Monetary Authority
of Singapore

Interlinking Networks Technical Whitepaper

Contents

Disclaimer

This report and its contents are made available on an "as-is" basis without warranties of any kind. The content in this report does not constitute regulatory, financial, legal or any other professional advice and should not be acted on as such. MAS shall not be liable for any damage or loss of any kind howsoever caused as a result from the use of the information contained or referenced in this report.

This paper does not seek to address policy objectives or recommend any specific technical solution. Whilst the content strives to provide more clarity on the interlinked network model, the authors of this paper make no representation or guarantees on the performance or adequacy of the proposed technical solutions. The examples used in the paper are only for illustration purposes.

Document Version

Version	Date	Author	Rationale
1.0	Nov 2023	Monetary Authority of Singapore	First publication

1 Introduction

The introduction of digital assets is challenging conventional thinking about financial transactions, money as a medium of exchange and the role of trusted intermediaries. Today, financial institutions perform critical roles as trusted financial intermediaries. Messages are exchanged and transactions are cleared amongst financial institutions usually on private infrastructure such as over-the-counter services before settlement through various intermediaries. If there were more direct ways of transacting, this could improve the current state of financial markets.

As part of ongoing efforts to improve efficiency of financial systems, financial institutions are exploring asset tokenisation and distributed ledger technology (DLT) to enable atomic settlement or the simultaneous exchange of two linked assets in real-time. This removes duplicative reconciliation and reduces the need for large pre-funding accounts. With fewer intermediaries required to facilitate transactions, counterparty risks are reduced which could result in faster processing and lower costs. Research by McKinsey estimates that if DLT were used in cross-border transactions, it could bring about cost savings of $4 billion annually[1].

To capture this potential, financial institutions have developed capabilities across various distributed ledgers, with some setting up DLT platforms within their own ecosystems. However, this leads to proliferation of platforms in the market and fragmentation of liquidity. Instead, a preferred approach would be the establishment of a common network where financial activities can be concentrated. That said, establishing common networks while maintaining independence requires significant legal, regulatory and policy coordination across jurisdictions[2]. An alternative is to connect each network bilaterally to enable digital assets to flow between networks.

Achieving interoperability with existing financial infrastructure and mitigating against fragmented markets are themes examined under Project Guardian. Project Guardian was established by MAS as a collaborative initiative with the financial industry to explore applications in asset tokenisation while managing risks to financial stability and integrity.

This paper builds upon the earlier published *Project Guardian: Enabling Open and Interoperable Networks* report. There are three prevailing approaches towards achieving open and interoperable networks today. First, the establishment of a common infrastructure based on a flat network structure. Second, a layered approach, with a foundational digital infrastructure providing the base global layer upon which other networks could be developed. The third approach is to interlink heterogenous digital asset networks which is the focus for this paper. The paper will present a technical overview of cross network linkages and proposes a common model that can be used to enable asset transfers across networks.

[1] Blockchain and retail banking: Making the connection (McKinsey & Company, 2019)
[2] Project Dunbar: International Settlements using multi-CBDCs (MAS, 2022)

2 Problem Statements and Motivation

Good progress has been made in proof of concepts and pilots of digital assets. However, the proliferation of digital asset networks which are closed and siloed could lead to greater fragmentation of liquidity in the wholesale funding markets in the long run and limit the institutional adoption of digital assets.

Some of the key challenges to commercialisation and scale will be highlighted in this section.

2.1 Fragmentation of markets

Distributed ledger technology-based networks provide a single source of record keeping for transactions across different participating financial institutions. However, the lack of convergence towards a common universal platform with harmonisation across technical, legal, regulatory and product standards has increased the risk of market fragmentation.

Due to prudence, financial institutions have primarily focused on private and permissioned blockchains which provide assurances that transactions happen with known counterparties. In the absence of interoperability, the risks of liquidity fragmentation are exacerbated if these platforms are built as isolated walled gardens, where access is only granted to selected partners or customers of a financial institutions. In such arrangements, investors would need to directly open accounts and pledge collaterals bilaterally with multiple platforms, or indirectly through intermediaries with access to these platforms. This limits their ability to pool assets together and curtails trading across multiple venues, resulting in a reduced network effect and hampers innovation.

To address this, concerted efforts by the public and private sector are needed to link digital assets and networks together. Whilst digital asset initiatives gaining traction through pilots or experimentation across the different asset classes, the urgency to unify efforts for scale have intensified.

2.2 Network Structures

Settlement systems can be built as standalone platforms with access limited to a small group of participants; alternatively, access can be extended to a wider group of participating entities through interlinking arrangements with other settlement systems. This section provides a recap of the three network structures archetypes discussed in the *Project Guardian: Enabling Open and Interoperable Networks paper*[3].

Model 1: Flat networks

In flat networks, participants join a common platform and may transact bilaterally or with multiple counterparties. Transactions are atomically settled on a delivery-versus-payment (DvP) or payment-versus-payment (PvP) basis.

[3] Project Guardian: Enabling Open and Interoperable Networks (BIS and MAS, 2023)

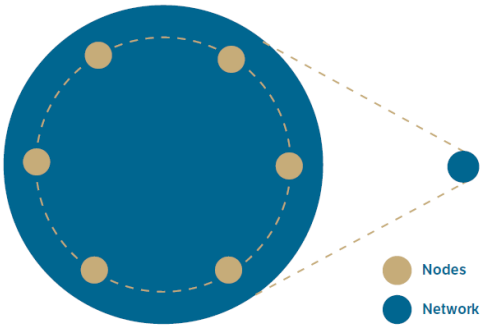

Figure 1: Illustration of a flat network

Flat networks require a common set of governance terms (e.g., settlement finality, access, etc) and alignment onto a common technical stack and standards. Establishing a multi-party governance structure while maintaining independence requires coordination across jurisdictions. Examples of such networks include Project Dunbar[4] and mBridge[5] where multi-CBDC platforms were explored for cross-currency and cross-border payments.

Model 2: *Layered networks*

The layered network is set up as a series of networks where participants transact in the upper layers while these transactions are consolidated and committed to the lower levels' ledger. This structure allows for transactional efficiency in the upper layers. Participants can transact in the upper layers (e.g., Layer 2 or L2) in such a network where individual transactions are processed and recorded on its own ledger while a summary of the transactions are then posted on to the lower levels' ledger (e.g., Layer 1).

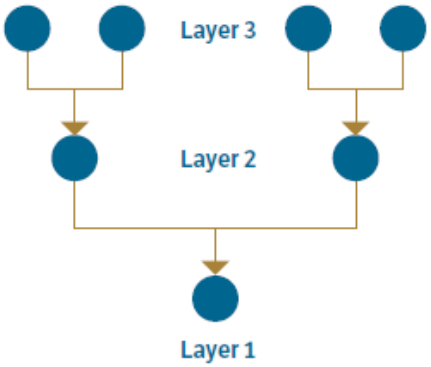

Figure 2: Illustration of a layered network

Such a setup reduces the traffic hitting the core ledger (e.g., Layer 1 or L1), and consequently improves the scalability and performance of the layered network as a whole. This implementation when applied to financial transactions ensures that costs remain viable, although this increases the time taken for a transaction to be finalised.

Model 3: Interlinking distinct networks

In situations where participants may not agree to join a single unified ledger or if the applications are better suited to occur on a separate ledger, there is a need for a mechanism to connect different networks. Interlinked networks can consist of a network of independent or layered networks,

[4] Project Dunbar: International Settlements using multi-CBDCs (MAS, 2022)
[5] Project mBridge: Experimenting with a multi-CBDC platform for cross-border payments (BIS, 2023)

application-specific chains, or sidechains, each with their own distinct governance framework and other customisations. This set up allows for bridges to connect independent or layered networks through cross-network protocols.

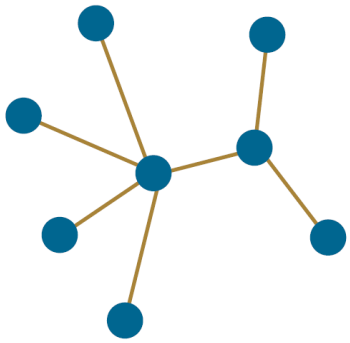

Figure 3: Illustration of interlinked networks

Such forms of interlinking can enable use-cases involving transactions of digital assets and digital currencies. Specifically, cross-network communication allows for digital currencies and digital assets to be transacted across separate networks (i.e., Token vs Account based) for cross-border transactions.

For instance, digital currencies on separate networks can be transferred from the originator to intermediaries and ultimately to the beneficiary. In Cedar x Ubin+[6], the concept of vehicle currencies was explored in a cross-border cross-currency payment. With intermediary banks facilitating the FX component in the cross-border payment, the simultaneous settlement of all transaction legs within a multi-currency cross border payment across different ledgers was attained.

Beyond the connectivity to new DLT infrastructure, interoperability with traditional settlement systems will also be considered.

This paper focuses on model 3, *Interlinking distinct networks* and provides an Interlinked Network model (INM) that can be referenced to support i) the movement of assets across networks; and ii) orchestrate the coordination of several asset transfers within their respective originating ledgers.

[6] Project Cedar Phase II x Ubin (New York Innovation Center (NYIC) & MAS, 2023)

3 Interlinked Network Model (INM)

Currently, connectivity between financial infrastructures is achieved through message passing, or application programming interfaces (API) calls to centralised ledgers. However, a future state financial infrastructure, where tokenised representations of financial assets are transferred directly and atomic settlement occurs across different ledgers, would require a vastly different approach.

This section discusses the INM as reference for exchanging digital assets and currencies seamlessly across different networks. Bridges are employed to interlink networks and use cross-network protocols to conduct messaging and asset transfers between these networks. To ensure interoperability with traditional rails, this would also cover the communication between DLT-based networks and traditional settlement systems.

Figure 4 provides an overview of the INM and the interactions between the components that enable cross-network messaging and cross-network asset transfers.

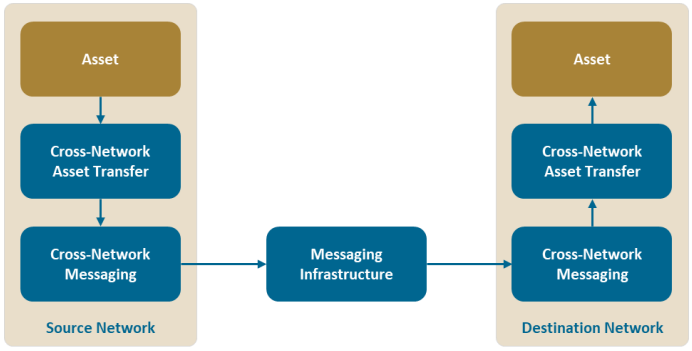

Figure 4: INM overview

Cross-network messaging

To facilitate messaging between networks, bridges use cross-network protocols such as the General Message Passing (GMP) protocols to send messages between these networks. They enable interoperability between different networks, subnets, or layers across the ecosystem. These messages pass information such as request for quotes (RFQs) and trade confirmations, queries around KYC and other credentials, digital asset, and currency transfers, and more from the source network to the destination network.

In some instances, GMP protocols constitute part of the core network architecture and enable intra-network interoperability (e.g., Avalanche's Warp Messaging and Cosmos' Inter-Blockchain Communication Protocol), while in other instances, they are used to effectuate inter-network interoperability (e.g., Axelar's General Messaging Protocol, Chainlink's Cross-Chain Interoperability Protocol, LayerZero's Omnichain Interoperability Protocol).

This can also be applied to interconnecting DLT-based networks with existing payment systems as explored by Swift[7].

[7]Swift unlocks potential of tokenisation with successful blockchain experiments (Swift, 2023)

Security is of high importance for such cross-network protocols as there is a need to ensure authenticity and integrity of the messages and data passed across different networks. Many bridges today employ GMP protocols that rely on one or more nodes (referred to as validators, relayers and oracles) to pass messages from the source network to the destination network.

Cross-network asset transfers

Cross-network asset transfers involve the movement of digital assets or asset entitlements and ownership from one network to another. To facilitate this, bridges are built on top of cross-network protocols. Generally, bridges are operated by networks of validators or oracles to validate transfers of some type between networks. The trust level, degree of centralisation, and security level are highly dependent on the operator of these nodes, the number of nodes, the identity of the validators or oracles, the distribution of nodes and the consensus mechanism. Additionally, cost is a consideration as validators require incentives to provide such services, which would impact costs to the users.

The use of cross-network protocols enables private and public networks to connect without the need for participants to be part of a common platform. For instance, private networks such as the Calastone[8] network could be connected to the ADDX[9] platform through bridges for digital assets to be transferred from one platform to another.

3.1 Models of Bridges

This section features three models of interlinking networks with bridges. These bridging models can be combined or modified according to specific requirements and constraints on the connecting network. Each has its advantages, trade-offs, and ideal use cases, and the choice of bridge type often depends on factors like security needs, transaction latency, and cost considerations which will be covered below.

- **Lock and Mint**
- **Burn and Mint**
- **Atomic Swap**

Lock and Mint

In lock and mint, originating asset tokens are locked on the source network within a smart contract before they are subsequently minted on the destination network. This model essentially creates a new asset on the destination network, also known as a wrapped asset. The lock mechanism secures the originating asset in the source network which backs the wrapped asset on the destination network.

In order to coordinate the lock and mint condition, a separate message hub is required alongside the bridges deployed on the source and destination network as illustrated in Figure 5 below.

[8] Calastone is a global funds network for financial organisations that aims to digitalise the global investment funds marketplace.

[9] ADDX is an investments platform that provides access to private investments such as private equity and hedge funds.

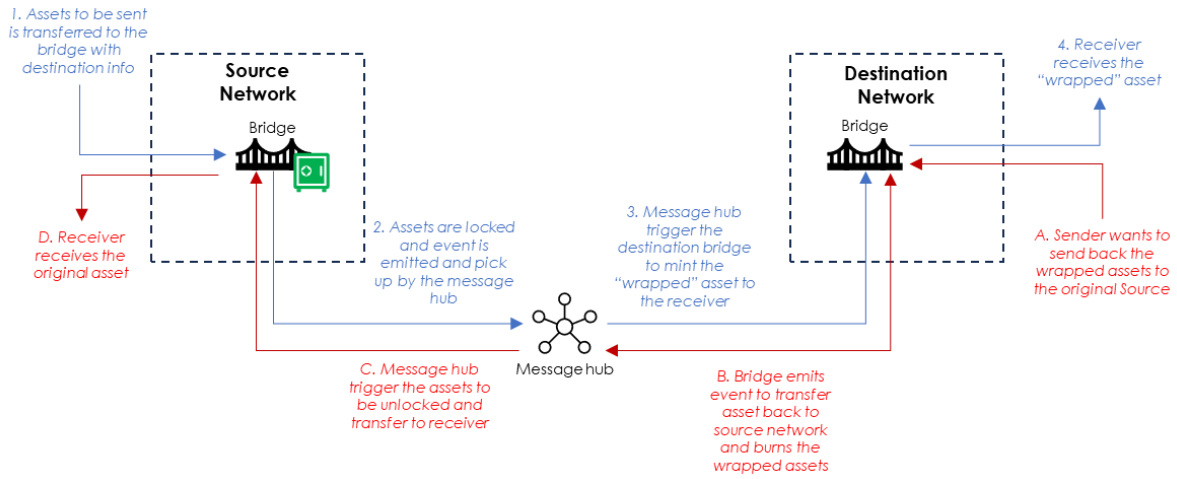

Figure 5. Lock and mint flow

The message hub plays a key role here to monitor the events emitted from its connected networks. It will also trigger the appropriate mint or unlock event messages to the receiving bridges, while ensuring that quantity of the originating assets in the source network and the quantity of wrapped assets in the destination network are balanced, to prevent double-spending scenarios. Bridge smart contracts are required on each network to secure the assets by locking them either i) in the bridge, or ii) on a connected vault service. The bridge also plays the role of minting the wrapped assets on the destination network.

Pros

- Any asset or token could be wrapped even if it was not developed with such a capability. This allows for a wrapped representation of the token to be minted on the destination chain.
- This model enables the issuer the flexibility to allow the bridge operator to create wrapped assets with the originating assets in the source network. This means that the issuer would not be required to operate or maintain the bridging infrastructure as such issuers will likely be financial institutions. However, this also creates a risk which will be covered below.
- Digital assets are detained rather than erased, preserving asset liquidity from the source network. This ensures a tangible link between the original asset and the wrapped asset, and that the locked assets remain retrievable. Furthermore, digital asset owners are provided the assurance that the assets still exist in the source network.

Cons

- Lock and mint bridges can potentially create asset fragmentation depending on the bridge used. For instance, an asset could have multiple wrapped versions in the same destination network if different bridges were used for the asset transfer. There could be cases where the asset is wrapped across multiple networks which creates complexity in the redemption process.
- As lock and mint bridges enable the trading of multi-assets on a single network, it inadvertently also creates a honeypot for malicious actors. Therefore, the bridges need to be secured adequately to withstand the various attacks from such malicious actors.
- In situations where third parties such as bridge operators can create wrapped assets on behalf of the issuer, the assets are transferred from the issuer to the bridge operator. For this, the bridge operator will need to ensure the originating assets are held securedly on behalf of the

asset owner until a transfer back to the source network is triggered, and the wrapped asset on the destination network is burnt.

- Common security vulnerabilities relating to lock and mint bridges include weak on-chain and off-chain validation, collateral checks, improper handling of native tokens and misconfigurations. Furthermore, all possible attack vectors must be tested against, alongside constant monitoring and regular updates against new forms of vulnerabilities and attacks.
- Other significant risks for this model include double counts, potential issues with asset restitution (in case of error or fraud), risks where controls implemented could be circumvented on the smart contract level, and the potential for assets to become locked if the cross-network protocol has an outage of key nodes.

Burn and Mint

In burn and mint, asset tokens are burnt on the source network and minted on the destination network. This model was also explored and employed in Project Mariana[10].

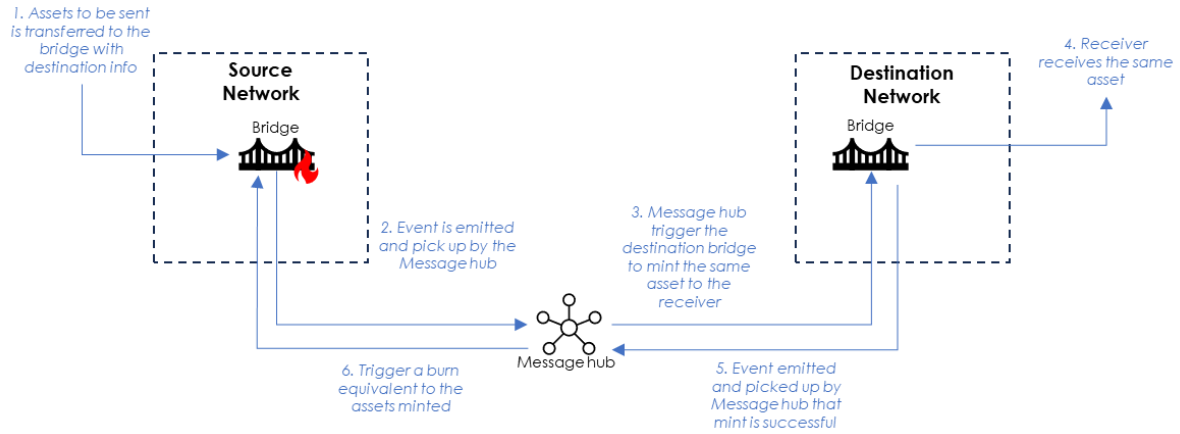

Figure 6. Burn and mint model

Similar to the lock and mint model, the burn and mint model requires a message hub between the network bridges to coordinate the asset transfer. The asset is first transferred to the bridge on the source network and subsequently emits a mint event. This mint event emitted from the Source network is picked up by the message hub and subsequently relayed to the destination network. Once the mint is successful on the destination network, the event emitted will be picked by the message hub which will trigger a message to burn the originating assets in the bridge on the source network. Subsequently, the equivalent asset is minted on the destination network.

Pros

- As burn and mint model bridges are typically maintained by the asset issuers and tend to support asset transfers of all the issuer's assets, this reduces potential third-party risks highlighted in the lock and mint model, and the assets will remain in the control of the asset issuer in the mint to burn process.
- Assets that are transferred using burn and mint bridges are natively issued on the destination networks. Unlike the lock and mint model where there could be multiple forms of wrapped tokens depending on the bridge used, natively issued assets would only exist as-is across networks.

[10] Project Mariana: Cross-border exchange of wholesale CBDCs using automated market-makers (BIS, 2023)

- This reduces risks such as double counting as the asset will only exist on one network.

Cons

- Burn and mint model bridges can still be compromised by malicious actors. There is a risk where malicious actors can possibly obtain control of the bridge to freely mint and burn assets. An example would be the infinite token mint where the attackers could create malicious transactions to falsify the burning of tokens in the source network while also being able to trigger the "infinite" minting of the token in the destination network.
- In the case where the asset issuer decides to use a bridge operated by a third-party provider, although the asset issuer will not need to operate and maintain the bridge infrastructure, this introduces third-party risks such as the transfer of asset ownership to the third-party. Thus, in addition to the security design of bridges, disaster recovery is also key aspect that needs to be further explored.

Atomic Swap

In Atomic Swap, asset tokens on the Source network can be directly exchanged for asset tokens in the Destination network. Under this mechanism, the digital assets do not move across networks but instead remain in their respective native networks. Thus, on top of connecting DLT networks, this allows for connectivity between traditional infrastructure and DLT networks for digital assets to be atomically exchanged.

To enable communication between these networks, bridging solutions such as Hash Time Lock Contracts (HTLCs) can be employed to coordinate the movement of assets between participants in the native networks. The message hub in this model is an intermediary that facilitates the routing of assets between separate networks by maintaining accounts on multiple networks that are used to settle transactions, while cross-network notaries are responsible for validating a transaction at the source and destination network before the funds are released. HTLCs are deployed on both the source and destination networks to facilitate the atomic exchange of the assets. This design is employed in Cedar x Ubin+ where CBDCs are exchanged across two or more different networks to facilitate a cross-border wholesale payment.

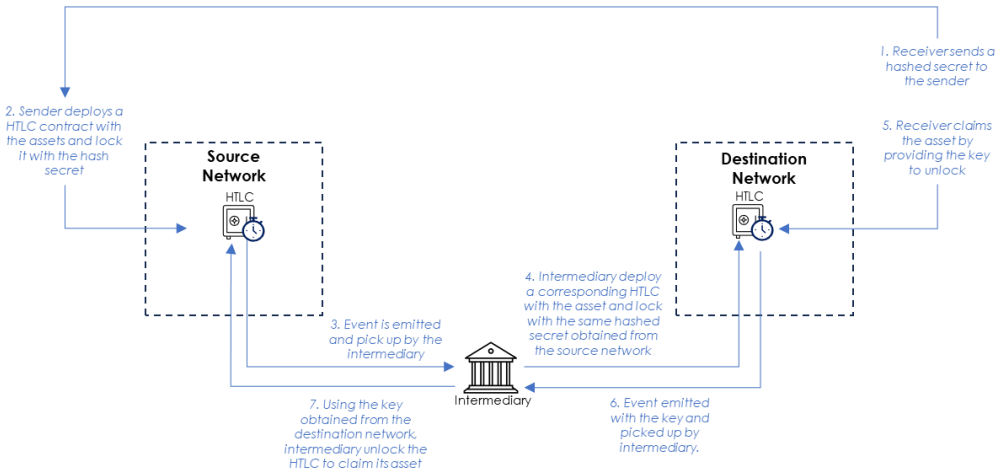

Figure 7. HTLC process flow

Figure 7 illustrates the atomic swap with HTLCs.

1. A secret and its corresponding hash are generated by the receiver, and the hashed secret is relayed to the sender.
2. On the source network, the sender transfers the originating asset to the originating HTLC addressed to the intermediary and locks it with the hashed secret while setting a time lock period for the funds to be claimed. If the originating assets are not claimed within the specified time lock period, the sender can initiate a re-claim.
3. The originating HTLC transaction event is emitted from the source network and picked up by the intermediary.
4. The intermediary deploys a corresponding HTLC in the destination network addressed with the destination assets to the receiver and locks it with the same hashed secret in the originating HTLC.
5. The receiver, upon receiving the notification of the destination HTLC transaction event, proceeds to unlock the destination HTLC with the key (secret) and claims the destination assets. This triggers an event with the hashed key being published to the intermediary in the destination network.
6. The intermediary picks up the event and uses the hashed key to unlock the originating HTLC and claims the originating assets.

The HTLC model bears similarity to the symmetric key cryptography where it requires the sender and receiving party to have prior knowledge of a shared secret, while the key in this case is only known by the receiver. In addition to the hash key, information on the originating and destination asset, time hash (time period), receiver's address, and transaction references is also required.

<u>Pros</u>

- Enables parties in a liquid FX cross-border transaction to deal directly without centralised platforms or exchanges, minimising intermediaries which in turn reduces inefficiencies such as costs and speed.
- Parties to the transaction must acknowledge the transaction which reduces risks of fraud and default.
- Assets remain on their source networks which preserves native attributes and benefits.
- Ensures either all legs of the multi-leg payment to settle or none settle at all.
- Exchange of assets can take place across traditional and DLT networks.
- Time period for expiry of HTLCs ensures that assets are not locked indefinitely.

<u>Cons</u>

- If time locks are not properly set up, there could be situations where the receiver can claim the destination assets, and the sender can initiate a re-claim on the originating asset before the intermediary is able to do so. Thus, the time expiry set in the originating HTLC must be greater than that in the destination HTLC to ensure the intermediary has sufficient time to reclaim the originating asset in the source network.
- Where illiquid currencies are involved, intermediaries are still required to be to facilitate the transactions between the source and destination networks.
- Automated by smart contracts which could be attacked maliciously.

3.2 Components

The core components of an INM are as follows:

Asset Transfer Module

The asset transfer module manages the assets in both the source and the destination networks while the asset is transferred across networks.

- In the source network, this module validates an asset transfer before it locks or burns an asset.
- In the destination network, this module mints and transfers the asset to the receiver.

Communication Module

The communication module handles the messages between the source and destination network via a trusted infrastructure.

- In the source network, it validates and ensures the accuracy of the messages before potentially routing and emitting an event for the trusted infrastructure.
- In the destination network, it verifies the incoming messages against the source network via a verifier of the attested message by the trusted infrastructure.

Trusted Infrastructure

The trusted infrastructure provides a channel for messages to be securely transmitted between different networks. This infrastructure can be implemented as a traditional centralised system or as a separate network.

- It monitors events in a source network, verifies the finality of the block/event and forwards the event to a destination network.
- It also provides a verification and attestation mechanism to ensure transactions/asset states in the source and destination network remain in sync. Some of these verification mechanisms may involve cryptographic signing, multi-party computation (MPC), zero knowledge and/or other optimistic proofs.

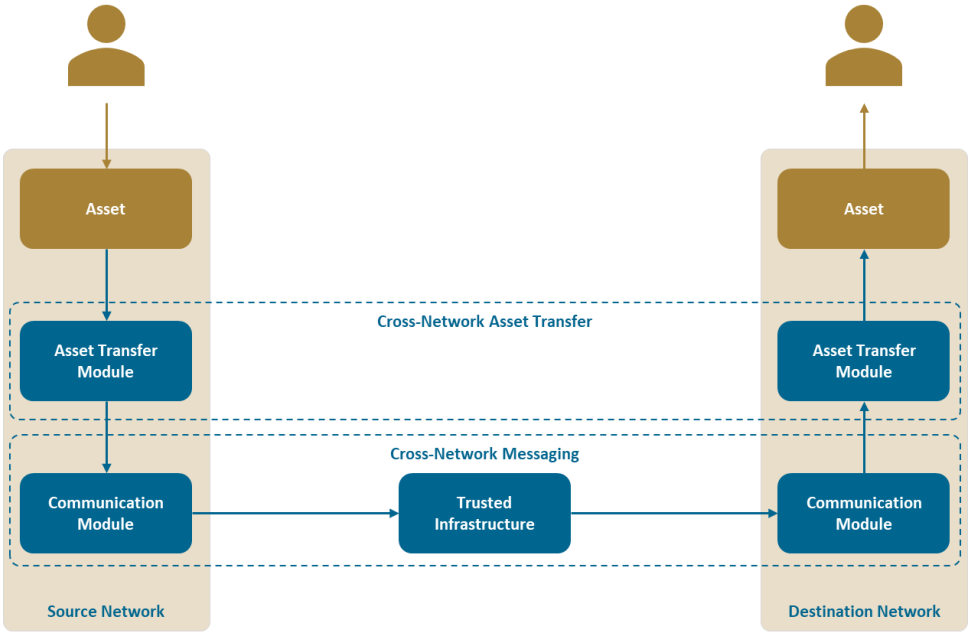

Figure 8: INM components

3.3 Lifecycle of Cross-Network Asset Transfers

This section shows a generic flow of how an asset can be transferred between two networks and the interactions between these components. This flow is not the only implementation of cross-network asset transfers and other implementations may include components and features to address scalability, security, transaction fees of different networks and such, which is out of scope for this section.

The asset transfer can be categorised into 3 sub-flows: (1) source network, (2) trusted infrastructure, and (3) destination network.

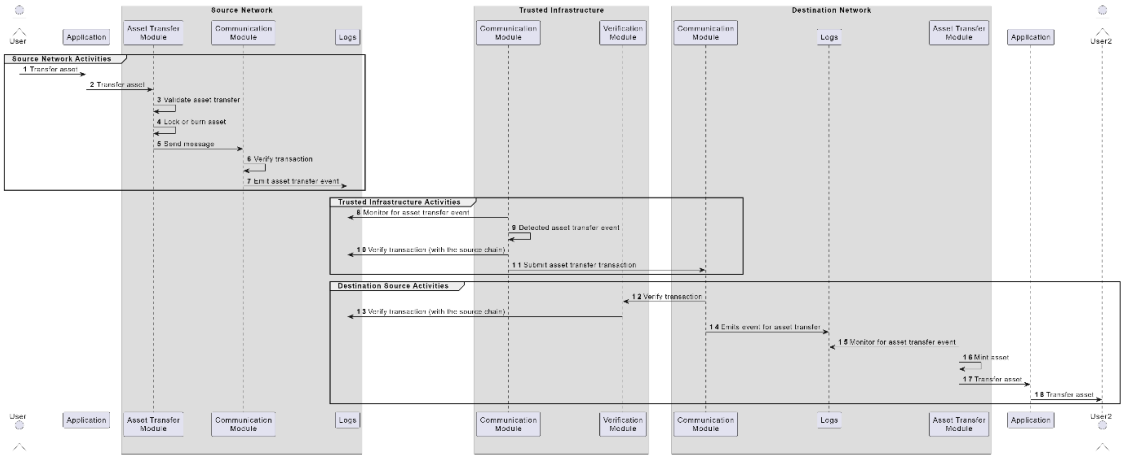

Figure 9: Generic flow of a cross-network asset transfer

Source Network

Steps 1-4: User initiates the transfer of assets through an application. The asset is transferred to the asset transfer module which will either lock or burn the asset.

Steps 5-7: The asset transfer module sends a message to the communication module. The communication module emits an asset transfer event which will be picked up by trusted infrastructure.

Trusted Infrastructure

Step 8: Multiple nodes in the infrastructure monitor for an asset transfer event in the source network.

Steps 9-10: If an asset transfer event is detected, the transaction must reach finality with the source network before validation. The trusted infrastructure can be implemented in different ways depending on the requirements and design considerations. It can also be implemented via another trusted network. In this scenario, the trusted network will validate the event in the source network and records the proof on its own network.

Step 11: If an asset transfer event is verified, the trusted infrastructure will submit a transaction to the destination network.

Destination Network

Steps 10-14: When the communication module receives a transaction, it verifies the transaction in the source network via the verifier module in the trusted infrastructure. If the verification is successful, it emits an event to inform the asset transfer module to perform the asset transfer.

Steps 15-18: If an asset transfer event is verified using the accepted proof/attestation, the asset transfer module will then mint and transfer the asset to the user.

4 Design Considerations

This section discusses the design considerations of the INM for these arrangements to operate safely and efficiently.

4.1 Governance

The establishment of robust cross-network governance is critical as they will define a wide range of aspects including participation, decision-making processes, accountability, legal compliance, conflict resolution, risk management, system capacity management, and system upgrades. Robust governance is especially important if the bridge is decentralised, to promote trust among the participants.

4.2 Security

Security should be a core focus when designing bridges. The impact of a compromised bridge would lead to loss of funds and control over the assets or services linked to it such as the unauthorised creation or deletion of assets. Hundreds of millions of dollars in user funds have already been lost due to bridge hacks.[11] Potential threats or vulnerabilities can compromise the confidentiality, integrity, and availability of data or assets during transit. A key challenge is finding a balance between the secured interoperability between different networks, efficiency, and user experience for market participants, while ensuring that the assets are secured.

There are five types of decentralisation and risk management methods that affect the overall security for cross-network activities that should be considered:

1. Single Server. This is the most basic form of cross-network security, with a single administrator using a single server and single private key to manage both the bridge and the message hub.
2. Centrally Managed Network. A single administrator utilises two or more servers and multiple private keys under their control to manage the bridge and message hub.
3. Decentralised Hub Network. A single decentralised network made up of independent nodes with distinct private keys that forms consensus about the validity of all cross-network transactions and messages.
4. Multiple Decentralised Networks. Distinct decentralised networks are used to secure each distinct bridge and message hub between different DLTs, separating the security of each lane between source and destination networks.
5. Multiple Decentralised Networks with separate risk management. This is the most sophisticated form of cross-network security, with multiple, independent decentralised networks securing a single cross-network bridge and message hub between different DLT networks, along with an additional risk management system tasked solely with identifying and mitigating risks. 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.

4.3 Independent and Active Monitoring

Monitoring is critical to ensuring the accuracy, security, and reliability of the network interoperability. Doing so requires monitoring systems independent of the core interoperability bridges, which have the ability to detect and halt suspicious activity and support configurable risk parameters to account for different trust assumptions between stakeholders. This is essential to all mission-critical systems,

[11] Vulnerabilities in Cross-chain Bridge Protocols Emerge as Top Security Risk (Chainalysis, 2022)

especially of those that automate the transfer of value using data. It is also beneficial to have web interfaces for cross-chain transactions, which enable counterparties to verify in real-time the on-chain details of each transaction. This allows for easier checks on the current status of transactions and supports better investigation into potential disputes.

Furthermore, this is made complicated with some bridges relying on oracles to bring external data into the network. Monitoring becomes even more important to ensure the accuracy and reliability of the data. Ongoing monitoring must be robust and reviewed periodically or detected promptly to reduce the risk of compromising the bridge security.

Validators engaged to provide attestations to the data have to be monitored and subject to audits or checks as well to prevent malicious behaviours and underpinning the security and trust of the network.

4.4 Connectivity with Existing Infrastructure

Another important facet of INM is the ability for existing systems and networks to communicate with DLT networks via existing infrastructure. With the potential for hundreds to thousands of DLT networks —particularly as they are purpose-built to support specific use cases, asset classes, or geographies—existing systems need to be able to efficiently integrate with any public or private network. Instead of bilateral integration, 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. This reduces risk, accelerates adoption timelines, and reduces costs since minimal changes need to be made to the core infrastructure of existing systems.

4.5 Technical Interoperability Standards

Defining interoperability standards that allow different networks to communicate and exchange assets and data seamlessly is important for mass adoption. These standards will allow new networks that are built to continue interoperating with existing networks.

Creating interoperability standards will require supporting a wide range of heterogeneous systems. In practice today, this entails cross-network protocols being able to read data from and write data to Ethereum Virtual Machine (EVM) and non-EVM compatible networks, public and private, layered networks, and other forms of DLTs, while also supporting new and existing token standards (e.g., ERC-20). Cross-network protocols should also be able to exchange data, perform programmable token transfers, and interact with traditional value transfer systems. Such globally recognised standards enable more seamless and efficient cross-network solutions, including interactions with traditional value transfer systems that rely on message standards such as ISO 20022 for financial transactions today. This will accelerate adoption since the cost of integrating with networks can be greatly reduced.

For common DLT frameworks and token standards, examples include Cosmos SDK, Ethereum's ERC-20 and ERC-1400. For instance, in multi-chain networks, these technical standards will allow asset owners to employ bridges such as native or L1 bridges to move digital assets across the broader L1 ecosystem. Native bridges can support message passing and asset transfers, or both, which enables interoperability within its ecosystem, and cross-network activities. An example of a native bridge that supports asset transfers this is the Avalanche bridge.

4.6 Transferring Value and Messages Simultaneously

More advanced cross-network protocols can also support programmable token transfers. This mechanism allows users to transfer tokens and message instructions for the tokens to be executed once the tokens arrive at the destination network. This is enabled by triggering function calls within smart contracts on a destination blockchain and passing value (tokens) within that instruction. All this

is done in a single transaction for greater efficiency as the value and context are intertwined and settled atomically. This allows for asset issuers to efficiently distribute digital assets across networks without needing to own native wallets or addresses on the destination networks, which greatly reduces integration costs.

4.7 Legal and Compliance

Legal and compliance considerations are critical in designing and implementing cross-network protocols, as they can have a significant impact on the protocol's operation and viability. This is especially so where transactions tend to be cross-border in nature. The following are some illustrative legal considerations for cross-network protocols to be adopted:

Jurisdictional compliance

Compliance with the laws and regulations of the applicable jurisdiction is key towards the operation and sustainability of cross-network protocols, considering the cross-border nature of such protocols. Some jurisdictions have existing regulatory frameworks to cover the products, services and/or activities conducted on cross-network protocols while other jurisdictions may not have such frameworks or are in the process of developing appropriate regulatory frameworks.

Know-your-customer (KYC) and Anti-Money Laundering (AML)

The KYC and AML risks relating to the cross-network protocols need to be mitigated and the activities need to fit into the appropriate AML and counter-financing of terrorists (CFT) frameworks to be compliant with the Financial Action Task Force (FATF) standards. According to a recent 2023 Elliptic report, cross-chain crime had exceeded $4.1 billion involving illicit or high-risk funds that have been laundered through decentralised exchanges (DEX), interlinking network bridges and coin swap services[12]. This means that some form of identity management is required which could be through Trust Anchors such as licensed financial institutions with solutions such as verifiable credentials or whitelisting to identify the participants within these networks. Oracles can also be employed to connect to external systems and use smart contracts to bring KYC or AML information on-chain.

Financial regulations

The legal characterisation of digital assets such as tokens that are issued, burned and/or transferred across networks would depend on the jurisdictional regulations. In some jurisdictions, such digital assets may be recognised as securities, in which case the relevant securities laws relating to the issuance, sale and transfer will apply. In other jurisdictions, digital assets may be recognised as "funds", in which case the relevant laws relating to funds transfer, deposit-taking and safeguarding customers' funds and such may apply. In some other jurisdictions, the digital assets may fall outside of regulatory perimeters if there is no applicable legislation.

Tax implications

Policymakers in several jurisdictions have established legal and regulatory frameworks for the taxation of digital assets. This is especially relevant as cross-network asset transfers tend to translate into cross-border and/or cross-currency digital asset exchange or transfers which will touch two or more jurisdictions. The degree of change in taxes such as the withholding tax will depend on the tax laws in each of the transacting jurisdictions.

[12] The State of Cross-chain Crime 2023 (Elliptic, 2023)

Data privacy

Data privacy concerns in distributed ledgers arise from the inherent transparency and persistency of the ledger. For instance, where personal data is published on, or accessible via a distributed ledger, the applications on such networks should be designed in compliance with personal data protection obligations under the respective jurisdictional data protection laws. For instance, in many jurisdictions including the UK and E.U., specific legislations place restrictions on owners and processors of data, relating to data protection and privacy, as well as the usage, storing and sharing of data. There are solutions to address data privacy concerns such as implementing off-chain storage for personal data and storing a reference or a hash on the distributed ledger. Another solution being adopted in the industry is the use of advanced cryptographic techniques such as zero knowledge proofs to ensure that the original data remains confidential and made accessible only by authorised parties.

Intellectual property rights

Distributed ledgers allow for the storage of information in a secure and consistent manner using cryptography. As an illustration, tokens mainly represent two different kinds of underlying assets, namely the digital representation of real-world assets or natively issued digital tokens that exist on a ledger. In both scenarios, intellectual property rights could potentially take the form of a token which would warrant a higher level of secrecy and privacy.

Legal basis

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. It is important to clearly define liability and risk allocation among participants in case of unforeseen events, like bugs or attacks in the bridge's code. Legally binding agreements need to be put in place between participants to address these issues. The nature, scope, and responsibilities of each participant in cross-network protocols should be documented in writing and agreed at the outset so that there is clear understanding of the respective roles and responsibilities of the participants. The legal agreements should also address disclosures, representations made, and also provide rules on any applicable governance of the cross-network protocols.

When using network linkages across borders, the risks arising from any potential conflict of laws across jurisdictions should be identified and mitigated. The inclusion of exclusive governing laws and jurisdictional clauses is essential to provide legal certainty in the event of a dispute. Such inclusions should ensure that parties have legal certainty as to the law to be applied to determine the rights and obligations of the parties to the agreement and which courts will adjudicate the disputes.

Liability and recourse mechanisms

The emergence and use of INM present the challenge of how recourse and disputes are handled. Recourse and dispute management should be properly established upfront at the design stage. Appropriate laws protecting investors and consumers in traditional finance markets should also be extended to protect investors and consumers for digital assets under the principle of “same activity, same risk, and same regulatory outcomes”.

4.8 Scalability

Scalability is essential for ensuring that the protocol can accommodate a growing number of networks and an increasing amount of value without compromising its functionality or security. It is important to ensure the protocol can handle increased workloads, such as higher transaction volumes and sudden spikes in demand, while maintaining its performance, efficiency, and responsiveness. This is

especially so for financial markets where trillion dollars of assets are moved on a daily basis. That said, this will be difficult to achieve on a single monolithic network, but more viable on an INM.

Other important areas of scalability include having a readily available network 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. A readily available and trusted network abstracts away the complexity of transaction processing, empowering users to conduct business in a more efficient manner. It's also important for the network to be able to scale its security as the value moving through its system increases, such as being able to add more nodes to the network or increase security.

4.9 Business and Operating Models

Business and operating models encompass various aspects related to how the protocol will sustain and operate efficiently. It is important at the early stages to explore incentives structures for users to participate in the network, such as support for additional value-added services on top of the cross-network protocol. For instance, being able to utilise off-chain or on-chain bridge infrastructure to service assets from an existing backend as part of the interoperability stack makes it easier to onboard users, with a more complete solution as opposed to a piecemeal one. Additionally, this will also cover the management of business and operations on a daily basis, and back-up systems, fallbacks and contingency plans for business continuity management.

4.10 Risk Management

Risk management is the process of supplementing the security of an interoperability solution through defence-in-depth measures. This should include pre-emptive and reactive verification of cross-network transactions by an independent network that is distinct from the primary network in technology and operations. The risk management network should also detect anomalies, whereby various risks are monitored across both the cross-network protocol and the source/destination networks. If anomalies are detected, an emergency halt can be triggered in order to minimise value loss. Token rate-limiting can also be a risk management feature whereby the amount of value that can flow across the networks during a given period of time is restricted to minimise risks. Ideally, users should be able to customise risk management conditions related to the movement of tokens across network.

5 Applications of the INM

5.1 Case Study 1: Enabling Cross-Network Tokenisation of Asset-backed Securities with Trade Receivables

Background

As part of Project Guardian, Standard Chartered collaborated with Linklogis to develop an initial token offering platform for real-world assets and successfully piloted the issuance of asset-backed security (ABS) tokens with underlying trade receivables. This demonstrated the practical application of an open and interoperable network, which prevents the fragmentation of market liquidity and enables investors across various ecosystems to participate in such a tokenised economy. This enables investor and issuer interaction across digital asset networks, provides access to decentralised applications, and heightens innovation and development in digital asset network ecosystems.

Approach

This example illustrates ABS tokens in cross-network ecosystems using the lock-and-mint method via a two-way peg mechanism, while taking into consideration its scalability, flexibility, and security characteristics.

Process overview

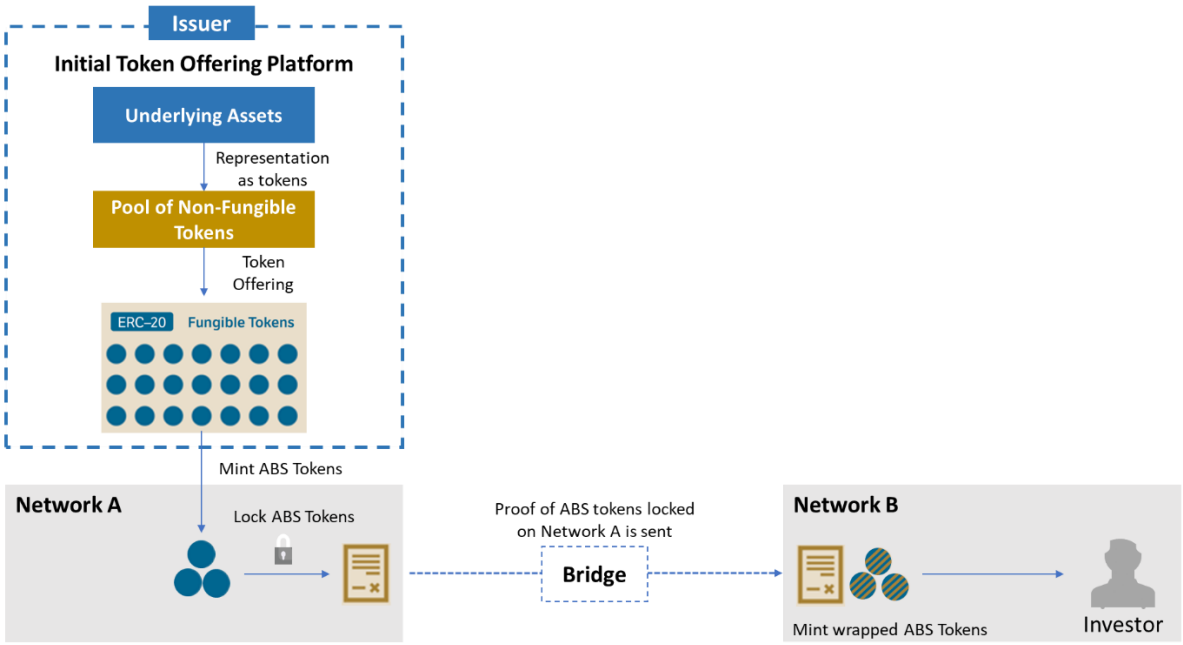

Figure 10: Overall technical architecture of the ABS tokens with a bridge

Figure 10 illustrates a scenario where an issuer and investor reside on separate networks, Network A and Network B respectively. The issuer would need to send the ABS tokens issued on Network A to the investor wallet address on Network B. This can arise when (a) an investor has limited access to Network A; (b) an investor prefers a different cross-network protocol to take advantage of certain unique features; or (c) an investor requires access to decentralised applications on another network. Typically, in such situations, the issuer of the ABS tokens would be unable to reach a broader range of networks and investors. Thus, if the investor wants to purchase these ABS tokens, they must onboard onto Network A, or onto the issuer's platform, which is often impractical given that the investor will

need to fragment their liquidity across multiple platforms to diversify their holdings. With the introduction of interlinking solutions such as bridges and cross-network protocols, investors can pool liquidity on their network or the platform of their choice, provided that the technical interoperability standards are in place. To illustrate this scenario, Network A could be a unified public-permissioned network like the Guardian Network, and Network B could be a private-permissioned network.

The transfer of ABS tokens between networks is achieved through the lock and mint model. The tokens on Network A are first locked and the corresponding wrapped ABS tokens are minted on Network B[13]. The key steps involved are as follows:

Step 1: The issuer sends the ABS tokens to be locked in the smart contract of the bridge on Network A and provides the receiving wallet address of the investor on Network B

Step 2: Network B's validator node verifies that the ABS tokens has been locked on Network A before the bridge mints the wrapped ABS token and sends it to the receiving address. Once this is completed, the number of ABS tokens in circulation on Network A is reduced, and the corresponding equivalent of wrapped ABS tokens is generated on Network B.

Step 3: In the event where the issuer does a call-back or if investors request to redeem the tokens, the wrapped ABS tokens are sent to the smart contract of the bridge on Network B.

Step 4: In this case, the wrapped ABS tokens are burnt on Network B. Network A's validator node verifies that the wrapped ABS tokens have been burnt on Network B and proceeds to unlock the ABS tokens on Network A and sends it to the issuer's wallet address.

A potential implementation of the bilateral connectivity between Network A and Network B could be based on a partitioned model with sidechains or relayers initiating a two-way peg mechanism. This technology provides a scalable framework capable of self-verifying transaction data, thereby preserving the integrity of transactions across varying networks while enhancing interoperability. This benefits both issuers and investors. Furthermore, it can extend the functionality of existing networks by allowing for more features such as operating distinct governance models.

However, there are technical challenges to consider – for example, the implementation complexity and the compatibility required for both networks. This requires harmonisation of technical standards covered above in section 4.5 Interoperability Standards. Additionally, the integration is made more complex with existing settlement systems [14] which requires the implementation of locking mechanisms through primitive earmarking or escrow functionalities.

Additional considerations of the INM

There are an increasing number of cross-network bridges that aim to tackle the interoperability challenge in across different network ecosystems. One key consideration when deciding the type of bridge is the risk of cyberattacks in such bridge solutions. Bugs in smart contracts, or other weaknesses including human errors, can be exploited by bad actors which may result in significant financial loss. For example, in 2022, Beosin, a blockchain security company reported a total loss of approximately USD 1.89 billion due to 12 cross-network bridge security incidents[15]. It is therefore critical for financial institutions to evaluate not only the underlying technology protocol, but also if these bridges have been subject to rigorous third-party smart contract audits and is governed by strict security policies.

[13] Blockchain Interoperability Data Authentication and Communication Protocol. (IEEE Std 3205™-2023)
[14] An in-depth Guide to Cross-chain Protocols Under Multi-Chain World (Zheng, Lee, & Qian, 2023)
[15] Global Web3 Security & AML Report (Beosin, 2022).

In addition, it is important to ensure compliance with relevant laws and regulations in different jurisdictions, especially when transferring digital assets and/or sensitive data across different networks. The key considerations include the assurance that the bridge supports atomic swaps or similar mechanisms in order to guarantee that a transaction on one network either entirely succeeds or fails, as well as the compliance with data protection laws to address data privacy concerns. These technical and legal considerations tend to be closely related, as ensuring legal compliance often relies on implementing the right technical solutions.

5.2 Case Study 2: Next Generation of Discretionary Portfolios with Access to Alternative Investments

Background

The development of multi-asset shared ledgers with automated workflows – enabled by distributed ledger technology – has created new possibilities for asset and wealth management firms.

Within the wealth management industry, building and managing discretionary portfolios for wealthy individuals is a $5.5 trillion business[16] that enables millions of investors to meet their financial goals. The financial institutions in this space have built robust and sustainable businesses that have delivered results for their investors. However, wealth management firms' ability to create innovative solutions and realise further efficiencies is limited due to existing technology infrastructure.

Additionally, these discretionary portfolios have not historically included access to alternative investments due to complex operational processing and liquidity constraints, limiting individuals' ability to benefit from the portfolio enhancing potential of alternative investments.

Approach

Onyx by J.P. Morgan and Apollo collaborated under Project Guardian to create a step-change in the asset and wealth management industry. The parties leveraged emerging technologies such as DLT, smart contracts and tokenisation to deliver a proof-of-concept (POC) discretionary portfolio solution.

Furthermore, the parties sought to address a common critique of DLT's potential: the emergence of fragmentation of assets across many blockchain implementations. This is occurring today as different assets are tokenised on disparate networks that utilise varying standards and environments, creating isolated digital islands of activity.

A key aspect of the POC, therefore, was enabling interoperability across a variety of different permissioned networks whilst taking steps towards their vision. Cross-chain messaging was employed within the solution structure to allow for the orchestration of activities across multiple networks such as deploying the strategy model, executing the portfolio rebalancing and settlement. This approach could also potentially be extended to traditional financial systems as long the message structures are widely recognised and accepted by financial institutions.

Further information on this initiative can be found in the joint report from Onyx and Apollo[17].

[16] U.S. Managed Accounts 2023 Decisions About Discretion (Cerulli, 2022).

[17] Project Guardian – Onyx by J.P. Morgan

Process overview[18]

Proof of Concept goal: Enable a portfolio manager to seamlessly manage a large number of discretionary portfolios - preserving unique investor-level account customisations - that are invested in a multitude of traditional and alternative investments that have been tokenised across a variety of networks.

To achieve this, a multi-faceted group of fund managers, infrastructure providers, interoperability solutions and tokenisation platforms was assembled to create an end-to-end ecosystem of assets and connected networks.

The parties sought to connect Ethereum Virtual Machine ('EVM') and non-EVM compatible networks, and to experiment with different interoperability design paradigms. Furthermore, they explored how newer architectures that enable permissioned instances of public blockchain infrastructure could be leveraged. Finally, to determine how the solution could provide frictionless user experiences to traditional wealth managers, the parties leveraged Account Abstraction technology that removes the complexities relating to acquiring and managing gas token balances to cover transaction fees.

The set up was as follows[19]:

- Onyx Digital Assets ('ODA') was used as the base network that connected to other DLT networks in the project via designated permissioned interoperability solutions. ODA is an institutional-grade, multi-asset tokenisation platform that J.P. Morgan established in 2020 and has processed approximately $900 billon of tokenised assets since its launch. As an EVM platform with connectivity to J.P. Morgan infrastructure, it provided the optimal launchpad for executing the POC.
- A representative portfolio manager established discretionary portfolios, model portfolios and cash balances for representative investors on ODA. Each discretionary portfolio was linked to a specific model such that the portfolio would automatically re-balance to the target asset allocation as defined by that model.
- Representative traditional and alternative investment strategies (fund vehicles) from J.P. Morgan Private Bank, Apollo and WisdomTree were tokenised on three blockchain networks: Onyx Digital Assets, Provenance Blockchain and Avalanche. All three instances were established as permissioned networks—a permissioned zone in the case of Provenance blockchain, and a permissioned subnet in the case of Avalanche (for ease we will refer to these permissioned instances simply as Provenance Blockchain and Avalanche). A standardised token, the Onyx Digital Assets Fungible Asset Contract (ODA-FACT), was used to enable consistent interaction and represent funds on each network. Using the ODA-FACT token standard, Onyx tokenised J.P. Morgan Private Bank, Apollo and WisdomTree funds on Onyx Digital Assets, and WisdomTree funds on the Avalanche chain. Oasis Pro tokenised Apollo funds on Provenance Blockchain.
- Interoperability solutions were put in place to provide connectivity between the networks. Specifically, Axelar was used to connect ODA (an EVM chain) to Provenance Blockchain (a non-

[18] Please note: WisdomTree tokenises WisdomTree digital funds today through their own tokenisation platform and transfer agency. This proof of concept is intended to showcase the end-to-end ability to streamline portfolio management processes and is not intended to be representative of WisdomTree's existing infrastructure for tokenised funds in the market today.

[19] Note: Asset Managers can deploy funds onto any settlement network (one or multiple) where they would like to make their funds available to investors. The solutions discussed herein are not live product offerings and there is no guarantee that J.P. Morgan, Apollo, or WisdomTree will develop or offer such solutions.

EVM chain), and LayerZero was used to connect Onyx Digital Assets to Avalanche (also an EVM chain).

- Biconomy's Account abstraction infrastructure and contracts were established on Avalanche to prevent the fund manager needing to manage or pay their own gas fees on that network.

With the infrastructure in place, the parties executed a series of tests to demonstrate what the next generation of portfolio management could look like.

Notably they showed that the portfolio manager was able to update the target asset allocation for a given model (i.e., replace one asset for another), and the system automatically rebalanced all investor portfolios that tracked that model by initiating, placing, and settling orders to redeem from and subscribe into the relevant funds, even though those funds were held on three different chains.

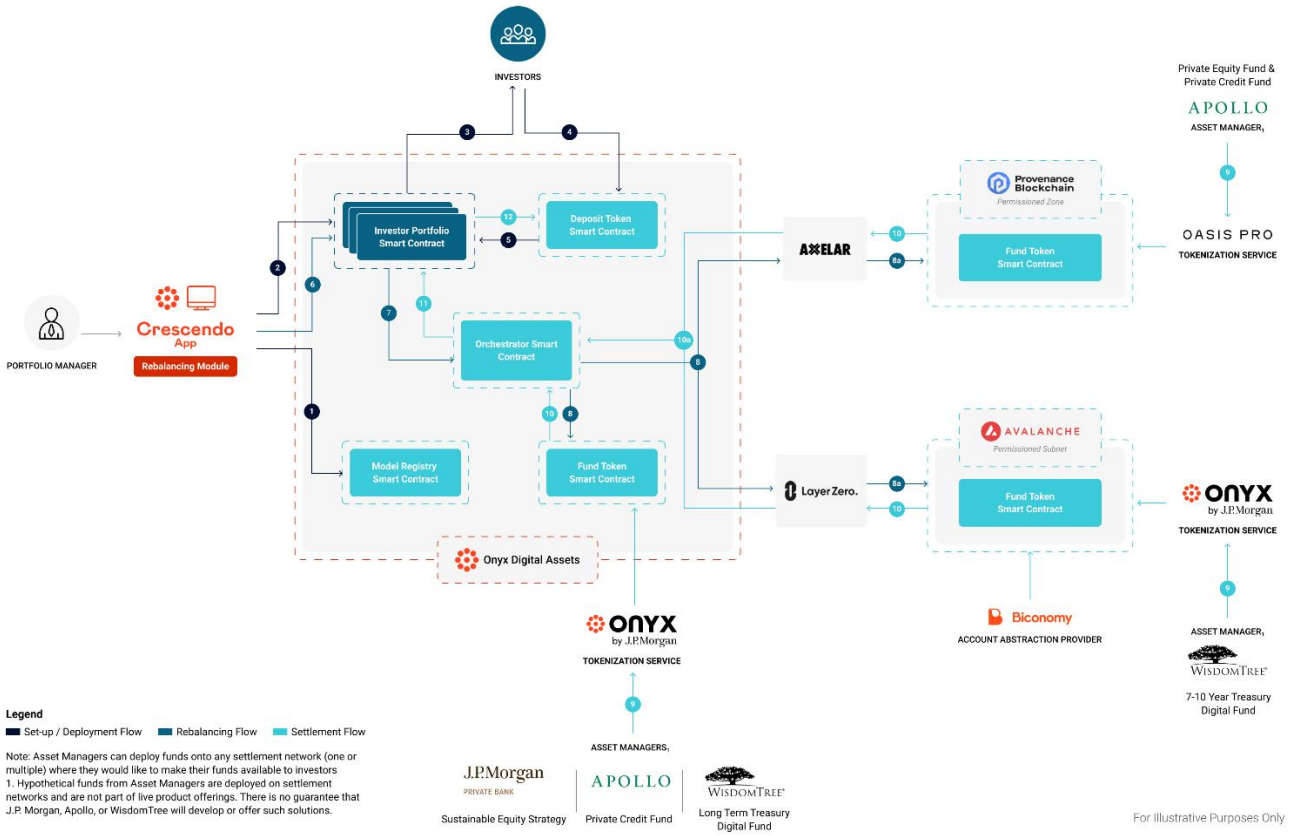

Figure 11: End-to-end process flow

Step 1: Portfolio Manager creates the model and deploys to the Model Registry Smart Contract on ODA.

Step 2: Portfolio Manager sets up discretionary portfolios to follow these models for a number of investors (there is one Investor Portfolio Smart Contract per investor) on ODA.

Step 3: Investor's portfolio is linked to the selected model and the investor.

Step 4: Investor establishes cash balance on-chain through the Deposit Token Smart Contract on ODA.

Step 5: Investor transfers the required Deposit Token amount to their Investor Portfolio Smart Contract, preparing for investment. This process took place on ODA.

Step 6: The Investor's portfolio is 100% invested in cash, requiring rebalancing. Subscription orders required to align the investor's portfolio with the model are calculated by the Rebalancer Module – and routed to the Investor's Portfolio Smart Contract on ODA.

Step 7: The orders are sent from the Investor Portfolio Smart Contract to the Orchestrator Smart Contract where the orders are queued and routed to the relevant chains – with funds on ODA, Provenance Blockchain and Avalanche.

Step 8: For funds on ODA, orders are received by the asset managers on ODA (Apollo, J.P. Morgan Private Bank, and WisdomTree) who can see that cash had been positioned for settlement on ODA.

Step 8/8a: For funds on the Provenance Blockchain and Avalanche networks, orders are routed from ODA to Provenance Blockchain and Avalanche through the interoperability infrastructure, Axelar and LayerZero; asset managers (Apollo on Provenance Blockchain, WisdomTree on Avalanche) receive the orders and can see that cash had been positioned for settlement on ODA.

Step 9: Orders are approved by the asset managers and fund units are issued to the relevant investors. On Avalanche, Biconomy's Account Abstraction infrastructure is leveraged to cover gas fees incurred by the Asset Manager when approving orders.

Step 10: For funds on ODA, messages confirming settlement are sent to the Orchestrator Smart Contract on ODA.

Step 10/10a: For funds on Provenance Blockchain and Avalanche networks, messages confirming settlement are sent back to ODA from Provenance Blockchain and Avalanche through the interoperability infrastructure, Axelar and LayerZero – hitting the Orchestrator Smart Contract on ODA.

Step 11: The messages confirming settlement are sent from the Orchestrator Smart Contract to the Investor Portfolio Smart Contract where records of the asset positions across multiple fund investments within a specific portfolio are held.

Step 12: Finally, once the state of all orders in the Investor Portfolio Smart Contract are recorded as settled, Deposit Tokens are transferred from the Investor Portfolio Smart Contract to the respective asset managers' address on ODA.

Additional considerations of the INM

Within the project, the parties focused on the cross-chain messaging approach to interoperability, having identified several advantages over the asset bridging approach including having a single source of truth for ownership recording, and the flexible utility that user defined messages can provide.

The following requirements were established to assess different cross-chain messaging solutions for the POC:

- **Low integration overhead**: Solutions should not require onerous integration effort nor significant application re-write but should have high potential for reuse.
- **Breadth of supported Chains**: Solutions should support a high number of and various types of networks (i.e., multiple EVM and non-EVM compatible networks).
- **Scalability**: Solutions should minimise the number of required connections between systems. Connectivity at a blockchain-to-blockchain level was seen as the most scalable approach.
- **Decentralisation**: Interoperability solutions should allow for the decentralisation of both technical infrastructure and governance mechanisms.

    - Decentralised infrastructure provides more flexibility for developers and operators to select their preferred setup.
    - Decentralised governance could take the form of distributed validators checking each other's behavior or an aggregate configuration of different organisations, individually verifying messages.
- **Security**: 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.

Consistent with the criteria above, the Parties implemented instances of Axelar and LayerZero for exploration of interoperability in the POC.

5.3 Case Study 3: Cross-network Distribution of Tokenised Investment Vehicles

Background

The project proposes to implement a tokenised investment vehicle (TIV) for a Schroders investment strategy. This TIV makes use of the source network to mint and allocate tokens as entitlement for the underlying investments. The source network can then interlink with other networks through bridges for the distribution of these tokens.

Approach

To enable the distribution of the TIV tokens, a lock and mint model is explored to synchronise the tokens that are held on the source and destination networks.

1. The architecture is based on a distributed network architecture where the minting and allocation of tokens is performed on the source network and the data is pushed out to the destination network for reconciliation and distribution by third parties. All transactions are encoded into the ledger on the source network which acts as an immutable record for all transactions and allocations at any given point in time.
2. Periodic snapshots of the current positions and transactions are pushed to partners for distribution, reconciliation, and querying purposes. This could be implemented as a read-only node of the network provided to the partners.
3. Utilising a lock and mint model, a lock safe is implemented to immobilise the TIV tokens on the source network, to be minted as 'wrapped assets' on the destination network. For transfers back from the destination to the source network, the TIV tokens are burnt in the destination network and unlocked in the source network. This simplifies the reconciliation process and bidirectional movement of tokens.
4. The lock and mint model allow the use of a centralised count function of total tokens minted. This then acts as the global counter for all tokens across all networks that prevents token supply discrepancies.

Process overview

A core design requirement for the tokenised investment vehicle is the issuance of tokens that represent shares in a Variable Capital Company (VCC) structure. In the case of open ended VCCs, tokens are minted on the source network on demand. Token valuation and market data services can be accessed via an oracle service that can be utilised across source and destination networks.

The transfer of tokens across networks makes use of the lock and mint model and implements this via a bridge mechanism from the source chain.

Step 1: Lock and mint on destination network

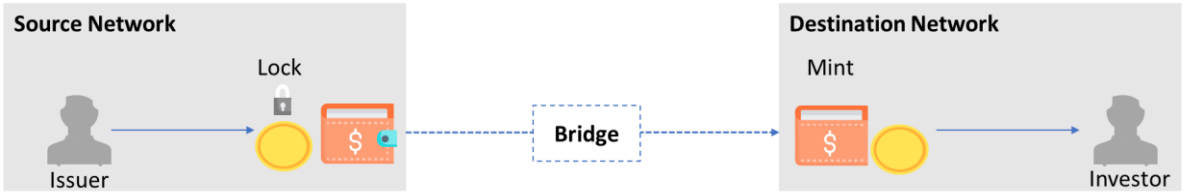

Figure 12: Lock on source network and mint on destination network

- The issuer sends the TIV token through the bridge on the source network.
- The tokens are then locked and owned by a contract (Safe) implementation.
- Upon locking of the tokens, an event is emitted on the source network through the bridge to mint the wrapped TIV tokens before it is sent to the investor on the destination network.
- The bridge will be responsible for transaction management, ensuring concurrency and consistency across the chains during the lifecycle of the lock and mint process.

Step 2: Redemption on destination network

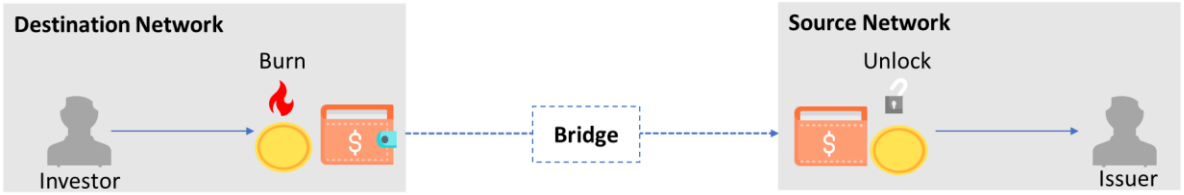

Figure 13: Burn on destination network and unlock on source network

- The token contract on the destination network is owned by Schroders and has the feature of a burn function.
- When the investor requests for a redemption of the token, the wrapped asset token is then burnt with this function on the destination network.
- After the token is burnt, the unlock event is emitted from the destination network to the source network through the bridge.
- Once workflow verifications have completed, the immobilised token will be unlocked and transferred to the issuer on the source network.
- The bridge will be responsible for transaction management ensuring concurrency and consistency across the chains during the lifecycle of the burn and unlock process.

Additional considerations of the INM

- Minting could introduce some latency due to the settlement time on the underlying network.
- The bridge represents an external and attackable component of the end-to-end transaction process which does not carry the same inherent distributed protection of the network. Therefore, sufficient monitoring and security measures would need to be designed and implemented to maintain resilience of the bridge as part of the overall platform security.
- Failsafe and rollback procedures must be implemented via a business process due to the immutable nature of the ledgers.

- The lock and mint process provides traceability across the networks as the total minted tokens on the source network will match up to the sum of the tokens across all the destination networks. This makes cross-network reconciliation easier.
- In the case of a private chain, a high level of multi-region redundancy (and multi cloud potentially) should be considered.
- An allow list will be maintained to permission access for secondary market transactions on the TIV token spanning across the networks.

6 Future Work

Networks are the foundation of the digital asset ecosystem. This paper provides a framework for understanding the design considerations and potential solutions in interlinking disparate networks. However, given the nascency of the digital asset ecosystem, it is expected that the solutions described in this paper would be superseded by developments in the future. The following areas have been identified as potential areas of research in the future.

Industry grade protocols

Today, a concern of networks, bridges and cross-network protocols points back to the fundamental security of such infrastructure to be used as financial market infrastructure. Given the high-value and/or large notional of financial assets that are traded in financial markets today, infrastructure security is a necessary focus to ensure financial markets can continue to flow seamlessly. The integration of cross-network protocols to multiple networks brings potential security vulnerabilities that needs to be mitigated and protected against.

Common technical standards

For cross-network protocols to be scalable, there needs to be common technical standards at the asset and network levels to ensure networks are designed to be open and interoperable. This will enable assets to be moved across these networks without requiring massive custom integration work to be performed to facilitate digital asset transfers.

Trust anchors

A key role of financial institutions is the screening and KYC of participants to ensure counterparties are known when financial activities occur, this becomes complex with global networks and cross-network transactions. Global networks are likely to host a suite of cross-jurisdictional financial activities, and cross-network asset transfers would likely involve some form of cross-border transactions. Identity management across networks is essential to identify counterparties to the transaction, and the purpose of such transactions to prevent illicit financial activities.

7 Conclusion

Fostering innovation while still managing risks responsibly is essential to establish the foundations for a sound, sustainable and scalable global digital asset ecosystem. This paper builds upon the foundational work started with Project Guardian and in particular the concept of open and interoperable networks, which envisions a financial landscape with heterogenous networks implemented on diverse ledger technology. This paper is jointly developed with financial institutions, FinTechs and industry groups who provided perspectives on prevailing solutions and implementations.

To ensure that the proliferation of tokenised assets and market venues does not come at the expense of liquidity, there needs to be interoperability across financial networks and for digital assets to be exchanged seamlessly. To address this, the paper proposed the concept of INM as a common framework for exchanging digital assets across independent networks. By interlinking networks, financial institutions can transact with each other without the need for all of them to be on the same network.

The paper details how networks may be interlinked in practice and the design considerations for implementing different solution options. Nevertheless, it is important that the paper does not seek to endorse any solution or technology. The examples cited in this paper are for illustration purposes only and to support understanding of this subject area.

Future work could involve other solution options that are not involved in this paper. Members of the FinTech community are encouraged to build upon this paper and contribute future developments and learnings back to the community to foster greater interoperability in network design, and greater efficiency in financial markets.

8 References

1. McKinsey & Company. (2019, June 7). Blockchain and retail banking: Making the connection. Retrieved from: https://www.mckinsey.com/industries/financial-services/our-insights/blockchain-and-retail-banking-making-the-connection
2. Bank for International Settlements (BIS). (2022, March 24) Project Dunbar: International Settlements using multi-CBDCs. Retrieved from: https://www.mas.gov.sg/publications/monographs-or-information-paper/2022/project-dunbar
3. Bank for International Settlements (BIS), Monetary Authority of Singapore (MAS). (2023, June 26) Project Guardian: Enabling Open and Interoperable Networks (Monetary Authority of Singapore (MAS), 2023). Retrieved from: https://www.mas.gov.sg/publications/monographs-or-information-paper/2023/project-guardian-open-interoperable-networks
4. Bank for International Settlements (BIS). (2023, October 23) Project mBridge: Experimenting with a multi-CBDC platform for cross-border payments. Retrieved from: https://www.bis.org/about/bisih/topics/cbdc/mcbdc_bridge.htm
5. New York Innovation Center (NYIC), MAS (2023, May 18). Project Cedar Phase II x Ubin. Retrieved from: https://www.mas.gov.sg/publications/monographs-or-information-paper/2023/project-cedar-phase-ii-x-ubin
6. Swift. (2023, August 31). Swift unlocks potential of tokenisation with successful blockchain experiments. Retrieved from: https://www.swift.com/news-events/press-releases/swift-unlocks-potential-tokenisation-successful-blockchain-experiments
7. Bank for International Settlements (BIS). (2023, April 11). Project Mariana: Cross-border exchange of wholesale CBDCs using automated market-makers. Retrieved from: https://www.bis.org/publ/othp75.htm
8. Chainalysis. (2022, August 2). Vulnerabilities in Cross-chain Bridge Protocols Emerge as Top Security Risk. Retrieved from: https://www.chainalysis.com/blog/cross-chain-bridge-hacks-2022/
9. Elliptic. (2023). The State of Cross-chain Crime 2023. Retrieved from: https://www.elliptic.co/resources/state-of-cross-chain-crime-2023
10. European Standards. (2023a). Blockchain Interoperability Data Authentication and Communication Protocol. Retrieved from: https://www.en-standard.eu/ieee-3205-2023-ieee-standard-for-blockchain-interoperability-data-authentication-and-communication-protocol/
11. Zheng, J., Lee, D. K., & Qian, D. (2023, June 12). An in-depth Guide to Cross-chain Protocols Under Multi-Chain World. Retrieved from: https://www.worldscientific.com/doi/10.1142/S2811004823500033
12. Beosin. (2022a). Global Web3 Security & AML Report. Retrieved from: https://beosin.com/resources/Global_Web3_Security_Report_2022_.pdf
13. Cerulli. (2022, Q4). U.S. Managed Accounts 2023 Decisions About Discretion. Retrieved from: https://www.cerulli.com/reports/us-managed-accounts-2023

9 Appendix

This paper is authored and published by the Monetary Authority of Singapore with contributions from:

Contributors

Financial Institutions and Industry Groups	
1	Apollo
2	DBS Bank Ltd
3	Hongkong and Shanghai Banking Corporation (HSBC)
4	Onyx by J.P. Morgan Chase & Co
5	SBI Digital Asset Holdings
6	Shroder Investment Management Limited
7	Standard Chartered
9	Swift
9	UBS
10	United Overseas Bank Limited
FinTechs	
1	Ava Labs
2	Chainlink Labs
3	LayerZero