providers or internal systems; validate transactions against historical snapshots. **Corrective:** Switch to backup infrastructure with verified ledger state; delay or cancel affected transactions; documented failover plans.

		Mitigation strategies	
Risk	**Description**	**Public blockchain ecosystems**	**Financial institutions**
	Impact: Operational disruption, degraded trust in blockchain reliability, potential financial loss from delayed or failed transactions, and reputational or regulatory consequences.		
Cyber risk events			
Consensus attack	**Description:** Risk that an attacker gains disproportionate influence over a public blockchain's consensus mechanism and uses it to disrupt normal network operation, including altering transaction ordering, excluding valid transactions, or rewriting recent blocks. **Driver:** Open validator participation combined with concentration of mining or staking power; lack of node diversity; insufficient protocol-level safeguards to prevent coordinated control of block production or finalization. **Event:** An attacker or colluding group surpasses consensus control thresholds (e.g., 51% of hash power or stake), enabling manipulation of the ledger through transaction censorship, chain reorganization, or double spending. **Impact:** Loss of transaction integrity and finality, operational disruption, potential financial loss for affected parties, and reduced confidence in the reliability of the blockchain.	**Preventive:** Promote decentralized validator participation through incentive structures and staking caps; implement protocol safeguards such as slashing for collusion or malicious behavior; support diverse client and hardware setups to reduce concentration risk. **Detective:** Continuously monitor validator set composition, consensus voting patterns, and block production concentration; alert on signs of collusion, dominance, or validator misbehavior; analyze finality delays or suspicious chain reorganizations. **Corrective:** Activate governance-based removal or suspension of malicious validators; coordinate community-wide forks or protocol overrides; deploy emergency updates to restore network consensus and integrity.	**Preventive:** Select networks with mature decentralization practices and governance safeguards; assess consensus design and economic concentration risks during selection process; diversify exposures across multiple blockchains where feasible. **Detective:** Track validator concentration, network health metrics, and chain reorganizations; leverage third-party analytics to detect anomalies in consensus operations; assess block confirmation depth and timing. **Corrective:** Pause transaction flows during instability; escalate incident response and evaluate exposure to potentially invalidated transactions; migrate assets or workflows to unaffected networks if consensus is compromised.
Denial of service (DOS) attacks	**Description:** Risk that public-facing nodes or consensus participants are targeted by DOS attacks—such as spam transactions—disrupting network availability and degrading transaction processing performance. **Driver:** Public accessibility of public blockchains without network-layer protection; insufficient rate limiting or anti-spam measures in protocol design; open mempool and transaction submission mechanisms that can be abused at scale. **Event:** Attackers generate high volumes of transactions or traffic to overwhelm specific nodes, validators, or mempool	**Preventive:** Implement protocol-level rate limiting, minimum fees, and spam protection; deploy DDoS mitigation at node and API levels; promote decentralized node infrastructure and relay networks. **Detective:** Continuously monitor traffic volumes, mempool activity, and validator throughput; detect spikes in invalid or redundant transactions; trigger alerts for congestion or node responsiveness degradation. **Corrective:** Reroute network traffic to unaffected relays; prioritize legitimate transactions through dynamic fee adjustments or temporary filters; apply	**Preventive:** Assess resilience of blockchain to DoS vectors as part of selection process; establish operational buffers for time-sensitive transactions. **Detective:** Monitor transaction propagation times, mempool congestion, and fee volatility; detect delays in settlement and confirmation flows; leverage third-party monitoring services for real-time alerts. **Corrective:** Postpone or reroute critical transactions; temporarily shift activity to alternate networks or bridges; escalate incident response procedures and coordinate with potentially outsourced infrastructure providers.

		Mitigation strategies	
Risk	**Description**	**Public blockchain ecosystems**	**Financial institutions**
	components, leading to processing backlogs and degraded network responsiveness. **Impact:** Delayed or failed transaction confirmations, increased congestion and fee volatility, potential service outages for dependent applications, and reduced reliability of the blockchain for institutional operations.	emergency configuration changes or block propagation throttling.	
Cryptographic vulnerabilities	**Description:** Risk that future advances in quantum computing or other cryptanalytic techniques compromise the cryptographic primitives used in public blockchains, particularly digital signature schemes, leading to unauthorized access to funds and systemic breakdown of trust. **Driver:** Most public blockchains currently rely on quantum-vulnerable cryptographic algorithms (e.g., ECDSA, EdDSA) for transaction authentication and wallet access; long-term data immutability also exposes past transactions to eventual key recovery. **Event:** A sufficiently powerful quantum computer or novel decryption method is used to derive private keys from public keys, enabling malicious actors to forge transactions, redirect funds, or impersonate network participants. **Impact:** Widespread unauthorized access to assets, collapse of ledger trust assumptions, rapid deterioration in market confidence, and heightened regulatory and institutional scrutiny of blockchain security models.	**Preventive:** Integrate quantum-resistant signature schemes into protocol roadmap; minimize public key exposure by delaying key reveal until transaction execution; promote hybrid cryptography for transitional periods. **Detective:** Monitor for quantum computing research developments and cryptanalytic breakthroughs; conduct periodic cryptographic audits and readiness assessments; track unusual transaction patterns indicating signature forgery. **Corrective:** Deploy emergency upgrade paths to quantum-secure protocols; initiate coordinated key rotation or migration plans.	**Preventive:** Adopt post-quantum cryptographic key management for custody systems; reduce reuse and early exposure of public keys; select blockchain networks with committed post-quantum transition plans. **Detective:** Monitor blockchain analytics for irregular signature schemes or rapid movement from long-dormant wallets; subscribe to industry alerts on cryptographic vulnerabilities; audit transaction signing infrastructure. **Corrective:** Rotate or reissue vulnerable keys under institutional control; quarantine assets or access points suspected of compromise.
Smart contract errors and exploits	**Description:** Risk of permanent adverse consequences due to logical errors or vulnerabilities in immutable blockchain smart contracts. Complexity and immutability make post-deployment corrections difficult, increasing the likelihood of permanent asset losses or operational disruptions. **Driver:** Inherent complexity of blockchain smart contracts; insufficient pre-deployment testing, auditing, or formal verification.	**Preventive:** Rigorous coding standards and audits; comprehensive pre-deployment verification; support upgradeable contract frameworks. **Detective:** Continuous anomaly detection in smart contract execution; active community-driven monitoring and vulnerability reporting. **Corrective:** Emergency contract upgrades or halts through governance; rapid security patch distribution and coordinated disclosures.	**Preventive:** Strict pre-deployment smart contract audits; reliance on pre-audited libraries; upgradeable design for critical contracts; multi-party authorization processes. **Detective:** Real-time monitoring for execution anomalies; continuous performance tracking; regular security disclosures review.

		Mitigation strategies	
Risk	**Description**	**Public blockchain ecosystems**	**Financial institutions**
	Event: Undetected errors or vulnerabilities lead to unexpected behavior, permanent transaction failures, unauthorized asset transfers, or critical operational disruptions post-deployment. **Impact:** Irrecoverable asset loss, disruption of smart contract functions, erosion of operational reliability, and loss of stakeholder trust.		**Corrective:** Rapid activation of predefined emergency halts or patches; asset isolation and stakeholder notification; swift migration to secure contract versions.
Risk of data privacy breach / confidentiality mismanagement			
On-chain exposure of sensitive or confidential data	**Description:** Risk that personal, confidential, or regulated information is recorded on a public blockchain in an immutable and universally accessible form, resulting violation of privacy and subsequent legal or compliance violations. **Driver:** Inadvertent or uninformed use of public blockchain infrastructure for transmitting or storing sensitive data; lack of effective data minimization, encryption, or redaction controls at the application layer. **Event:** Personal data (e.g., identifiers, financial details, private messages) or institutional secrets are published to a public ledger, either directly or through metadata leakage, making them permanently visible and searchable. **Impact:** Irreversible privacy violations, breach of data protection regulations (e.g., GDPR), reputational harm, enforcement actions, and long-term exposure of individuals or institutions to misuse or profiling.	**Preventive:** Promote best practices for off-chain data handling and encryption at the application layer; support architecture models (e.g., rollups, hybrid chains) that separate transactional and data storage layers. **Detective:** Deploy network-level scanning tools and indexing services to detect common data formats or known identifiers; encourage community-led audits and flagging of inappropriate data uploads; monitor for metadata leakage patterns. **Corrective:** Facilitate referencing alternatives through smart contracts or proxy mappings; issue advisories and remediation guidance to ecosystem developers.	**Preventive:** Enforce strict internal controls prohibiting transmission of sensitive data on-chain; use privacy-preserving technologies such as zero-knowledge proofs or off-chain encryption and hashing; select platforms that support compliant data segregation. **Detective:** Monitor application inputs and transaction payloads for inadvertent disclosure; implement automated detection of personal or regulated data in transaction metadata; conduct regular privacy audits of blockchain integrations. **Corrective:** Migrate business logic away from affected contracts or addresses; notify stakeholders; replace or mask exposed data references where feasible and document exposure incidents in internal risk reporting.
De-anonymization through public transaction data analysis	**Description:** Risk that transaction patterns and pseudonymous addresses on public blockchains are analyzed to reveal identities of individuals or institutions, undermining privacy and enabling surveillance or profiling. **Driver:** Inherent transparency of public blockchain ledgers enables advanced analytics, clustering techniques, and off-chain data correlation; lack of effective privacy-preserving mechanisms at the protocol or application layer.	**Preventive:** Support development and integration of privacy-preserving transaction mechanisms (e.g., zero-knowledge proofs, or stealth addresses); enable optional confidentiality layers at the protocol level.	**Preventive:** Use privacy-preserving wallets and transaction methods where permitted; avoid address reuse and maintain operational separation between institutional identities and transaction endpoints; implement transaction aggregation or timing strategies.

		Mitigation strategies	
Risk	**Description**	**Public blockchain ecosystems**	**Financial institutions**
	Event: Adversaries or third parties link addresses to identifiable entities through transaction flows, timing analysis, IP tracking, or integration with external datasets (e.g., exchanges, social platforms). **Impact:** Unintended exposure of client behavior, financial relationships, or business operations; privacy violations; potential regulatory concern; erosion of trust.	**Detective:** Monitor for emerging de-anonymization tools, address clustering methods, and linkage analysis platforms; assess data leakage vectors via transaction graph analytics; track effectiveness of obfuscation features. **Corrective:** Promote migration to enhanced privacy-enabled transaction formats; release protocol updates supporting stronger pseudonymity primitives; enable users to rotate addresses.	**Detective:** Audit transaction patterns for behavioral fingerprinting risks; monitor public analytics platforms for clustering of institutional addresses; assess exposure through off-chain integrations such as exchanges or service providers. **Corrective:** Update key and address management policies; rotate on-chain identities or intermediaries; consider shifting to networks or layers with native privacy support if institutional requirements are not met.
Risk of improper data access			
Misuse of transaction data and roles	**Description:** Risk that public visibility of blockchain transactions or privileged roles (e.g., transaction relayers or node operators) enable bad actors to exploit advance knowledge of transactions. **Driver:** On-chain transaction flows, wallet activity, or certain instructions are visible on public blockchains before final settlement or execution; lack of internal controls around access to client trading data or custody operations. **Event:** An insider leverages transaction visibility or privileged access to profit from a client's trade, replicate a profitable strategy, or misappropriate digital assets prior to or during execution. **Impact:** Direct financial losses for clients, breach of fiduciary or contractual obligations, reputational harm to the institution, and potential regulatory or legal consequences due to failure to prevent abuse of market-sensitive data.	**Preventive:** Encourage development of protocol features that delay transaction visibility until finalization (e.g., commit-reveal schemes, encrypted mempools); encourage alternatives to account-based data architectures; support best practices for transaction privacy at the application layer. **Detective:** Facilitate integration with monitoring tools that analyze mempool activity and ordering anomalies; promote community research on front-running detection and mitigation techniques. **Corrective:** Enable opt-in reordering protections or fair sequencing mechanisms at the protocol level; provide documentation and tooling for relayers and developers to implement anti-front-running measures.	**Preventive:** Perform due diligence on blockchain MEV mitigation features**,** implement transaction submission strategies that reduce exposure (e.g., batching, submission via private relays); maintain strict controls on internal access to transaction intent and client trading data. **Detective:** Monitor execution timing, slippage, and sequencing anomalies for signs of front-running or misuse; review internal activity logs for conflicts of interest. **Corrective:** Trigger internal investigations and freeze impacted accounts or operations; engage service providers or ecosystem governance to address persistent ordering manipulation; update execution policies and client disclosures as needed.

		Mitigation strategies	
Risk	**Description**	**Public blockchain ecosystems**	**Financial institutions**
Privilege misconfiguration	**Description:** Risk that improperly configured permissions within smart contracts or decentralized applications allow unauthorized actions or disruptions. Misconfigured privileges enable unauthorized parties to escalate access, conduct unauthorized transactions, or disrupt normal operations, causing financial and reputational harm. **Driver:** Overly permissive or incorrectly assigned smart contract permissions; insufficient oversight or complexity of decentralized governance. **Event:** Unauthorized exploitation of privilege misconfigurations leads to operational disruptions, unauthorized transactions, or compromised asset integrity. Impact: Unauthorized transfers, operational disruptions, increased regulatory scrutiny, loss of trust, and potential financial damage.	**Preventive:** Automated privilege-linting integrated in deployment processes; clearly defined permission standards and best practice documentation. **Detective:** Continuous monitoring and auditing of smart contract privilege use; community oversight mechanisms for detecting unauthorized privilege escalations. **Corrective:** Coordinated smart contract updates to rectify misconfigurations promptly.	**Preventive:** Internal privilege audits and controls aligned to least privilege; continuous refinement of role-based and attribute-based access policies. **Detective:** Real-time monitoring of privilege access patterns; periodic reviews of privilege assignments and access logs. **Corrective:** Immediate revocation and escalation of compromised privileges; transparent stakeholder communications and remediation; prompt reconfiguration and redeployment of affected contracts or applications.

Financial crime risks and mitigation approaches

This section consolidates mitigation strategies for financial crime risks due to the substantial overlap in control measures, focusing on shared preventive, detective, and corrective practices for both public blockchain ecosystems and financial institutions.

Table 7:

		Mitigation strategies	
Risk	**Description**	**Public blockchain ecosystems**	**Financial institutions**
Risk of money laundering and terrorism financing			
Obfuscation via complex multistep transfers[7]	**Description:** Risk that the use of public blockchains enables the layering of transactions in ways that obscure the origin and flow of funds, complicating monitoring and compliance efforts. **Driver:** Use of decentralized exchanges, cross-chain bridges, mixers, and smart contract automation without identity linkage or consistent transaction metadata. **Event:** Transactions are routed through multiple on-chain hops, services, and protocols to intentionally or unintentionally reduce the traceability of fund origin and counterparties. **Impact:** Reduced effectiveness of transaction monitoring and anti-money laundering (AML) measures; increased difficulty in meeting regulatory compliance obligations and identifying suspicious activity.	**Preventive:** Promote open transaction transparency standards, encourage integration with compliance analytics, and facilitate ecosystem-wide adoption of opt-in compliance tooling. **Detective:** Enable accessible blockchain data structures to support analytics, anomaly detection, and community-based transaction pattern monitoring. **Corrective:** Provide mechanisms for optional tagging, rapid asset isolation tools, and community-driven response frameworks.	**Preventive:** Implement robust KYC/KYT procedures, strictly restrict interactions to whitelisted counterparties, and integrate transaction profiling tools. **Detective:** Conduct real-time analytics monitoring of transaction behaviors for suspicious activity and anomalous patterns. **Corrective:** Rapidly freeze implicated assets, escalate internally, initiate forensic investigations, and promptly report incidents to regulatory bodies.
Illicit fund(s) integration[7]	**Description:** Risk that weaknesses in customer due diligence and transaction monitoring during asset issuance, trading, and using on- and off-ramps enable the integration of illicit funds into the financial system via blockchain-based assets. **Driver:** Inconsistent or insufficient application of AML/CFT measures at critical control points such as token		

[7] Risk of money laundering and terrorism financing mitigation strategies consolidated

		Mitigation strategies	
Risk	**Description**	**Public blockchain ecosystems**	**Financial institutions**
	generation, listing, or trading — particularly in decentralized or cross-border environments. **Event:** Illicit actors acquire and exchange tokens through on-chain or off-chain venues to obscure the origin of funds and introduce them into legitimate financial flows. **Impact:** Reduced effectiveness of AML frameworks, increased difficulty in tracing fund provenance, heightened legal and regulatory exposure, and potential erosion of trust in blockchain-based financial products.		
Terrorist financing[7]	**Description:** Risk that public blockchains are used to facilitate terrorist financing when effective AML/CFT controls are not applied at access points such as token issuance platforms, exchanges, or wallet providers. **Driver:** Public blockchains allow pseudonymous participation and may support privacy-enhancing tools (such as mixers, privacy coins, stealth addresses), which—if not monitored—can hinder the traceability of fund flows. **Event:** Terrorist financiers leverage public blockchains to transfer or conceal funds, exploiting gaps in oversight at on- and off-ramps or within decentralized protocols lacking embedded compliance measures. **Impact:** Regulatory breaches, failure to detect prohibited transactions, legal and reputational exposure for institutions interacting with tainted assets, and heightened scrutiny of blockchain-based financial services.		
Risk of sanctions violation			
Sanctions evasion risk[8]	**Description:** Risk that sanctioned individuals or entities use public blockchains to bypass international financial restrictions, exposing institutions interacting with these networks to regulatory non-compliance and enforcement actions.	**Preventive:** Encourage address-screening mechanisms and transaction metadata standards, support third-party compliance integrations.	**Preventive:** Perform real-time sanctions screening and rigorous due diligence during onboarding; screening of jurisdiction watchlists; limit transactions to vetted wallets and counterparties.

[8] Risk of sanctions violations mitigation strategies consolidated

		Mitigation strategies	
Risk	**Description**	**Public blockchain ecosystems**	**Financial institutions**
	Driver: Global, permissionless access to blockchain infrastructure without embedded identity verification; lack of consistent screening at decentralized access points such as smart contracts, peer-to-peer transfers, or decentralized exchanges. **Event:** Sanctioned actors transact via public blockchains using pseudonymous wallets, privacy-enhancing tools, or indirect intermediaries to move or convert assets, avoiding detection by traditional screening systems. **Impact:** Unwitting facilitation of prohibited transactions, breach of sanctions regulations, exposure to financial penalties, reputational harm, and potential regulatory scrutiny for institutions engaged with or building on such networks.	**Detective:** Maintain transparent transaction data access and facilitate analytics for detecting sanctioned address interactions. **Corrective:** Foster community-led flagging of suspicious transactions and rapid intervention protocols.	**Detective:** Continuously monitor transaction flows, leverage blockchain analytics, and maintain watchlists to detect sanctioned interactions. **Corrective**: Swiftly freeze implicated assets, halt transactions associated with sanctioned activities, escalate internally, and notify regulatory authorities.
Insufficient screening of on-chain transactions and counterparties [8]	**Description:** Risk that the institution is unable to effectively detect or prevent prohibited activity due to limitations in transaction screening and counterparty identification on public blockchains. **Driver:** Pseudonymous nature of public blockchain transactions; absence of built-in identity verification or sanctions screening in decentralized protocols; limited integration of blockchain analytics or risk scoring into institutional compliance processes. **Event:** Sanctioned individuals or entities conduct transactions through the blockchain without detection, interacting with wallets, smart contracts, or token services used by the institution or its clients. **Impact:** Execution of prohibited transactions, inability to reverse or freeze illicit activity, breach of regulatory compliance obligations, legal exposure, and reputational damage.		

		Mitigation strategies	
Risk	**Description**	**Public blockchain ecosystems**	**Financial institutions**
Risk of bribery and corruption			
Crypto-facilitated bribery	**Description:** Use of pseudonymous, cross-border token transfers to conceal improper payments to public officials or corporate insiders. **Driver:** Anonymity and international transfers facilitate concealed bribery. **Event:** Officials or executives accept token bribes, potentially bypassing traditional financial controls. **Impact:** Undetected bribery, legal exposure under anti-corruption statutes, reputational damage, and potential asset freezes.	**Preventive:** Provide infrastructure to integrate analytical tools. **Detective:** Enable analytics and monitoring tools to detect unusual or anomalous payment patterns across the blockchain. **Corrective:** Support community-based governance protocols to address bribery-oriented concerns	**Preventive:** Implement multi-party authorization processes for high-risk transactions; politically exposed person scans; conduct enhanced due diligence to detect anomalous behaviors. **Detective:** Utilize specialized blockchain analytics tools to flag unusual payments indicative of bribery or corruption risks. **Corrective:** Rapidly freeze affected transactions or accounts, conduct internal investigations, escalate incidents to compliance teams, and report to authorities.
Risk of KYC / transaction monitoring control failures			
Absence of KYC and adequate monitoring	**Description:** Pseudonymity allows users to transact without formal identification, increasing exposure to money laundering, fraud, and sanction breaches. **Driver:** Direct peer-to-peer transfers and onboarding flows that lack mandated KYC checks. **Event:** An unidentified user acquires, trades, or redeems tokens through the institution's services without passing appropriate due diligence controls. **Impact:** Regulatory penalties; compliance breaches; increased risk of illicit financial activity.	**Preventive:** Encourage adoption of optional identity verification standards and transaction monitoring integrations at the network and smart contract level. **Detective:** Facilitate ecosystem-wide access to real-time blockchain transaction data and compliance analytics tools. **Corrective:** Enable decentralized, community-driven flagging and incident reporting mechanisms for suspicious activities.	**Preventive:** Implement strict onboarding procedures involving robust identity verification (KYC/KYT); adopt comprehensive transaction monitoring solutions. **Detective:** Conduct continuous real-time transaction audits and monitoring, employing analytics tools to detect suspicious transaction patterns. **Corrective:** Immediately suspend implicated transactions, quarantine impacted accounts, initiate internal compliance reviews, escalate incidents, and report to regulatory bodies.

Business continuity risks and mitigations approaches

Table 8:

		Mitigation strategies	
Risk	**Description**	**Public blockchain ecosystems**	**Financial institutions**
Inadequate business continuity planning/event management			
Inadequate business continuity and recovery planning	**Description:** Risk of inability to maintain operations or recover critical services in a timely manner following a disruption affecting a public blockchain. **Driver:** Limited integration of public blockchain-specific failure scenarios into the institution's business continuity management (BCM) framework; absence of coordinated recovery protocols with third-party infrastructure or service providers; reliance on external decentralized networks without clear fallback options. **Event:** A network disruption (e.g., blockchain halt, validator outage, or infrastructure failure) occurs, and the institution lacks predefined procedures, resources, or governance to switch to alternative systems or recover operations within acceptable timeframes. **Impact:** Inability to process or verify transactions, delays in settlement or asset transfers, breach of client SLAs, regulatory non-compliance, and reputational damage due to prolonged service interruption.	**Preventive:** Encourage open communication channels with ecosystem participants on upgrade schedules and fault scenarios; promote modular node architecture and stateless client options to support rapid redeployment. **Detective:** Monitor network health and validator availability in real-time; support open benchmarking and stress testing of protocol components. **Corrective:** Coordinate community-driven recovery documentation; provide tooling for rapid node state rehydration or resync after disruption.	**Preventive:** Integrate blockchain-specific scenarios into enterprise business continuity management planning; establish clear fallback systems and multi-network access strategies; operate institutional nodes or infrastructure components to reduce reliance on third-party providers; validate recovery strategies via real-time protocol monitoring and governance participation. **Detective:** Continuously assess network resilience indicators and dependency risks across connected service providers. **Corrective:** Activate pre-defined contingency playbooks including failover to alternate infrastructure, re-routing of workflows, or protocol migration plans; engage in protocol coordination (e.g., via working groups, open governance calls) to support timely network recovery.

		Mitigation strategies	
Risk	**Description**	**Public blockchain ecosystems**	**Financial institutions**
Dependency on external governance for network recovery	**Description:** Risk that the institution cannot influence or coordinate recovery efforts during a public blockchain disruption due to reliance on decentralized governance processes with no formal escalation path. **Driver:** Public blockchains are maintained by distributed communities with asynchronous or informal governance mechanisms that delay decision-making during emergencies. **Event:** A protocol bug, security incident, or liveness failure occurs, and the community requires time to coordinate and implement a fix or soft fork. **Impact:** Extended downtime, inability to process transactions, reputational and legal exposure due to failure to meet obligations.	**Preventive:** Foster transparent governance frameworks with clear emergency processes; encourage diverse participation and proactive coordination mechanisms. **Detective:** Monitor protocol governance forums and proposal pipelines for recovery-related activity; track responsiveness to incidents. **Corrective:** Support tooling for expedited patch distribution and node upgrade coordination; enable voluntary rollbacks or soft forks through opt-in mechanisms.	**Preventive:** Conduct due diligence on governance structures and responsiveness of selected networks; maintain relationships with ecosystem stakeholders to stay informed; directly participate in governance to strengthen resilience in the absence of centralized escalation paths. **Detective:** Track network governance activity and detect signs of delayed or contested incident responses. **Corrective:** Activate fallback infrastructure or multi-network contingency strategies; initiate internal communication and client management procedures during extended recovery periods.

Third party risks and mitigations approaches

Table 9:

		Mitigation strategies	
Risk	**Description**	**Public blockchain ecosystems**	**Financial institutions**
Third party management control failure			
Reliance on public blockchains	**Description:** Reliance on public blockchain networks operated by decentralized nodes introduces risks due to limited direct control and accountability, particularly through traditional contracting mechanisms. **Driver:** Decentralized operational model, absence of enforceable SLAs or contractual performance guarantees. **Event:** Network disruption, consensus failure, or performance degradation occurs, leading to operational impacts. **Impact:** Operational disruption, delays in settlement or transaction processing, breaches of client obligations, regulatory scrutiny, and potential reputational harm.	**Preventive:** Encourage broad validator decentralization and diversity, establish transparent governance structures and clear upgrade processes, and regularly publish network performance metrics. **Detective:** Continuously monitor network health indicators including validator distribution, throughput levels, consensus liveness, and latency; track governance responsiveness and protocol upgrade activities. **Corrective:** Provide governance coordination mechanisms for rapid response, facilitate community-driven corrective actions and patches.	**Preventive:** Proactively develop and deploy multi-chain architectures or failover systems, embed blockchain-failure scenarios into business continuity planning, and maintain documentation of failover plans. **Detective:** Continuously monitor blockchain performance metrics, validator decentralization, and network health analytics. **Corrective:** Initiate immediate failover to alternative blockchains or backup infrastructure, promptly communicate impacts to clients, and execute pre-documented recovery processes.
Inability to effectively manage providers	**Description:** Risk of relying on external blockchain infrastructure providers (e.g., oracles, node gateways, wallet services) who introduce service disruptions, compliance failures, or performance degradation due to insufficient oversight, limited accountability, or non-traditional governance structures. **Driver:** Dependence on specialized service providers—some of which operate in a decentralized or non-corporate structure—limits the applicability of traditional third-party risk management approaches. **Event:** A critical service provider fails, is compromised, or acts outside expectations, resulting in loss of functionality, data integrity issues, or institutional non-compliance. **Impact:** Operational disruption, failed or delayed transactions, legal or regulatory exposure, and increased difficulty in replacing or remediating affected services.	**Preventive:** Promote standardized transparency practices for decentralized service providers; incentivize disclosure of operational status, governance structure, and resilience planning. **Detective:** Encourage community-led monitoring and evaluation of oracle networks, node services, and other key infrastructure contributors; support open reporting of outages or compliance failures. **Corrective:** Facilitate coordination mechanisms or forums to replace or deprecate underperforming services; provide fallback tools or community-supported alternatives.	**Preventive:** Conduct rigorous due diligence on third-party blockchain service providers; establish appropriate SLAs where available; favor providers with clearly defined governance and risk frameworks; diversify across multiple providers to reduce dependency. **Detective:** Continuously monitor provider performance, uptime, and compliance posture; assess adherence to contractual or public service-level commitments. **Corrective:** Activate contingency plans and pre-identified replacement providers in the event of failure; document and regularly update exit strategies for critical service relationships.

Legal risks and mitigation approaches

Table 10:

		Mitigation strategies	
Risk	**Description**	**Public blockchain ecosystems**	**Financial institutions**
Lack of attributable counterparty (ORX Level-2 risk category - Mishandling of legal processes)	**Description:** Risk that the absence of a clearly identifiable and accountable legal counterparty limits the ability to enforce obligations, resolve disputes, or ensure service delivery when failures or disruptions occur. **Driver:** Public blockchains operate without a central legal entity responsible for performance or accountability; governance is decentralized or pseudonymous; no general contractual relationships or service-level agreements exist between the actors in a public blockchain ecosystem. **Event:** A service disruption, protocol failure, or dispute arises, and affected users cannot identify a legally recognized counterparty for recourse, enforcement, or liability. **Impact:** Inability to resolve disputes or enforce claims; legal and regulatory uncertainty; loss of user trust and institutional adoption barriers; increased exposure to jurisdictional risk and systemic enforcement gaps.	**Preventive:** Promote clear governance frameworks and community governance escalation mechanisms. **Detective:** Maintain transparent logs of governance activity and protocol changes; monitor developments related to accountability structures and jurisdictional relevance. **Corrective:** Support opt-in dispute resolution mechanisms (e.g., on-chain arbitration); facilitate community-led response pathways to resolve incidents.	**Preventive:** Conduct legal and governance due diligence; identifying and utilizing contractable counterparties for ancillary services where possible, assess view of prudential regulator **Detective:** Participate in or monitor protocol governance and development activity; track operational performance of key contributors; evaluate ongoing risk exposures based on ecosystem behavior and responsiveness. **Corrective:** Document and disclose control measures to regulators.
Risks that arise from contractual rights / obligations failure	**Description:** Risk of errors or off-chain disputes when using smart contracts, which can act as an execution tool for contractual obligations. **Driver:** Complex logic, limited pre-deployment legal review **Event:** A latent bug, drafting error, or false implementation causes a smart contract to perform contrary to the legal intentions, and the immutability of the chain delays or prevents correction. **Impact:** Permanent asset loss, stalled business processes, costly legal disputes, and reputational damage.	**Preventive:** Encourage best practices and standardized, audited templates and promote independent security and legal reviews. **Detective:** Support on-chain metadata and event logging that simplify continuous monitoring of contract execution and anomaly detection. **Corrective:** Publish tooling for rapid migration to patched contract versions.	**Preventive:** Perform rigorous multidisciplinary audits of smart contracts; favor upgrade-enabled designs and vetted code libraries. **Detective:** Monitor smart contract events versus expected business logic and track external vulnerability disclosures. **Corrective:** Documented failover plan; pause interactions, migrate assets to replacement contracts, notify stakeholders, and pursue legal remediation.

Transactions and process execution risks and mitigations approaches

Table 11:

		Mitigation strategies	
Risk	**Description**	**Public blockchain ecosystems**	**Financial institutions**
Processing/ execution failure relating to clients and products	**Description:** Irreversible blockchain transactions amplify losses from user or technical errors. **Driver:** Weak front-end validation, unclear user interface cues, or contract parameter mishandling. **Event:** A client submits an erroneous transfer that cannot be rolled back. **Impact:** Permanent asset loss, customer complaints, and reputational damage.	**Preventive:** Define strict transaction-format standards and reference user interface code; developing and encouraging best practices for data checks. **Detective:** Facilitating anomaly alerts for technical errors. **Corrective:** Rapid governance responses to explore "pause"/freeze hooks where applicable.	**Preventive:** Require dual approval or strong user confirmation for high-value transfers; train users on common errors. **Detective:** Flag transactions breaching preset limits. **Corrective:** Run off-chain remediation (client notice, compensating payment) or insurance claims where contractual, re-issuance where applicable.

Data management risks and mitigations approaches

Table 12:

		Mitigation strategies	
Risk	**Description**	**Public blockchain ecosystems**	**Financial institutions**
Inadequate data architecture / IT infrastructure	**Description:** Transparent nature of public blockchains creates risks of inadvertent leaks of personal, confidential, or sensitive institutional data. **Driver:** Insufficient safeguards, lack of anonymization and privacy practices at protocol or node-level architecture. **Event:** Personal data, banking secrets, or proprietary trade information inadvertently disclosed or publicly visible. **Impact:** Breaches of data privacy laws (e.g., GDPR), compromised confidentiality, and reputational damage.	**Preventive:** Provide standards and best practices for data privacy and anonymization; encourage privacy-preserving tooling integration. **Detective:** Facilitate transparent monitoring of data leakage risks; publish anonymization efficacy metrics. **Corrective:** Support community-led privacy enhancements; enable emergency protocol adjustments to mitigate inadvertent disclosures.	**Preventive:** Perform thorough risk assessments on data exposure risks of specific public blockchain use-cases; adopt privacy-preserving technologies, hybrid on/off-chain data storage, and private batch-processing methods. **Detective:** Continuously monitor data interactions; utilize analytics for early warning of breaches. **Corrective:** Implement documented failover plans; quarantine sensitive data; execute predefined incident response and reporting protocols.

Glossary

Below are standard definitions for terminology used throughout the document.

Term	Definition
51% attack	When a malicious actor compromises more than half of the validators of a blockchain infrastructure.
Atomic settlement	Instant exchange of two assets, such that the transfer of one occurs only upon transfer of the other one.
Blockchain	A blockchain is a distributed digital ledger that is immutable for the individual user that stores data in "blocks" linked together chronologically using cryptographic tools.
Bridge	Technique used to transfer assets between ecosystems by, typically, creating a synthetic representation of a blockchain-specific asset on a different blockchain and locking the original asset while the representation is used.
Bug bounty program	Initiative where developers offer rewards to ethical hackers to find and report security vulnerabilities.
Consensus mechanism	The process by which data validators on a blockchain infrastructure agree on the state of a distributed ledger.
Digital asset	Digital representation of value that can be used for payment or investment purposes or to access a good or service.
Digital tokens	Entries in a database that are recorded digitally and that can contain information and functionality within the token itself
Digital twin	An electronic controllable record representing an asset that has been immobilized on another system of record, and reconciled with that original system of record to ensure ownership is reflected precisely.
Digital wallet	An application or interface that allows users to interact with a blockchain infrastructure for transactions e.g., in stablecoins or other tokens.
Distributed ledger	Database that runs on computers around the world; it is shared and synchronized among network participants so there is no single point of failure.
Distributed ledger technology (DLT)	The processes and related technologies that enable nodes in a network (or arrangement) to securely propose, validate and record state changes to a synchronized ledger that is distributed across the network's nodes.
Financial market infrastructure (FMI)	A multilateral system among participating institutions, including the operator of the system, used for the purposes of clearing, settling or recording payments, securities, derivatives or other financial transactions.
Hardware wallet	Noncustodial physical single-purpose storage devices.
Interoperability	The technical, semantic and business compatibility that enables a system or mechanism to be used in conjunction with other systems; allows participants in different systems to conduct, clear and settle transactions across systems without participating in multiple systems.
Linting	Automated process of analyzing smart contracts to identify and flag potential privilege misconfigurations or permission-related issues.
Ledger	A ledger is a record-keeping system used to track financial transactions.

Term	Definition
Ledger fork	Split in a single blockchain or distributed ledger into two or more independent paths, each maintaining a valid but different history of transactions. Can be the result of disagreement among network participants about the ledger's rules or when two blocks are created simultaneously, which is usually resolved by the network.
Memory pool	Holding area where in a blockchain network where unconfirmed transactions are stored prior to being included in a block.
Off-chain	Any activity that takes place outside blockchain infrastructure.
On-chain	Any activity that takes place on blockchain infrastructure.
Operator	Those who can create new data blocks and interact with a blockchain for that purpose.
Oracle	A service that provides outside ("off-chain") information for use within a public blockchain ecosystem (e.g., for a smart contract).
Private key	A private key is a secret cryptographic code that is used to decrypt data encrypted by its corresponding public key, or to create a digital signature. It forms one half of a public-private key pair.
Public blockchain ecosystem	A decentralized network of nodes that operates on an open and transparent blockchain infrastructure, allowing anyone to participate as a user, validator, or developer.
Public key	A cryptographic code that can be openly shared and is used to encrypt data or verify digital signatures. It forms one half of a public-private key pair, where the corresponding private key is kept secret and used for decryption or creating digital signatures.
Public permissioned blockchains	Fully open networks where anyone can read data, submit transactions, or participate in validation without prior approval.
Public permissionless blockchains	Retain public visibility of data and activity but restrict participation in key roles (such as validation or governance) to approved or identified entities.
Relayer	Intermediary that facilitates transmission of data or transactions between parties and blockchain networks.
Security token	A token that satisfies the applicable regulatory definition of a security or financial instrument under local law.
Smart contract	Computer program that is stored and runs on a blockchain infrastructure; it may incorporate the elements of a binding contract.
Stablecoin	Privately issued, digital token that aims to maintain a stable value relative to a peg specified by a reference asset(s) and designed to minimize value fluctuations relative to these reference assets(s).
Staking	The process of locking up blockchain assets for a set period to help secure and support the operation of a blockchain infrastructure, typically in return for a share of transaction fees or other incentives.
Tokenization	The process of generating and recording a digital representation of traditional assets on a blockchain infrastructure.

Term	Definition
Tokenized security	A token that represents an underlying security or financial instruments issued on a different platform (such as a traditional CSD or registrar).
Transaction	A record of an event or exchange, such as the transfer of cryptocurrency or data, which is cryptographically signed and submitted to the blockchain infrastructure for validation and inclusion.
Validator	An entity that verifies data for a blockchain.
Wallet	Application or device for storing private keys.

About Global Blockchain Business Council

Global Blockchain Business Council (GBBC) is the trusted non-profit association for the blockchain, digital assets, and emerging technology community. Founded in 2017 in Davos, Switzerland, GBBC comprises more than 500 institutional members and 284 Ambassadors across 124 jurisdictions and disciplines.

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

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