

Institutional Interoperability:

How Financial Institutions Navigate a Multichain World

WHITE PAPER WITH INSIGHTS FROM



Deutsche Bank



mastercard



NORTHERN
TRUST



PRODUCED BY



METRIKA

CONTENTS

EXECUTIVE SUMMARY	1
INTRODUCTION: TOO MANY BLOCKCHAINS	4
INTEROPERABILITY REQUIREMENT: FLEXIBLE COMPLIANCE	6
INTEROPERABILITY REQUIREMENT: FLEXIBLE SECURITY	7
BLOCKCHAIN SECURITY CONCERNS.....	7
CONSENSUS PROTOCOL THREATS.....	8
SMART-CONTRACT THREATS.....	9
SOLUTIONS: MITIGATING SECURITY RISK AT MULTIPLE LEVELS.....	10
CODE AUDITS.....	10
CONFIGURABLE SECURITY POLICIES.....	10
NETWORK TOPOLOGY.....	11
SOLUTIONS: OPEN-SOURCE TECHNOLOGY & MODULARITY.....	12
INTEROPERABILITY REQUIREMENT: PRIVACY	13
INTEROPERABILITY REQUIREMENT: RISK ASSESSMENT	14
INTEROPERABILITY REQUIREMENT: TRANSPARENCY & MONITORING	18
GAS-FEE ABSTRACTION.....	18
INTEROPERABILITY REQUIREMENT: SCALABILITY	21
SOLUTIONS: NETWORK ADAPTABILITY.....	21
SOLUTIONS: NETWORK TOPOLOGY.....	23
CONCLUSION	25
SPOTLIGHT: CITI	27
SPOTLIGHT: DEUTSCHE BANK	32
SPOTLIGHT: MASTERCARD	36
SPOTLIGHT: NORTHERN TRUST	40
SPOTLIGHT: CENTRIFUGE	45

CONTRIBUTORS



BISER DMITROV
GLOBAL HEAD, DLT CENTER OF EXCELLENCE
CITI



ALTIN HOXHA
HEAD OF DIGITAL ASSETS PLATFORM ENGINEERING
CITI



CAROLINE LIN
DIGITAL ASSETS ASSOCIATE
CITI



SORCHA SULLIVAN-WILLIAMS
SENIOR VP, DIGITAL ASSETS PRODUCT MANAGER
CITI



BOON-HIONG CHAN
INDUSTRY APPLIED INNOVATION LEAD
HEAD, APAC MARKET & TECHNOLOGY ADVOCACY
DEUTSCHE BANK



COLIN DELARSO
CRYPTO PRODUCT PARTNERSHIPS
& COMMERCIALIZATION LEAD
MASTERCARD

CONTRIBUTORS



OSKAR DURIS
GLOBAL HEAD, BLOCKCHAIN PRODUCT DEVELOPMENT
MASTERCARD



RASHI GOYAL
DIRECTOR, PRODUCT DEVELOPMENT,
BLOCKCHAIN & DIGITAL ASSETS
MASTERCARD



SOUMYAJIT MITRA
DIRECTOR, PRODUCT MANAGEMENT - TECHNICAL
BLOCKCHAIN & DIGITAL ASSETS
MASTERCARD



ALVIN CHIA
SENIOR VP
HEAD OF DIGITAL ASSETS INNOVATION, APAC
NORTHERN TRUST



SEAN MULLINS
SENIOR VP, HEAD OF PRODUCT EXECUTION
DIGITAL ASSETS & FINANCIAL MARKETS
NORTHERN TRUST



BHAJI ILLUMINATI
CMO
CENTRIFUGE

CONTRIBUTORS



MARIANNA ANGELOU
DIRECTOR, BLOCKCHAIN ANALYTICS
METRIKA



ALEX NATHAN
CO-FOUNDER, VP ANALYTICS
METRIKA

FOREWORD

The role of financial institutions in the digital asset world is an important narrative in 2024. Just look at the SEC's approval of spot Bitcoin ETFs in the United States. This widely anticipated event seems to have played a key role in surging crypto prices. It also suggests that for crypto to reach mainstream adoption, it may need some support from financial institutions and governments.

This might seem like a contradiction, as Bitcoin was created to be independent of these entities. At the same time, crypto needs to exist in the real world. I often think about this tension. I first got into crypto because I was drawn to the idea of decentralization. I was a co-founder of a blockchain startup that focused on the Asia market, but I have also worked in the US government. Over the past few years I have written a lot about global crypto trends, and have spoken with regulators and financial institutions all over the world.

The question now is: How can financial institutions embrace digital assets without sacrificing the decentralization and efficiency that blockchain technology is supposed to bring?

As this paper shows, it won't be easy. Some of the content in this paper is based on research by the Monetary Authority of Singapore. Axelar Foundation and Metrika, producers of the paper, also contributed research. The technical solutions proposed in the paper represent possible paths to solve this challenge – not necessarily my personal views. My main interest is in sparking more conversation about an important problem. Blockchains are supposed to represent a single source of truth and to simplify overly complex processes.

But as more financial institutions enter the digital asset space, we are likely to see further proliferation of different blockchains, which threatens to create fragmentation.

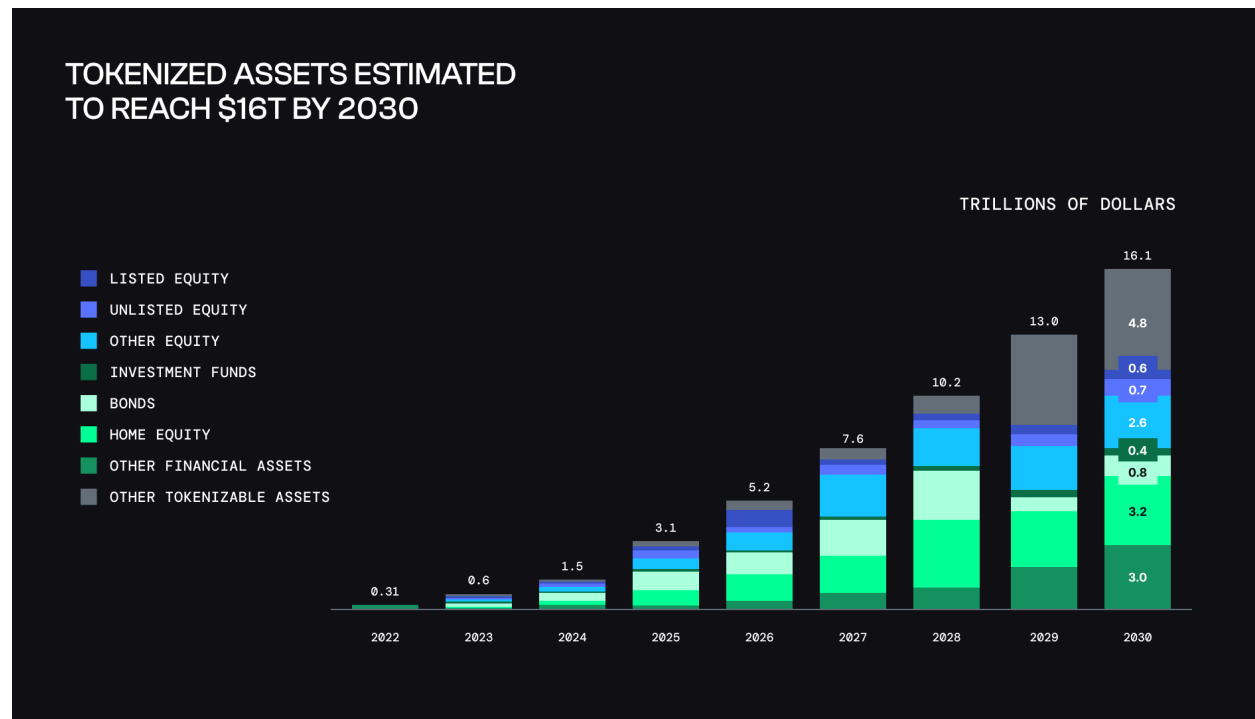
The answer, of course, is not to force everyone to use the same blockchain. One solution lies in interoperability, or finding ways to make blockchains work together in order to preserve the original promise of this technology.



-EMILY PARKER, LEAD AUTHOR

EXECUTIVE SUMMARY

Blockchain technology has the potential to streamline traditional finance. Tokenization could bring greater accessibility and liquidity, unlocking an estimated \$16 trillion in value by the year 2030, [according to a 2022 report](#) by Boston Consulting Group and ADDX, a market operator established in Singapore.



Source: World Economic Forum – Global Agenda Council, [BCG Analysis](#).

Blockchain technology promises to increase liquidity and accessibility for investments that have historically been complex, hard to manage, restricted to certain investment classes and/or with limited short-term liquidity, [according to a 2023 report](#) that Onyx by J.P. Morgan and Bain & Company published. Tokenization, most simply defined, translates ownership into blockchain code. This enhances automation and exposes a broader pool of investors to previously hard-to-reach asset classes. Tokenization widens the investor base for asset classes like real estate and private equity and has potential benefits in a wide range of categories – including precious metals, raw materials, agricultural products, real estate, artwork and music licensing, [according to a 2023 article](#) by the Algorand Foundation.

Problem: Liquidity Fragmentation

There is still a gap, however, between the ideals of blockchain technology and the realities on the ground. In theory, public blockchains act as transparent ledgers that create a shared source of truth. In practice, growing adoption of blockchain technology threatens to create fragmentation, even as it demonstrates adoption by the financial services industry. This is partly due to the growing number of blockchain use cases in the financial world.

“[Interlinking Networks](#),” a 2023 technical paper by the Monetary Authority of Singapore (MAS), explains this problem: “Financial institutions have developed capabilities across various distributed ledgers, with some setting up distributed ledger technology (DLT) platforms within their own ecosystems. However, this leads to proliferation of platforms in the market and fragmentation of liquidity.” This fragmentation could undermine the increased liquidity and accessibility that make asset tokenization attractive in the first place.

Another [paper](#) by Onyx by J.P. Morgan, a participant in MAS’s [Project Guardian](#), highlights the same problem. “Dozens of permissionless public and permissioned private networks have resulted in isolated ecosystems, with disjointed users, applications, and liquidity pools,” the report says. “These networks employ different security models, consensus mechanisms, and development environments, preventing value and data flow between networks.”

The proliferation of ledgers threatens to exacerbate the very problem they were supposed to solve – i.e., barriers to access and liquidity. So, how do financial institutions incorporate blockchain technology in a way that stays true to its original promise as a shared source of truth, while mitigating the risks associated with it? The key is to find the safest path to blockchain interoperability.

SOLUTION: BLOCKCHAIN INTEROPERABILITY

The MAS paper, which explores how to “interlink heterogeneous digital asset networks,” provides a useful framework for exploring this problem and discovering potential paths to solutions, which are described by the firms spotlighted later in this report. It lays out key requirements for blockchain interoperability, including flexibility, security, privacy, transparency, transaction monitoring and scalability. In this paper, we discuss potential paths to solutions in these areas. We also provide a framework designed by Metrika for assessing risk in these solutions.

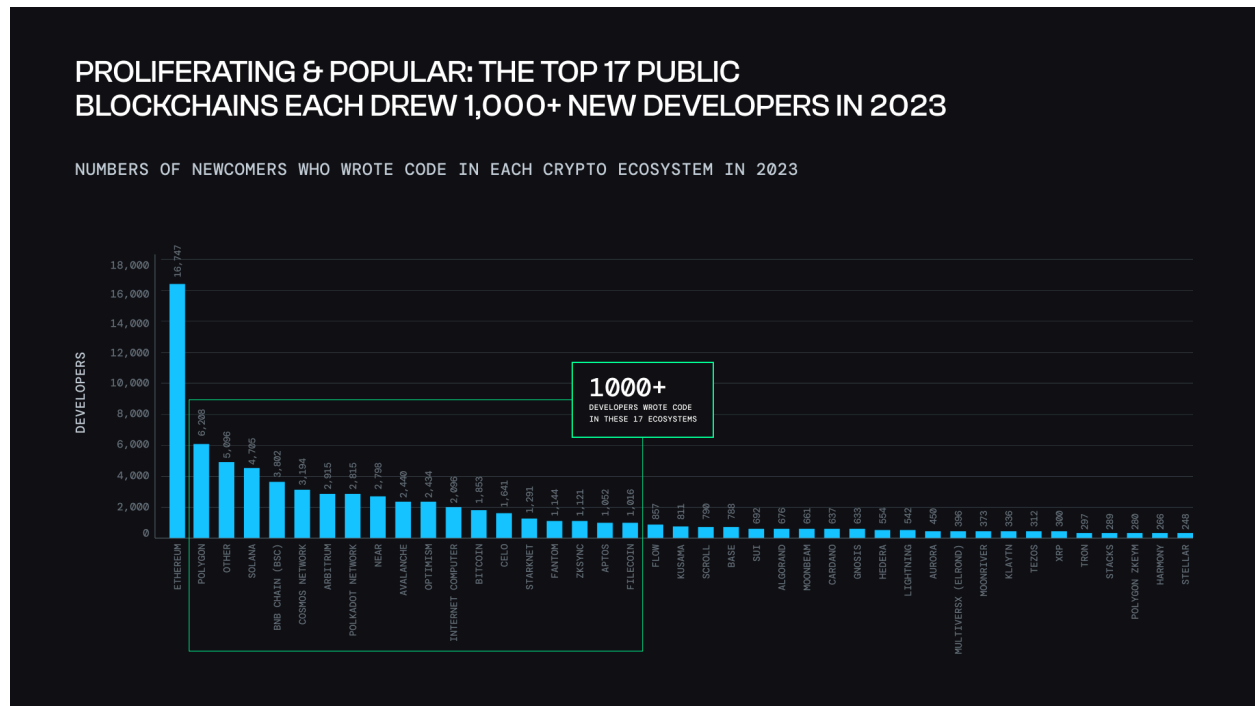
This paper will frame the discussion around some of the guidelines proposed by MAS and supplement them with practical know-how based on our interviews with financial players managing blockchain interoperability challenges. The goal is to highlight options for financial institutions hoping to reap the benefits and manage the risks of distributed ledger technology. For additional reading, the [World Bank](#) and the [World Economic Forum](#) have also published papers on blockchain interoperability. The Bank of International Settlements [outlines a vision for](#) “multiple financial ecosystems interconnected with each other.”

The advantages of blockchain technology span a range of use cases. This paper will include spotlight sections on blockchain concepts and solutions developed by the following institutions:

- **Citi** is developing a spectrum of digital assets products, deploying a multi-asset approach across the firm’s business lines. Citi’s digital assets explorations span digital money, trade, securities, custody and asset servicing.
- **Deutsche Bank** is investigating factors such as managed anonymity, on-chain risks, wallet capabilities, custody, smart contracts, conditional settlement, evolving market structure and associated regulations – on systems that span multiple private and public-permissioned blockchains.
- **Mastercard** is exploring both public and permissioned blockchains for building applications and products that provide customers, merchants and businesses with more choice and connectivity in how they move digital value.
- **Northern Trust** has a wide range of blockchain use cases and has applied the technology to everything from private equity to bond fractionalization to carbon credits.
- **Centrifuge** provides the infrastructure to tokenize, manage and invest in a diversified portfolio of tokenized real-world assets (RWAs), ranging from treasury bills to consumer credit and real estate.

INTRODUCTION: TOO MANY BLOCKCHAINS

For years, blockchain enthusiasts have been striving for greater mainstream adoption. Now, with traditional finance players exploring tokenization, the industry may be moving down a practical path to that once-elusive goal. Blockchain technology is supposed to bring efficiency and simplicity by introducing a shared, transparent method of recordkeeping. This might have been easier over a decade ago when the Bitcoin blockchain was the star of the show. Since then, increasing interest in distributed ledger technology has given rise to a wide variety of independent blockchains.



Source: [Electric Capital Developer Report, 2023](#).

Today, financial institutions choose from a variety of existing platforms with different regulatory and product standards. In some proofs of concept, institutions have developed their own private or permissioned blockchains. Private and public blockchains each have pluses and minuses. Private blockchains could arguably exacerbate the problem of fragmentation. However, financial institutions must ensure compliance with the regulatory environment and must safeguard client funds. Some will not be comfortable relying entirely on decentralized, public blockchains, which may have KYC challenges and lack a “customer support” option if something goes wrong. As tokenization emerges, many institutions will likely develop systems that incorporate multiple public, public-permissioned and private blockchains.

In order to achieve tokenization's goals of improved liquidity and accessibility, it will be essential to find a way to get these various blockchains to work together. This is also known as *blockchain interoperability*. A lack of such interoperability would limit the liquidity and accessibility of new investment products issued on blockchains. Insufficient interoperability limits investors' "ability to pool assets together and curtails trading across multiple venues, resulting in a reduced network effect and hampers innovation," [according to MAS](#). There are various ways to address this problem; the path proposed by MAS is an interlinked network model (INM), which refers to the exchange of digital assets and currencies across network borders. Each blockchain is a network, with its own rules for internally verifying information. These networks would be connected by cross-network protocols that deliver verified messages and securely transfer assets between various independent blockchains.

Given the abundance of blockchain networks and use cases, MAS recommends that existing systems should be able to integrate with any public or private network. "It will be more efficient if existing systems can integrate with a single multilateral network that provides global connectivity across DLT networks directly from their existing infrastructure," the report says. As such, cross-network protocols should be able to facilitate integration across a wide variety of networks.

INTEROPERABILITY REQUIREMENT: FLEXIBLE COMPLIANCE

With global reach being a key benefit of tokenization, blockchain interoperability must be flexible enough to support diverse regulatory regimes.

The challenges of interoperability are not simply technical. Not only is there a proliferation of ledgers, users of those ledgers are distributed all over the world. Blockchain technology may be borderless – and it should be, to realize the benefits of expanded liquidity and accessibility – but that doesn't change the fact that different countries have different rules. For example, compliance usually requires specific know-your-customer (KYC) and anti-money-laundering (AML) frameworks. Blockchain systems that work across borders must take all these rules into account (and with blockchain technologies creating new types of intermediaries, it may be unclear which rules would apply).

“An interlinking network model should have a well-founded, clear, transparent, and enforceable legal basis for each material aspect of its activities in all relevant jurisdictions,” the MAS report recommends. At present, crypto regulations vary greatly around the world; this variation has implications for interoperability. Some jurisdictions may have regulations that cover certain products or services, while other jurisdictions will not. Cross-network protocols will need to support flexibility so that institutions can deploy global solutions that take these local differences into account.

INTEROPERABILITY REQUIREMENT: FLEXIBLE SECURITY

Cross-network systems must be transparent for visibility into potential code faults, flexible to allow application-layer security policies that mitigate risk, and designed to enable those policies to be effective, should faults occur.

In the above section, we discussed the importance of an open and flexible system for compliance with global regulatory regimes across interlinked networks. Flexibility is also critical for security: an interoperability solution must deliver both flexibility in the diversity of blockchains that it connects, as well as transaction paths and security configurations on the interoperability network itself. In other words, the connector itself should be configurable for the needs of various connected parties, transaction flows and scenarios. As MAS puts it, “In addition to decentralised architectures providing an element of security, features such as customisable security configurations, prevention of malicious actions and appropriate audit trails were seen as critical attributes.”

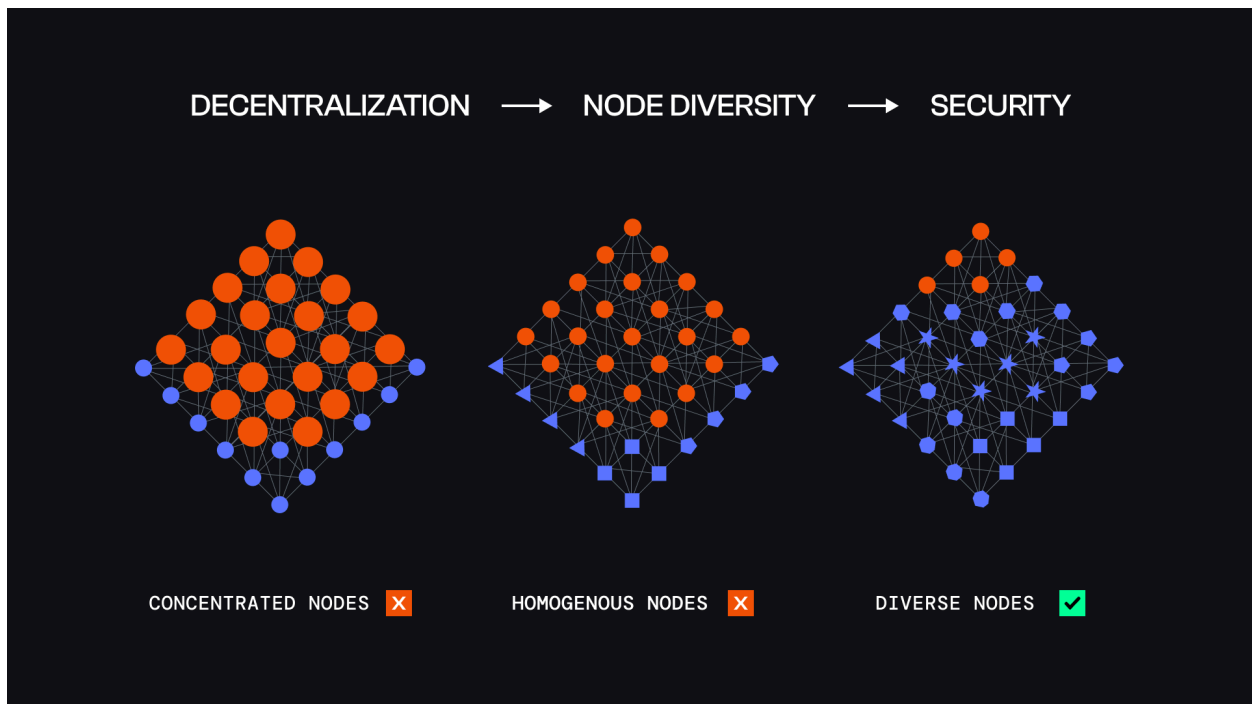
Blockchain Security Concerns

Storing value in a decentralized manner, with a large network of validators to confirm transactions, would seem to be much safer than having assets concentrated in a single place, otherwise known as a “honeypot” for attackers. But in reality, the many headlines about crypto hacks over the past few years can give the impression that blockchain technology is deeply insecure. Before tackling the interoperability challenge, financial institutions must first find ways to mitigate critical security risks.

The [World Economic Forum](#) identifies a few main threats, including: consensus protocol threats, breach of privacy and confidentiality, compromising of private keys, and smart-contract defects. In a cross-network system, these threats can affect both connected blockchains and any cross-network protocol that aims to make them interoperable.

CONSENSUS PROTOCOL THREATS

Let's start with consensus protocol threats. For a public blockchain or cross-network protocol to meet institutional security needs, its validator set must be large enough and diverse enough to prevent *51% attacks*. This term describes attacks by validators who control the majority of hash power (as in a proof-of-work blockchain such as Bitcoin), staked cryptocurrency (as in a proof-of-stake blockchain such as Ethereum) or simply designated validators (as in a proof-of-authority validation system, sometimes called a multisignature system). On proof-of-stake blockchains, distribution of stake is a critical measure of the network's diversity and its robustness against a 51% attack. Methods such as [quadratic voting](#) can improve distribution of stake. Quadratic voting makes it harder for proof-of-stake validators to accumulate voting power and take over majority control, because voting power does not increase linearly with stake.



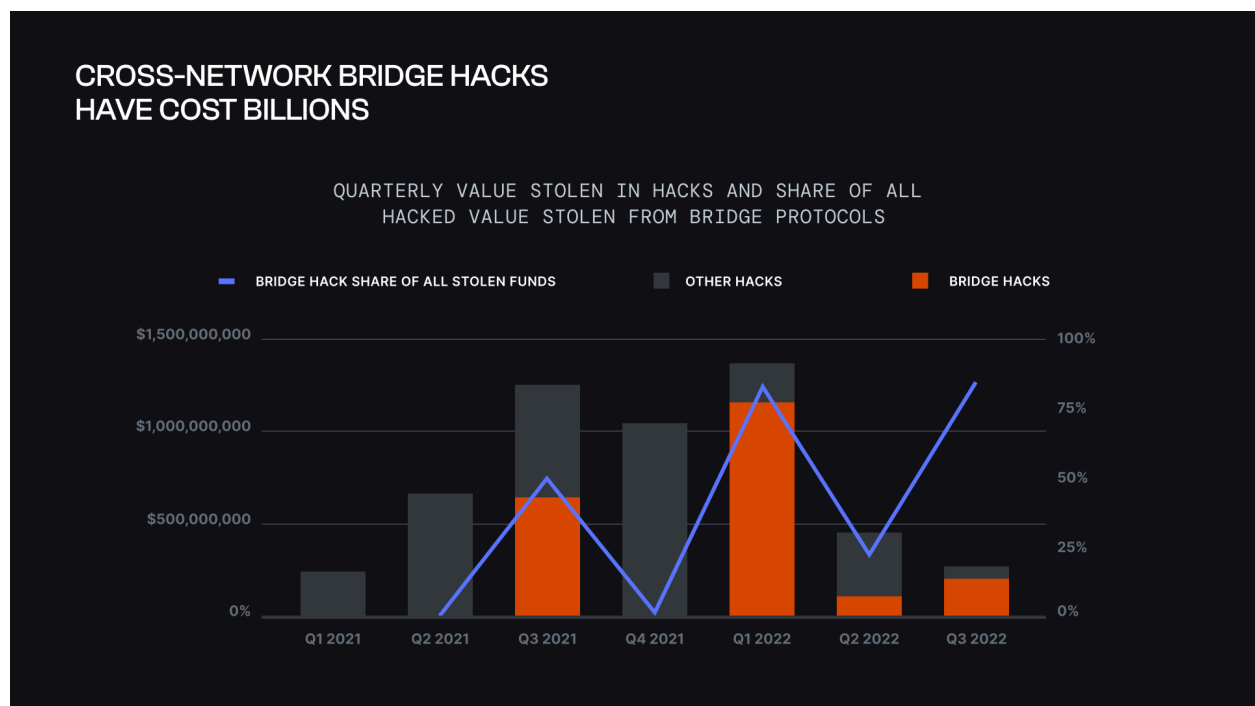
Source: [Axelar](#).

Mechanisms like quadratic voting can increase distribution of voting power. Better voting-power distribution makes collusion among validators more difficult. It also raises the bar for an outside attacker, who might compromise the private keys of validators in order to steal funds – as occurred in the [exploit of Axie Infinity's Ronin Bridge](#) in 2022.

Even with a large and diverse validator set, a persistent attacker might, in time, compromise a majority of voting power. To avoid the compromising of private keys, validator security policies such as mandatory [key rotation](#) can be implemented.

SMART-CONTRACT THREATS

Smart contracts are essentially code that takes actions, such as disbursing funds, when predetermined conditions are met. Smart contracts can improve transparency and reduce the likelihood of human error or theft. In smart contracts, it's often said, "code is law." Simply put, this means the outputs of a smart contract are valid, regardless of outcome, since it acted as the code stated it would act. A smart contract can be audited by depositors and can't be contravened by human go-betweens. Since its actions are often automatic and final, a smart contract can become a vulnerability point, if errors in code allow malicious actors to trigger functions that weren't intended by parties to a transaction.



Source: [Chainalysis](#).

Chainalysis defines cross-network bridges as protocols for delivering crypto from one blockchain to another, "usually by locking the user's assets into a smart contract on the original chain, and then minting equivalent assets on the second chain." A large amount of funds may be stored on these smart contracts, creating a honeypot for malevolent actors. In 2022, [Chainalysis estimated](#) that \$2 billion in cryptocurrency was stolen across 13 cross-network bridge hacks. Attacks on bridges accounted for nearly 70% of crypto stolen that year, leading Chainalysis to identify it as a "top security threat." Bridges can be vulnerable at the smart-contract layer or at the consensus layer (see above).

Solutions: Mitigating Security Risk at Multiple Levels

Security is a multifaceted problem with binary outcomes. There is no silver bullet. An effective strategy for mitigating security risk will involve prudent configuration and planning at multiple levels.

CODE AUDITS

One way to limit smart-contract risk is to perform regular, independent audits of smart contracts and run [bug-bounty programs](#) that expose smart contracts to third-party platforms and/or security researchers. End-to-end open networks facilitate this security safeguard, enabling the largest number of eyes checking code for vulnerabilities.

CONFIGURABLE SECURITY POLICIES

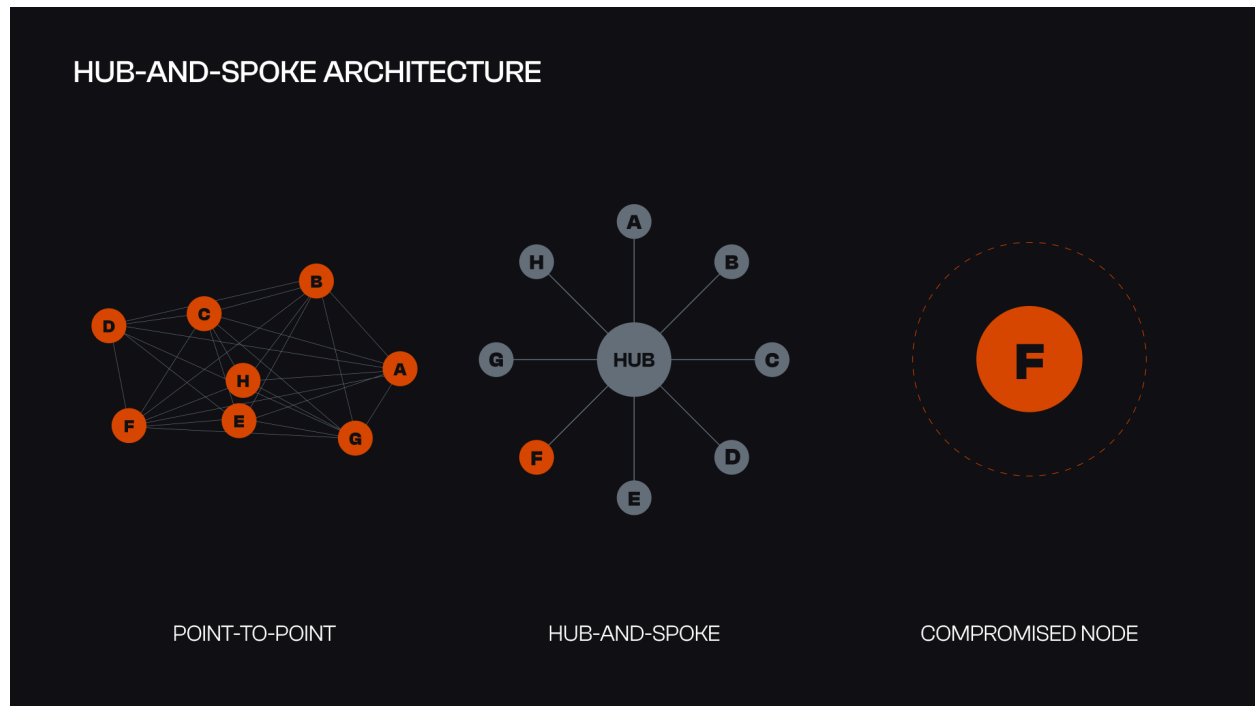
Independent review can prevent avoidable vulnerabilities, but faults can always slip through. A multi-layered approach to cross-network risk management is advised – with policies in place that mitigate damage when faults occur. A multi-layered risk management approach should include the capability to customize application-level security policies. These policies might include, for example:

- Additional validation policies for large transfers or transfers from specific accounts.
- [Rate limits](#) that cap the amounts that can be transferred over a set time period.
- Limits on repeat transactions or other red-flag patterns.

“The inclusion of risk management in bridge architectures allows them to consistently improve in their ability to reduce the risk of a transaction and reduce cost, while also increasing the speed of transactions,” according to the MAS report.

NETWORK TOPOLOGY

Multi-layered risk management is most effective on a network that is designed so that problems can be contained. In a system of interlinked networks, faults may occur on any connected blockchain. It's important for the network topology – the way nodes are arranged and connected – at the cross-network layer to be designed in such a way that those faults can be isolated.



Source: [Axelar](#).

For example, hub-and-spoke and point-to-point (also called pairwise) are two commonly used network topologies. A hub-and-spoke network routes messages to multiple nodes through a single hub. Point-to-point networks relay messages from one node to another. Each has its advantages. A point-to-point network may be able to connect new nodes at a lower cost. On networks where security is critical, hub-and-spoke provides visibility across the network, which is ideal for rapid isolation of problem connections. On point-to-point networks, each node sees only its direct connections and will unknowingly pass along messages from compromised nodes. Hub-and-spoke topology can help contain contagion from faulty chains – without the necessity of shutting down the entire network. (See the section on scalability for a more complete discussion of network topology.)

Solutions: Open-Source Technology & Modularity

There are several attributes of blockchain technology that can help achieve the flexibility required to meet the regulatory, security and privacy requirements of various financial institutions. (Privacy requirements are discussed in more detail below.) One is open-source technology. Open-source software has the benefit of composability, meaning code is open to the public and can be [readily modified](#) for different purposes. It also provides the benefit of allowing a larger number of developers to review code for potential problems. That doesn't inoculate open-source software against vulnerabilities, however. In general, potential downsides of open-source software include a lack of uniformity in applying best practices and end-user challenges in identifying all open-source components used in a solution, [according to a 2023 report](#) from the US government's Open-Source Software Security Initiative.

Another important ingredient for flexibility is modularity. A [report by Visa](#) describes a modular blockchain as one in which component blockchains each specialize in a select set of tasks. Typically, this includes execution, settlement, consensus and data availability. In monolithic blockchains, by contrast, all necessary tasks are handled by a single blockchain. Modular blockchains "boast high adaptability with specialized chains for specific tasks, offering greater design flexibility," the Visa report says.

In blockchain interoperability systems, a modular architecture supports configurability and flexibility. Modular components can be swapped in and out and customized according to the user's requirements. Blockchain industry debates may rage about the advantages and disadvantages of modular vs. monolithic approaches for specific networks. However, for INMs that connect various blockchains and other ledgers and databases, the modular approach can deliver the degree of flexibility that institutions require.

INTEROPERABILITY REQUIREMENT:

PRIVACY

Public blockchains sacrifice privacy for a decentralized verification model. INMs must be flexible enough to integrate systems that keep some transaction data private.

Privacy is yet another area in which blockchain technology can act as a double-edged sword. One of the benefits of blockchain technology is that it makes information transparent and viewable to the public. How can such a system be used for transactions that involve sensitive, private data? How can systems prevent information from being viewed – and exploited – by bad actors? The WEF recommends that organizations evaluate their blockchain use “to ensure that only permitted data is shared without exposing any private or sensitive information.” MAS suggests storing personal data off-chain and keeping a reference or hash on a distributed ledger.

Private blockchains, which are open only to a designated set of participants and validators, are well-known in the finance industry. [Zero-knowledge proofs](#) are a form of encryption that is emerging, allowing privacy-preserving transactions on a public ledger. There may be further methods yet to emerge that will help draw a bright line around private or sensitive data, while still allowing participants to benefit from access to global systems that rely on transparency for rapid and secure settlement of transactions.

Even today, a privacy-preserving system is likely to employ more than one of the abovementioned technologies – from off-chain databases and cryptographic hashes to zero-knowledge proofs. To deliver interoperability today, cross-network protocols should be able to integrate all of the above. And, to be adaptable to future needs and technologies, they should be able to integrate diverse forms of consensus, perhaps including some that have not yet been identified.

INTEROPERABILITY REQUIREMENT: RISK ASSESSMENT

INMs involve increased complexity and a lengthened list of components that must be given appropriate due diligence prior to being fully utilized by financial institutions.

As discussed above, there are various security and compliance risks that financial institutions must consider before adopting any distributed ledger system. Addressing and managing risks associated with digital assets and their underlying blockchain networks is a nascent field poised to gain increasing attention as distributed ledgers see wide adoption. A recent [paper in the *Journal of Risk Management in Financial Institutions*](#), authored by Metrika, a firm that specializes in the derisking of digital assets, proposes a comprehensive risk assessment framework that helps financial institutions navigate the intricacies of blockchain technology. The framework incorporates concepts from traditional finance risk management, adapting them to accommodate for the unique characteristics of digital assets, including the 24/7/365 nature of blockchain networks, as well as their decentralized structure. The proposed taxonomy breaks down risk into different categories: centralization, network reliability and performance, financial, security, people, and regulatory. Similarly, Ernst and Young recently presented a token due-diligence [framework](#), which identifies six critical pillars for consideration: reputational and strategic, technical, financial, legal and compliance, cybersecurity, and auditability. Risk frameworks such as these are essential to safely integrate blockchain technologies into traditional operational strategies.

Once a risk framework and its respective risk areas have been finalized, risk practitioners and analysts can assign a series of Key Risk Indicators (KRIs) to each category to monitor and measure risk exposure. KRIs are quantifiable metrics that are crucial in managing, monitoring and reporting on risk. These KRIs are associated with specific thresholds, aligned with an organization's risk appetite, which trigger real-time alerts and notify responsible stakeholders when crossed.


To illustrate, decentralization is an important area to assess as it permeates many components of the stack on which an asset relies. It includes a plethora of KRIs related to public blockchains and digital assets themselves, such as the size of the validator/miner pool and the distribution of client/software implementations among validators. It also involves tracking decentralization in asset ownership, geographic locations, staking entities and developers.


Applying a structured assessment to tokens and protocols is an important first step in the digital assets journey of any organization; however, INMs add another layer of complexity. For a bridge to be used, financial institutions first need to identify all components constituting an interlinked network. These components typically include the source and destination blockchain networks that can be managed in a similar manner to the approach outlined above. Uniquely, INMs include a cross-network protocol and an asset to be transferred between source and destination chains.


When selecting a cross-network protocol, it's important to recognize that there is no perfect solution. The design choices impact the protocol's performance, cost, scalability and decentralization. Understanding these tradeoffs is vital for institutions to make informed decisions aligned with their objectives and risk appetite. Furthermore, the landscape of cross-network protocols is diverse, encompassing various approaches such as lock and mint, burn and mint, and atomic swap. Each model exhibits its own variability in implementation, introducing unique challenges, which in turn have direct implications on the assets that are transferred across chains. Taking the lock-and-mint model as an example, assets are susceptible to asset recovery and restitution when the cross-protocol network suffers outages or other vulnerabilities. Additionally, asset fragmentation poses a significant risk. This can occur if multiple cross-network protocols are used for transfers, resulting in multiple representations of the same wrapped asset on a destination network. Such fragmentation further complicates the redemption process, adding complexity to the task of managing these assets.


While security and trust implications of the various cross-network protocols have garnered a lot of attention, there are other, equally important risk factors that should not be ignored.

BEYOND SECURITY:
ASSESSMENT FACTORS FOR CROSS-NETWORK PROTOCOLS

**LATENCY:** HOW LONG DOES IT TAKE TO MOVE DATA/ASSETS TO AND FROM A CHAIN?

**COST:** HOW MUCH DOES IT COST TO MOVE DATA/ASSETS TO AND FROM A CHAIN?

**SCALABILITY:** CAN A CONGESTED BRIDGE BECOME A BOTTLENECK?

**DECENTRALIZATION:** IS THE INTEROPERABILITY SOLUTION SUFFICIENTLY DECENTRALIZED ON THE INFRASTRUCTURE AND GOVERNANCE LEVEL?

Source: [Metrika](#).

As mentioned above, once the risk criteria of the framework has been established, the next step involves specifying the relevant KRIs. The table below showcases some KRIs that span all components of an interlinked network:

INTERLINKED NETWORK COMPONENTS + KEY RISK INDICATORS	
1. IDENTIFYING THE COMPONENTS OF AN INTERLINKED NETWORK	
a) Source Blockchain.	
b) Destination Blockchain.	
c) Cross-Network Protocol.	
d) Asset to be transferred across Source Chain and Destination Chain.	
2. ESTABLISHING KRIs IN INTERLINKED NETWORK COMPONENTS	
a) Source Blockchain: Uptime (Network Reliability and Performance), Node/Validator Count (Centralization), Value Staked (Centralization), Large Inflows/Outflows monitoring (Financial).	
b) Destination Blockchain: All the above apply.	
c) Cross-Network Protocol: Last Security Audit (Security), previous malicious attacks (Security), total transfers (Network Reliability and Performance), amount bridged (Financial), volume bridged (Financial), number of smart contracts involved (Security), decentralized governance evidence (People).	
d) Assets: Market cap (Financial), net amount locked/burnt on chain A (Financial), net amount bridged (Financial), number of wrapped representations in chain B (Network Reliability and Performance), number of blacklisted accounts (Security).	

Source: [Metrika](#).

Once the initial step of due diligence is complete, it's essential to engage in continuous monitoring of all KRIs that impact the various components of the INM implementation. Continuous monitoring not only helps in early detection of potential issues, it also ensures that financial institutions remain compliant with their own internal risk-tolerance levels and evolving regulatory standards, and adapt to threats as they arise.

INTEROPERABILITY REQUIREMENT: TRANSPARENCY & MONITORING

Lack of transparency in some cross-network systems has recently emerged as a potential vector for money laundering.

Hacks are not the only threats to INM security. Another is money laundering. According to a 2023 [report by Elliptic](#), a blockchain forensics firm, \$7 billion in crypto has been laundered through cross-network services. Blockchain proponents will argue that the relative transparency of blockchain technology actually makes it easier to track criminal activity – but the Elliptic report revealed opacity in some cross-network connections as a weak link in the audit trail. Sophisticated tracking of on-chain asset movement is offered by entities like Elliptic, Chainalysis, TRM Labs and other companies that specialize in forensics. Visibility into asset movement should be at its best in transactions across open, public networks. As the Elliptic report revealed, some cross-network connectors include off-chain components that can be used to obscure the source or destination of on-chain funds.

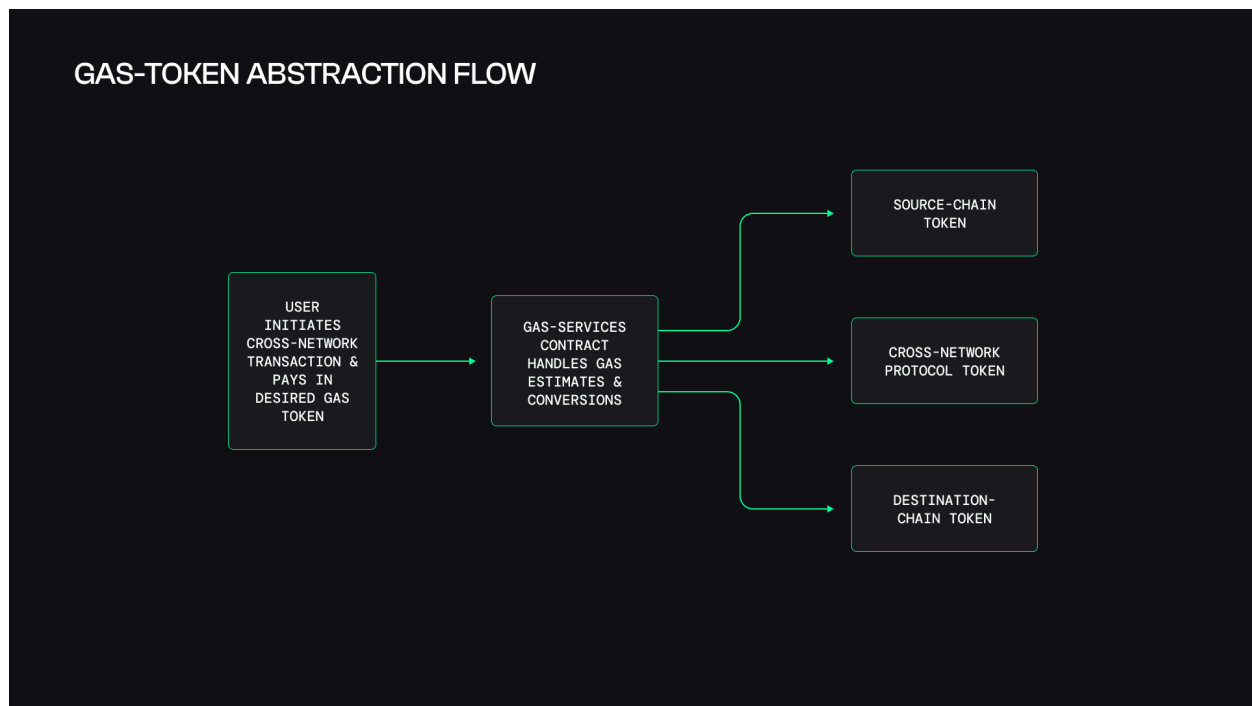
This is not viable for blockchain interoperability to succeed in an institutional context. Active monitoring of cross-network activity is necessary from end to end. The MAS report emphasizes the need for verification of cross-network transactions by an independent network that can detect anomalies. This is vital not only for AML compliance but to secure funds – for example, to trigger an emergency stop to limit losses in the event of a security breach.

GAS-FEE ABSTRACTION

Gas payments present a particularly challenging facet of compliance risk in interlinked network solutions. On public blockchains, users pay for transaction validation and computation in fees called *gas*, often using native gas tokens, issued on the blockchain they are using. These tokens may not pass risk assessment – or financial institutions simply may find it inconvenient or costly to obtain and custody such tokens. In addition, there is risk of gas fees being paid to sanctioned actors. One solution is gas-fee abstraction.

According to a paper by Onyx by J.P. Morgan, gas-free abstraction can “allow for gas to be paid in different tokens or on behalf of users to simplify gas-free management and encourage usage.” The paper also describes how “by leveraging a smart contract wallet, we were able to provide a seamless way for the fund manager to deploy Fund Token Contracts and accept minting and burning requests without the need to obtain gas tokens to cover the required transaction fees.”

One way to deliver gas-free abstraction is for the cross-network protocol itself to support gas-token conversions. A gas receiver contract on the protocol can accept gas payments in the user’s token of choice, then convert them into the token or tokens required for gas payments, returning any “change” made in the course of the transaction due to variations in gas fees or conversion rates.



Source: [Axelar](#).

This functionality is desirable for optimized user experience in all verticals, not just institutional finance. Without gas-free abstraction at the cross-network protocol layer, users involved in multichain transactions would have to hold multiple gas tokens. Imagine Amazon requiring its users to obtain a local bank account, funded with local currency, in order to make a purchase from a foreign seller – instead of using payments infrastructure that handles currency conversions on the back end.

Components of potential gas-free abstraction solutions have also been proposed at the protocol layer on specific blockchains. In their solution spotlight included in this paper, Deutsche Bank details how a paymaster feature proposed for the Ethereum protocol in a standard called ERC-4337 allows a method for paying gas fees from known on-chain addresses.

INTEROPERABILITY REQUIREMENT: SCALABILITY

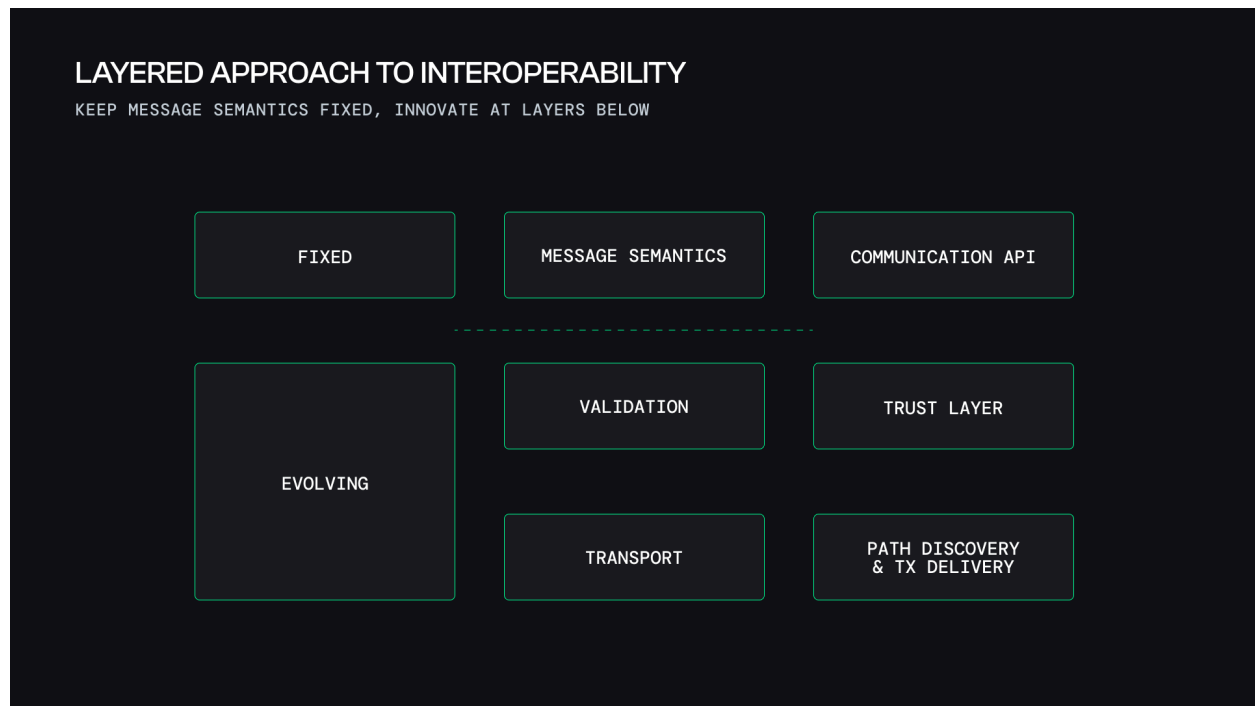
INMs face dual scaling challenges of emerging technology and the potential for explosive growth in transaction volume and the number of connected networks.

As financial institutions explore their options to achieve interoperability, scalability is an important consideration. More institutions adopting blockchain technology means that the demands on protocols will increase. More ledgers are likely to be involved and larger amounts of money will be transferred. The challenge is to create a structure that can withstand these demands without compromising security or efficiency. MAS recommends having “a readily available network in place made up of high-quality nodes with verifiable reputations as opposed to stakeholders having to construct their own networks when they want to engage in a business relationship or having to rely on networks with unknown nodes.”

Solutions: Network Adaptability

A readily available network of high-quality nodes is a good starting point today. However, new connections, increased volume and advancements in blockchain technology are likely to demand improvements to this network in the future. This represents a challenge: will applications need to be updated with each future upgrade? The answer is, not necessarily: with a technology stack optimized for adaptability, a cross-network protocol can meet this demand without requiring undue updates from connected applications. A cross-network protocol can be thought of as operating at three layers:

1. **Message semantics** (the structure of messages sent between networks by applications).
2. **Validation** (the trust layer, where transactions are verified).
3. **Transport** (setting and following the route from source to destination blockchains).



Source: [Axelar](#).

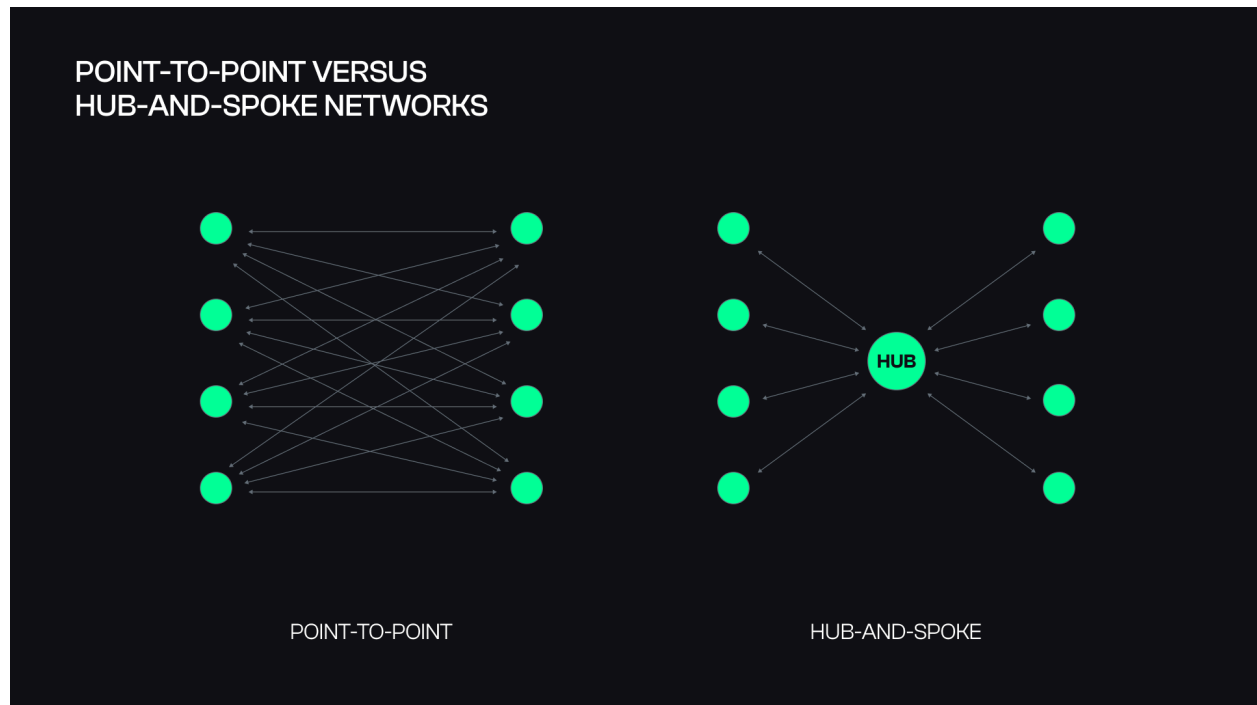
In a technology stack optimized for adaptability, developers build applications based on specific message semantics that remain constant. Meanwhile, the validation and transport layers are subject to future adaptations as needed.

Solutions: Network Topology

Network scalability also depends greatly on topology, the logic or pattern on which nodes in a network are arranged. The section of this paper titled “Mitigating Security Risk at Multiple Levels” covers network security considerations in network topology. Not surprisingly, topology also has significant impact on scalability of networks. Once again, there is evidence to support a preference for hub-and-spoke topology over pairwise alternatives. For a point-to-point network to connect N nodes, the number of potential connections grows exponentially with the number of nodes. (The formula is $N(N-1)/2$.) Thus, a point-to-point INM that connects five blockchains will require up to 10 connections – and a point-to-point INM that connects 100 blockchains will require up to 4,950. The connection requirements of a hub-and-spoke INM will [scale linearly](#): five blockchains require up to five connections to the hub; 100 blockchains require up to 100 connections. Each new connection immediately benefits from network effects with the entire network, via the hub. In their paper on INMs, MAS puts it simply: “Instead of bilateral integration, it will be more efficient if existing systems can integrate with a single multilateral network that provides global connectivity.”

Physical networks are helpful by way of analogy: many transportation options, such as freight and air travel, use hub-and-spoke network topology. “The Geography of Transport Systems” is an authoritative textbook that is used in university courses on transportation systems. In addition to efficiencies achieved as the number of connected nodes increases, the text [outlines three scale advantages](#) of hub-and-spoke topologies: economies of scale on connections, at the hubs and in the use of shared transshipment facilities.

- “Economies of scale on connections by offering a high frequency of services. For instance, four services per day could be possible instead of one service per day between any two pairs in a point-to-point network.”
- “Economies of scale at the hubs enable the potential development of an efficient distribution system since the hubs handle larger quantities of traffic.”
- “Economies of scope in the use of shared transshipment facilities. This can take several dimensions, such as lower costs for the users as well as higher quality infrastructures.”



Source: [The Geography of Transport Systems](#).

Network topology considerations such as these will be familiar to systems architects. In INMs, the envisioned scale is global and the future number of required network connections is potentially massive. The need for careful attention to network topology in INMs is critical.

CONCLUSION

There is no question that tokenization brings great potential for financial institutions, which is why so many are actively engaging with blockchain technology. But as this paper discusses, building distributed ledgers as walled gardens threatens to undermine the accessibility and liquidity that this technology is supposed to increase. As this field matures, financial institutions will need to weigh a wider range of technical and legal considerations, as well as increasingly complex risks. Rather than evaluating individual blockchains or tokens, financial institutions may have to consider the safest and most efficient ways for different blockchains to work together. This paper provides some of the tools and resources needed for that evaluation process.

INSTITUTIONAL SPOTLIGHTS



SPOTLIGHT: CITI

Citi continues to develop blockchain-related products and initiatives across its lines of business. In the past year, Citi has announced multiple digital assets initiatives and has been building foundational capabilities for the future. Citi's digital assets explorations span digital money, trade, securities, custody and asset servicing.

Selective Citi Initiatives

1. TOKENIZATION OF PRIVATE MARKETS

Citi, along with certain asset manager clients, successfully completed a proof of concept on the tokenization of private funds, utilizing smart-contract capabilities. This initiative demonstrated how tokenization and the use of smart contracts may improve distribution of private funds, increase automation and operational efficiencies, and frame compliance by encoding rules into tokens. It also showed how tokenization could unlock new capabilities and use-cases, such as utilizing private funds as collateral to borrow more liquid assets.

2. DIGITAL CUSTODIAN

Citi was the first digital custodian on BondbloX Bond Exchange (BBX), a fractional bond exchange which uses distributed ledger technology (DLT). BBX simplifies bond investing by enabling electronic tracking and trading of bonds and making fractionalized bonds accessible to a broader range of investors. Through this partnership, Citi's clients that are eligible to become BBX participants gain access to BBX along with Citi's provision of seamless settlement and custody services. In addition to enhancing transparency and accessibility in bond markets, this initiative shows Citi's commitment to investing in digital financial market infrastructure and partnering with Bondblox, its portfolio company, to provide innovative solutions and support the evolving needs of its clients.

3. CITI TOKEN SERVICES

Citi introduced and tested Citi Token Services for cash management and trade finance. Citi Token Services is a key component of Citi's digital assets offerings, which use blockchain and smart-contract technologies to deliver digital assets solutions for institutional clients. Citi Token Services involves the integration of tokenized deposits and smart contracts into Citi's global network, in order to upgrade core cash management and trade finance capabilities. As institutional clients have a need for "always-on" programmable financial services, Citi Token Services aims to provide cross-border payments, liquidity and automated trade finance solutions on a 24/7 basis.

Citi Token Services for Cash uses interbranch tokenized deposits aiming to enable a new digital treasury management solution. Without directly having to hold "tokens," participating institutional clients would be able to initiate instant payments and liquidity movement between their accounts at Citi branches on a 24/7, real-time basis. Benefits may include simpler client liquidity management by minimizing cut-off times and making client liquidity movement more fluid across their geographic locations. Although not currently available to all clients, select Citi corporate clients have successfully tested the transfer of USD funds between New York and Singapore.

Citi Token Services for Trade intends to allow clients to fund smart contracts which their counterparty would then be able to execute to receive cash for services and/or goods provided. It should deliver a fully digitized and automated process with instant transactions that is available 24/7 and with lower operational costs. It is expected to reduce transaction processing times from a few days to a few minutes, as well as make trade financing more cost efficient for clients.

Through successful live test transactions with partners, Citi demonstrated the potential for tokenized deposits to streamline processes, reduce transaction processing times and provide seamless global liquidity management capabilities.

4. ISSUING AND PAYING AGENT FOR DIGITALLY NATIVE NOTE

Citi acted as the first Issuing and Paying Agent for a Digitally Native Note (DNN) issuance via Euroclear's Digital Financial Market Infrastructure DLT platform. The issuance of a EUR 100 million three-year DNN showcases the potential for T0 settlement and lays the groundwork for a fully digital transaction lifecycle in the bond market. This collaboration contributes to the bond market's transparency, digitalization and accessibility while also underscoring Citi's overarching efforts to improve efficiency and unveil growth opportunities through the integration of this technology into traditional infrastructure.

Considerations Around Blockchain Interoperability

When considering interoperability across both public and private blockchains, the following challenges may apply.

- **Security:** Maintaining security, continued operability and enterprise resilience for interoperability solutions is an important requirement.
- **Transaction atomicity:** While it is easier to attain interoperability and transaction atomicity between multiple blockchains that use the same protocol, it is harder between blockchains that use different protocols and potentially even more challenging when blockchains need to interoperate with traditional systems.
- **Data privacy and data retention:** Challenges arise when there is a need to selectively disclose certain data elements but not others, even between two transacting parties that have established a secure interoperable solution between their respective blockchains. Blockchains by their nature may retain all transactions and other data, which creates a challenge for use cases that might involve data classified as personally identifiable information (PII).
- **Tokenized asset servicing:** There may be challenges ensuring that activity conducted off-chain (e.g., asset servicing and corporate actions on legacy rails) are properly reflected on-chain.
- **Standardization:** Blockchain protocols may employ different standards for asset tokenization and messaging communication, which may lead to coordination issues. For instance, a token model in one blockchain network might be different from the token model in another blockchain network, which necessitates either point-to-point model translation or a third canonical model that acts as a translator.

In addition to the above factors, there are supplementary considerations that need to be taken into account and addressed when looking at interoperability with public blockchains. These considerations include, among others, clear regulatory permissibility as a key requirement, compliance and legal conditions, technical capabilities around transaction finality, and practices established to ensure enterprise resiliency and security.

Any Citi initiative discussed or mentioned in this paper may be subject to regulatory and/or internal approval and may be subject to change.

© 2024 Citigroup Inc. Citi, Citi and Arc Design and other marks used herein are service marks of Citigroup Inc. or its affiliates, used and registered throughout the world.

Deutsche Bank



SPOTLIGHT: DEUTSCHE BANK

Deutsche Bank Securities Services (SES), a leading global post-trade securities servicing provider, is experimenting with blockchain and tokenization technologies to achieve cost-effective, efficient and faster value creation for clients with nontraditional business models.

Deutsche Bank took notice of cryptocurrencies and blockchains when they broadened their appeal to the retail space as a peer-to-peer payment mechanism that could disrupt financial services. Value could be transferred in about 10 minutes compared to days. The cost of transfer was also significantly lower, with a narrow bid-offer spread instead of high remittance fees. These disruptor benefits could have displaced some volume from established channels, but cryptocurrencies' volatility challenged its viability for transfers. Together with the advent of cheaper and faster cross-border payments and regulations, cryptocurrencies' impact and reach became limited.

This all led to questions about how the unique features of blockchain and smart-contract technologies could be applied to regulated capital markets. Deutsche Bank began investigating coin and ledger anonymity, on-chain and integrity risks, wallet capabilities, custody, smart contracts, hashed time-locked contracts (HTLC) for conditional settlement, and the evolving market structure, as well as associated rules and regulations.

Building on these foundations, its recent experiments include tokenized securities (for example, Project Benja in 2021), exploring what they mean for market structure and operating models. With a fintech collaborator that specialized in environmental, social and governance (ESG) investing, the project assessed the problems and opportunities of interoperability, delivery-versus-payment settlement, data payloads and how certain intermediary activities could be streamlined by smart contracts.

In 2023, Deutsche Bank completed Project DAMA (with another fintech collaborator versed in the DeFi space) that addressed different problems: Asset managers looking to launch a digital asset fund need to deal with a variety of intermediating activities. Transfer agents, fund administrators, custodians and payments providers all need to be ready to service digital assets. As on-chain readiness across these intermediaries is not consistently available, this adds considerable time and cost to the process. It is also cumbersome for investors to move from fiat currency to digital assets. Designed to provide open-architecture, single-window access to post-trade services, DAMA included fiat-digital cash ramps, digital identity for governance, mass customization servicing, and "composable" on-chain methods for fund and asset services.

Why Multiple Blockchains?

A key assumption behind Deutsche Bank's experiments and proof of commercialization is that there will be a proliferation of blockchains. Different clients will use different blockchains and different blockchains could better fit certain use cases. Each blockchain, including their stacks like Layer 2 or sidechains, will be likely to have multiple beneficiaries and host multiple types of digital assets including digital cash and smart-contract-based applications.

Hence, interoperability is a practical necessity. Implemented with governance capabilities, interoperable public blockchains that are permissioned for use by particular digital assets and funds would allow participants to avoid unnecessary up-front costs to set up their own blockchains, get to market faster, minimize fragmentation of nascent liquidity from walled private gardens, and lower entry barriers to allow supply and demand volumes to form more quickly.

Other benefits of these open-architecture blockchains include no lock-in for investors and activities on private blockchains, the ability to access potential new digital asset classes from different manufacturers, as well as personalization benefits. With digital verified credentials, financial information can also be seamlessly distributed to participants to inform and support their market activities. The ability for securities service providers to service multichain interoperability will probably become necessary for success if their clients adopt different chains.

Challenges of Interoperability

As the industry progresses towards a digital future of finance with blockchains, clarification of what interoperability means is important to facilitate institutional adoption and regulatory clarity. For example, should interoperability mean the transfer of digital assets per se, common data communication protocols across chains, or both? How should information across chains be aggregated for holistic views and reporting?

Other technical considerations include blockchain, bridge and network security, consensus/fault tolerant and governance postures, differences in deemed settlement finality, double-spending risks, data availability and record integrity, and the regulatory outcomes from the choices made. Efficient settlement of digital assets requires an equally efficient way to exchange money (cash leg) to be on the same chain. However, during this industry transition period from traditional to digital, the cash leg for settlement with digital tokenized assets can still be on traditional rails. This adds new workflows and controls

with each additional chain, thus reducing cost efficiency which can be avoided if a digital form of cash can be used.

To help address such considerations, information availability and accessible community expertise on blockchain and interoperability intricacies will be valuable resources. It will also be essential to have industry-accepted due diligence questionnaires for adopters like asset managers, distributors, investors and intermediaries. These questionnaires would address the risk assessments needed to facilitate adoption. To be effective, such questionnaires would also require some agreement on terminologies and a degree of standardization in smart-contract protocols.

Potential Benefits From Integration With Traditional Technology

A potentially overlooked feature of interoperability is the integration of blockchains with traditional technology systems. This “backward compatibility” can significantly reduce the costs and risks of market entry from a client-centric perspective. These integrations also allow for comprehensive reporting of assets while ensuring information security and legality are governed by familiar and established regulations.

Regulatory Considerations

Finally, regulatory sandboxes remain essential for the private sector and regulators to jointly review the risks and uses of blockchains that are public, public-permissioned or private. Each of these blockchain variants has its own pros and cons. For example, there are concerns that gas fees in public chains can potentially fund undesirable state actors operating as validators. The use of private chains introduces other concerns, such as fragmentation of market-formation activities, cost and anticompetitive practices.

To address these concerns, private-public-sector sandboxes can explore possible solutions, such as the use of Layer-2 blockchains in a public-permissioned deployment with batched commits, or updates, to Layer 1. In this approach, gas fees are minimized to reduce the size of risks associated with paying to the wrong parties. The Account Abstraction feature of Ethereum ERC-4337 allows a “Paymaster” function to be created that can centralize paying gas fees from known on-chain addresses. This innovation can potentially facilitate on-chain analytics of transaction patterns to further mitigate the risks of an already minimized gas payment to possible sanctioned validators.

These sandboxes can help establish good industry practices for risk management.



SPOTLIGHT: MASTERCARD

The rise of blockchain technology has opened a world of opportunities in the realm of digital assets, transforming the way financial transactions are conducted and assets are managed. However, a notable obstacle in the existing landscape of blockchain-based solutions is the challenge of asset interoperability.

Mastercard anticipates a future environment where central banks, commercial banks and financial institutions will introduce new regulated assets such as Central Bank Digital Currencies (CBDCs), tokenized versions of banking deposits, regulated stablecoins or tokenized Real-World Assets (RWA), all onto their preferred asset platforms. Parallel to this development, application developers will continue to innovate, creating applications on platforms best suited to their unique needs and requirements.

In this context, Mastercard will focus on ensuring the interoperability and fungibility of assets across various asset platforms, allowing these diverse assets to coexist and function harmoniously. Mastercard aims to establish an enabling environment where regulated assets can be effortlessly managed, exchanged and settled across different asset platforms. At the same time, Mastercard endeavors to provide application developers with the tools they need to create innovative applications on their platform of choice, bolstering the expansive potential of the blockchain universe.

Blockchain innovation is impacting various areas of payments, including cross-border transactions, where it offers solutions to longstanding issues such as high costs and slow processing times. It's also revolutionizing the concept of digital identity and authentication, making transactions more secure. Additionally, blockchain is enabling new forms of programmable money and smart contracts, which can automate and streamline complex financial processes.

Interoperability With Public Blockchains

Today, credit-card payment rails provide interoperability across bank ledgers. Consider Alice looking to purchase a good from Bob. The real-time authorization at the point of sale (often manifested as “card approved”) is a classic example of this interoperability. In this example, Alice's spending power as recorded in Bank A's ledger is made usable for purchasing a good from Bob whose account is recorded in Bank B's ledger. Blockchains make these ledgers verifiable, by creating a tamper-proof form of record-keeping.

Mastercard envisions an era where information of all types exists on such verifiable ledgers. These ledgers, an array of private and permissioned blockchains that are all interoperable through robust and standardized mechanisms, would collectively comprise the new type of internet, sometimes referred to as Web3. This paradigm, where a heterogeneous set of underlying systems is brought together to achieve seamless execution of business use cases, is exactly where Mastercard has specialized experience, spanning several decades.

To embark on a similar journey in Web3, Mastercard would need to interoperate with public blockchains, and Mastercard would need to establish secure, efficient and scalable channels for cross-network communication. This includes the implementation of standardized protocols to ensure seamless asset transfers and data sharing. Mastercard would also need robust mechanisms for transaction validation and consensus across different blockchain architectures, as well as advanced cryptographic techniques to maintain security and privacy while enabling transparent and traceable transactions.

Interoperability with blockchains can significantly enhance existing payment rails by introducing real-time settlement capabilities, reducing counterparty risks and lowering transaction costs. It can also provide a new level of transparency and traceability in transactions, which is vital for compliance and fraud prevention. Moreover, blockchain integration can facilitate access to new asset classes and liquidity pools, expanding the scope and efficiency of payment networks like Mastercard.

Using Multiple Blockchains

Public blockchains are based on the tenets of decentralization and transparency, while permissioned blockchains allow more privacy and control for authorized participants. Different public and permissioned blockchains have emerged to cater to diverse use cases and meet the specific needs of users. Multiplicity of blockchains also improves network performance and scalability, and offers more choice and flexibility to developers for application customization and innovation.

Mastercard is exploring both public and permissioned blockchains for building applications and products that provide customers, merchants and businesses with more choice in how they move digital value. As part of its Mastercard's Multi-Token Network (MTN), Mastercard is working with banks and application providers to facilitate transactions using tokenized bank deposits over permissioned blockchains and DLTs.

Short- and Long-Term Outlook

In the short run, blockchain will likely enhance Mastercard's transaction efficiency, security and transparency, particularly in cross-border payments and settlements. In the long run, over the next 5-10 years, blockchain could fundamentally transform the financial industry's infrastructure, enabling Mastercard to operate in a more interconnected, innovative and efficient manner. This could involve embracing new business models, entering new markets and offering a broader array of financial services that are aligned with the evolving digital economy.

In the near future, major financial entities, such as central and commercial banks, are likely to embrace blockchain technology by issuing new forms of regulated digital assets. These assets could range from CBDCs, which aim to digitalize national currencies, to tokenized banking deposits and real-world assets, creating a more fluid and dynamic financial ecosystem. As these institutions adopt their preferred blockchain platforms, there will be an increasing demand for solutions that can bridge these diverse assets, fostering a more integrated financial landscape.

Interoperability Challenges, Opportunities and Solutions

Mastercard's strategic vision is geared towards creating a seamless and interoperable environment where assets from various platforms can interact without friction. By focusing on the interoperability and fungibility of assets, Mastercard aims to remove barriers between different blockchain networks, enabling assets to move and be recognized across these platforms. This approach not only enhances the utility and accessibility of digital assets but also paves the way for a more interconnected and efficient blockchain ecosystem.

A key challenge to blockchain interoperability is to ensure that the security and integrity of blockchain networks is not compromised due to increased attack surface and implementation complexity. Interoperability solutions must also accommodate data protection and regulations across jurisdictions, meet compliance requirements, and maintain privacy for cross-network transactions.



NORTHERN
TRUST

SPOTLIGHT: NORTHERN TRUST

Northern Trust started its blockchain adoption journey in 2015 and has brought multiple use cases to the market.

In 2017, Northern Trust observed that there were numerous inefficiencies in the fund administration processes for private equity (PE) funds. This led to the development of a blockchain-based solution to resolve pain points like complex PE lifecycles and the lack of real-time insights and transparency for all parties, including regulators.¹

In 2018, Northern Trust further developed a solution to support an automated, “end-to-end” capital-call process, enabling a real-time audit of PE lifecycle events directly from a blockchain and deploying legal clauses as smart contracts to streamline the traditionally document-heavy process. The solution was subsequently transferred to [Broadridge](#) in 2019 for further development into an industry-wide utility.²

In 2019, Northern Trust announced a collaboration with [BondValue](#) to develop and deliver a bond-fractionalization solution using blockchain technology. Northern Trust was aligned with BondValue’s vision of leveraging tokenization and fractionalization to expand the investor base of corporate bonds. Northern Trust also supported BondValue’s R&D process. In 2020, together with BondValue, Northern Trust completed its first fractionalized, blockchain-based bond trade.³

In 2023, Northern Trust announced the development of an institutional voluntary carbon-credit marketplace. The transaction on the initial minimum viable product (MVP) digital carbon-credit platform validated the assumption that blockchain technology could streamline a carbon-credit market that is impeded by problems associated with data provenance and lack of institutional-grade solutions. It marked a first step toward providing an industry-wide solution enabling institutional investors to digitally access carbon credits from leading project developers.⁴ With the successful MVP transaction, Northern Trust plans to deliver the full launch of the voluntary carbon-credit marketplace in 2024.⁵

Northern Trust’s blockchain adoption journey is rapidly evolving. While use cases might have changed over time, there remains a consistent emphasis on equipping clients with data-driven insights, addressing inefficiencies and providing a secure platform to trade.

¹ [Northern Trust and IBM Pioneer Use of Blockchain Technology to Help Transform Private Equity Administration](#)

² [Northern Trust to Transfer Pioneering Private Equity Blockchain Technology Platform to Broadridge](#)

³ [BondValue and Northern Trust Collaborate to Complete World’s First Blockchain-based Bond Trade](#)

⁴ [Northern Trust Developing Digital Platform for Institutional Voluntary Carbon Credit Transactions](#)

⁵ [Northern Trust Bets on Carbon Credit Demand as Emission Goals Loom](#)

Using Multiple Blockchains

Within the next two to three years, there are likely to be additional financial market infrastructure providers coming into the marketplace to develop platforms and industry utilities. This risks further fragmentation of the market. The digital assets industry is still in its infancy and industry standards have yet to be established.⁶ The same could be said for banks that have built or are in the process of building infrastructure to support their digital asset ambitions. Fragmentation of the market would lead to a lack of liquidity across the marketplace, create additional barriers and increase transaction costs. Northern Trust's role is to explore as widely as possible and connect with multiple providers to test the viability of each use case. The ability to connect with different blockchains is key to this process.

On a longer-term basis, Northern Trust expects the market to consolidate, with dominant players providing standards and infrastructure to improve the adoption of digital assets. Northern Trust projects that by 2030, the size of its digital assets market will range from 5 percent to 10 percent of the approximately \$13 trillion USD it holds under custody today.⁷ To provide the best services to clients, Northern Trust will have to play the role of an active participant in the ecosystem, connecting to multiple blockchains but with different approaches at various points.

Northern Trust is currently working with private networks only. This is due to regulatory obligations and the organization's commitment to asset safety. While Northern Trust remains on private networks, it is preparing for the future by focusing on the usage of Ethereum Virtual Machine (EVM) chains to ensure compatibility with the broader ecosystem.

⁶ *Custody Reimagined: The Outlook for Global Securities Services in 2030*

⁷ *Leveraging Digitized Banking in Pursuit of Real-Time Payments*

Requirements for Public Blockchain Interoperability

Interfacing with public blockchains involves both regulatory compliance and technical considerations for global banks like Northern Trust. While regulations vary across jurisdictions, compliance typically involves an ability to:

1. Protect clients' private and confidential information.
2. Perform accurate know-your-customer (KYC) procedures.
3. Limit bad actors from money-laundering and terrorist-financing activities.

From a custodian perspective, Northern Trust must maintain effective control and ownership of clients' assets if they are on a public chain. While there are robust tools and services to help satisfy these requirements, there also needs to be more regulatory clarity and well-established case studies. In addition, approval from local regulators is important. There are different sets of requirements across various jurisdictions and that might affect speed in pursuing interoperability with public chains.

Other technical requirements include data traceability, data segregation, storage of keys and cloud data onshore, and establishing guardrails of captured data. Finally, the selection of a consensus mechanism and the return of incentive rewards, for example, will also affect the ability to interoperate with public chains, due to various regulatory requirements.

Blockchain Interoperability Challenges

Northern Trust has faced multiple challenges while attempting to achieve blockchain interoperability.

For example, having a disparate set of smart-contract languages became an unanticipated technical challenge. Another challenge is irreversible transactions across chains, which is more of an issue on public chains given that transaction times can vary. Other challenges include connectivity between chains, security of rails and the messaging needed for interoperability.

Northern Trust is currently conducting a research project with the Singapore Blockchain Innovation Program (SBIP) – a research institute based in National University of Singapore (NUS) to investigate the best ways to achieve interoperability for tokenized carbon credits.⁸ A key challenge includes the methods for swapping tokens. Mint-and-burn, mint-and-lock and atomic-swap approaches all have their own nuances and challenges to resolve.

One challenge of a mint-and-lock model is the legal questions around having an asset represented across two chains, which could lead to concerns about a duplication of value. There are also potential inefficiencies in reconciliations across different chains. While an atomic swap would be ideal in theory, it also introduces technical complexity. Northern Trust is thus identifying the best way to move tokens across chains.

Benefits of Public Blockchains

The often-discussed benefit of integrating with public blockchains is the ability to break down market access barriers and increase liquidity for on-chain assets. Integrating with public blockchains broadens access to assets. This is important as improved liquidity can help drive adoption with other ecosystem players, allowing Northern Trust to realize its longer-term vision with a shorter runway. While there are benefits to the adoption of public blockchain, Northern Trust will take guidance from the regulators to ensure that it adheres to the high standards of asset safety and security as a global custodian.

⁸ *Northern Trust, NUS School Of Computing and NUS Asian Institute of Digital Finance Join Forces to Support Blockchain Development for Institutional Use*



SPOTLIGHT: CENTRIFUGE

Centrifuge provides the infrastructure to tokenize, manage and invest in a diversified portfolio of tokenized real-world assets, ranging from treasury bills to consumer credit and real estate.

The idea is to remove unnecessary intermediaries from the financial supply chain to connect borrowers and lenders directly. This cuts costs and provides more equitable access to capital and credit. Through Centrifuge, asset managers can tokenize and manage their funds fully on-chain, automating many steps of the process to run more efficient operations. Investors get exposure to yield from tokenized assets, transparency of blockchain-enabled applications and efficiencies from on-chain composability.

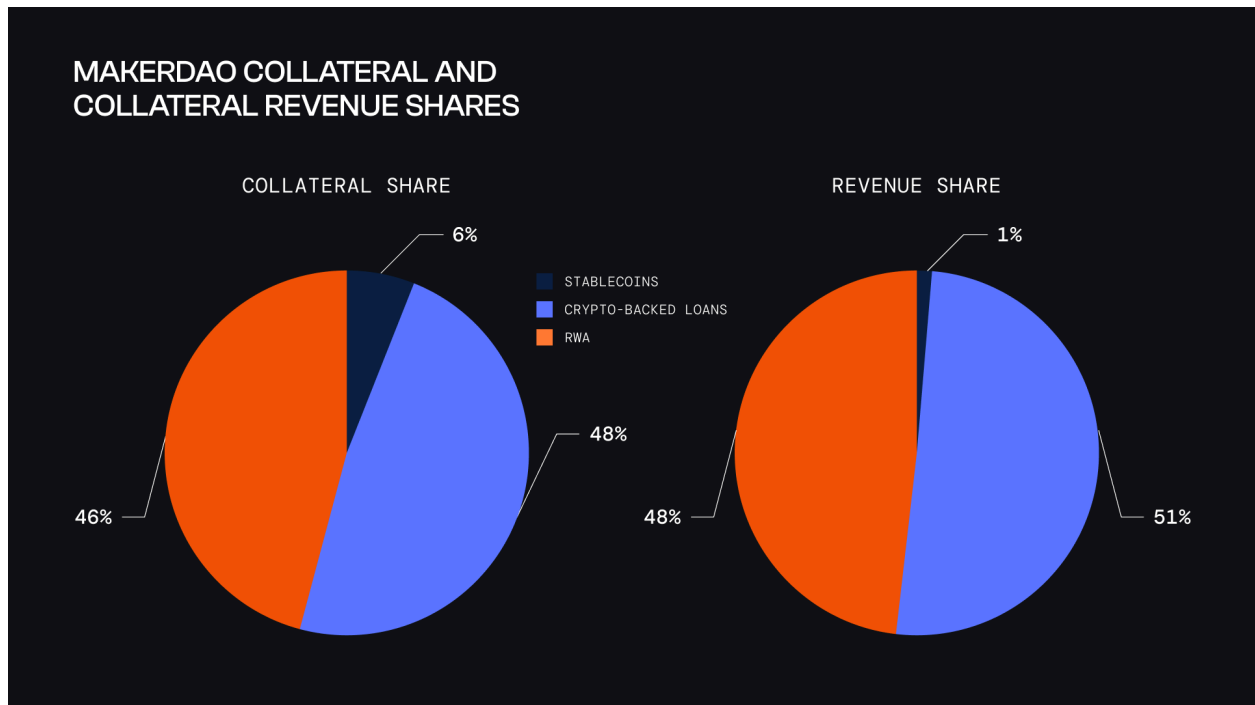
Where traditional financial markets are fragmented, opaque and inefficient, blockchain technology offers an opportunity for significant improvements. A fundamentally improved foundation for transparency, integrations and efficiency can begin to address significant gaps and challenges in traditional financial markets.

Centrifuge's goal is to use tokenization to reduce the cost of access to capital, which is often inflated and bloated due to expensive intermediary infrastructure. Blockchain technology can also heighten transparency and visibility within a specific investment asset or across many actors within a market. Shared and trusted ledgers can improve the nature of cross-border finance or even between siloed systems in the same region, such as different departments within a large asset manager that each use their own proprietary software for tracking transactions.

CENTRIFUGE TOTAL LOANS & ACTIVE LOANS			
PROTOCOL	NETWORK	TOTAL LOANS	ACTIVE LOANS
CENTRIFUGE	ETHEREUM	\$570,890,384	\$282,898,197

Source: [RWA.xyz](#).

Centrifuge is a live platform with \$283 million total value locked (TVL) and \$571 million in real-world assets financed all-time as of April 2024, according to industry tracker [RWA.xyz](#). Centrifuge believes decentralized finance has a significant role to play within tokenization, removing intermediaries and not creating new ones.



Source: [Galaxy Insights](#).

Founded in 2017, Centrifuge has been an early pioneer of RWA innovation. Its partnership with MakerDAO proved that stablecoins could leverage real-world assets for stability and revenue. Since then, RWAs have become an integral component of MakerDAO's economic success and its dollar-pegged stablecoin, DAI. According to Galaxy Insights, around 46% of DAI in circulation are collateralized by RWAs and 48% of MakerDAO's estimated annualized revenue comes from this collateral type.

Using Multiple Blockchains

Centrifuge has a modular, multichain architecture to enable flexibility in scaling and building an RWA ecosystem. Liquidity Pools, Centrifuge's cross-chain solution to aggregating capital across the fragmented blockchain space, is live on Arbitrum, Base, Celo and Ethereum with plans to launch on additional blockchains based on demand. The goal is to provide users with fast, low-cost transactions and seamless interaction across many networks and ecosystems.

Centrifuge's Liquidity Pools are smart contracts that can be deployed on any Ethereum Virtual Machine (EVM)-based chain to allow users on these chains to invest in pools on Centrifuge. Issuers using Centrifuge can source liquidity on any chain, in any currency, and manage it in one place.

To invest in RWA pools, investors need to pass know-your-customer/know-your-business (KYC/KYB) checks by the issuer of the pool. The Centrifuge multichain protocol automates the management of permissioned investors across all chains.

Interoperability Challenges

Centrifuge highlighted several challenges in ensuring blockchain interoperability:

- Building an experience where investors and issuers use the same simple product, regardless of the blockchain with which they interface.
- Building a secure multichain protocol. Centrifuge has engaged multiple audits and rewards researchers for discovering vulnerabilities.
- Indexing data from users across all chains. Centrifuge works with Subquery, which supports multichain indexing to solve this issue.

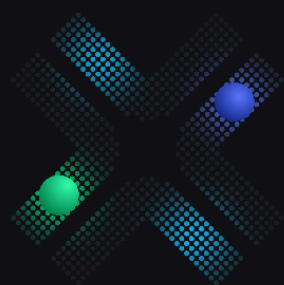
Benefits of Public Blockchains

Integrating public blockchains into Centrifuge brings several potential benefits to investors and issuers.

- **Cost savings:** Standardization and programmability in DeFi simplify processes and reduce the need for intermediaries, leading to cost savings for investors and depositors.
- **Efficiency:** Tokenizing assets on a public blockchain eliminates manual intervention and lowers operational costs. Integration with DeFi's ecosystem further enhances efficiency, making it a cost-effective alternative to traditional finance.
- **Transparency:** Public blockchains provide a transparent and immutable record of transactions, increasing trust and reducing the risk of fraud.
- **Automation:** Smart contracts on public blockchains automate steps in asset financing processes, reducing the need for human intervention and increasing efficiency.
- **Accessibility:** Public blockchains are available 24/7/365, allowing investors and depositors to access their assets at any time, from anywhere in the world.

Long-Term Goals

Centrifuge's goal is to bring the benefits of tokenization and on-chain finance to asset managers of all sizes to bring lower cost of capital to the world. By operating as a decentralized protocol, Centrifuge offers trust, transparency and security by removing middlemen, reducing costs, and providing global access to financial services and investments, empowering individuals and businesses alike.



PRESENTED BY

