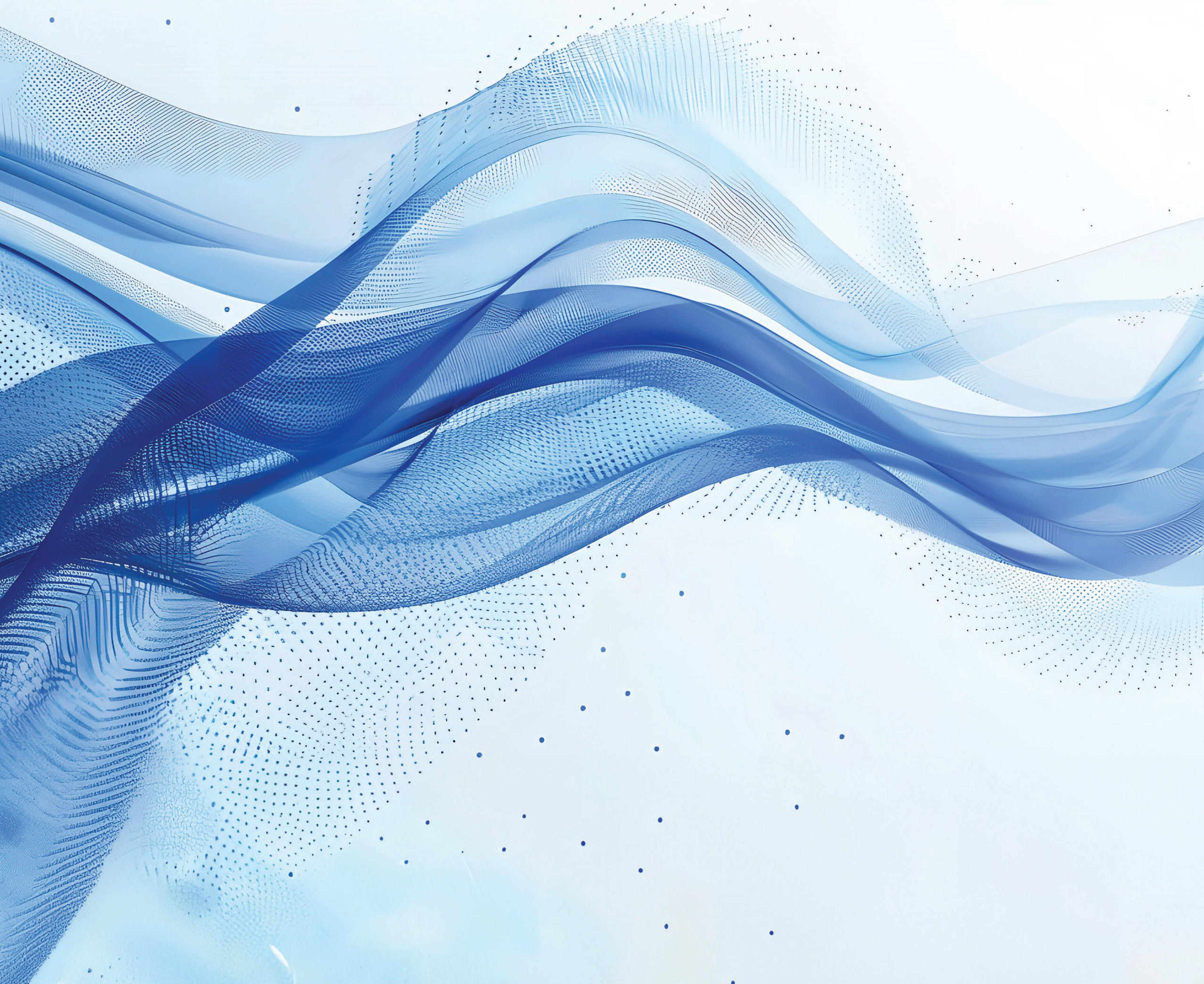
Technical feasibility report

REGULATED SETTLEMENT NETWORK (RSN)
PROOF OF CONCEPT
December 5, 2024



Contents

These materials are provided for informational purposes only. The materials may include views and/or opinions of the contributing institutions based on reasonable analysis of information available to the group. These materials and the information herein do not constitute legal, accounting, tax, or investment advice and the contributing institutions make no representation or warranty whatsoever as to the accuracy or completeness of any information contained herein or otherwise provided. This report does not necessarily reflect the views of the Federal Reserve Board, Federal Reserve Bank of New York, or any other component of the Federal Reserve System.

Executive summary[1]

The Regulated Settlement Network (RSN) Proof-of-Concept (PoC) is an industry initiative built upon the foundation established within the Regulated Liability Network (RLN) US PoC conducted in 2023 by a subset of United States financial institutions. The purpose of the RSN PoC was to explore how tokenized securities and tokenized central bank and commercial deposits could be deployed within a financial market infrastructure (FMI) leveraging shared ledger technology to advance settlement capabilities in comparison to today's standards. The RSN Technology workstream sought to prototype and to validate the RSN business requirements to enhance existing FMIs by implementing a shared ledger system that enables always-on, multi-asset, and interoperable settlement capabilities. These capabilities may provide a hypothetical, future FMI with the ability to potentially reduce risks and frictions in the settlement lifecycle.

This technical document details the outcomes of the RSN technology workstream and focuses on three key accomplishments: the prototype of a shared settlement venue, the development of a multi-asset infrastructure, and the addition of interoperability capabilities.

[1] The New York Innovation Center (NYIC) at the Federal Reserve Bank of New York was a technical observer in this PoC, and its role in this project was narrowly focused on observing the participants' research and experimentation.

The content of this report, including any potential regulatory or supervisory frameworks for the RSN, and the Federal Reserve's legal authority to participate in RSN or any similar arrangement, does not necessarily reflect the views of the Federal Reserve Bank of New York or any other parts of the Federal Reserve System.

Expected benefits

The technical workstream was established to design a system that could achieve the following attributes in the context of a PoC application:

- Availability: 24/7 operation
- Settlement finality: Capable of end-to-end legal finality of settlement
- Interoperability: Achieve broader reach to non-RSN institutions and third-party networks
- Programmability: Automation through on-ledger business logic
- Multi-asset: Capable of representing different regulated financial instruments on the same network
- Precise settlement capabilities: Provides firms the ability to settle simultaneously, in real-time or at a later agreed-upon time

Scope

The intent of the PoC application is to demonstrate the potential technical feasibility of the RSN FMI aligned with the overall RSN scope below:

Category	In Scope	Out of Scope
Currency	USD only	Multicurrency
Legal instruments	Tokenized central bank deposits, tokenized commercial bank deposits, tokenized US Treasury securities, and other tokenized assets	CBDC, cryptocurrencies, stablecoins, e-money tokens
PoC participants	US-based, regulated participants	• Non-US-based regulated institutions • Non-regulated institutions
Use cases	• Client-to-client investment grade (IG) bond DvP settlement • Centrally cleared dealer-to-dealer treasury delivery vs payment (DvP) settlement • Cross-network DvP settlement • Cross-network correspondent bank settlement • Cross-network intraday repurchase (repo) agreement settlement	• Retail use cases • Decentralized finance use cases
Technical scope	• Sandbox only • GUI access only • Functional and select non-functional requirements	Connection to bank legacy systems
Access to central bank money	Existing access criteria to central bank money	Expanded access to central bank money
Access to US securities	Existing access criteria to US securities	Expanded access to US securities
Wallet structure	Hosted wallets	Self-hosted wallets
Customer data	Simulated, dummy data	Live, real-value transactions
Settlement mechanism	• Real-time gross settlement • Precise, dynamic settlement • Net settlement	Liquidity savings mechanisms
Types of blockchain	Private blockchains	Public blockchains

Use case overview

1. **Client-to-client investment grade (IG) bond DvP settlement**
   - **Objective:** Client-to-client transaction consisting of tokenized IG bonds settled in real-time in tokenized central bank deposits and tokenized commercial bank deposits. By introducing a CSD partition to the RSN FMI, in which the CSD warehouses the entitlements to various securities on behalf of banking institutions, the working group aimed to test how simultaneous, 24/7 DvP settlement capabilities could be achieved on the RSN FMI.

   - **Outcome:** Enabled atomic[2] settlement of a DvP transaction and enhanced liquidity visibility on ledger. Smart contracts enabled the programmability for automated transaction processing and movement of assets across partitions.

2. **Centrally cleared dealer-to-dealer treasury DvP settlement**
   - **Objective:** Considered how RSN could comply with the upcoming SEC treasury clearing mandate by establishing a CCP partition within RSN. This allowed financial institutions to achieve precise settlement capabilities, allowing the institutions to fund their executed transactions and not require pre-funding for all transaction types. This crucial design choice between the two use cases sought to show that RSN could provide dynamic, precise settlement capabilities, conceptually providing both real-time gross settlement and net settlement.
   - **Outcome**: Achieved net position visibility and maintenance with atomic settlement of the net position, showcasing the potential for enhanced ownership visibility and tracking.

3. **Cross-network DvP settlement**
   - **Objective**: Demonstrated how a corporate client could use Mastercard's multi-token network (MTN) to securely purchase a tokenized real-world asset from a third-party platform that had integrated MTN as a payment solution using tokenized commercial bank deposits. The working group set out to understand if RSN could serve as an interoperable, 24/7 inter-bank settlement venue in tokenized central bank deposits for the payment leg of transactions carried out on other tokenized asset platforms.

   - **Outcome**: Enabled 24/7 settlement availability which provided coordinated settlement of the payment leg on RSN, and expanded the potential scope for different asset and transaction types enabled by MTN.

4. **Cross network correspondent bank settlement**
   - **Objective:** Analyzed how two Tassat banks that are non-RSN member banks could initiate payments off RSN by leveraging RSN member banks as settlement agents through a correspondent banking model to access the RSN FMI and achieve cross-network inter-bank settlement finality in tokenized central bank deposits. This use case intended to show that RSN could serve as an industry-wide settlement infrastructure through a correspondent banking model.

   - **Outcome**: Expanded access to RSN benefits to non-RSN banks using settlement agents, providing 24/7 settlement availability, and showing the capability to create an interoperable network of both RSN and non-RSN banks through a correspondent banking model. Achievement of coordinated settlement across the RSN and third-party system of the payment leg.

5. **Cross network intraday repurchase (repo) agreement settlement**
   - **Objective:** Engaged with Broadridge's distributed ledger repo (DLR) platform to test how two RSN members that are also Broadridge DLR members use DLR to initiate a two-hour intraday repo to better optimize its tokenized collateral on RSN and be able to provide intraday funding to settle same-day trade obligations. This use case intended to show how RSN's common settlement infrastructure containing various forms of tokenized collateral could allow firms to seamlessly access and deploy its collateral and provide real-time liquidity through an intraday funding solution.

   - **Outcome**: Enabled the coordinated settlement of the two legs of a repo transaction with functionality to automatically trigger and settle the second leg. Demonstrated how the transaction could initiate on a third-party network and still take advantage of the DvP functionality of the settlement venue. This increases the potential for constructing more complicated financial transactions that can rely on RSN as a potential industry settlement venue.

[2] The technical feasibility of atomic settlement should not be taken to imply its feasibility for broad adoption; the choice of settlement time-frame and model is shaped by business, risk, and operational considerations beyond technical capabilities

Key findings

Atomic DvP settlement venue: The RSN PoC achieved 24/7 atomic settlement capabilities with real-time visibility into transaction status and state for transacting parties. These capabilities extended the work performed in the RLN experiment by enabling the ability to perform atomic DvP transactions within the RSN FMI.

Multi-asset network: RSN incorporated multi-asset functionality into the settlement venue. The venue integrated various asset types, provided precise settlement capabilities, and included tokenized central bank deposits, tokenized commercial bank deposits, tokenized securities, and other regulated assets, within a single, shared ledger. The multi-asset infrastructure supported a wide range of asset types and transaction volumes, enhancing the versatility, scalability, and extensibility to other asset types within RSN. By enabling the settlement of diverse assets on a unified platform, the system offered a more comprehensive and flexible platform for financial transactions.

Interoperability: RSN introduced interoperability capabilities to coordinate transactions across different regulated financial networks. This was achieved by demonstrating the ability to utilize interoperability solutions. Two mechanisms were used to enable interoperability, the first leveraged Swift's interlinking prototype and a simulated version of its enhanced transaction management platform. Additionally, Mastercard enabled a direct connection between their MTN and RSN demonstrating this as part of the cross-network DvP settlement use case. The interoperability features ensured that transactions could achieve coordinated settlement across multiple platforms, increasing the versatility of the core RSN settlement venue and potentially extending various features of the system to other networks without requiring a direct relationship with RSN. This capability could facilitate a more interconnected and efficient global financial ecosystem and enable RSN access to a broader group of regulated end-users.

Composability: Utilizing a subset of the RSN functionality to precisely settle the payment leg of a larger transaction demonstrated the flexibility and composable nature of the RSN FMI. The benefits of RSN were extended to non-RSN members by settlement agents that were members of RSN. Additionally, the Swift interlinking prototype provided a reusable, common on-ramp to the RSN FMI that other third-party solutions could leverage to connect to RSN for purposes of composing such transactions. The exposure of such a standard interface could enable faster adoption to regulated end-users that do not require full atomicity for their workflows.

Future opportunities: The RSN PoC demonstrated atomicity for transactions within the system boundaries of the RSN FMI. However, when connecting with third-party networks, RSN was only able to achieve coordinated settlement between the systems and lost overall atomicity properties when crossing non-atomic solution boundaries. While this was the expected behavior based on the design of the RSN PoC, this is an avenue for further industry experimentation and could be achieved via native integration with the RSN technology rather than using a message-based integration.

Potential benefits

The findings of the RSN PoC are woven through the potential benefits such a platform could enable for multi-asset and cross-network settlement capabilities:

Precise settlement: The RSN FMI demonstrated atomicity for DvP transactions, the ability to create settlement windows, netting obligations, and to enable multiple asset functionality on RSN. The enablement of these features by the RSN FMI show the potential to create more optionality in financial transactions within shared ledger systems.

Network interoperability: The RSN FMI enabled coordinated settlement between RSN and third-party networks, established a standardized interface between RSN and third-party networks, and demonstrated the composability of the settlement finality RSN provided. These features demonstrated the potential that RSN could act as a common settlement venue in a future financial ecosystem.

Programmability: The inherent programmability driven by smart contracts within the system enabled the benefits found during the PoC. It allowed customization of the workflows within the various use cases while still providing a common settlement venue. It enabled different roles on the network (e.g., financial institutions, custodians), which led to the achievement of precise settlement finality shared across the use cases. It also allowed for the potential automation within the PoC environment.

Enhanced risk and compliance capabilities: While not a direct technical achievement by RSN, the inherent transparency and resiliency of such a shared ledger system could provide additional risk and compliance benefits explored further in the RSN Business Applicability Report.

By showcasing this functionality, the RSN PoC demonstrated the potential foundations of a future FMI, offering more efficient, interconnected, and versatile options for innovation in financial settlement.

Introduction

The RSN proof of concept

Building upon the findings of the Regulated Liability Network proof of concept (PoC), a subset of members from the US financial services industry reconvened to test the hypothesis of the Regulated Settlement Network , a 24/7 settlement network for multi-asset and cross-network transactions.

Considering the RLN US PoC focused on a shared-ledger FMI consisting solely of tokenized central bank and commercial bank deposits, the working group set out to evaluate the value of a single, shared ledger system that brings both cash and securities into a single settlement system. As the network now included more than just tokenized cash, the working group named this effort the Regulated Settlement Network, a common settlement infrastructure for multi-asset and cross-network transactions that has the potential to drive innovation in the regulated financial services industry and establish the next generation of market infrastructure. The PoC looked to cover three aspects of RSN:

- Business applicability
- Legal viability
- Technical feasibility

This report presents the findings of RSN's technical feasibility, in which the potential technical foundations of such a network were explored.

The primary objective of the technology workstream of the RSN PoC was to explore the technical feasibility of a multiaAsset FMI. This FMI was envisioned to include select, tokenized US securities, tokenized commercial bank deposits, and tokenized central bank deposits, with the goal of achieving atomic delivery versus payment and payment versus payment (PvP) settlement for multi-asset transactions. The PoC aimed to demonstrate the system's potential to operate continuously (24/7) and comply with existing regulatory frameworks, thereby serving as a key component of future financial market infrastructure.

The RSN PoC examined the application of shared-ledger technology to execute multi-asset transactions, delivering programmable and flexible settlement capabilities. Two primary scenarios were explored: multi-asset DvP settlement and cross-network settlement finality for transactions denominated in US dollars (USD).

For the multi-asset DvP scenario, two use cases were tested:

- Client-to-client investment grade (IG) bond DvP settlement
- Centrally cleared dealer-to-dealer treasury DvP settlement

The cross-network settlement finality scenario tested three use cases to examine whether RSN could serve as a settlement venue for interbank asset exchange between both RSN member banks and non-RSN member banks leveraging an interoperability solution:

- Cross-network interbank DvP settlement
- Cross-network interbank PvP settlement using correspondent banks
- Cross-network intraday repurchase (repo) agreement settlement

These use cases were simulated in RSN's technical sandbox and hosted on a public cloud deployment for participant access. The functionality was evaluated and compared to existing legacy systems to identify potential benefits and shortcomings of such a network.

Activities performed

To achieve these objectives, the technical workstream undertook several key activities:

RFP and vendor selection:

- **Vendor requirements:** Defined a vendor scorecard containing required capabilities and features of a prospective technology partner.
- **Vendor selection:** Evaluated potential vendors against the scorecard and selected Digital Asset based on the results of the scoring and demo process.

Design and build:

- **Designing requirements:** Defined functional and technical requirements necessary to support a multi-asset FMI.
- **Infrastructure and application development:** Built the necessary infrastructure and applications to support a prototype of the RSN FMI.
- **Smart contract development:** Created condition-based smart contracts to facilitate DvP and PvP settlements.
- **Interoperability development:** Facilitated interaction between the RSN FMI external regulated networks.

Test execution:

- **Test case design:** Designed test cases that covered various transaction scenarios and interoperability requirements.
- **Test case execution:** Executed designed test cases to validate the functionality and interoperability of the multi-asset FMI.

The remainder of this report documents the key findings of the RSN PoC, highlighting the system's potential as a candidate of a future-state FMI and providing considerations for future development.

RSN participants and their contributions

The RSN PoC was composed of a diverse group of participants from various sectors of the financial services industry. This included representatives from major banks, regional banks, fintech companies, and technology providers. The collective experience of this group was leveraged for the end-to-end design, development, and testing of the RSN FMI, ensuring it met the practical needs of a wide variety of financial industry participants while incorporating innovative solutions.

The Securities Industry and Financial Markets Association (SIFMA) served as program manager for the RSN PoC. RSN Working Group participants in the PoC included: Citi, J.P. Morgan, Mastercard, Swift, TD Bank N.A., U.S. Bank, the USDF Consortium, Visa, Wells Fargo, and Zions Bancorp.

The Working Group was supported by the law firm Sullivan & Cromwell LLP, technology provider Digital Asset, and Deloitte & Touche LLP, who provided advisory services to SIFMA.

The New York Innovation Center (NYIC) at the Federal Reserve Bank of New York was a technical observer in this PoC, and its role in this project was narrowly focused on observing the participants' research and experimentation. The content of this report, including any potential regulatory or supervisory frameworks for the RSN, and the Federal Reserve's legal authority to participate in RSN or any similar arrangement, does not necessarily reflect the views of the Federal Reserve Bank of New York or any other parts of the Federal Reserve System.

The content of this report does not reflect the views of the Federal Reserve Bank of New York or any other parts of the Federal Reserve System.

Other contributors

Digital Asset:

Digital Asset (DA) was chosen as the software provider for the RSN PoC, developing the system on their network solution, Canton Network, and using Daml, their smart contract software language that was utilized to enable the RSN settlement venue. DA collaborated in the design working sessions across the business, technical, and legal workstreams to ensure that the technical requirements were well documented and aligned with the business objectives, delivering a functional system that was built to enable RSN while leveraging the strengths of distributed ledger technology (DLT) systems.

Swift:

Swift, a global provider of secure financial messaging services, played a supportive role in the RSN PoC by providing its Swift interlinking prototype. This capability facilitated messaging and orchestration between the different DLT network solutions, which was essential for the RSN FMI to interface with other systems and enable use cases requiring cross-platform communication.

Mastercard:

Mastercard, a global technology company in the payments industry, supported the interoperability portion of the RSN PoC through its MTN, a private and secure blockchain network. Mastercard's involvement demonstrated the RSN FMI's capability to interact with other DLT networks, thereby enhancing its applicability in real-world financial transactions. Specifically, Mastercard provided access to their network in a sandbox environment, which allowed the RSN group to experiment between the RSN FMI and the MTN system.

Tassat:

Tassat, a provider of private DLT-based business-to-business solutions, supported the interoperability portion of the RSN PoC through its digital interbank network, a private DLT network. Tassat simulated access to their network, allowing the RSN group to test transactions between the RSN FMI and the digital interbank network. This partnership showcased the RSN FMI's versatility and applicability to potential real-world financial transactions.

Broadridge:

Broadridge, through its DLR platform, contributed to the RSN PoC by simulating access to their solution for the settlement of repo transactions on RSN. Broadridge's involvement demonstrated the RSN FMI's capability to handle complex financial instruments and transactions, further validating the system's applicability in regulated financial markets. The collaboration with Broadridge highlighted the potential for integrating traditional financial processes with advanced DLT solutions.

MITRE:

MITRE, a not-for-profit organization that operates federally funded research and development centers, played a supportive role in the RSN PoC, primarily contributing a cybersecurity perspective to the design activities and use case testing. MITRE provided valuable insights into cybersecurity governance and standards, ensuring the PoC adhered to industry security practices and mitigated potential cybersecurity threats.

RSN design

Design principles

The design of the solutions for the various RSN use cases was guided by a set of core design principles. These principles were largely consistent with and expanded upon those that steered the design of the RLN PoC conducted in 2022-2023.

Compliance and regulatory alignment

A key requirement for all RSN use cases is adherence to existing regulatory frameworks. Any system that facilitates the settlement of cash and/or securities must meet a range of regulatory obligations. Throughout the design process, a central focus was to demonstrate that both the RSN concept and the RSN FMI could be made compliant with current regulations and should be adaptable to changes as well as additional or entirely new compliance requirements across jurisdictions, irrespective of the system's distributed nature.

Privacy by design

The principle of privacy by design was given special attention and operates on two critical levels:

1. **Technological privacy:** The system's underlying technology must be able to provide the highest level of privacy, while being able to configure additional parties with whom some data would be shared. This allows the system to be tailored to meet the business and regulatory needs of each use case.

   This means that the underlying technology primarily enables access to information on a need-to-know basis while its configuration must allow each piece of data to be selectively shared or restricted as appropriate. Specifically, within the RSN PoC, Canton provided the following properties:

   - Every individual part of a transaction as well as its outcome is only sent to the relevant parties for approval
   - All communication is encrypted for the specific recipient
   - Data at rest only resides with immediate parties of any smart contract or data, and these entities can use standard database encryption to further protect their locally stored data.

2. **Data sharing and regulatory considerations:** The principle also covers the sharing of information driven by operational, auditing, or regulatory needs. The specific requirements of each process define the "need-to-know" basis for data sharing. However, auditing and regulatory demands may necessitate broader sharing beyond the initially established privacy boundaries. The RSN PoC did not test retention capabilities beyond making a copy of the transaction history available for the participants to show that it is available. Any data retention or replay requirements would be undertaken by the entities that are obligated to adhere to them. In a production environment, each participant would be responsible for its own record retention requirements by utilizing the data store available on a participant's node.

Modularity and decoupling/composability

An analysis of the payment flow during the RLN PoC revealed that, while the system provided clear benefits, the ability to atomically integrate the payment flow with its corresponding business context (i.e., the reason for the payment) should be explored further. To enable such integration and to support future system features, a design would necessitate a modular and composable structure on a use-case level.

Modularity is defined as the degree to which a system's components can be separated and/or recombined. The RSN FMI demonstrated the ability to reuse the settlement logic component across multiple use cases with different initiation paths and outcomes.

Composability is a system design principle that allows components to be combined in various ways to create larger, more-complex systems. This was key to enabling the cross-network use cases where the RSN FMI functionality was composed into various transactions initiated on other third-party systems.

For this PoC, five different use cases were explored, showcasing the wide range of applications for a system like RSN. The ability to accommodate such diverse use cases was strongly supported by adhering to the principles of modularity and composability, which have been foundational to both the RLN and RSN projects.

Atomicity

Atomic settlement is the principle that the entire transaction succeeds or fails as a single, indivisible unit and is simultaneous in nature.

Removing the risk of partial settlement is core to the design of the RSN FMI. This applies both in the example of a transfer, as well as during the execution of DvP processes.

This also ensures that updates to the books and records of all relevant entities (originator, beneficiary, and all intermediaries) are updated atomically.

When executing a DvP process, the RSN FMI additionally needed to ensure that both legs of the transaction settled together atomically.

These requirements were implemented for transactions within the RSN FMI and effectively removed the risk of partial settlement, in that there was no instance where securities were delivered but payment was not.

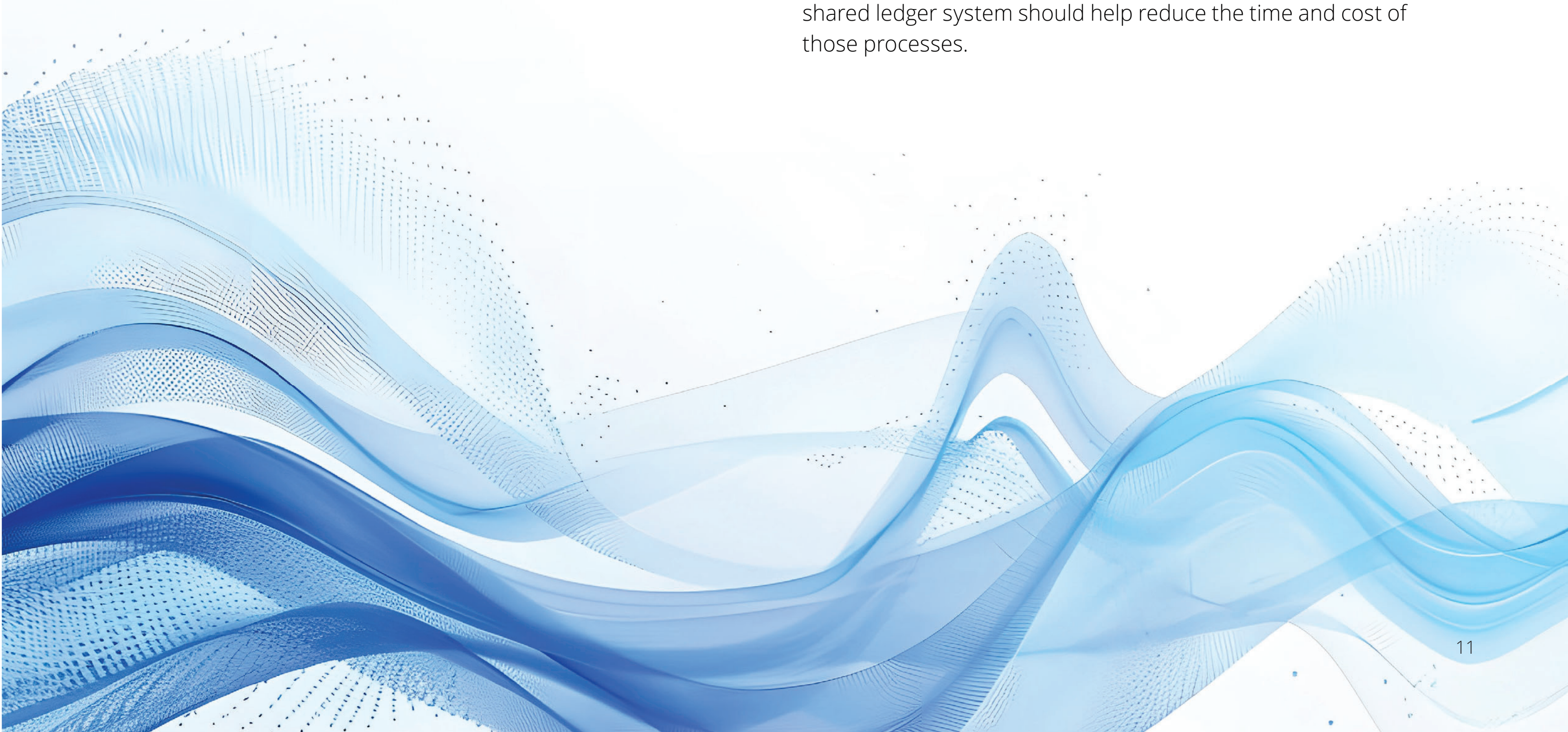
Interoperability

Interoperability with other platforms was a key requirement of the RSN PoC. RSN achieved this by designing workflows that enabled approved entities to initiate a transfer or DvP transaction and communicate those instructions to RSN to coordinate settlement. Relevant parties within RSN received the transaction details and evaluated whether to approve the proposed transactions.

This approach led to interoperability with multiple third-party tokenized platforms within the sandbox environment. Technically onboarding a new third-party platform involved translating the Swift message into the corresponding RSN action—which required no changes to the core functionality of the RSN FMI.

Reduced reconciliation processing

Reduction of the reconciliation process was a cornerstone of the RSN FMI. By enabling each participant to operate its own infrastructure for transaction processing and data storage, the RSN design reduced the need for post-transaction reconciliation for transactions within the RSN FMI. Each transaction party inherently possessed the source of truth based on the system design. In the RSN FMI, all participants had automatic access to consistent, up-to-date transaction data in which they were party to, which greatly reduced operational complexity and minimized the risk of errors. There would still be reconciliation considerations between RSN and external systems, but the single source of truth provided by the shared ledger system should help reduce the time and cost of those processes.



Modular vs. monolithic application design considerations

The decision to adopt a modular application design was based on a careful comparison between modular (functionality split between component parts with a flexible interaction model) and monolithic (tightly coupled single application including all functionality) approaches.

Solutions based on monolithic designs required adaptation to the core implementation when new capabilities or improvements are identified. This approach would result in a single, tightly coupled system that may become complex, inflexible, and difficult to maintain.

Conversely, a modular approach made it possible to implement the RSN's core implementation and expand the ecosystem's capabilities through separate, interoperable applications operated by third-party entities. These modular applications could leverage core functionalities of the RSN FMI, enabling greater flexibility and scalability. By distributing responsibilities across multiple applications, the modular design allows for targeted enhancements and minimizes dependencies. This design approach would make the overall system more adaptable to new use cases and could expedite the onboarding processes for such applications.

Privacy implications

In a monolithic application design, data for all use cases must be processed by, and therefore visible to, the system operator. This level of data exposure introduces risk considerations for participants, especially when sensitive information is involved.

To support the composability of applications and functionality, a key requirement was to ensure that the privacy requirements of one use case did not infringe upon another, even when both are processed within the same transaction. For instance, in the context of performing central clearing and netting functions, the FMI did not need to have visibility into the ongoing net positions of all participants or the specific actions that the central counterparty might take to address a failed delivery. The RSN FMI only needed to be aware of the final assets and amounts that required settlement at the conclusion of a netting window.

Multi-asset network vs. interoperable multi-ledger network

One of the primary research questions of the RSN PoC was to evaluate the trade-offs between a network capable of handling multiple asset types and an architecture of multiple interoperable ledgers. The RSN PoC explored both models.

First, the RSN PoC demonstrated the capability to process both funds and securities transfers within a single infrastructure, enabling atomic transactions across asset types.

Building on this functionality, the PoC also integrated with external ledgers that leveraged RSN for settlement in tokenized central bank deposits.

The key findings indicated that a multi-asset network offered several advantages to RSN workflows: simplified transaction processes, reduced implementation complexity, atomic settlement across asset types, and the reduction of reconciliation needs between RSN entities. However, achieving these benefits required the underlying system to support composability between use cases while maintaining privacy and data segregation, even within a single transaction.

In contrast, a multi-ledger network approach would facilitate the interaction between existing systems without requiring extensive redevelopment or locking into a single technology, which could lead to quicker time to market and the ability to leverage existing solutions. The multi-ledger network approach could enable coordinated settlement, which may be sufficient for certain use cases but does not guarantee atomicity for cross-network transactions. Additionally, a multi-ledger network would introduce integration considerations between networks.

In summary, transactions conducted across different technologies typically exhibit greater complexity and provide fewer guarantees than those processed on a single network. Nevertheless, interoperability remains essential for connecting existing systems. Therefore, an optimal system design should leverage the advantages of a multi-asset architecture wherever possible—ensuring atomicity and simplicity—while providing interoperability to extend the network's reach and utility.

Moving from RLN to RSN

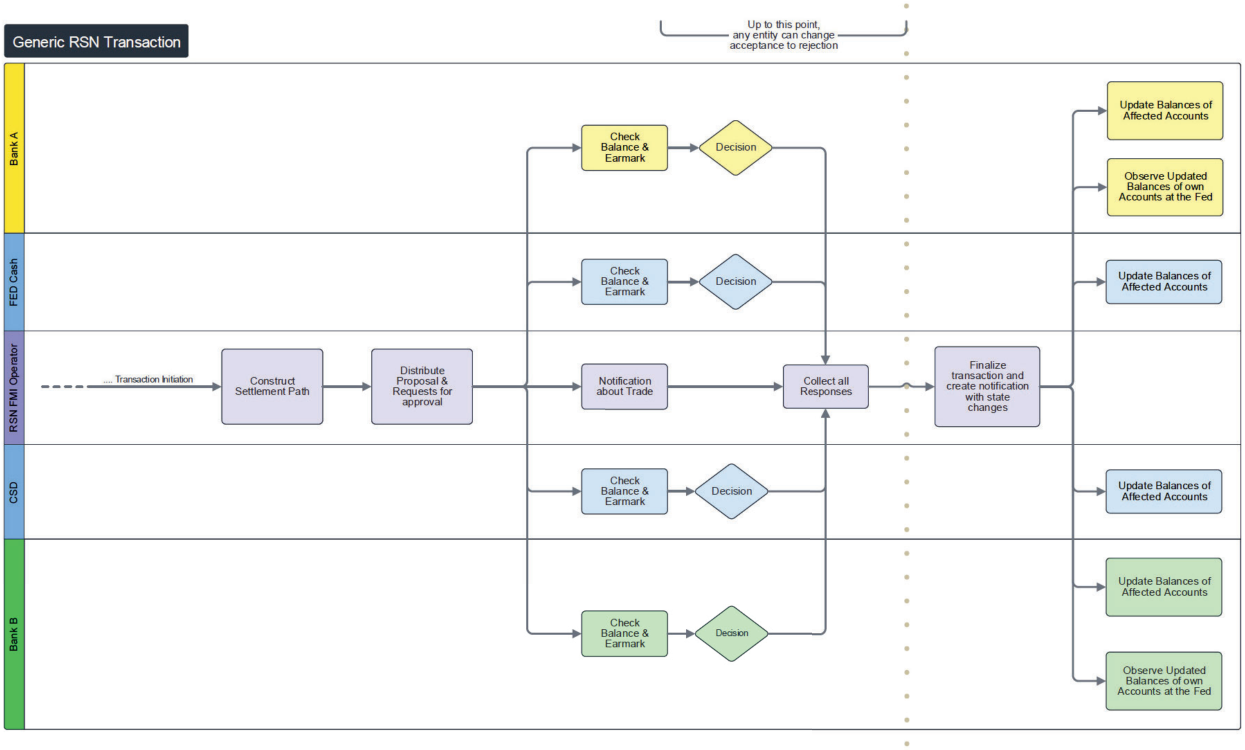
The RLN PoC, published in 2023, demonstrated the potential benefits and viability of a distributed system for executing payments, ensuring finality, and maintaining atomicity in transfers between banks. However, RLN did not explore multi-asset or cross-network settlement capabilities.

RSN aimed to address this gap while retaining all the advantages of the RLN PoC. This added capability allowed the RSN to not only coordinate transfers but also ensure the atomic DvP settlement for both assets and payments represented on the platform

Process flow

The process flow diagram outlines the transaction steps that were common across all use cases. While individual use cases varied in terms of how the flow is initiated, the types of assets being transferred, and the number of individual transactions involved, the core structure of the transaction process remained consistent.

Figure 1: Generic RSN Transaction

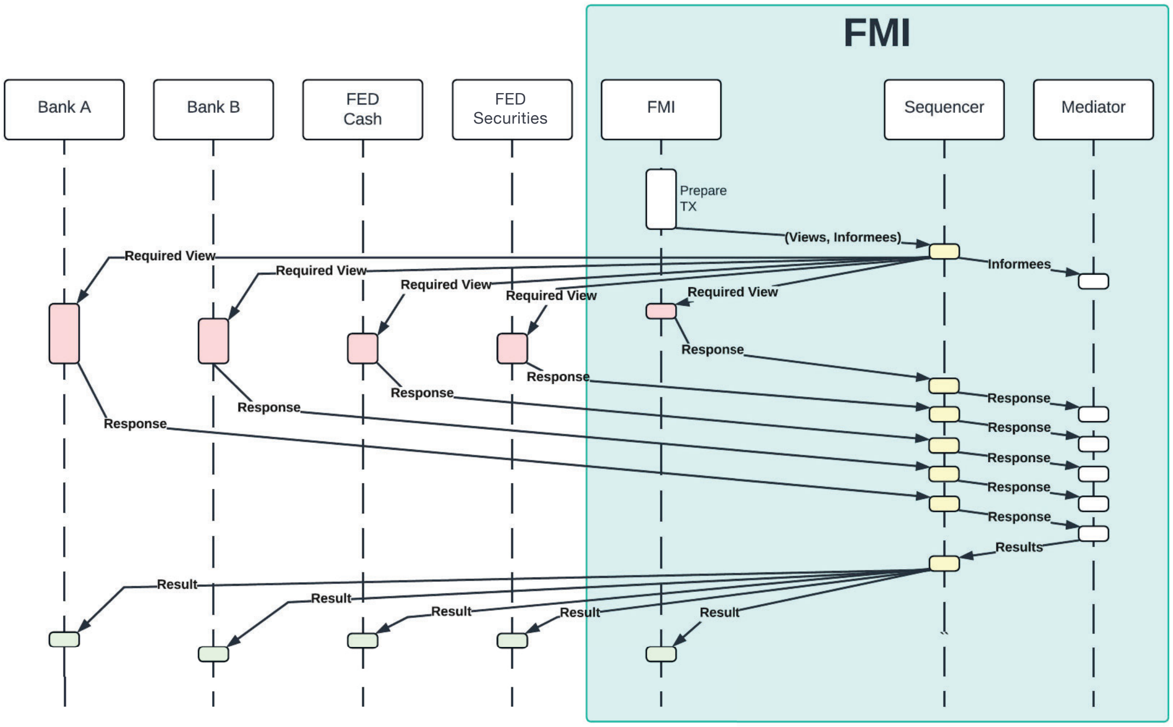

Generic RSN Transaction
Up to this point, any entity can change acceptance to rejection
Bank A
FED Cash
RSN FMI Operator
CSD
Bank B
.... Transaction Initiation
Construct Settlement Path
Distribute Proposal & Requests for approval
Check Balance & Earmark
Decision
Check Balance & Earmark
Decision
Notification about Trade
Check Balance & Earmark
Decision
Check Balance & Earmark
Decision
Collect all Responses
Finalize transaction and create notification with state changes
Update Balances of Affected Accounts
Observe Updated Balances of own Accounts at the Fed
Update Balances of Affected Accounts
Update Balances of Affected Accounts
Update Balances of Affected Accounts
Observe Updated Balances of own Accounts at the Fed

Sequence diagrams

The RSN platform for this PoC was implemented using the Canton distributed ledger technology (DLT), meaning that every technical transaction follows the steps defined by the Canton protocol. The sequence can be summarized as follows:

1. The initiating Canton participant node calculates the outcome of the proposed transaction, identifies the required signatories and informed parties, and generates the respective views for each party (i.e., which parts of the transaction need to be seen by informed parties and signed by signatories). These views are then encrypted for the intended recipients.
2. The initiating Canton participant sends the encrypted views to the Canton synchronizer (sequencer+mediator).
3. The Canton synchronizer forwards the encrypted views to the relevant parties.
4. Each signatory verifies the received view and cross-references it with their state. If everything is in order, an approval is sent back to the Canton synchronizer.
5. The Canton synchronizer collects all responses and, upon receiving the necessary approvals, finalizes the transaction and informs all parties of the state change.

Figure 2: RSN Transaction Sequence



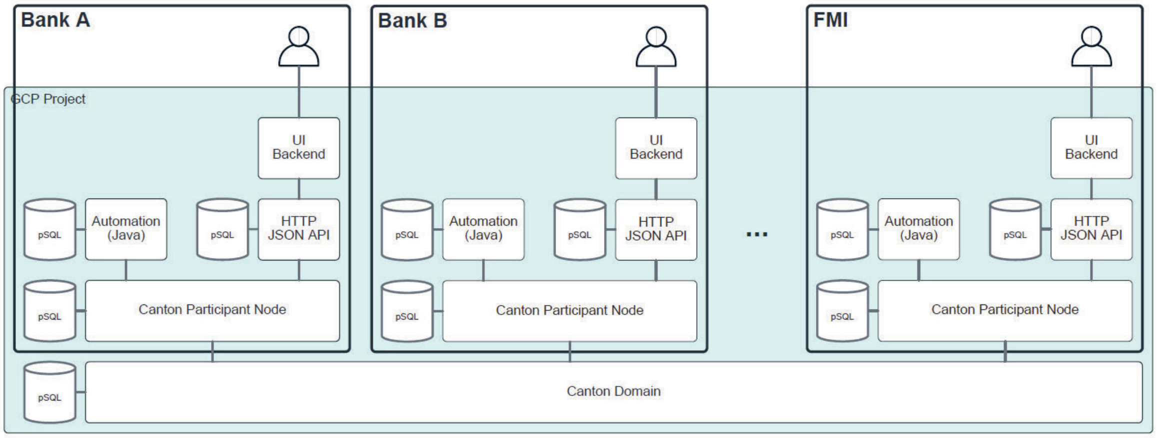
For more detailed information, please refer to the Canton documentation. Going forward, the remainder of this report will focus on the higher-level steps of business transactions rather than a detailed technical flow.

System architecture

A full stack of components was deployed for each participant, simulating a scenario where participants self-host their components within their own partition. This approach ensures that no multi-tenancy was utilized, reinforcing autonomy and control of each participant's infrastructure.

The partitions were hosted within a single Google Cloud Platform (GCP) project, which also housed the RSN FMI components and the Canton domain.

Figure 3: PoC System Architecture

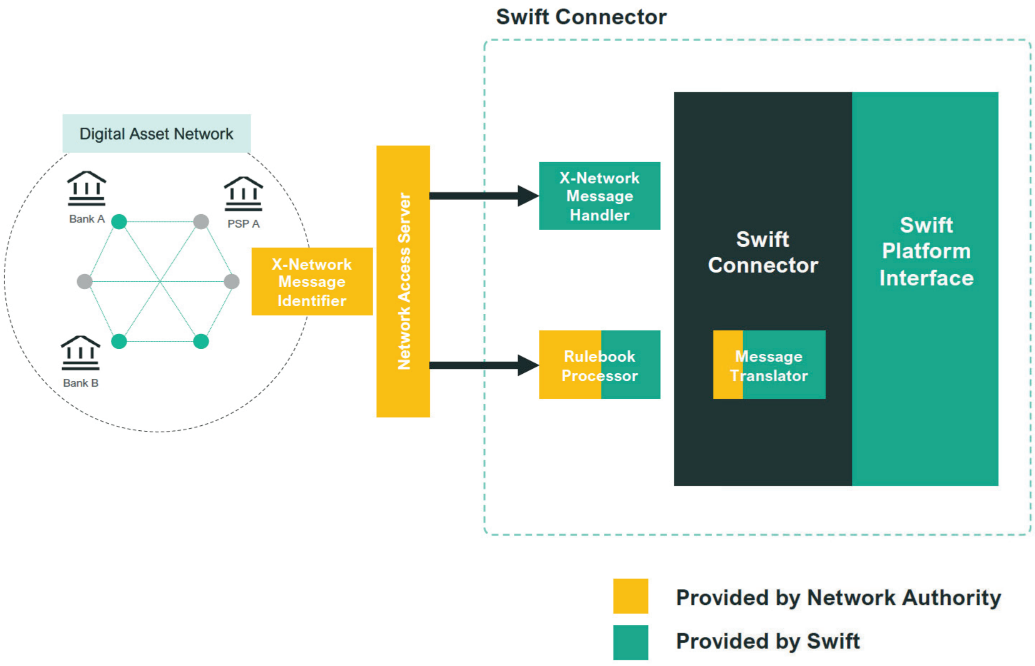


Swift interlinking prototype

The objective of achieving interoperability between multiple digital asset networks presents a unique technical challenge when comparing with existing FMIs, wherein Swift messaging enables timely delivery of payment and trade instructions between partnered financial entities. In support of this objective, Swift provides a novel interlinking prototype to enable interoperability between digital asset networks, which are often designed and implemented around differing standards and technology stacks. To achieve interoperability between digital asset networks, the core of Swift's interlinking prototype adapts and builds upon existing ISO-based messaging standards, thereby respecting how existing FMI operators coordinate with each other while innovating on the established communication pipelines.

The figure below provides a high-level component view of the Swift interlinking prototype integrated with a reference digital asset network:

Figure 4: Swift Connector Integration Model

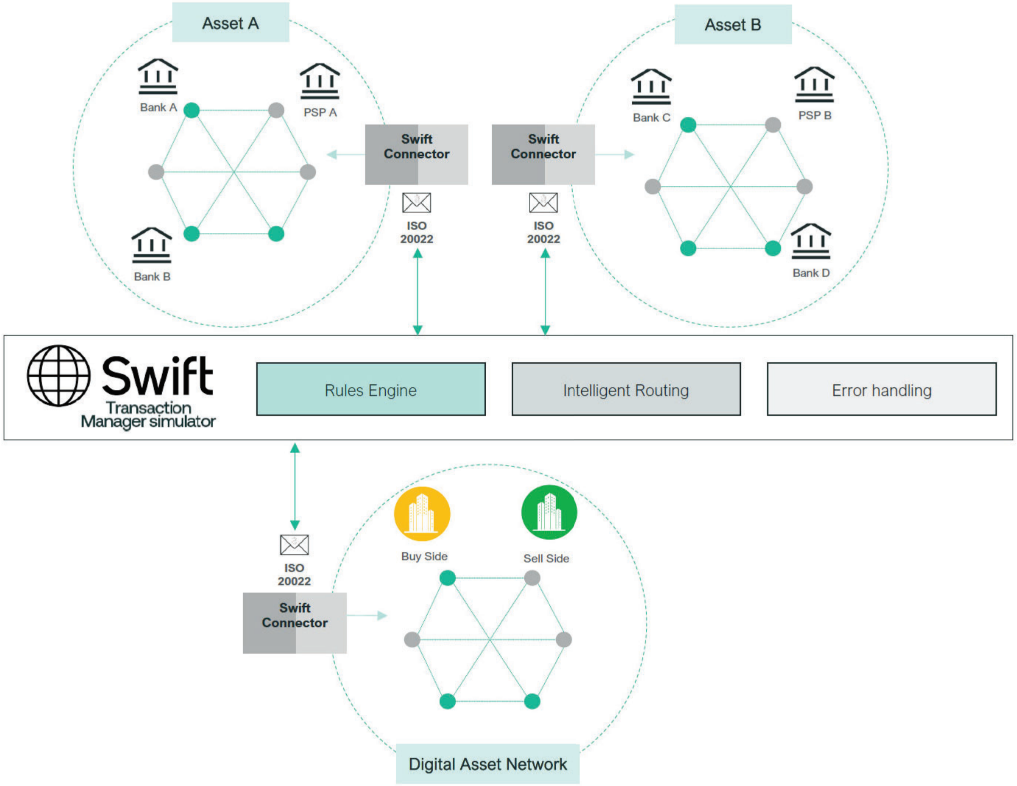


In terms of architecture, the Swift component – detailed above – is designed to integrate with a given digital asset network, providing the necessary translations between ISO-based messages and instructions specifically designed for that digital asset network. Each Swift connector instance is able to communicate and coordinate with the Swift Transaction Manager Simulator (TMS), which constitutes a simulated and lightweight version of the Swift Transaction Manager platform – also detailed below. Swift TMS provides the necessary orchestration to coordinate and pair actions performed on different networks as part of the same flow. Together, the Swift TMS and connector components constitute a hub-and-spoke model to enable seamless straight-through processing of cross-network flows leveraging the standards of ISO-based messages. The hub-and-spoke model provides a scalable approach to integrating new digital asset networks with both existing FMI and with other digital-native networks.

The Swift connector has a microservice-based architecture where each service is containerized for deployment. This microservice-based approach also enables flexibility with respect to the design, transaction modeling, and security of a given digital asset network. The Swift TMS leverages a REST API interface and lightweight service layer to provide the orchestration capabilities necessary to achieve cross-network flows. Leveraging the existing standard of Swift business identification codes (BICs) along with unique network identifiers, TMS routes instructions across networks mapping to a given Swift connector and associated network entity. Usage of the existing BIC standard created by Swift also enables this solution to integrate with an existing FMI.

The diagram below provides a high-level view of a broader reference architecture that incorporates several Swift connector instances, their respective digital asset network and associated financial actors, and the Swift TMS.

Figure 5: Swift Reference Network Architecture



Methods

Requirement gathering

The requirements and expected behavior of the use cases were defined through working group discussion, which included the technology vendor.

Software implementation

The smart contracts were implemented in Daml, utilizing the Daml finance library to accelerate development. Backend automation and system integrations were developed in Java, while all frontend applications were built using React.

Deployment

A full solution stack was deployed individually for each entity, including the Canton participant, Java automations and integrations, and the frontend user interface (UI). All deployments were provisioned on Google Cloud Platform with Kubernetes used for container orchestration.

Integration

Third-party platforms—including Mastercard's MTN, Tassat interbank network, and Broadridge's DLR—operated outside of the RSN infrastructure but connected to RSN through either the Swift interlinking prototype or direct API integration with a Canton node. To facilitate Swift connections, a Swift connector was deployed both in the RSN infrastructure and within the infrastructure of the third-party platforms.

PoC use cases[3]

Client-to-client investment grade (IG) bond DvP settlement

Use case hypothesis/overview

The IG bond DvP use case was intended to prove that RSN could work as a settlement infrastructure for simultaneous multi-asset settlement. The use case aimed to show that by having a shared-ledger infrastructure containing tokenized securities, tokenized central bank deposits, and tokenized commercial bank deposits, participants could achieve 24/7 simultaneous settlement capabilities, enhancing settlement transparency and reducing counterparty risk.

From a technology perspective, the hypothesis is that the settlement of the asset leg should function similarly to the cash transfers shown during the RLN PoC. The key difference for the RSN PoC is that the finality of both settlements—payment and asset—must be linked to the same event. This linkage ensures atomicity between the movement of deposits and assets, providing simultaneous settlement and removing risk of partial settlement.

Technical solution design and architecture

This use case adhered to the solution design and architecture outlined in the RSN design section, with the only variation being the initiation of the flow.

This scenario involved the settlement of a trade executed through traditional means, negotiated and agreed to outside of RSN and resulted in both parties submitting their understanding of the agreements to the RSN FMI. The DvP proposals submitted by each party were bilaterally matched together in the RSN FMI. DvP approvals were visible to each party, allowing each to reference their own proposal when accepting the counterparty's. This enabled the system to cross-check the relevant values, ensuring that both parties had a consistent understanding of the OTC trade.

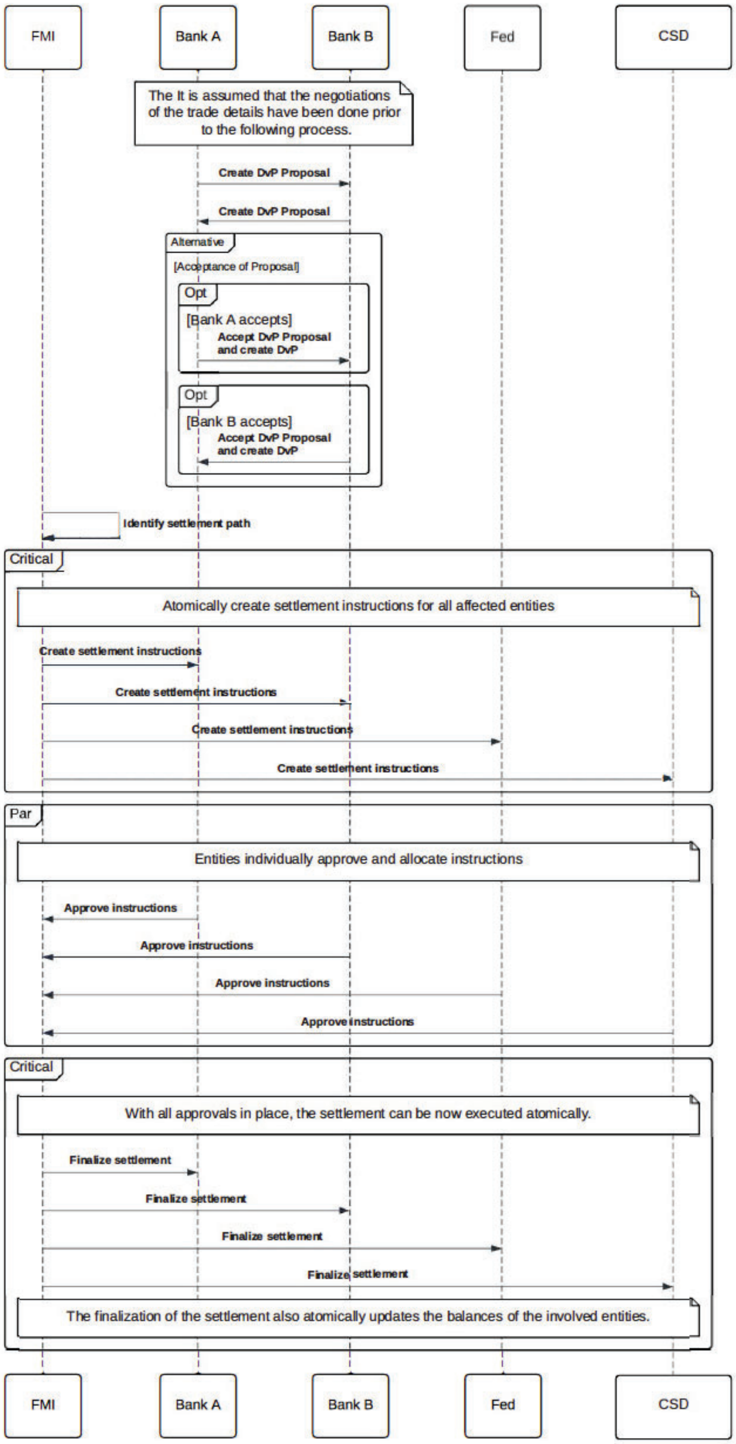
Once the DvP proposal is accepted by the counterparty to the trade, the settlement process is initiated, following the standard RSN process flow. The initiation of the settlement process is encoded within the Daml smart contracts. These contracts specified that once the DvP proposal is accepted, a DvP contract is created that is visible to both trading parties as well as the FMI. The FMI is then responsible for continuing the RSN process steps upon receipt of the DvP approvals.

Assumptions

- Trade details were agreed upon prior to the tested process.
- The settlement of the investment grade bond happened at the CSD partition.
- The settlement of the tokenized central bank deposit happened at the Fed Cash partition within the RSN FMI.
- Transaction initiation, validation, compliance, and balance checks by all parties were simulated for the purpose of transaction testing.

[3] The use cases and assumptions defined below does not necessarily reflect the views of the Federal Reserve Bank of New York or any other parts of the Federal Reserve System, including with respect to the Federal Reserve's legal authority to participate in RSN or any similar arrangement.

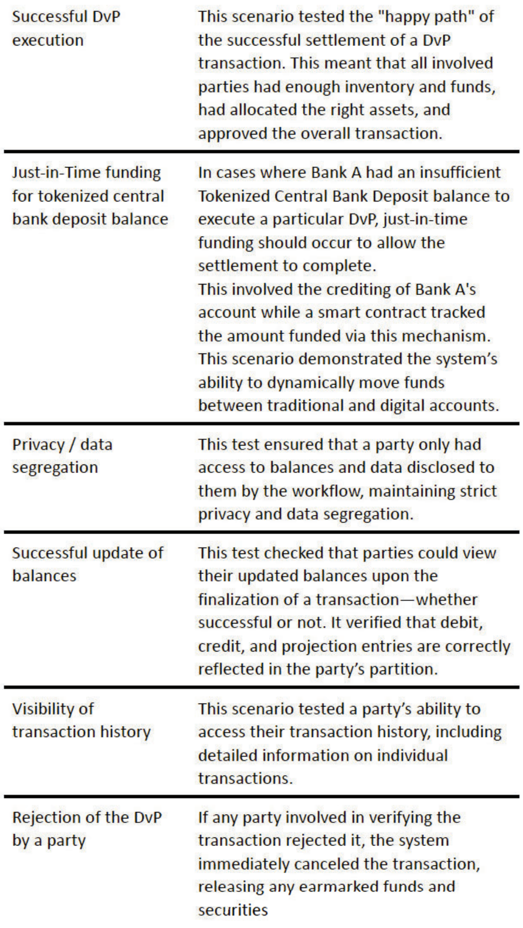
Figure 6: Client-to-Client Investment Grade (IG) Bond DvP Settlement Sequence Diagram


FMI
Bank A
Bank B
Fed
CSD
The It is assumed that the negotiations of the trade details have been done prior to the following process.
Create DvP Proposal
Create DvP Proposal
Alternative
[Acceptance of Proposal]
Opt
[Bank A accepts]
Accept DvP Proposal and create DvP
Opt
[Bank B accepts]
Accept DvP Proposal and create DvP
Identify settlement path
Critical
Atomically create settlement instructions for all affected entities
Create settlement instructions
Create settlement instructions
Create settlement instructions
Create settlement instructions
Par
Entities individually approve and allocate instructions
Approve instructions
Approve instructions
Approve instructions
Approve instructions
Critical
With all approvals in place, the settlement can be now executed atomically.
Finalize settlement
Finalize settlement
Finalize settlement
Finalize settlement
The finalization of the settlement also atomically updates the balances of the involved entities.
FMI
Bank A
Bank B
Fed
CSD

Use case testing methodology and scenarios

All tests were conducted by participants of the working group, who interacted with the system via UIs. The test cases were designed to verify correct system behavior across both success and failure scenarios. The following test cases were executed:

Figure 7: Client-to-Client Investment Grade (IG) Bond DvP Settlement Test Scenarios

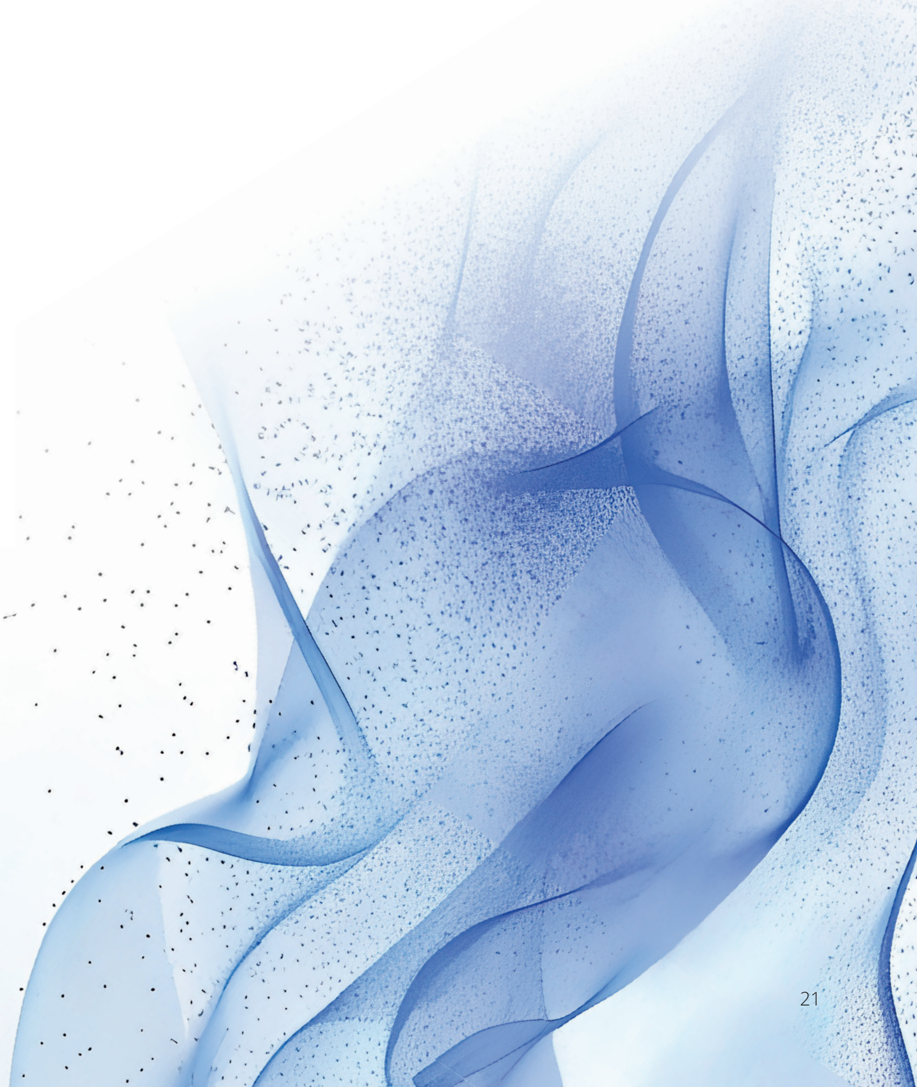


Successful DvP execution	This scenario tested the "happy path" of the successful settlement of a DvP transaction. This meant that all involved parties had enough inventory and funds, had allocated the right assets, and approved the overall transaction.
Just-in-Time funding for tokenized central bank deposit balance	In cases where Bank A had an insufficient Tokenized Central Bank Deposit balance to execute a particular DvP, just-in-time funding should occur to allow the settlement to complete. This involved the crediting of Bank A's account while a smart contract tracked the amount funded via this mechanism. This scenario demonstrated the system's ability to dynamically move funds between traditional and digital accounts.
Privacy / data segregation	This test ensured that a party only had access to balances and data disclosed to them by the workflow, maintaining strict privacy and data segregation.
Successful update of balances	This test checked that parties could view their updated balances upon the finalization of a transaction—whether successful or not. It verified that debit, credit, and projection entries are correctly reflected in the party's partition.
Visibility of transaction history	This scenario tested a party's ability to access their transaction history, including detailed information on individual transactions.
Rejection of the DvP by a party	If any party involved in verifying the transaction rejected it, the system immediately canceled the transaction, releasing any earmarked funds and securities

Key findings and future considerations

The use case showed how the RSN FMI provided atomic settlement capabilities to a DvP transaction. By enabling settlement of both the payment and IG bond legs of the transaction to be driven off the same event (gathering of all appropriate signatures), RSN ensured that the entire transaction succeeded or failed at that point which provided atomic settlement between the counterparties of the transaction.

The use case also demonstrated a set of transaction initiation rails where two parties could agree on a trade proposal that was decided outside of the settlement venue itself. By offering assurance that the agreed-upon terms were met while also providing the flexibility to dictate custom terms, the settlement capability of the RSN FMI showed its potential to be used outside the narrow construct of cash for IG bond. This setup could potentially be extended to other asset types represented on ledger and the RSN settlement venue could potentially be used as a composable piece of infrastructure for more complicated business workflows.



Centrally cleared dealer-to-dealer treasury DvP settlement

Use case hypothesis/overview

As the US financial services industry prepares for the upcoming SEC treasury clearing mandate, the second use case the RSN working group explored was how RSN could serve as an industry settlement venue for centrally cleared treasury DvP transactions. This use case expanded on the client-to-client IG bond DvP settlement use case by introducing a central counterparty (CCP) partition and custodian bank partition to the RSN FMI, while also introducing multiple settlement windows within a trading day to allow firms to still achieve T+0 settlement, while also realizing the existing efficiencies provided by netting.

In the centrally cleared dealer-to-dealer treasury DvP settlement use case, it is assumed that counterparties have already submitted their trades to the CCP outside the RSN platform. The CCP matched and novated these trades, with the resulting obligations contributing to the net position and net obligations of each party. These net obligations are coordinated through the RSN and visible to the appropriate participants in real time which allowed for more efficient inventory management.

As individual trades accumulated, the net positions and obligations are continuously updated and coordinated across participants. Once the CCP's netting window closed, the net obligations between all parties and the CCP were settled as novated trades between each institution and the CCP in line with the SEC treasury clearing mandate. If a participant failed to deliver funds or securities, other obligations continued to settle, while the defaulting party's net obligation carried over to the next settlement window.

The hypothesis tested was whether real-time visibility of net obligations toward the CCP enhances inventory management, and if RSN FMI could provide significant value not only in real-time gross settlement (RTGS) scenarios but also in netted delayed settlement scenarios.

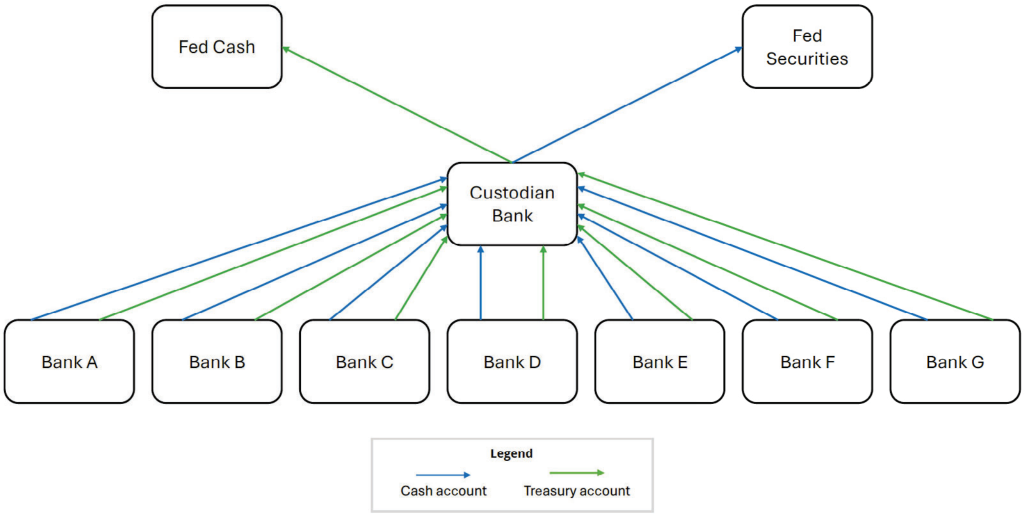
Technical solution design and architecture

This use case introduced several new concepts that extended beyond the standard design of the RSN solution. In the previous use case, RSN was primarily applied to RTGS. However, this use case scenario involves novation, netting, and timed settlement, while ensuring a coordinated view of obligations between the CCP and participants.

The settlement of individual obligations followed the same process as outlined in the design section, maintaining consistency with the established flow.

For the centrally cleared dealer-to-dealer treasury DvP settlement use case, the following account and relationship structure was implemented:

Figure 8: Centrally Cleared Dealer-to-Dealer Treasury DvP Settlement Account Structure

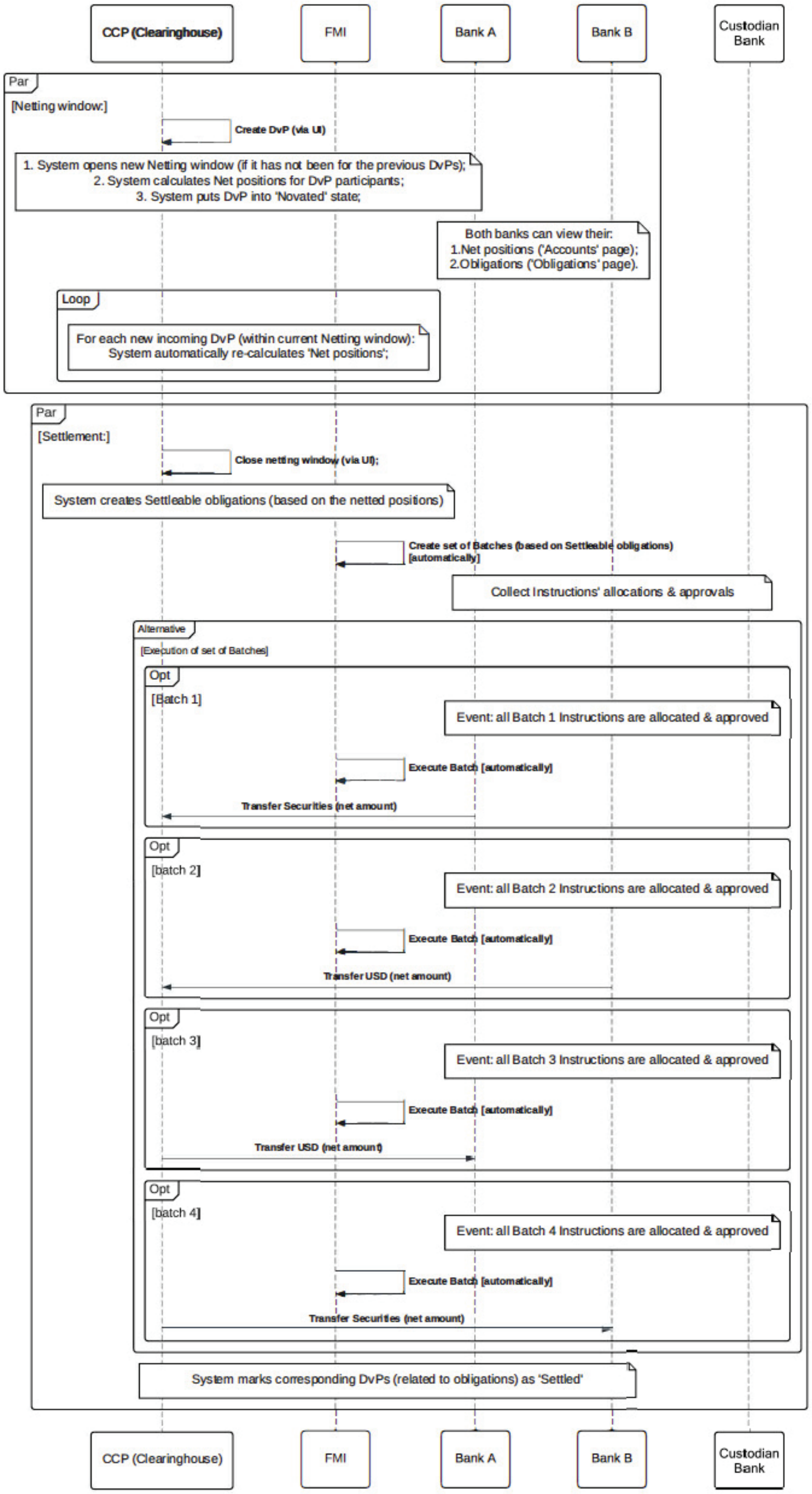


The sequence diagram to the right illustrates the complete flow of a successful execution of the centrally cleared dealer-to-dealer treasury DvP settlement scenario.

Assumptions

- Trade details were agreed upon prior to the tested process.
- Trade details were sent to the CCP by both trading parties prior to the tested process.
- Trade details were matched by the CCP prior to the tested process.
- The tested process started with the CCP capturing the DvP on the RSN network.
- The settlement of both cash as well as securities happened on the Clearing Bank's partition.
- Transaction initiation, validation, compliance, and balance checks by all parties are simulated for the purpose of transaction testing.

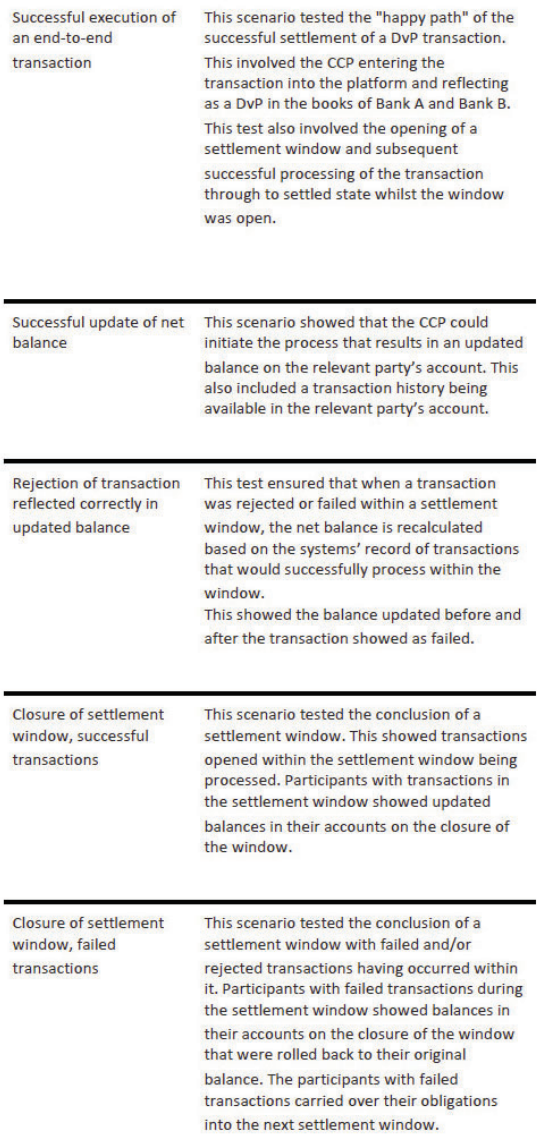
Figure 9: Centrally Cleared Dealer-to-Dealer Treasury DvP Settlement Sequence Diagram


CCP (Clearinghouse)
FMI
Bank A
Bank B
Custodian Bank
Par
[Netting window:]
Create DvP (via UI)
1. System opens new Netting window (if it has not been for the previous DvPs);
2. System calculates Net positions for DvP participants;
3. System puts DvP into 'Novated' state;
Both banks can view their:
1.Net positions ('Accounts' page);
2.Obligations ('Obligations' page).
Loop
For each new incoming DvP (within current Netting window):
System automatically re-calculates 'Net positions';
Par
[Settlement:]
Close netting window (via UI);
System creates Settleable obligations (based on the netted positions)
Create set of Batches (based on Settleable obligations) [automatically]
Collect Instructions' allocations & approvals
Alternative
[Execution of set of Batches]
Opt
[Batch 1]
Event: all Batch 1 Instructions are allocated & approved
Execute Batch [automatically]
Transfer Securities (net amount)
Opt
[batch 2]
Event: all Batch 2 Instructions are allocated & approved
Execute Batch [automatically]
Transfer USD (net amount)
Opt
[batch 3]
Event: all Batch 3 Instructions are allocated & approved
Execute Batch [automatically]
Transfer USD (net amount)
Opt
[batch 4]
Event: all Batch 4 Instructions are allocated & approved
Execute Batch [automatically]
Transfer Securities (net amount)
System marks corresponding DvPs (related to obligations) as 'Settled'
CCP (Clearinghouse)
FMI
Bank A
Bank B
Custodian Bank

Use case testing methodology and scenarios

All tests were conducted by participants of the working group, who interacted with the system via UIs provided in the PoC sandbox. The test cases were designed to verify correct system behavior across both success and failure scenarios. The following test cases were executed:

Figure 10: Centrally Cleared Dealer-to-Dealer Treasury DvP Settlement Test Scenarios



Successful execution of an end-to-end transaction	This scenario tested the "happy path" of the successful settlement of a DvP transaction. This involved the CCP entering the transaction into the platform and reflecting as a DvP in the books of Bank A and Bank B. This test also involved the opening of a settlement window and subsequent successful processing of the transaction through to settled state whilst the window was open.
Successful update of net balance	This scenario showed that the CCP could initiate the process that results in an updated balance on the relevant party's account. This also included a transaction history being available in the relevant party's account.
Rejection of transaction reflected correctly in updated balance	This test ensured that when a transaction was rejected or failed within a settlement window, the net balance is recalculated based on the systems' record of transactions that would successfully process within the window. This showed the balance updated before and after the transaction showed as failed.
Closure of settlement window, successful transactions	This scenario tested the conclusion of a settlement window. This showed transactions opened within the settlement window being processed. Participants with transactions in the settlement window showed updated balances in their accounts on the closure of the window.
Closure of settlement window, failed transactions	This scenario tested the conclusion of a settlement window with failed and/or rejected transactions having occurred within it. Participants with failed transactions during the settlement window showed balances in their accounts on the closure of the window that were rolled back to their original balance. The participants with failed transactions carried over their obligations into the next settlement window.

Key findings and future considerations

The centrally cleared dealer-to-dealer treasury DvP settlement use case expanded upon the base DvP use case scenario by showcasing how a DvP transaction could be constructed and settled on the system in accordance with the upcoming treasury clearing rules:

- The transaction initiation to the RSN FMI for this use case was designed to allow novated, matched, and cleared DvP records onto the FMI through a central clearing party.
- The CCP logic enabled a net position functionality between each party and the CCP to maintain a running summary of the DvPs open on the system. This net position construct enables a real-time look at each parties' obligations to the CCP party.
- The RSN FMI enabled a settlement window functionality where the accrued net positions were settled atomically between each party and the CCP entity. This could occur regardless of any other party's settlement status, allowing each bank to receive finality with respect to their obligations to the CCP.

These additional constructs layered onto the core settlement rails demonstrated in the RSN design section and showed the flexibility of the RSN FMI to potentially comply with regulatory scenarios that do not map directly to its core functionality.

Cross network DvP settlement

Use case hypothesis/overview

A potential application of the RSN is to serve as a settlement venue for other platforms, which was the focus of the cross network DvP settlement use case.

This use case demonstrated how a corporate client could use MTN to securely purchase a tokenized real-world asset from a third-party platform that had integrated MTN as a payment solution using tokenized commercial bank deposits. MTN intended to safely and securely coordinate the movement of commercial bank deposits on MTN with the corresponding inter-bank central bank deposit movement occurring within RSN.

The hypothesis tested if the RSN FMI could be effectively used as a settlement venue, offering multiple integration options with external platforms. MTN ensured that the asset and funds leg of the transaction were coordinated with the money settlement. It is worth noting the same settlement flow defined in the original RLN pilot can be applied, as is currently used for the payment leg of a DvP coordinated settlement.

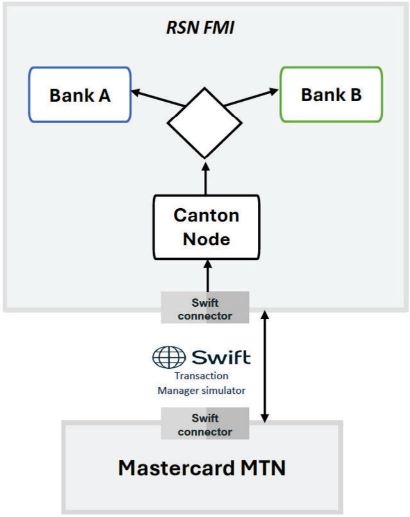
Technical solution design and architecture

From the perspective of the RSN, the technical design and the process flow for this use case leveraged an identical payment leg as that from the client-to-client IG bond DvP settlement scenario. In the approach tested by this use case:

- The cross-network settlement is initiated through one of two methods:
  - A direct integration from MTN to the RSN APIs
  - An API-based integration between Mastercard's MTN and Swift's interlinking prototype
  - The inter-bank payment instruction is processed atomically on the RSN platform, and the final customer payment is processed on the MTN upon successful confirmation of inter-bank settlement on RSN via either the RSN API or Swift (depending on the connectivity model used).
  - The direct connectivity to RSN model was tested using a set of restful APIs that were exposed by RSN enabling MTN to initiate an inter-bank payment instruction and retrieve that status of the transaction.
  - The Swift interlinking prototype was installed on the RSN and managed by the FMI operator to enable straight-through processing between MTN-based transactions and inter-bank settlement on the RSN, allowing banks that use both MTN and RSN to leverage the benefits of RSN.

The Swift interlinking prototype component is run by the FMI operator and allows external entities to interact with the RSN platform.

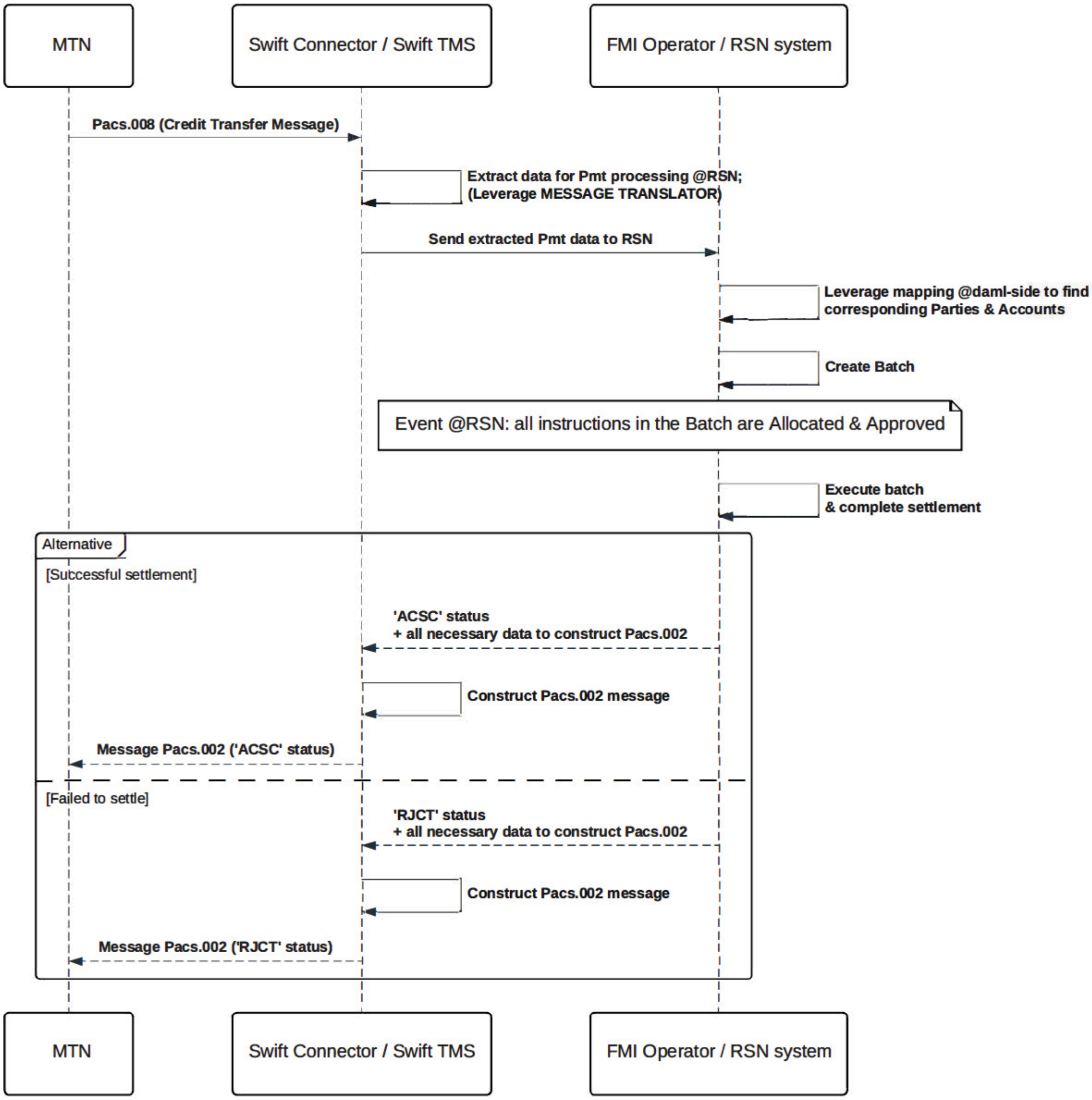
Figure 11: MTN with Swift Integration



Given that the DvP transaction spans multiple technology stacks, achieving atomicity between the settlement of funds and assets is not feasible. However, the settlement of the funds leg on RSN, which involves updating the books and records of multiple entities, occurs atomically. This mirrors the transfer and payment use cases explored in the US RLN PoC during 2023.

The sequence diagram below illustrates the complete flow of a successful execution of the MTN use case.

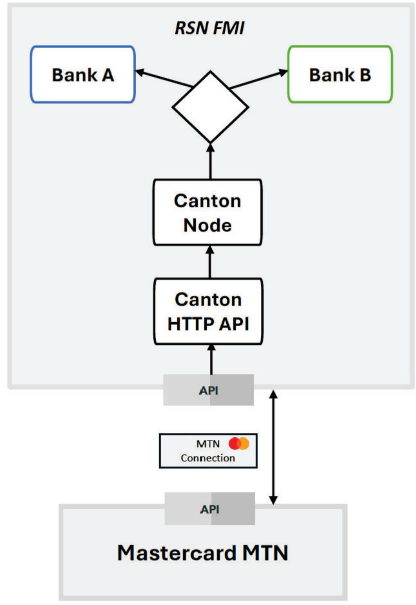
Figure 12: Cross Network DvP Settlement Sequence Diagram


MTN
Swift Connector / Swift TMS
FMI Operator / RSN system
Pacs.008 (Credit Transfer Message)
Extract data for Pmt processing @RSN;
(Leverage MESSAGE TRANSLATOR)
Send extracted Pmt data to RSN
Leverage mapping @daml-side to find
corresponding Parties & Accounts
Create Batch
Event @RSN: all instructions in the Batch are Allocated & Approved
Execute batch
& complete settlement
Alternative
[Successful settlement]
'ACSC' status
+ all necessary data to construct Pacs.002
Construct Pacs.002 message
Message Pacs.002 ('ACSC' status)
[Failed to settle]
'RJCT' status
+ all necessary data to construct Pacs.002
Construct Pacs.002 message
Message Pacs.002 ('RJCT' status)
MTN
Swift Connector / Swift TMS
FMI Operator / RSN system

Direct RSN connectivity model

An alternative setup where the MTN platform directly integrates with a Canton native API using ISO-based message structures was explored.

Figure 13: MTN with Swift Integration



This approach did not alter the atomicity characteristics of the DvP process but simplified the integration by reducing the number of components and translation layers.

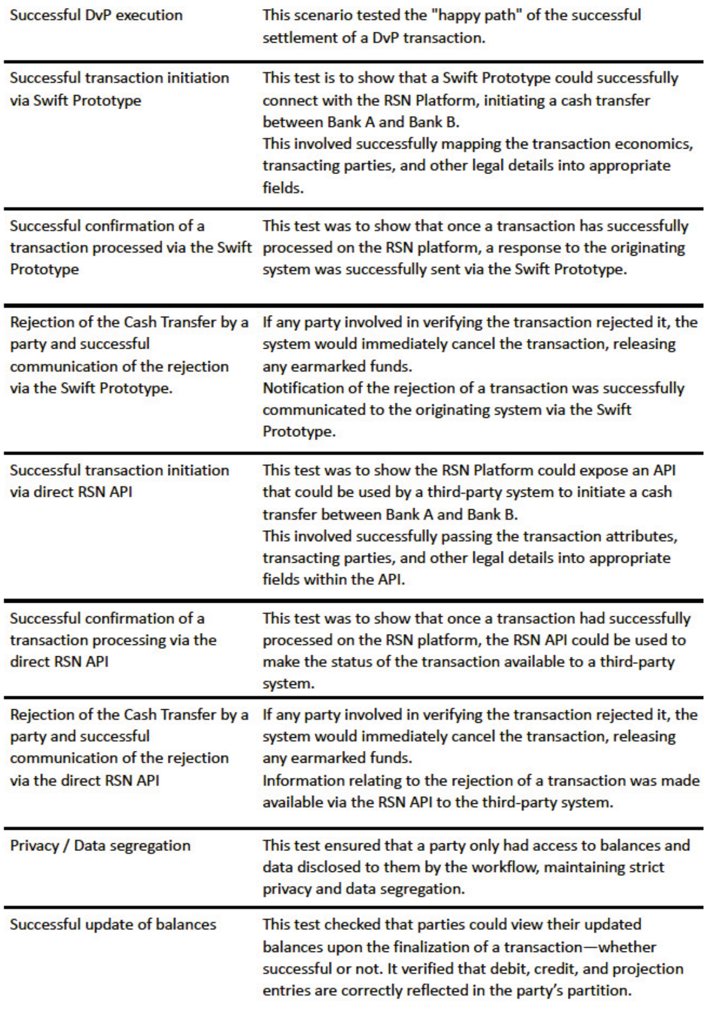
Assumptions

- Trade details were agreed upon on the MTN platform.
- All sanctions and OFAC checks were performed by the respective financial institutions that are part of MTN.
- The inter-bank settlement of the inter-bank payment was triggered on the RSN platform via incoming messaging process.
- The settlement of the tokenized central bank deposits took place on the Fed cash partition within the RSN FMI.
- The banks that were trading counterparties on MTN were also represented on the RSN.
- Transaction initiation, validation, compliance, and balance checks by all parties were simulated for the purpose of transaction testing.

Use case testing methodology and scenarios

All tests were conducted by working group participants, who interacted with the system via UIs. The test cases were designed to verify correct system behavior across both success and failure scenarios. The following test cases were executed:

Figure 14: Cross Network DvP Settlement



Successful DvP execution	This scenario tested the "happy path" of the successful settlement of a DvP transaction.
Successful transaction initiation via Swift Prototype	This test is to show that a Swift Prototype could successfully connect with the RSN Platform, initiating a cash transfer between Bank A and Bank B. This involved successfully mapping the transaction economics, transacting parties, and other legal details into appropriate fields.
Successful confirmation of a transaction processed via the Swift Prototype	This test was to show that once a transaction has successfully processed on the RSN platform, a response to the originating system was successfully sent via the Swift Prototype.
Rejection of the Cash Transfer by a party and successful communication of the rejection via the Swift Prototype.	If any party involved in verifying the transaction rejected it, the system would immediately cancel the transaction, releasing any earmarked funds. Notification of the rejection of a transaction was successfully communicated to the originating system via the Swift Prototype.
Successful transaction initiation via direct RSN API	This test was to show the RSN Platform could expose an API that could be used by a third-party system to initiate a cash transfer between Bank A and Bank B. This involved successfully passing the transaction attributes, transacting parties, and other legal details into appropriate fields within the API.
Successful confirmation of a transaction processing via the direct RSN API	This test was to show that once a transaction had successfully processed on the RSN platform, the RSN API could be used to make the status of the transaction available to a third-party system.
Rejection of the Cash Transfer by a party and successful communication of the rejection via the direct RSN API	If any party involved in verifying the transaction rejected it, the system would immediately cancel the transaction, releasing any earmarked funds. Information relating to the rejection of a transaction was made available via the RSN API to the third-party system.
Privacy / Data segregation	This test ensured that a party only had access to balances and data disclosed to them by the workflow, maintaining strict privacy and data segregation.
Successful update of balances	This test checked that parties could view their updated balances upon the finalization of a transaction—whether successful or not. It verified that debit, credit, and projection entries are correctly reflected in the party's partition.

Key findings and future considerations

The MTN use case showcased the potential of the RSN solution to operate as a settlement venue for not just its own transactions but could potentially offer the guarantees of inter-bank settlement of tokenized central bank deposits to other platforms that consist of RSN members. The MTN use case demonstrated a few key features that enable this construct:

- The RSN successfully integrated to the MTN network via both the Swift interlinking prototype and a direct RSN API integration.
- Use of the Swift interlinking prototype as a standard messaging platform allowed MTN and RSN to coordinate a settlement transaction across both of their platforms via the usage of ISO20022 messaging standards.
- Use of the direct API connection resulted in a simple connectivity model allowing initiation of transaction and the retrieval of their outcomes.
- While not fully atomic due to the cross-platform nature, the coordinated settlement occurred simultaneously and was sequenced appropriately to handle the settlement of both the funds and asset sides of the transaction.
- The payment leg on the RSN settlement venue functions atomically. Once all approvals for the transfer of money have been collected, the resulting update of all involved books and records on RSN happen atomically, including the initiation of sending the response message. Like the standard RSN flow, the payment leg is considered to have reached settlement finality during this time.
- RSN was used to settle a transaction in tokenized central bank deposits that originated on another platform for an asset that was not moving on the RSN.
- MTN realized settlement finality in tokenized central bank deposits for an asset otherwise transferred on their network with only commercial bank deposits.

This use case reinforces the composability of the RSN venue across a broader ecosystem of networks and applications. The successful transaction initiated by MTN, either directly via the RSN API or via Swift, showcases that the RSN can operate as a central hub and allow other platforms to potentially benefit from the various proposed RSN features.

Cross-network correspondent bank settlement

Use case hypothesis/overview

The cross-network correspondent bank settlement use case examined the potential of using RSN as a common settlement infrastructure for transactions initiated between corporate clients of two separate non-RSN member banks. Unlike the cross-network DvP settlement use case, it was assumed that the transacting banks involved in this use case are not RSN members. Instead, settlement agents were utilized to affect the payments on behalf of these banks.

Hence, RSN was tested as a settlement venue for non-RSN member banks to achieve settlement through a correspondent banking model that consisted of RSN member banks. Connecting to RSN through an interoperability protocol such as Swift's interlinking prototype or through direct API integration allowed for potentially extending some benefits of RSN to non-RSN members using settlement agents who were RSN members.

Technical solution design and architecture

The technical solution for the cross-network correspondent bank settlement use case was similar to the cross-network DvP settlement use case. The main difference was in the way Tassat interbank network interacted with the Swift interlinking prototype. The Tassat interbank network utilized the connector component of the Swift interlinking prototype versus integrating directly to the Swift TMS.

This allowed the leveraging of the Swift interlinking prototype connector to initiate transfers and learn about their outcome.

Figure 15: Tassat and Swift Integration

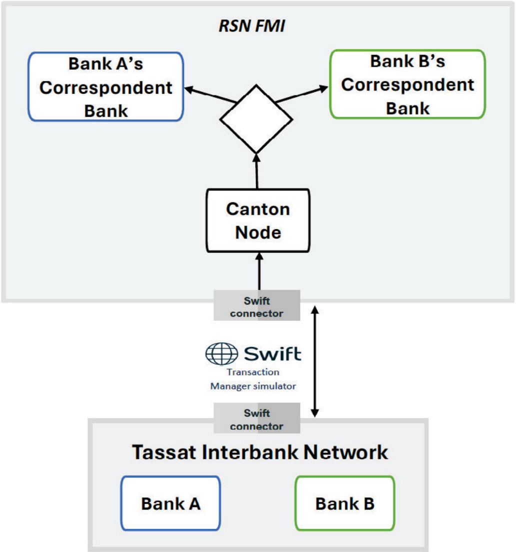
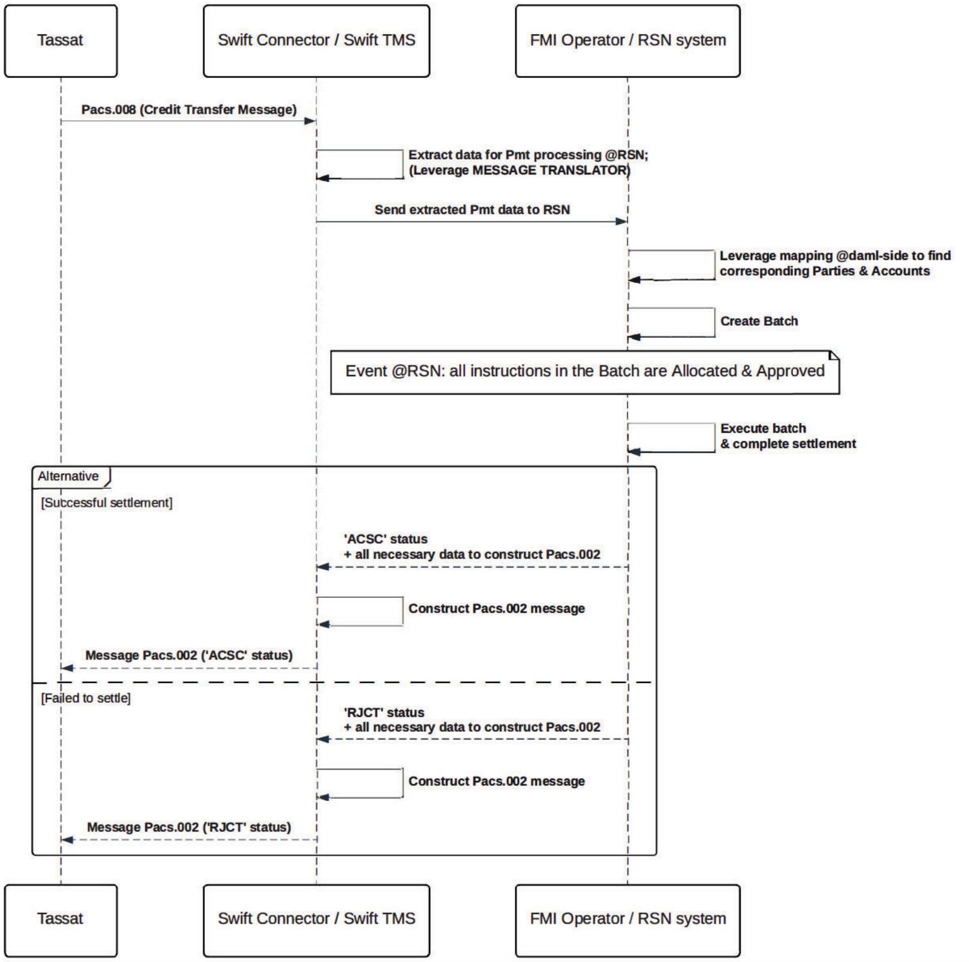


Figure 16: Cross-Network Correspondent Bank Settlement Sequence Diagram


Tassat
Swift Connector / Swift TMS
FMI Operator / RSN system
Pacs.008 (Credit Transfer Message)
Extract data for Pmt processing @RSN;
(Leverage MESSAGE TRANSLATOR)
Send extracted Pmt data to RSN
Leverage mapping @daml-side to find
corresponding Parties & Accounts
Create Batch
Event @RSN: all instructions in the Batch are Allocated & Approved
Execute batch
& complete settlement
Alternative
[Successful settlement]
'ACSC' status
+ all necessary data to construct Pacs.002
Construct Pacs.002 message
Message Pacs.002 ('ACSC' status)
[Failed to settle]
'RJCT' status
+ all necessary data to construct Pacs.002
Construct Pacs.002 message
Message Pacs.002 ('RJCT' status)
Tassat
Swift Connector / Swift TMS
FMI Operator / RSN system

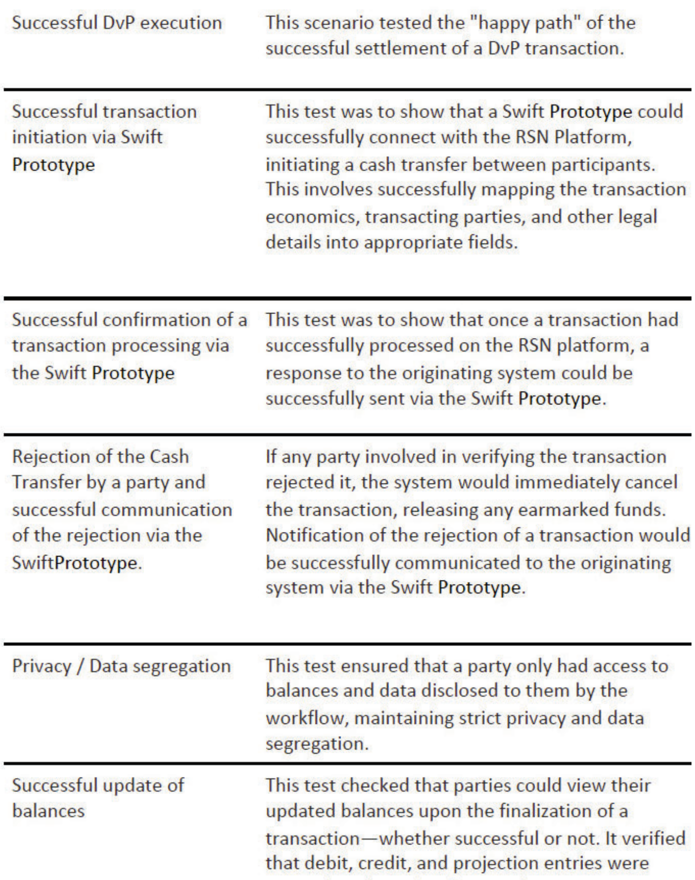
Assumptions

- Trade details were agreed upon on the Tassat interbank network.
- All sanctions and OFAC checks are performed by the trading parties on the Tassat interbank network.
- The settlement of the inter-bank payment on the RSN FMI was triggered via incoming messaging.
- The settlement of the tokenized central bank deposits took place on the Fed cash partition within the RSN FMI.
- The banks that were trading counterparties on the Tassat interbank network were not represented on the RSN. The settlement occurred through correspondent banks that were represented on RSN.
- Transaction initiation, validation, compliance, and balance checks by all parties were simulated for the purpose of transaction testing.

Use case testing methodology and scenarios

All tests were conducted by participants of the working group, which interacted with the system via UIs. The test cases were designed to verify correct system behavior across both success and failure scenarios. The following test cases were executed:

Figure 17: Cross-Network Correspondent Bank Settlement Testing Scenarios



Successful DvP execution	This scenario tested the "happy path" of the successful settlement of a DvP transaction.
Successful transaction initiation via Swift Prototype	This test was to show that a Swift Prototype could successfully connect with the RSN Platform, initiating a cash transfer between participants. This involves successfully mapping the transaction economics, transacting parties, and other legal details into appropriate fields.
Successful confirmation of a transaction processing via the Swift Prototype	This test was to show that once a transaction had successfully processed on the RSN platform, a response to the originating system could be successfully sent via the Swift Prototype.
Rejection of the Cash Transfer by a party and successful communication of the rejection via the SwiftPrototype.	If any party involved in verifying the transaction rejected it, the system would immediately cancel the transaction, releasing any earmarked funds. Notification of the rejection of a transaction would be successfully communicated to the originating system via the Swift Prototype.
Privacy / Data segregation	This test ensured that a party only had access to balances and data disclosed to them by the workflow, maintaining strict privacy and data segregation.
Successful update of balances	This test checked that parties could view their updated balances upon the finalization of a transaction—whether successful or not. It verified that debit, credit, and projection entries were

Key findings and future considerations

The cross-network correspondent bank settlement use case further demonstrates the potential of the RSN settlement venue to act as a composable solution for other networks or platforms looking to utilize the settlement finality provided by the system in tokenized central bank deposits via RSN settlement agents. The use case demonstrated a few key features:

- RSN and Tassat interbank network were linked by the Swift interlinking prototype to enable coordinated messaging between the RSN network and the Tassat interbank network.
- Conformance to ISO20022 messaging standards enabled communication between the Tassat interbank network and the RSN settlement venue.
- RSN could theoretically extend the benefits of settlement in tokenized central bank deposits to non-RSN members, given there being a connecting party that is an RSN member (e.g., the settlement agents in this use case).
- The payment leg on the RSN settlement venue functions atomically. Once all approvals for the transfer of money have been collected, the resulting update of all involved books and records on RSN happen atomically, including the initiation of sending the response message. As in the standard RSN flow, the payment leg is considered to have reach settlement finality during this time.

The use case reinforced that the RSN could theoretically extend various potential benefits (e.g., settlement in tokenized central bank deposits) to non-RSN members via the correspondent banking model. Utilizing the Swift interlinking prototype in this use case shows that the tooling provided by Swift when combined with RSN can be flexible, standardized and enhances the composability features potentially desired by market participants.

Cross-network intraday repurchase (repo) agreement settlement

Use case hypothesis/overview

A shared ledger financial market infrastructure, incorporating both tokenized central bank deposits and tokenized commercial bank deposits, could support other transaction types, including cross-network, bilateral, dealer-to-dealer intraday repo transactions. By connecting RSN and Broadridge DLR through Swift interlinking prototype, the system could provide additional transaction optionality to RSN members.

The hypothesis tested whether this infrastructure could facilitate the development of an intraday repo market, allowing financing to occur throughout the day rather than being limited to overnight transactions.

This use case investigates the potential of RSN as a settlement venue for more complex financial processes, where both the asset and funds are transacted directly within the RSN. Broadridge DLR initiates the repo transactions, monitors the process, and would have the responsibility to handle any transaction errors or failures of which they were notified.

Technical solution design and architecture

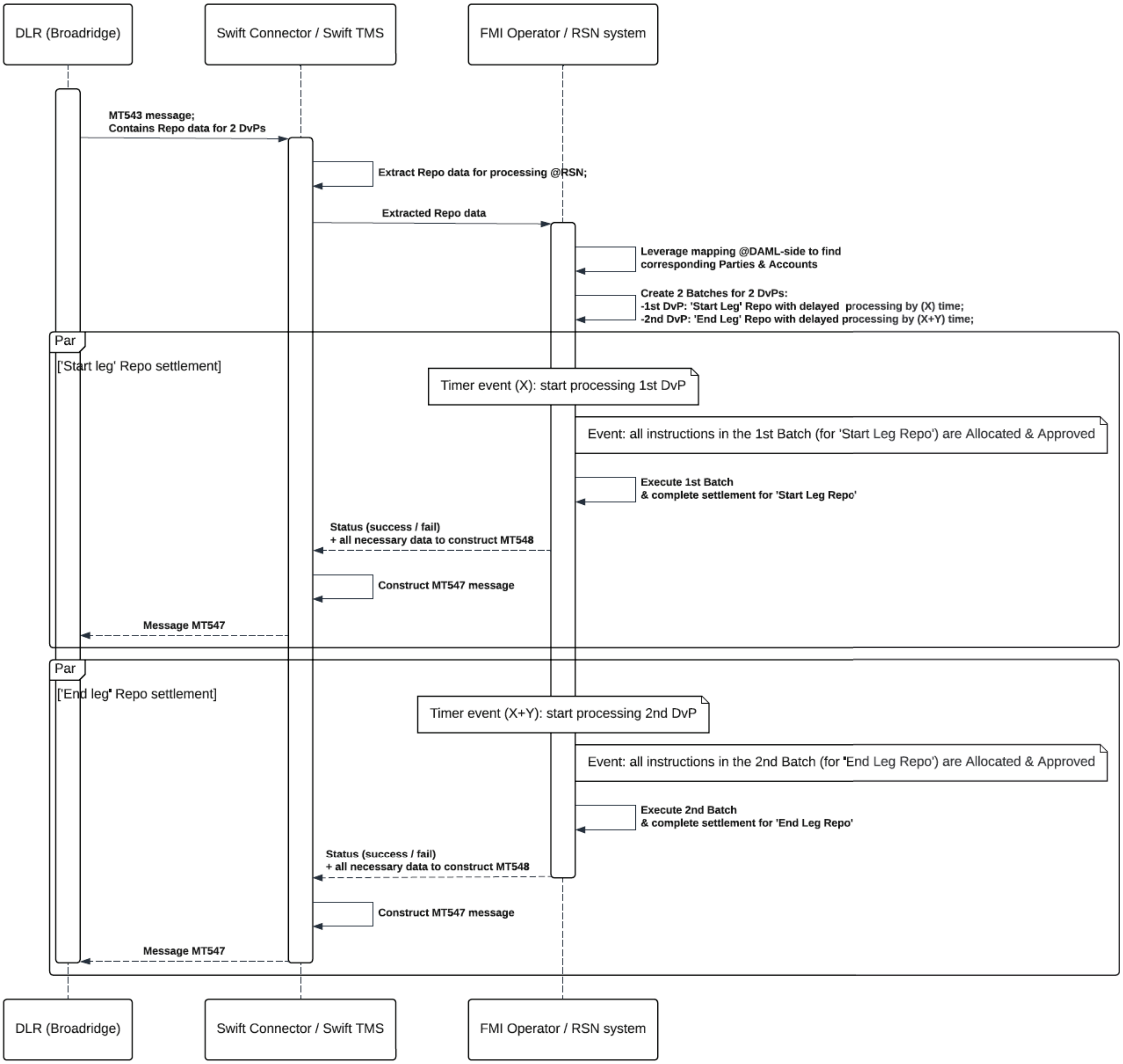
In line with other interoperability scenarios, RSN's capability to serve as a settlement venue for third-party platforms, enabling 24/7 settlement of intraday repo transactions was tested.

The tested approach is outlined as follows:

- Repo agreement: Banks agreed on the terms of the tokenized treasuries repo transaction using Broadridge's DLR platform.
- Settlement instructions: Settlement instructions for both the opening and closing legs of the repo were transmitted to RSN through Swift's interlinking prototype.
- DvP transaction creation: Upon receiving the instructions, RSN processed them and generated the corresponding DvP transactions on the RSN platform for both the open and close legs of the repo.
- DvP processing: Both DvP transactions were processed according to the same workflow established for the non-cleared DvP use case with the only difference being that the DvP in this use case contained time-based execution.
- Status notification: After the completion of each DvP transaction, Broadridge DLR, as the initiating platform, was notified of the status of the individual DvPs.
- Swift translator: To enable communication with Swift's transaction manager simulator and RSN, Broadridge DLR operates a Swift translator, which facilitates interaction with the TMS.

This design demonstrates how RSN could provide continuous settlement functionality and improve integration with external platforms for intraday repo transactions.

Figure 18: Cross-Network Intraday Repurchase (Repo) Agreement Settlement Sequence Diagram


DLR (Broadridge)
Swift Connector / Swift TMS
FMI Operator / RSN system
MT543 message;
Contains Repo data for 2 DvPs
Extract Repo data for processing @RSN;
Extracted Repo data
Leverage mapping @DAML-side to find corresponding Parties & Accounts
Create 2 Batches for 2 DvPs:
-1st DvP: 'Start Leg' Repo with delayed processing by (X) time;
-2nd DvP: 'End Leg' Repo with delayed processing by (X+Y) time;
Par
['Start leg' Repo settlement]
Timer event (X): start processing 1st DvP
Event: all instructions in the 1st Batch (for 'Start Leg Repo') are Allocated & Approved
Execute 1st Batch
& complete settlement for 'Start Leg Repo'
Status (success / fail)
+ all necessary data to construct MT548
Construct MT547 message
Message MT547
Par
['End leg' Repo settlement]
Timer event (X+Y): start processing 2nd DvP
Event: all instructions in the 2nd Batch (for 'End Leg Repo') are Allocated & Approved
Execute 2nd Batch
& complete settlement for 'End Leg Repo'
Status (success / fail)
+ all necessary data to construct MT548
Construct MT547 message
Message MT547
DLR (Broadridge)
Swift Connector / Swift TMS
FMI Operator / RSN system

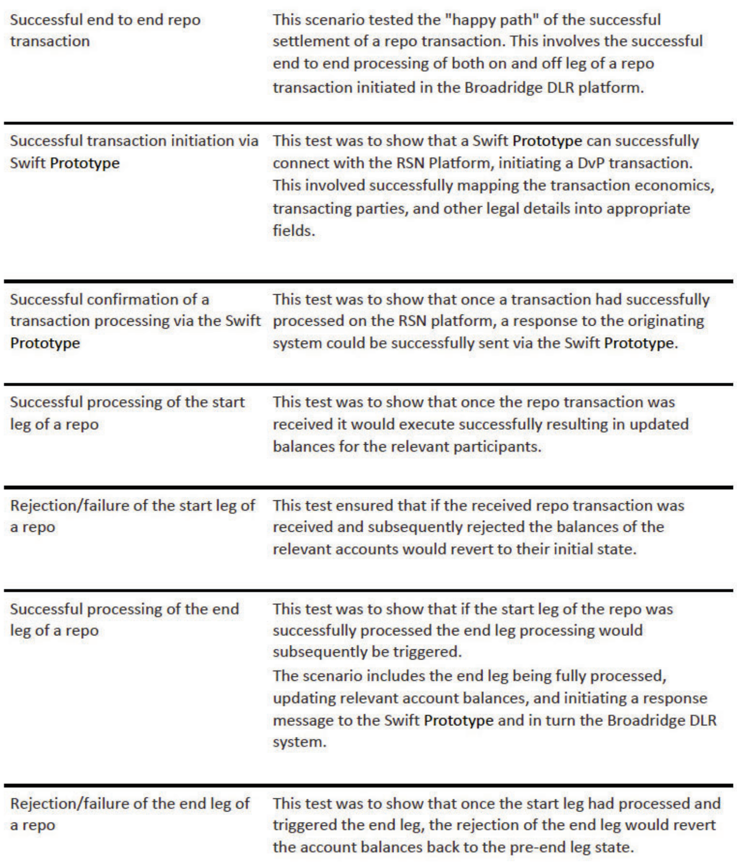
Assumptions

- Trading terms of the repo were agreed upon within the Broadridge platform.
- The settlement of tokenized treasuries as well as tokenized central bank deposits takes place on the RSN FMI within the Fed securities and Fed cash partitions respectively.
- The settlement of the repo was instructed as two individual DvP transactions, both of which were settled atomically.
- The banks that were trading counterparties on Broadridge DLR were also represented on the RSN.
- Transaction initiation, validation, compliance, and balance checks by all parties were simulated for the purpose of transaction testing.

Use case testing methodology and scenarios

All tests were conducted by participants of the working group, who interacted with the system via UIs. The test cases were designed to verify correct system behavior across both success and failure scenarios. The following test cases were executed:

Figure 19: Cross-Network Intraday Repurchase (Repo) Agreement Settlement Testing Scenarios



Successful end to end repo transaction	This scenario tested the "happy path" of the successful settlement of a repo transaction. This involves the successful end to end processing of both on and off leg of a repo transaction initiated in the Broadridge DLR platform.
Successful transaction initiation via Swift **Prototype**	This test was to show that a Swift **Prototype** can successfully connect with the RSN Platform, initiating a DvP transaction. This involved successfully mapping the transaction economics, transacting parties, and other legal details into appropriate fields.
Successful confirmation of a transaction processing via the Swift **Prototype**	This test was to show that once a transaction had successfully processed on the RSN platform, a response to the originating system could be successfully sent via the Swift **Prototype**.
Successful processing of the start leg of a repo	This test was to show that once the repo transaction was received it would execute successfully resulting in updated balances for the relevant participants.
Rejection/failure of the start leg of a repo	This test ensured that if the received repo transaction was received and subsequently rejected the balances of the relevant accounts would revert to their initial state.
Successful processing of the end leg of a repo	This test was to show that if the start leg of the repo was successfully processed the end leg processing would subsequently be triggered. The scenario includes the end leg being fully processed, updating relevant account balances, and initiating a response message to the Swift **Prototype** and in turn the Broadridge DLR system.
Rejection/failure of the end leg of a repo	This test was to show that once the start leg had processed and triggered the end leg, the rejection of the end leg would revert the account balances back to the pre-end leg state.

Key findings and future considerations

The Broadridge DLR use case highlighted the interoperability of the RSN settlement venue. Again, paired with the Swift interlinking prototype the RSN FMI:

- Enabled a connection to the Broadridge system to simulate a cross-platform intra repo transaction.
- The Swift interlinking prototype provided a coordinated messaging protocol between the two systems and enforced an MT messaging standard for the transaction.
- The use case allowed Broadridge DLR to initiate an intraday repo transaction that the RSN FMI enabled.
- The RSN FMI added functionality by enabling a two-leg DvP transaction setup.
- The RSN FMI enabled a delayed settlement mechanism that would trigger the second leg of the repo transaction upon request.
- The use case took advantage of the atomic nature of an individual DvP construct on the RSN receiving settlement finality of each leg of the transaction in sequence according to the designed workflow.
- The cross-network settlement was coordinated via Swift interlinking prototype but not atomic due to the cross-platform nature of the transaction.

This use case demonstrated the potential of the RSN to be a composable piece of market infrastructure. In this use case the RSN offered the full DvP settlement functionality of tokenized central bank deposits for tokenized treasuries, allowing Broadridge DLR to call on the RSN FMI as part of its transaction flow and utilize the state of the RSN FMI within its workflows.

Conclusion

The RSN PoC has successfully demonstrated the technical feasibility and potential advantages of implementing a shared ledger system within the regulated financial market. By prototyping shared ledger technology within the existing financial regulatory frameworks, the RSN PoC has potentially paved a way for innovation in securities settlement processes through enhanced operational efficiency, real-time liquidity access, and potential reduction of settlement risk.

Key technical insights

- **Atomic settlement capability:** The PoC achieved atomic DvP settlement of regulated securities within the RSN FMI. The shared ledger technology enabled simultaneous balance sheet updates across participants, potentially eliminating traditional delays associated with proprietary databases and batch processing.
- **Secure multi-asset infrastructure:** The RSN FMI supported various asset classes on a single ledger, demonstrating the scalability and versatility required for modern financial transactions. The RSN FMI successfully enabled tokenized central bank deposits, commercial bank deposits, and securities within a shared ledger FMI.
- **Interoperability:** The PoC showcased interoperability with multiple networks, enabling coordinated settlement across diverse platforms. By leveraging interoperability solutions such as the Swift interlinking prototype and direct API integrations, the RSN FMI demonstrated its capacity to connect with other DLT solutions.
- **Composability:** The PoC showcased the flexibility of the RSN FMI and its ability to be utilized within transaction workflows originating on third-party platforms. This composability could potentially speed the adoption of an RSN-based solution as it could be integrated within existing workflows and processes in the market without requiring extensive redevelopment.

The RSN PoC has contributed to the technical feasibility of a shared ledger system in a regulated financial environment. By achieving key technical milestones in precise settlement, secure multi-asset infrastructure, and interoperability, the RSN PoC has established a solid foundation for potential future innovation in securities settlement. Continued technical innovation will be essential in realizing the full potential of the RSN FMI, with the goal of enhancing the efficiency, speed, and security of financial transactions across the industry.

Appendix

Cyber security addendum

MITRE was engaged by SIFMA to participate in the RSN PoC as an observer for security and technology observations, findings, risk(s) assessment, and recommendations. Beginning April 2024, MITRE participated in weekly stakeholder meetings where the concepts of the RSN network were discussed, how and where Digital Asset (DA) fit in, and the deployment of a PoC network was done and demonstrated its fitness for the business solution.

There were separate security and IT briefings parallel to the PoC process. MITRE analysis is based on compare/contrast to system(s) the DA RSN network would replace, the people, processes, and technologies involved in the PoC or that would be used in a production DLT network.

Cost, while important to the long-term prospects of a production environment, was not a factor MITRE used in its assessment of the project; the fitness of purpose for the business need, while important, was not a factor MITRE considered in its assessment as it was out of scope for our engagement.

MITRE's assessment is based on accepted industry practice and reference, past MITRE experience, and engineering judgment. As a baseline MITRE consider NIST cybersecurity risk assessment guidelines[4] among other industry standards like ISACA,[5] the US Treasury Financial Services Oversight Council,[6] and notably Sept 2024 BIS assessment[7] of safety and security of DLTs.

Observations are statements of verifiable fact corroborated by multiple human sources or present in documented artifacts. Research, inquiry, and recommendations are based on best practices for federal cyber capabilities, industry standards, and modern technology trends.

[4] NIST CSF

[5] ISACA June 2021 Evolving Your Cybersecurity Through Cyber Maturity

[6] Treasury Financial Stability Oversight Council – 2022

[7] BIS Working Paper 44 Aug 2024 - Novel risks, mitigants, and uncertainties with permissionless distributed ledger technologies

Observations, findings, risk(s) assessment

Cybersecurity governance & standards

Digital Asset

Digital Asset was selected as the software vendor for the PoC for RSN based on their industry standing and prior work for the RLN PoC. By independent accounts and research, it is a well-regarded software developer in the distributed ledger technology field. Customers of DA include major international financial institutions, some of which are a part SIFMA's RLN and RSN PoCs.

We met with the DA CISO and security colleagues over the course of two meetings during which the CISO and security staff from DA provided an overview of their security program in a standard presentation. In the first meeting they took questions and provided the presentation to the audience after the meeting. The subsequent interview was a follow-up where MITRE and PoC stakeholders probed various security points and questions from the general perspective of security posture for a software vendor and specifically for a DLT. DA stakeholders and the CISO presented a well-established security program with broad and appropriately deep posture.

One of the main strengths of the DA security program is the openness to third-party, external audit – a standard industry presumption but not always achieved. DA has submitted to SOC2[8] audits since 2019 (all have resulted in unqualified opinions) and ISO27001 since 2021 from credible auditors and reports a program of regular penetration and software code testing by third parties. Other standards to which they adhere include ISO 20022 for electronic data interchange (EDI), public key infrastructure (PKI) for encryption, and open-source transparency for some products and integrations in close-source products, GDPR,[9] TruSight,[10] Cloud Security Alliance[11] membership, and extensive business operational security protocols (BCP, DR, security awareness training, background checks).

DA maintains a trust center on its public website that details their security posture with extensive narratives and documentation about their software and development practices. Their security blog contains extensive posts and has been actively maintained for several years. Notably, their security posture document is an extensive, 36-page document[12] explicating in policy format the public and private standards and practices they employ for their security posture.

Infrastructure (software/hardware)

The DA PoC infrastructure consists of various nodes and mediating elements set up among the participants (a subset of the widely deployed DA Canton network[13]) that communicate by way of the open-source protocol Canton synchronizing smart contracts written in Daml.[13] Daml is a programming language originally created by DA as digital asset modeling language (DAML) and rebranded apart from DA directly (open-sourced in 2019 as Daml) and has been available on GitHub for at least five years with an active community of core developers and more than 13,000 commits. The software that runs the nodes of the DLT is installed on standard operating systems (PoC suggested 2VCPU, 4GB RAM, 10GB disk, for instance) via virtual machines, cloud resources, or bare metal servers. Communications among components (front-ends, back-ends, and among node sites) is reported to be PKI-encrypted via transport-layer security (TLS 1.2 and 1.3) using BoringSSL,[14] an open source project maintained by Google, protocol suite, a common open source TLS implementation. Data-at-rest can be encrypted by whatever storage layers a customer may be using and its native protocols, or disk encryption. The database layer format and protocol in use is PostgreSQL, a mature, open-source, industry standard for this kind of application system.

[8] What is a SOC2 – Cloud Security Alliance

[9] General Data Protection Regulation (GDPR) – Legal Text (gdpr-info.eu)

[10] Home - TruSight Solutions

[11] Home | CSA (cloudsecurityalliance.org)

[12] Digital Asset Security Posture - July 2023 - DRAFT

[13] DA ecosystem The Canton Network Ecosystem and example: Goldman Sachs And Microsoft Are Quietly Using AI To Lay The Groundwork For The Next Bitcoin, Ethereum And Crypto Price Bull Run (forbes.com)

[14] GitHub - digital-asset/daml: The Daml smart contract language

[15] GitHub - google/boringssl: Mirror of BoringSSL

The software distribution is via DA URLs with checksums provided for authenticating the successful download and other software bill of materials (SBOM) security protocols. Future plans for software updates were reported to be via mechanisms within the software interface for convenience and enhanced security, possibly being automated, as well. DA published major and minor releases and works closely with customers for support on the private source software, while open source components are the direct responsibility of the customer.

Authentication within the software interface is using Keycloak[16] (open source) or Auth0[17] (commercial, Okta product), two standard, security authentication implementations that could include multi-factor authentication (MFA) in the future but do not appear to do so at this time and DA supports any standard Auth0 provider.

Post-quantum awareness

When queried directly about post-quantum computing (PQC) preparations, the CISO and other security stakeholders at DA expressed their shared awareness, understanding, and concern with the issue. They attested to being ready, willing, and able to integrate whatever standards and algorithms are promulgated and their involvement in such efforts (through Cloud Security alliance, for instance, though not necessarily attempting to shape the direction) would be implemented as soon as practicable. Their software security stacks are currently modular and can support future needs for implementing PQC algorithms.

They also attested to inherent security from download now, decrypt later (DNDL) threats because of the factionalized nature of the stored data – there is no single node with a global state, only the portions that pertain to the given node and the "domain node," which tends to have more knowledge of the network than nodes, is tightly aged to reduce its long-term data value. Thus, an attack on one node with the intent to decrypt contents at later date would be limited in its overall value.

The state of the industry for PQC is that NIST[18] released only in August of 2024 three PQC encryption standards and the industry has not yet begun producing PQC software for end-users to consume. DA relies on open-source code and commercial code for its application and is an end-user essentially waiting for its vendors to integrate PQC components, at which point DA could use it for its products.

DLT networks and node hosting risks

For the purposes of the PoC, the nodes were set up in DA development infrastructure (Google Cloud), however a production RSN DLT would be set up on various host systems spread around the world communicating via private network connections (direct connect or VPN) not open internet-facing networks with or without IP address filtering to maintain a private/permissioned system. However, the software is robust enough that an open access system with secure authorization could be developed and be secure should the stakeholders ever have a need for such a system.

Additionally, no node communicates with any other end node rather instead by connecting through a "sync domain" node that relays transactions. This is consistent with a very high security profile appropriate for sensitive communications. We'd expect that these networks would be regularly cyber-exercised by an adversary emulation system to test defenses and train personnel. Something like MITRE's CALDERA[19] tool can be used to conduct autonomous red/blue team exercises from offensive (red) to defensive (blue).

Decentralized and distributed ledger technologies have inherent risk in the decentralized nature. There are more participants on diverse platforms and infrastructure. But with the proper standard security practices, which DA appears to be championing, the total cost of ownership, fluidity, and flexibility of the DLT system may reduce cost and operational friction and risk (PoC hypothesis 1).

[16] GitHub - keycloak/keycloak: Open Source Identity and Access Management For Modern Applications and Services

[17] Auth0: Secure access for everyone. But not just anyone.

[18] NIST PQC

[19] MITRE CALDERA

Smart contract risks

The essence of the DLT is the smart contract language (Daml) and its conformance to standard cyber security concerns of confidentiality, integrity, availability (CIA). The CIA triad contains essential contours of privacy and least privilege among the DLT network participants and for third parties related to the DLT stakeholders. Daml appears well-suited to be a reliable open-source smart contract protocol because of its long-standing SDLC on GitHub and the rigor to which DA submits the organization and its maintenance of Daml.

The single greatest risk to Daml usage is *human error* in the creation and usage of the smart contracts, while the integrity of the code itself is a close second in risk. If the code for Daml is perfectly secure, a human can configure it to do things that may be inconsistent with the overall intentions of the DLT. If the programming of the smart contract is perfectly executed, a weakness in the underlying smart contract code could be exploited. Therefore, we recommend rigorous testing and monitoring of performance and intended or expected smart contract execution – pre-production environments and periodic auditing of DLT performance.

MITRE considers the risk to smart contract usage in the same way there is inherent risk to wire transfers where human error (sending to the wrong recipient) is different than a malicious actor redirecting a properly addressed transfer. For a comprehensive review of DLT threats, see AADAPT framework in forthcoming BIS Project Polaris Report #5.

Recommendations

Common framework for discussing CVE[20] and public disclosure

As the size of an ecosystem grows, the attack surface increases, as does the potential reward for nefarious actors. While the RSN's current security apparatus is robust, we suggest that RSN participants develop a framework to typologize cyber vulnerabilities, threats, and attacks as well as share that information with partners and the broader community. DA attests to sharing vulnerabilities with customers in their ecosystem (in preparation for DA's patching, or for the customer to mitigate the issue direct) and this is a good start, but full public disclosure of vulnerabilities is essential to the long-term security of the platform if it is to remain commercial and closed source.

In terms of frameworks, we suggest industry recognized frameworks like MITRE's ATT&CK[21] framework or others. Post attack analysis that utilizes such a framework allows for internal and external audiences to speak the same language, mitigate persistent threats, and collaborate on securing the network. There are also open-source efforts at this in the cryptocurrency space, such as OSWAR.

Participation in industry information sharing partnerships, including public-private

In terms of information sharing, we suggest that RSN participants engage with information sharing and analysis centers and related entities, like FS-ISAC,[22] Crypto ISAC,[23] or SEAL ISAC.[24] Partnership in multiple of these arrangements will facilitate fast dissemination and remediation of cyber vulnerabilities or intrusions.

[20] CVE db

[21] MITRE ATT&CK

[22] Financial Services Information Sharing and Analysis Center (FS-ISAC)

[23] https://www.cryptoisac.org/

[24] https://isac.security alliance.org

Glossary of terms

Term	Definition
Atomic	The principle that the entire transaction succeeds or fails as a single, indivisible unit and is simultaneous in nature.
CCP	Central Counterparty
Correspondent Banking Model	Process where one bank (the correspondent or settlement agent) provides services on behalf of another bank (the respondent) typically to facilitate transactions where the respondent bank does not have direct access to a specific type of asset
Composability	A system design principle that allows components to be combined in various ways to create larger, more complex systems.
Coordinated Settlement	Coordinated completion of transactions across different third-party networks or platforms at the same time
Cross-Network Settlement	Process of completing and finalizing transactions between different blockchain networks to enable the transfer of assets and data across various third-party platforms or networks
CSD	Central Securities Depository
DvP	Delivery versus Payment, settlement mechanism where the transfer of securities occurs only if the corresponding payment is made simultaneously
FMI	Financial Market Infrastructure
Immutability	Characteristic that once data has been written to the blockchain, it cannot be altered or deleted
Interoperability	Ability of different blockchain networks to communicate, share data, and interact with one another seamlessly to enable the transfer of assets and information across various blockchain platforms without the need for intermediaries
ISO20022 Messaging Standard	Standard for financial messages that enables interoperability between financial institutions, market infrastructures and the Banks' customers
Modularity	The degree to which a system's components can be separated and/or recombined.
MT541 Message	Message sent from an account owner to an account servicer to instruct the receipt of financial instruments against payment
MT543 Message	Message that instructs an account servicer to deliver financial instruments against payment
MT548 Message	Status update message sent by an account servicer to an account owner or designated agent to provide information about a settlement instruction
Net Settlement	Process of consolidating multiple transactions between parties within a defined settlement window into a single net amount
Pacs.002 Message	Message sent by an instructed agent to a party in the payment chain to report on the status of a payment instruction
Partition	Smaller, independently operated segment of a blockchain network that processes its transactions and smart contracts
Precise Settlement	Ability of financial systems and institutions to accurately and efficiently settle transactions, ensuring that all parties involved receive their due payments or securities at a predetermined time and in an error-free manner.
Private, Permissioned Blockchain	Type of blockchain network where access is restricted to a specific group of participants who have been granted permission
Resiliency	Ability of a blockchain network to continue operating and maintain its integrity despite failures, attacks, or other adverse conditions
Shared Ledger Technology	Digital system for recording the transaction of assets in which the transactions and their details are recorded in multiple places at the same time
Simultaneous Settlement	Process where settlement is conditional and occurs if, and only if, obligations are fulfilled by all transacting parties (e.g., delivery and payment)
Tokenization	Process of converting rights to an asset into a digital token on a blockchain, where each token represents ownership or a share of the underlying asset
Tokenized Central Bank Deposits	Traditional central bank deposits that have been converted into digital tokens on a blockchain or distributed ledger and represent the same value as the original deposits
Tokenized Collateral	Assets that have been converted into digital tokens on a blockchain or distributed ledger which can be used as collateral in financial transactions
Tokenized Commercial Bank Deposits	Traditional commercial bank deposits that have been converted into digital tokens on a blockchain or distributed ledger and represent the same value as the original deposits
Tokenized Securities	Traditional financial securities (e.g., IG Bonds, US Treasuries, etc.) that been converted into digital tokens on a blockchain or distributed ledger and represent the same value as the original securities
Transparency	Characteristic of blockchain technology that allows participants to view and verify transactions on the network which they are permissioned to see