Connecting blockchains: Overcoming fragmentation in tokenised assets

Swift's interoperability experiments connecting to public and private blockchain networks

Swift

Results report
August 2023

Contents

1. Executive summary

Most institutions would prefer to evolve their existing infrastructures and applications to enable them to access tokenised asset markets.

Tokenisation is on the rise, but fragmentation remains a challenge

Global interest in tokenised forms of value continues to intensify. Players from across the industry highlight a wide range of benefits that could be gained through tokenisation – including the potential to unlock market liquidity, drive post-trade processing efficiencies, enable automation, and increase transparency. Market sentiment is strong, with a recent survey showing that 97% of institutional investors think that tokenisation is set to revolutionise asset management.

Significant challenges remain, however, driven notably by the current fragmentation in legal and regulatory frameworks relating to tokenised assets that exist around the globe. On a technical level, the current lack of interoperability between the various blockchain networks that host different tokenised asset types presents another challenge. When combined, these hurdles threaten to prevent the market for tokenised assets from reaching its potential.

There are multiple potential paths toward the future of tokenisation

In a 2023 report on the topic, the Bank for International Settlements (BIS) highlighted two distinct approaches that have the potential to define the future of tokenisation. The first more transformational approach would see Central Bank Digital Currencies (CBDCs), tokenised deposits, and tokenised assets brought together on a common 'unified ledger'. The second, more incremental, path would see the coexistence of multiple ledgers that are interlinked with existing systems and infrastructures.

The initial feedback we've received from the community on this question has indicated that most institutions would prefer to evolve their existing infrastructures and applications to enable them to access tokenised asset markets – rather than having to build entirely new infrastructure and technology stacks from scratch.

Swift is working to ensure global interoperability of emerging technologies and platforms

We're focused on delivering instant and frictionless cross-border transactions. As part of our strategy, we've been exploring how we can enable interoperability between different emerging platforms for some time. In 2021, we published an initial white paper that assessed the potential impact of CBDCs and how Swift could support the financial community as new currencies are developed.

In 2022, we conducted a series of experiments which tested how the Swift network could be leveraged to support the seamless integration of both CBDCs and tokenised assets into the existing financial system. And, earlier this year, we tested our new CBDC interlinking solution with 18 central and commercial banks in a sandbox environment.

We've worked on developing a blockchain interoperability solution as part of this new set of experiments

Our view is that a common connectivity layer is critical to eliminating friction and enabling interoperability between the existing financial system and blockchains to create a unified global market.

Therefore, as part of our current project, we leveraged the Swift network, and the Chainlink Cross-Chain Interoperability Protocol (CCIP), to create an experimental solution. The goal was to test whether we could enable financial institutions to use their existing back-end systems to interact with tokenised assets and transact across both public and private blockchains platforms.

We further collaborated with over a dozen financial institutions and financial market infrastructures – including Australia and New Zealand Banking Group Limited (ANZ), BNP Paribas, BNY Mellon, Citi, Clearstream, Euroclear, Lloyds Banking Group, SIX Digital Exchange (SDX) and The Depository Trust & Clearing Corporation (DTCC) – to discuss technical and non-technical considerations that would need to be addressed to make a proposed solution commercially feasible.

The experiments have highlighted the role that a blockchain interoperability protocol could play in transferring data and value across blockchains.

The project proved successful and yielded valuable insights

The experiments successfully demonstrated that Swift connectivity and messaging standards – in combination with an interoperability protocol such as the Chainlink CCIP – can be used to achieve interoperability between traditional financial systems and emerging blockchain networks. As well as advancing our understanding of technical and business requirements, the experiments have highlighted the role that a blockchain interoperability protocol could play in transferring data and value across blockchains.

The feedback gained from the collaborative working group sessions with the institutional participants – covering aspects such as data privacy and governance, business processes, operational risk, and legal liability – will be highly valuable as we iterate our solution design and prepare to support the transfer of tokenised value over the Swift network.

The key findings can be summarised as follows:

Technical findings

- Token handling mechanisms may vary by use case.
- Nonce management is critical for avoiding replay attacks.
- An abstraction layer is necessary to manage the complexity of blockchains.

Business findings

- A ‘Designated Depository’ role is important to satisfy regulatory obligations.
- Regulatory clarity remains the market’s largest need.
- Data privacy is fundamental to any commercial solution.
- Liability and recourse must be clearly addressed for cross-chain transfers.
- Cross-chain use cases lack maturity, but development is expected to ramp up.

We’re committed to continuing our work to support tokenisation and blockchain interoperability

Following the success of these experiments, and positive feedback from project participants, we’re continuing to work with the financial services community to create an approach to interoperability across multiple blockchains that leverages market participants’ existing Swift capabilities and new open interoperability standards.

Moving forward, we will expand our exploration to different types of blockchain ledgers, including public permissioned ledgers, as well as various on-chain and off-chain Delivery versus Payment (DvP) payment options. We will also explore other possibilities to address institutional needs such as transactional data privacy.

2. Business context

The market trend towards tokenised assets has gained significant traction in recent years. There is growing belief across the financial industry that tokenisation – the process of converting physical and non-physical real-world assets such as stocks, bonds, property, or even art into digital tokens – has the potential to become a new source of significant value, as well as driving greater efficiency, security and transparency in post-trade processes.

There is growing belief across the financial industry that tokenisation has the potential to become a new source of significant value.

Indeed, current market sentiment around tokenisation is very positive: 97% of institutional investors believe that tokenisation will revolutionise asset management[1], and 95% of capital markets firms in the US, UK, and Canada believe that blockchain will play an important role in settlement processes going forward[2]. Furthermore, Boston Consulting Group has projected the total market size of tokenised illiquid assets alone will reach $16 trillion by the end of the decade[3].

Tokenisation: The potential benefits

Institutions have identified a range of benefits that regulated tokenised assets could offer, including:

- **Deliver increased liquidity:** By enabling fractional ownership and facilitating secondary market trading. This liquidity would, in theory, attract a broader range of investors and enhance overall market efficiency and risk diversification.
- **Offer cost-saving opportunities:** By enhancing current value chains and streamline the issuance, settlement, and transfer processes – reducing administrative and operational expenses.
- **Increase automation:** By enabling programmability of functions which could further reduce costs.
- **Enhance transparency and security:** By providing an immutable and auditable record of ownership and transactions, reducing the risk of fraud, improving compliance, and potentially enabling the development of new products.

[1] BNY Mellon and Celent, 'Migration to digital assets accelerates; 2022 Survey of Global Institutional Clients | Asset Managers, Asset Owners, and Hedge Fund'

[2] Accenture, 'How your T+1 program could help pave the way to T+0'

[3] Boston Consulting Group, 'Relevance of on-chain asset tokenization in 'crypto winter'

A significant hurdle is the current lack of secure interoperability between the different blockchain networks that host the tokens.

Significant hurdles still need to be overcome

Given the optimism surrounding tokenisation, and high levels of continued investment, the wider adoption of tokenised assets looks likely to continue. Yet significant challenges remain that could prevent the market from truly scaling.

For instance, with the legal and regulatory frameworks still evolving in this domain, remaining compliant when making tokenised asset transactions is an extremely complex challenge for institutions.

Another significant hurdle is the current lack of secure interoperability between the different blockchain networks that host the tokens. This particular issue is leading to significant inefficiencies and a poor user experience for current market participants. It also has the potential to fragment market liquidity moving forward.

The future of tokenisation is yet to be fully defined

In its recent report on the topic, the BIS described two broad approaches for bringing tokenisation to fruition in a future monetary system[4]. The first approach would involve a transformation that brings together CBDCs, tokenised deposits, and tokenised assets on a common 'unified ledger'. Various industry efforts are exploring how this could be done.

The second approach would entail incremental improvements through the interlinking of existing systems. In this case, market scalability would be achieved by financial institutions connecting their existing systems and applications to multiple blockchain-based networks in a secure and trusted way – just as they do today when facilitating the trading and settlement of traditional assets.

There's potential to leverage Swift to support blockchain interoperability

The feedback we have received from consultations with our members to date has shown that the second, more incremental, approach is likely to be the most plausible for market development in the near-term.

Most institutions have indicated they are not inclined to build new infrastructure and technology stacks entirely from scratch. Firms prefer to leverage their existing infrastructure, message implementations, and proven business processes to connect to blockchain ledgers, where tokens are recorded in a way that is both compliant and secure. This could help firms simplify their architecture and operations, minimise investment costs and reduce the risk of technology obsolescence.

It is in this context that we are conducting this set of experiments. The goal: to test how Swift could support members in re-using their existing Swift infrastructure as a single entry-point to the public and private blockchain networks needed to transact tokenised assets.

[4] III. Blueprint for the future monetary system: improving the old, enabling the new (bis.org)

3. Our tokenisation journey to date

As part of Swift's vision to deliver instant and frictionless cross-border transactions, we've been focusing on how we can ensure interoperability between emerging platforms that are at risk of becoming unconnected 'digital islands'. As well as exploring how we can interlink the world's central bank digital currencies (CBDCs), we've conducted experiments to test how we can enable interoperability between multiple tokenised asset platforms.

There was strong interest within the community in collectively exploring open questions around interacting with public permissionless blockchains.

Our first set of experiments on tokenised assets in 2022 included major market infrastructures and custodians. This work demonstrated how our infrastructure could serve to interconnect multiple private tokenisation platforms and different types of cash payments, offering a single access point to institutions for tokenised assets.

Developing a blockchain interoperability model

Following the completion of these initial experiments, we received strong support from the community to continue our innovation efforts and enable secure interoperability in the tokenised asset space more broadly. To inform our next steps, we held consultations with over 20 global financial institutions and financial market infrastructures. These resulted in several key insights:

- There is increasing investor demand for both digitally native and tokenised assets.
- The future is expected to be 'multi-chain' and will require access to a series of networks.
- There is broader preference for unlisted, illiquid, or underserved asset classes.
- Institutions prefer to leverage existing infrastructure and investments wherever possible.

Many of these findings reinforced our existing assumptions. However, a key point of differentiation was the interest in extending the scope of interoperability between platforms to include public blockchains as an underlying settlement layer.

As such, there was strong interest within the community in collectively exploring open questions around interacting with public permissionless blockchains, as well as appetite for understanding how this can be supported in a secure and compliant manner.

4. Project workstreams and use cases

The objectives

Based on the feedback we received from our consultations, we set out to design a set of experiments with the following key objectives:

- To demonstrate that there is a simple, secure, and scalable way for financial institutions to connect to multiple types of blockchain networks leveraging their Swift infrastructure and message implementation.
- To advance industry understanding around both the technical and business requirements for interacting with public and permissioned blockchain networks.
- To explore the value of using a blockchain interoperability protocol to securely transfer data between legacy systems and an increasing number of chains.

In line with our commitment to collaborative innovation, we welcomed over a dozen financial institutions and financial market infrastructures from around the globe to co-develop a potential solution and debate the associated considerations necessary to deliver it.

The project

The experiments were structured into two distinct workstreams:

Workstream 1: Solution design

The first workstream centred around the business design and technical development of a proposed solution. The design of a solution was predicated on a set of critical requirements for participants. For example, institutions needed to be able to send and receive existing MT formatted messages. Another requirement was that blockchain wallet (see our glossary of terms here) private keys would remain in the possession of the asset owners or their custodians.

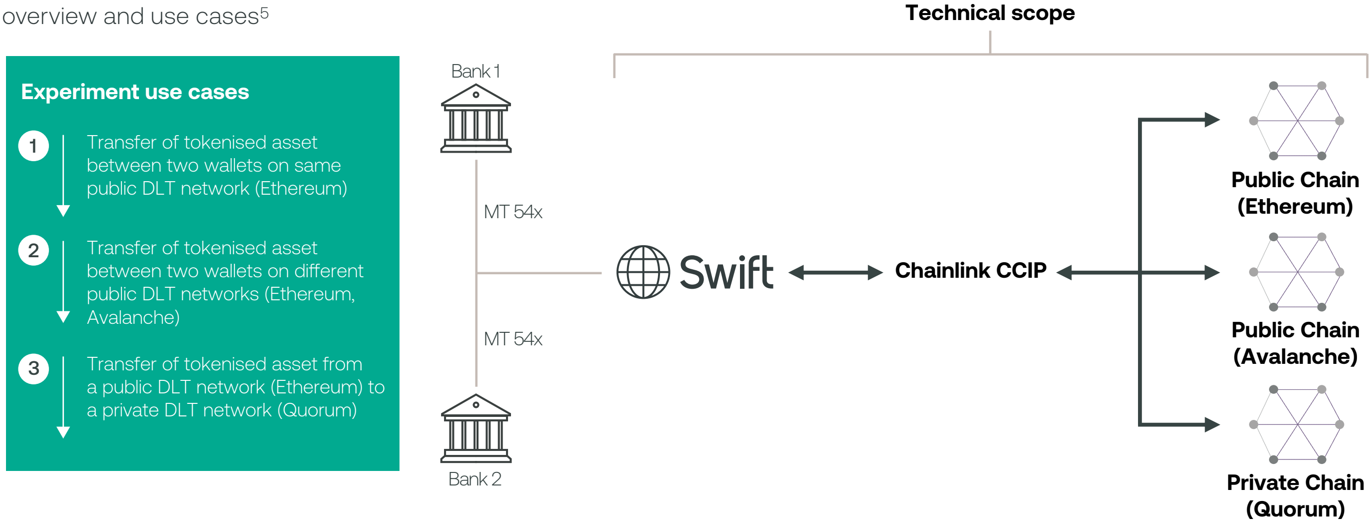
Although the solution was designed jointly with participants, the technical development work was simulated entirely by Swift and Chainlink. See Figure 1 for an overview of the experiment design and use cases tested.

The project participants

More than a dozen major financial institutions and market infrastructures joined the project, including Australia and New Zealand Banking Group Limited (ANZ), BNP Paribas, BNY Mellon, Citi, Clearstream, Euroclear, Lloyds Banking Group, SIX Digital Exchange (SDX), and The Depository Trust & Clearing Corporation (DTCC).

Chainlink, a Web3 services platform, provided connectivity across public and private blockchains for these experiments. Our experiments leveraged Chainlink's open-source protocol – the Cross Chain Interoperability Protocol – to enable the secure and efficient transfer of asset tokens across multiple blockchain networks.

Figure 1: Experiment design overview and use cases[5]



Experiment use cases

1. Transfer of tokenised asset between two wallets on same public DLT network (Ethereum)
2. Transfer of tokenised asset between two wallets on different public DLT networks (Ethereum, Avalanche)
3. Transfer of tokenised asset from a public DLT network (Ethereum) to a private DLT network (Quorum)

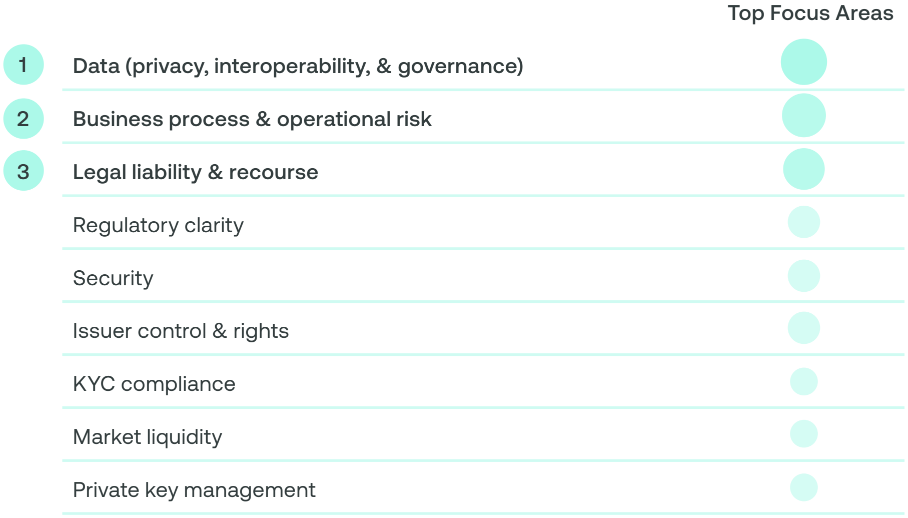
[5] Note: Beyond the example blockchains used in this experiment, Chainlink CCIP can be extensible to any public or private blockchain network.

Workstream 2: Non-technical considerations

The second workstream encompassed working group discussions to identify and discuss non-technical considerations that would need to be addressed to make a proposed solution commercially feasible.

For example, focus was given to topics such as data privacy and governance, operational risk, and legal liability based on prioritisation results from the participating institutions (see Figure 2 for the areas of focus for Workstream 2 in priority order). Discussions related to regulatory and policy considerations were deferred as they were outside the control of participants and the scope of the experiment.

Figure 2: The non-technical areas of focus in order of priority



Set-up and preparation

To execute the experiment, Swift and Chainlink simulated the technical environments for financial institutions and Swift itself, as well as for a wallet infrastructure with various addresses. In doing so, we simulated various processes on behalf of financial institutions, including but not limited to, the following activities:

- Generating MT files
- Integrating and enriching data for blockchain transactions
- Integrating with blockchain wallets (held within simulated bank digital custody platforms)

Tokens also needed to be minted and issued to one of the wallet addresses hosted and managed by Swift. DTCC performed the minting and issuance operations, creating the 'BondTokens' and distributing them to Swift's designated test wallets. To ensure the tokens' compatibility with Chainlink CCIP, an extension was included in the token contract.

In combination with Chainlink CCIP, the EIP-712 standard was also used to simplify integration with various blockchain technologies. This enabled institutions to create and sign a blockchain message using their existing infrastructure and rely on a 'trusted forwarder' to process messages on-chain without incurring 'gas fees' (the amount paid to reward the computational effort required to execute a transaction).

Swift and CCIP acted as the 'trusted forwarder' that managed these gas fees, and CCIP was responsible for adding the gas fees when creating the blockchain transaction.

5. Our solution

The proposed solution for this experiment aimed to minimise the level of investment and change required for financial institutions to be able to instruct the transfer of tokenised assets. It also sought to sustain the key roles and functions that need to be performed in post-trade settlement as required by regulators.

Throughout the course of the experiment, we executed approximately 50 token transfers across the three use cases using the described solution. This involved the single leg delivery of BondTokens across six unique wallet-private-key pairs for both the sender (BondToken seller) and receiver (BondToken buyer). We also included around 20 unhappy path scenarios that primarily tested single incorrect inputs to confirm expected transfer failures – these included the reuse of the same nonce (see our glossary here), passing an incorrect token version, and insufficient funds. Through CCIP, status updates were securely passed back to institutions using existing Swift infrastructure.

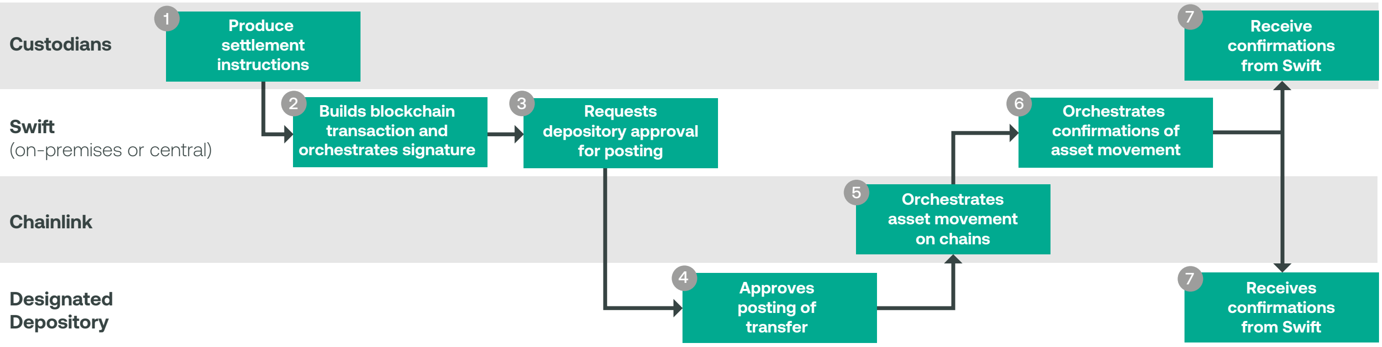
By leveraging the existing Swift infrastructure in place today, our approach minimises the need for substantial additional investments, enabling financial institutions to optimise their current operations. As such, firms could reap the benefits of Swift's security and reliability, in addition to the existing network effects in place across 11,500+ financial institutions.

The solution process flow

The process steps below describe the solution that was conceived by Swift in collaboration with the project participants.

In line with Swift's aim to sustain the roles and functions as required by regulation, it was important to introduce the concept of the 'Designated Depository' (see our glossary here). It was also important to ensure the role of a settlement system owner, and to have a single, clearly identified legal institution performing the role, irrespective of the technical construct used to do so (i.e. public vs. private ledger) or the programmability of the assets. Figure 3 provides a summarised view of these steps in sequential order, with each step explained in more detail in the following section.

Figure 3: The solution process flow



Custodians
Swift
(on-premises or central)
Chainlink
Designated Depository
1 Produce settlement instructions
2 Builds blockchain transaction and orchestrates signature
3 Requests depository approval for posting
4 Approves posting of transfer
5 Orchestrates asset movement on chains
6 Orchestrates confirmations of asset movement
7 Receive confirmations from Swift
7 Receives confirmations from Swift

The solution process flow: A step-by-step guide

1. Create the settlement instructions

The settlement posting process is triggered by producing two settlement instructions: one from the buyer's custodian, and one from the seller's custodian. These instructions are sent using common standards – expected to be ISO 15022, but ISO 20022 is also possible – and are exchanged using the custodians' existing Swift infrastructure.

This activity is very similar to the existing process to issue instructions. However, custodians need a digital custody solution to hold the investors' private keys. They also need the right set of data to target the corresponding token, wallet and smart contract addresses, and blockchain network.

These message types are largely suitable for the task but would require some additional blockchain data in a narrative field with custom codes. In a future standards update, these elements could be formally captured in dedicated fields.

2. Build the blockchain transaction and orchestrate signature

This activity prepares the information required to post the settlement on one or two ledgers, depending on the specific flow.

Swift's experimental Software Development Kit (SDK) digests the settlement instruction in the form of a Swift message, extracts the specific fields needed to post on the blockchain ledger, and enhances the content with other potential specific items derived from the destination chains (e.g. nonce to prevent replay attacks). The SDK would be deployed within the banks' secure Swift environment.

It then orchestrates the signature of the resulting payload with the relevant private keys held by the custodian (defined by the target wallet of the instructing institution).

The outcome of this activity is a formed payload that can be captured by Swift's platform to process the settlement. By signing the blockchain message with private keys, banks ensure no one can tamper with the message content, thereby achieving non-repudiation.

3. Request depository approval for posting

In this step, Swift transports the two incoming instructions from custodians, which we've assumed for this experiment to be matched, with a consistent Unique Transaction Identifier (UTI) tracked by Swift. Detecting that these instructions are blockchain-related, the Swift platform adds a request to trigger the settlement posting confirmation recorded by the Designated Depository.

Although the DLT ledger allows banks to post directly on-chain, to ensure compatibility and minimal disruption with existing back-end systems, certain functions might be required in the settlement instruction processing. Assuming these functions can be technically defined, a range of entities could look at fulfilling the Designated Depository role to ensure better interoperability with existing systems.

4. Record settlement instruction validation

At this point, the Designated Depository has received the two settlement instructions from Swift, with a consistent UTI flagged for posting confirmation in the technical header of the instruction message. The Designated Depository ensures that the required validation steps have been performed (e.g. business validation, pairing, settlement eligibility), and confirms posting of the delivery settlement instruction.

There are multiple options for how these validation steps could be performed. For example, it is conceivable that deterministic rules could be defined and performed by a technical provider that is delegated by the legally accountable market infrastructure.

5. Orchestrate asset movement on-chain

The Swift platform prepares the request to post the blockchain message onto the chain and sends it to CCIP as a secure abstraction layer for all blockchain interactions (see Figure 4 below depicting how the transaction is channelled from banks to CCIP through the Swift platform).

CCIP validates the request, creates a matching blockchain transaction, and submits it on-chain. CCIP then monitors the processing of the transaction on-chain and provides secure status updates of the on-chain processing back to Swift via the corresponding Swift API endpoint.

The resulting confirmations can cater for various statuses depending on the chain type (a complete set of the potential status confirmations is provided in the Appendix). These status updates are then mapped to ISO 15022 or ISO 20022 status messages towards the financial institutions.

6. Producing confirmation of token movement

Using the received status updates from CCIP, the Swift platform prepares Swift messaging-compliant confirmation of movement for the Designated Depository, and signs it. The confirmation is built leveraging the instruction payload and using the ISO 15022 or ISO 20022 standard.

7. Delivering confirmation of token movement as Swift messages

The confirmation messages can then be shared with the Designated Depositories and custodians. As settlement finality remains a legal construct, the responsibility to confirm as much would ultimately lie with the Designated Depository entity.

Once informed of the successful asset movement on-chain, custodians can then record the transaction in their off-chain book of records and pass confirmations on to their customers.

Translating on-chain events back into standardised message formats averts the need for back offices to build another parallel status integration layer, and thus represents a significant cost saving.

Key solution components

To execute our proposed solution in a way that met the needs of the participants, several key technical components were used:

The Swift experimental SDK

The experimental SDK was developed to serve several important functions and to minimise the amount of change required from sending institutions. A key design decision was to deploy this SDK in the banks' existing Swift connectivity infrastructure (on-premise or in the Swift cloud) to benefit from longstanding and trusted security features.

The key process steps performed by the experimental SDK include:

- Intercepting the MT message generated by the simulated back-office application and extracting the information required for generating a blockchain message. A dedicated parsing mechanism was developed.
- Constructing the blockchain message in adherence to the EIP-712 standard.
- Requesting the simulated wallet infrastructure to sign the blockchain message. The application communicates with the simulated wallet infrastructure through an API to request the signing of the blockchain message. The response received from the infrastructure is the signature, which is integrated into the MT field. Specifically, it is inserted under the tag and Qualifier 70E /SIGN.

In the future, the process for extracting data and constructing a blockchain message could be enabled by the Swift Translator, a widely used Swift solution that easily defines, maps, and validates messages from and to any format.

The Chainlink Cross-Chain Interoperability Protocol (CCIP)

Upon receiving the request from Swift, which contains both the metadata and the blockchain message signature, CCIP is used as an abstraction layer to create a blockchain transaction and securely transmit the transaction to the Forwarder Contract.

The Forwarder Contract address, which was initially involved in creating the blockchain message, undertakes multiple verification and validation processes, before forwarding the request to the designated token contract where the token transfer is initiated. This transfer can either occur within the same blockchain or use CCIP to securely reach the destination blockchain's wallet.

Throughout the cross-chain transfer process, each step and any exception returned by the smart contract while processing the transaction are monitored by CCIP as events. CCIP sends a status update for each of these events to Swift, which matches the received status update to the relevant Swift message and informs the relevant institutions of its progress. Middle and back-office systems rely on these updates for internal teams to provide transparency, manage risk and report transaction progress to all relevant parties.

Depending on the specified configuration, the CCIP router will immobilise a certain quantity of tokens within a 'token pool' (see our glossary here) on the source blockchain. Concurrently, wrapped tokens will be generated on the destination blockchain. This process involves the inclusion of CCIP fees and the creation of a message that incorporates the pre-existing information.

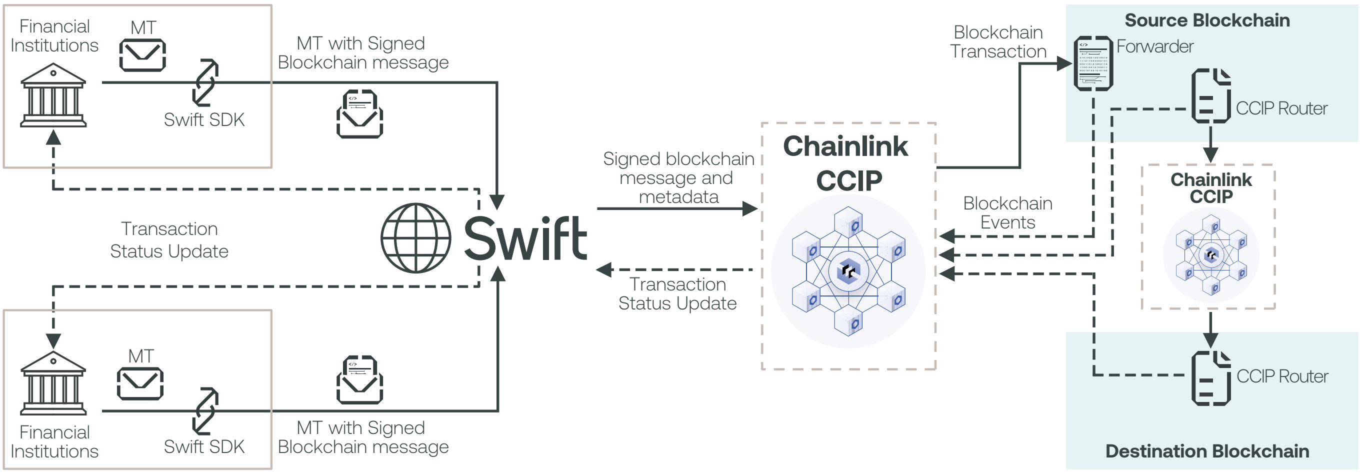
The inherent nature of blockchain transactions addresses the potential issue of a race condition arising from insufficient tokens in the token pool. Since all the instructions mentioned above are contained within a single transaction, the transaction can only succeed if all instructions are executed successfully. Note that the detailed mechanics for a cross-chain transfer can be found in the Appendix.

Messaging standards

To initiate the process of blockchain message creation within the financial institution's infrastructure, it is essential to gather a set of information in dedicated fields of the MT 543 Deliver Against Payment (detailed list described in the Appendix).

The message standards used in the example largely meet the requirements. However, a few new field options should be created to capture some blockchain-specific details formally, instead of relying on a market practice structure for a narrative field.

Figure 4: Overview of the architectural environments supporting end-to-end transaction flow



6. Findings

Overall, the results of the experiment give confidence that existing Swift connectivity and messaging standards can be enhanced, enabling financial institutions to transfer tokens within and across blockchain networks – all with minimal disruption to operations.

The range and diversity of the feedback received will enable us to iterate our solution design, and thereby serve our customers.

Open questions remain around the overall market readiness for tokenised assets. Nevertheless, the level of agreement about the market need for a secure and trusted cross-chain interoperability solution gives us confidence that we are focused on the right area for the Swift community.

Through the interactive collaboration working group sessions focused on non-technical considerations in Workstream 2, participants provided valuable input for us to consider as we continue our preparations to support the transfer of tokenised value over the Swift network. The range and diversity of the feedback received will enable us to iterate our solution design, and thereby serve our customers.

The box below gives an overview of the key findings from the experiments which are then detailed in the remainder of this section.

Overview of key findings

Commercial findings

- A 'Designated Depository' (or 'central account keeper') role is important to meet regulatory obligations
- Regulatory clarity remains the market's largest need
- Data privacy is fundamental to any commercial solution
- Liability and recourse must be clearly addressed for cross-chain transfers
- Cross-chain use cases lack maturity, but development is expected to ramp up

Technical findings

- Token handling mechanisms may vary by use case
- Nonce management is critical for avoiding replay attacks
- An abstraction layer is necessary to manage the complexity of blockchains

All participants cited legal and regulatory clarity as arguably the largest pending hurdle for widespread adoption.

A 'Designated Depository' (or 'central account keeper') role is important

While the latest regulations – e.g. the EU's Distributed Ledger Technology (DLT) Pilot Regime – are relaxing the complexity of trading in digital forms of regulated assets, the licensed DLT market infrastructure (MI) performing settlement is still required to:

- Monitor the recorded quantity of assets on the blockchain to ensure it matches the issued quantity of securities, and prevent their deletion or improper creation.
- Ensure segregation capabilities and manage participation to the settlement ledger. Non-institutional investors could be allowed to do this if they are knowledgeable about the risks and operations, and have provided their explicit consent.
- Prevent or address settlement fails, and provide settlement finality in near-real-time, intraday, and no later than the second business day after the conclusion of a trade.
- Enable the clear and accurate confirmation of transaction details, including payments that are by preference concluded in central bank money or in commercial bank money through the account of the DLT MI.

Regulatory clarity remains the market's largest need

All participants cited legal and regulatory clarity as arguably the largest pending hurdle for widespread adoption.

Compounding the issue further is the broad diversity of legal and regulatory frameworks across different jurisdictions, which makes the environment even more challenging to operate in a compliant manner for participants. As legislative and regulatory decisions are outside our control, we deliberately focused our discussions on other topics thought to be more directly within our collective control.

Data privacy is fundamental to any commercial solution

Participants noted that aside from legal and regulatory clarity, data privacy was the top priority that needs to be addressed in order to operate securely in cross-chain processing.

There was general agreement that data privacy is as important on private/permissioned chains as on public networks. However, there was no consensus among participants about which data should be stored on-chain vs. off-chain, as there are competing motivations such as scalability and performance, or automated functionality of smart contracts with transparent data.

For data that would be stored on-chain, various solutions are being considered by participants. These include zero-knowledge proofs and roll-ups, stealth addresses, and layered pseudonymity, among others.

It was also noted that many smart contract logs, which log the usage history and store data off-chain, have higher levels of visibility, and therefore should be reviewed with greater scrutiny.

Liability and recourse must be clearly addressed for cross-chain transfers

Participants agreed that decentralised blockchain networks should be treated similarly to open-source technologies. In other words, one cannot attribute liability to decentralised public blockchain networks. On the other hand, as soon as a token or application is defined under a jurisdiction's legal or regulatory framework, those associated definitions could invoke liability.

In the case of cross-chain token bridge solutions – in which tokens on the source chain are 'locked' in a smart contract token pool – many institutions felt that the responsibilities and related liabilities of the smart contract owner were unclear. Some participants suggested that liability might change if the token bridge solution was open-source code and had to be directly incorporated by a token issuer. However, most viewed the lack of control as the determining factor.

In the near-term, most participants expect there to be a greater focus on token transfers between private permissioned chains.

Cross-chain use cases lack maturity, but development is expected to ramp up

Participants broadly felt that cross-chain transfer use cases are still maturing, and held a range of different views on the prioritisation of suitable asset classes. But they did note that the need to support cross-chain transfers is widely anticipated over the next few years and is therefore driving the preparatory work within their institutions.

In the near-term, most participants expect there to be a greater focus on token transfers between private permissioned chains, with a longer-term direction of travel toward public blockchain networks.

Token handling mechanisms may vary by use case

Participants expressed contrasting views about the suitability of various token handling mechanisms (see our glossary here), e.g. burn-mint versus lock-mint. Some participants thought the lock-mint mechanism to be more favourable for cross-chain visibility of total issuance – however, questions remain about the legal basis of wrapped tokens and the vulnerabilities of collateral locked in bridging solutions.

Other participants suggested that the burn-mint mechanism may provide greater levels of control, but potentially at the expense of higher operational complexity. Another model to consider involves leaving the issued token on its native network and orchestrating ownership changes within each chain.

In any case, participants generally agreed that token handling mechanisms are likely to depend on specific use cases. As these mechanisms may introduce operational complexity, any solution should be designed to support multiple token handling mechanisms.

Nonce management is critical for avoiding replay attacks

Some participants suggested that digital wallet infrastructure to create and sign blockchain transactions should continue to be hosted and managed by financial institutions..

However, this increases the complexity of devising a solution to mitigate the risk of replay attacks that is inherent in blockchain transactions. In a typical scenario, the 'wallet nonce' (see our glossary here) can be employed to prevent a transaction from being executed multiple times within a single blockchain, or from being re-executed on another compatible chain.

To address this challenge, a potential solution could involve the implementation of a randomised nonce stored on the blockchain. This randomised nonce is checked during the processing of the blockchain message, thereby ensuring the prevention of replay attacks.

An abstraction layer is necessary to manage the complexity of multiple blockchains

Participants recognised that an abstraction layer and interoperability solution such as CCIP reduces the complexity of interacting with various blockchains.

The ability to connect institutions to various blockchains through existing infrastructure saves significant time and effort as it shields banks from the variety of signing, transaction formatting, and other differences between blockchains. And fragmentation will remain for some time as various chains are being adopted by market actors. Having the ability to keep internal systems updated about the progress of blockchain transactions across multiple chains will remove risk and ease integration.

7. Conclusions and next steps

With interest in tokenised assets growing, institutional investors – and the financial institutions serving them – require secure, scalable, and cost-effective ways of interacting with networks for post-trade processing and settlement.

The collaboration demonstrated the ability to transfer tokenised value efficiently and securely across public and private blockchains.

The collaboration between Swift, Chainlink, and the financial community represents significant progress towards enabling interoperability between traditional financial systems and emerging blockchain networks as next generation places of settlement. However, there is work to do to enable the broader tokenisation of capital markets.

Demonstrating the value of collaborative innovation

By bringing together a range of industry participants from multiple jurisdictions, and serving different parts of the value chain, we were able to design a potential solution that could work for a larger portion of the capital markets ecosystem. Participants benefitted from the richness of experience and expertise across the group, highlighting the importance of our collaborative approach to industry innovation.

By leveraging existing Swift infrastructure and Chainlink CCIP, the collaboration demonstrated the ability to transfer tokenised value efficiently and securely across public and private blockchains, using standardised messaging formats and proven business processes. These industry-wide trials have resulted in a greater understanding of the relevant technical and business requirements. They have also highlighted the potential value of a blockchain interoperability protocol in securely transferring data and value across different blockchains.

Open questions remain

While the successful completion of these experiments represents progress for the industry, a number of questions remain open. Putting regulatory clarity to one side, there are numerous areas that the private sector can work on together to advance the development of the tokenised asset ecosystem.

Solutions will be needed to address institutional requirements for adequate transactional privacy, and clearly defined liability within the tokenised asset value chain. The clear articulation of relevant use cases will be key in driving such solutions forward.

Based on the perceived market potential of tokenisation, and the broader alignment with Swift's strategy, we will invest in determining an appropriate set of capabilities to support the transfer of tokenised assets over the Swift network globally.

Areas for development

To tackle these challenges, Swift will continue working with the community to understand the most concrete use cases for tokenised asset adoption. We anticipate the most compelling business case for tokenisation in the near-term to be for the secondary trading of non-listed assets and private markets, given the potential for improvement in this area. We will therefore prioritise our efforts accordingly.

We remain focused on enabling the financial community to interact with tokenised assets by providing standardised channels, market guidelines, and orchestration of flows across networks. This will encompass DvP orchestration across the spectrum of payment leg types, including existing off-chain payments (e.g. correspondent banking and RTGS payment rails). To support market demand in the near-term, we will also explore on-chain payment methods (such as CBDCs and deposit tokens) to facilitate instant atomic settlement, as these channels become commercially available in the market.

Charting the future

Future work will require a heightened focus on the institutional requirements that were identified in our experiment, such as data privacy. To that end, we will continue our exploration of various types of blockchain implementations, with a greater focus on public permissioned ledgers that could provide the benefits of an open ecosystem, while ensuring adequate levels of transactional privacy.

We will also explore alternative possibilities, such as the provision of a private transactional data repository or the use of privacy-enhancing technologies like zero-knowledge proofs.

Moving forward, Swift is committed to remaining a key player in enabling blockchain interoperability, and enabling the widespread adoption of tokenised assets in financial services.

Want to learn more?

To provide feedback, or if you would like to learn more about our blockchain interoperability experiments and solutions, please reach out to your Swift account manager or contact innovate@swift.com.

8. Appendix

Glossary of terms

Blockchain wallet: This is a piece of software that manages one or multiple blockchain-specific public-private key pairs. The software typically includes functionality to generate and sign valid transactions for a supported blockchain network, or receive tokens at a valid address that is cryptographically linked to the public-private key pair.

EIP-712: This is an Ethereum standard (Ethereum Improvement Proposal) for the hashing and signing of typed structured data as opposed to just byte strings. It aims to improve the usability of off-chain message signing for use on-chain.

Designated Depository: This can be seen as the operational sponsor for a given asset on a blockchain-powered Settlement System, similar to the operational sponsor role performed by T2S (TARGET 2 Securities) before committing settlement on the T2S Securities Settlement ledger. Whilst we have classified it as the 'Designated Depository', this role could have various names depending on the jurisdiction and settlement flows encompassed, including 'central securities depository', 'central account keeper' and 'registrar', or 'master bookkeeper'.

Token pool: An essential component in the process of minting and burning wrapped tokens, this is a smart contract that keeps track of the assets deposited by users for creating wrapped tokens, and ensures the proper allocation of these tokens. The token pool also enables a secure and transparent auditing process for the wrapped token supply, which helps to maintain the peg of the token to its underlying asset. Overall, the token pool is a crucial aspect of the wrapped token ecosystem as it ensures proper collateralisation and the stability of the token value.

Nonce (wallet nonce): This is introduced to protect against the security risk of replay attacks. Via the bank wallet nonce, a blockchain message signed by the bank cannot be processed twice on the blockchain, whether submitted by Chainlink or by an adversary. The second time a signed blockchain message is submitted, the nonce validation in the smart contract fails and the transaction is rejected. The bank wallet nonce is validated by smart contract logic.

Token handling mechanism: Transferring a tokenised asset typically involves sending funds from sender to receiver. For token transfers across blockchains, there are two common mechanisms: (1) locking the transferred (native) tokens on the source chain and minting a representation of them on the destination chain, or (2) burning the (native) tokens on the source chain and minting them natively on the destination chain.

Wrapped token: This is a program or protocol that 'wraps' or encapsulates digital assets, such as cryptocurrencies or tokens, in a new format that makes them compatible with different blockchain networks. This enables easier transfer and interoperability between different platforms and networks. The token wrapper typically adds metadata and functionality to the wrapped tokens, such as smart contract capabilities or access control features. This allows the wrapped tokens to be used in decentralised applications (dApps) and other blockchain-based systems that may require additional functionality beyond basic currency transactions.

Cross-Chain Interoperability Protocol (CCIP) mechanics

In the event of a cross-chain transfer, the request is directed to the CCIP router. The below steps are taken to ensure tokens are sent securely to the destination blockchain:

1. Interface Interaction: The CCIP Router provides a user-friendly interface to interact securely with the cross-chain messaging system from existing institutional infrastructure.

2. Source Chain Validation: The CCIP Router validates the cross-chain message, ensuring that the destination blockchain is supported.

3. OnRamp Validation: If validation passes in the CCIP Router, the message is forwarded to the OnRamp, which performs further validation. Each institution can configure its preferred validation criteria, such as value and rate limits on specific tokens.

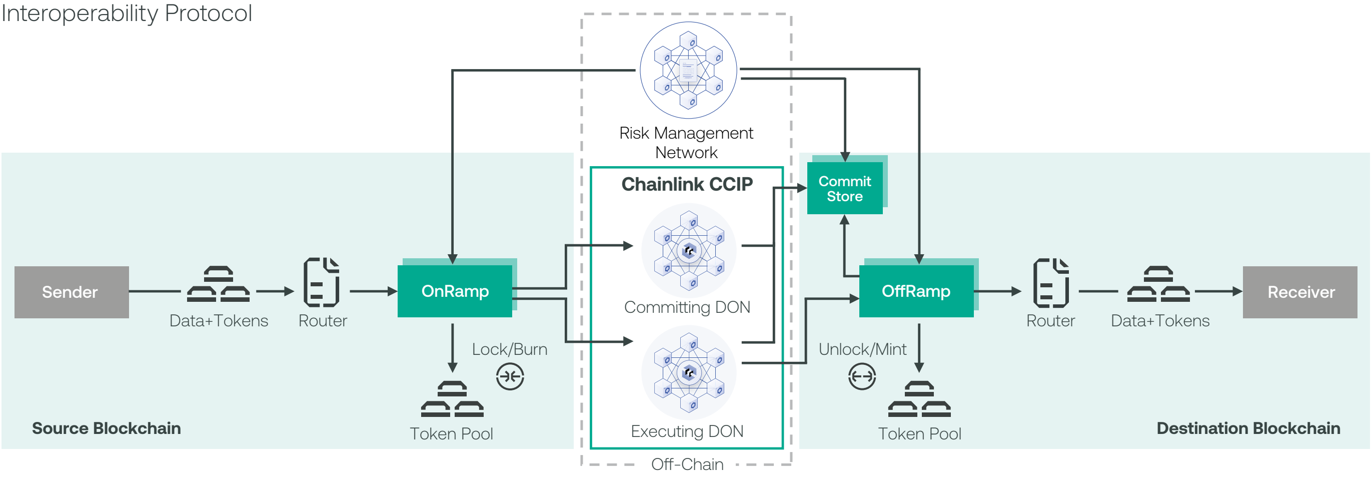
4. Token Handling: For each token included in the message (could be a single transfer or batch), the token handling mechanisms set by the issuer are applied. This can involve actions like lock-mint or burn-mint.

5. Oracle Network Processing: The OnRamp emits an event that triggers CCIP to process the message securely. CCIP works together with the additional Risk Management Network — an independent, secondary validation network — to ensure a robust and risk-mitigated approach to value movement across blockchains.

6. Destination Chain Validation: After CCIP processing, the token undergoes rigorous security and validation rules on the destination chain.

7. Token Minting: Once all validations are completed successfully, the token is minted and sent to the desired recipient on the destination chain.

Figure 5: The Cross-Chain Interoperability Protocol



Test scenarios

During this experiment we also tested several unhappy scenarios (non-exhaustive):

- Reuse same Nonce
- Expired ValidUntilTime
- Mismatch public address (From) and private address
- Send more token than available on the Wallet
- Wrong token name
- Wrong token version
- Wrong chain ID
- Wrong Forwarder Address
- Mismatch API request payload with blockchain message data

Message standards: MT 543

- **Quantity of the tokens which will be transferred**
- This data can be captured in the message with a dedicated field option :36D::SETT//DITU/
- **From:** Wallet address the tokens will be sent from
- This data can be captured in the message with a dedicated field option :97D::BCAW//
- **Receiver:** Wallet address the tokens will be sent to
- This data can be captured in the message with a dedicated field option :97D::BCAW//
- **Target:** Address of the tokens which will be transferred
- The message can currently formally handle the DTI identifier. This data can be captured in the message in :70E: Processing Instruction as ADDR/
- **Target name:** Name of the tokens which will be transferred
- This data can be captured in the message with the /NM/ tag for :35B: identification of the financial instrument
- **Target version:** Version of the tokens which will be transferred
- This data can be captured in the message with a /VRSN/ tag for :35B: identification of the financial instrument
- **Chain ID:** ID of the blockchain from which the tokens will be sent
- This data can be captured in the message with a structure for :70E: Processing Instruction
- **Destination chain ID:** ID of the blockchain to which the tokens will be sent
- This data can be captured in the message with a structure for :95Q::PSET
- **Valid until time:** Timestamp after which the transfer would no longer be valid
- This data can be captured in the message with a structure for :70E: Processing Instruction
- **Nonce:** Random value (non-sequential) stored on chain to avoid replay attacks
- This data can be captured in the message with a structure for :70E: Processing Instruction
- **Signature:** EIP-712 signature of the blockchain message
- This data can be captured in the message with a structure for :70E: Processing Instruction

Status confirmation codes

When queried, the Chainlink API provides detailed information regarding the current state of transactions. An initial response is provided as soon as a transaction has been submitted to Chainlink. The information returned includes:

chainlink_request_id: UUID. This is same as request_id returned by Chainlink for send_transaction API

status: status of meta-transaction. Can be one of the following:

- **CONFIRMED:** blockchain tx has 1 block confirmation on source chain
- **SOURCE_FINALISED:** blockchain tx on source chain is finalised (for cross-chain transfers only)
- **FINALISED:** blockchain tx finalised (on destination chain, for cross-chain transfers)
- **FAILURE:** failure
- tx_hash: transaction hash on source blockchain
- **ccip_msg_id:** CCIP Message ID (for cross-chain token transfers only)
- **failure_reason:** reasons for FAILURE status

The Chainlink status updates are mapped to the MT 548 message towards the financial institution.

9. Acknowledgements

Swift team

Tom Zschach
Chief Innovation Officer

Nick Kerigan
Managing Director, Head of Innovation

Jonathan Ehrenfeld
Head of Securities Strategy

Jack Pouderoyen
Innovation Market Engagement

Thomas Dugauquier
Tokenised Assets Product Lead

Charles Vinet
Senior Innovation Engineer

Fabrice Yans
Enterprise IT Architect

Tom Alaerts
Principal, Standards

Wes Harmon
Innovation Engineer

Chainlink team

Sergey Nazarov
Co-founder

Thomas Trepanier
Head of Capital Markets

Ryan Lovell, Director
Capital Markets

Pieter Pauwels
CCIP Market Strategy Manager

Swift would like to give a special thanks to our colleagues from over a dozen financial institutions that participated in these blockchain interoperability experiments.

Swift

About Swift

Swift is a global member-owned cooperative and the world's leading provider of secure financial messaging services. We provide our community with a platform for messaging, standards for communicating and we offer products and services to facilitate access and integration; identification, analysis and financial crime compliance. Our messaging platform, products and services connect more than 11,000 banking and securities organisations, market infrastructures and corporate customers in more than 200 countries and territories, enabling them to communicate securely and exchange standardised financial messages in a reliable way.

As their trusted provider, we facilitate global and local financial flows, support trade and commerce all around the world; we relentlessly pursue operational excellence and continually seek ways to lower costs, reduce risks and eliminate operational inefficiencies. Headquartered in Belgium, Swift's international governance and oversight reinforces the neutral, global character of its cooperative structure. Swift's global office network ensures an active presence in all the major financial centres.

For more information, visit
Web: www.swift.com
Twitter: @swiftcommunity
LinkedIn: Swift

Copyright

Disclaimer

Swift supplies this publication for information purposes only. The information in this publication may change from time to time. You must always refer to the latest available version.