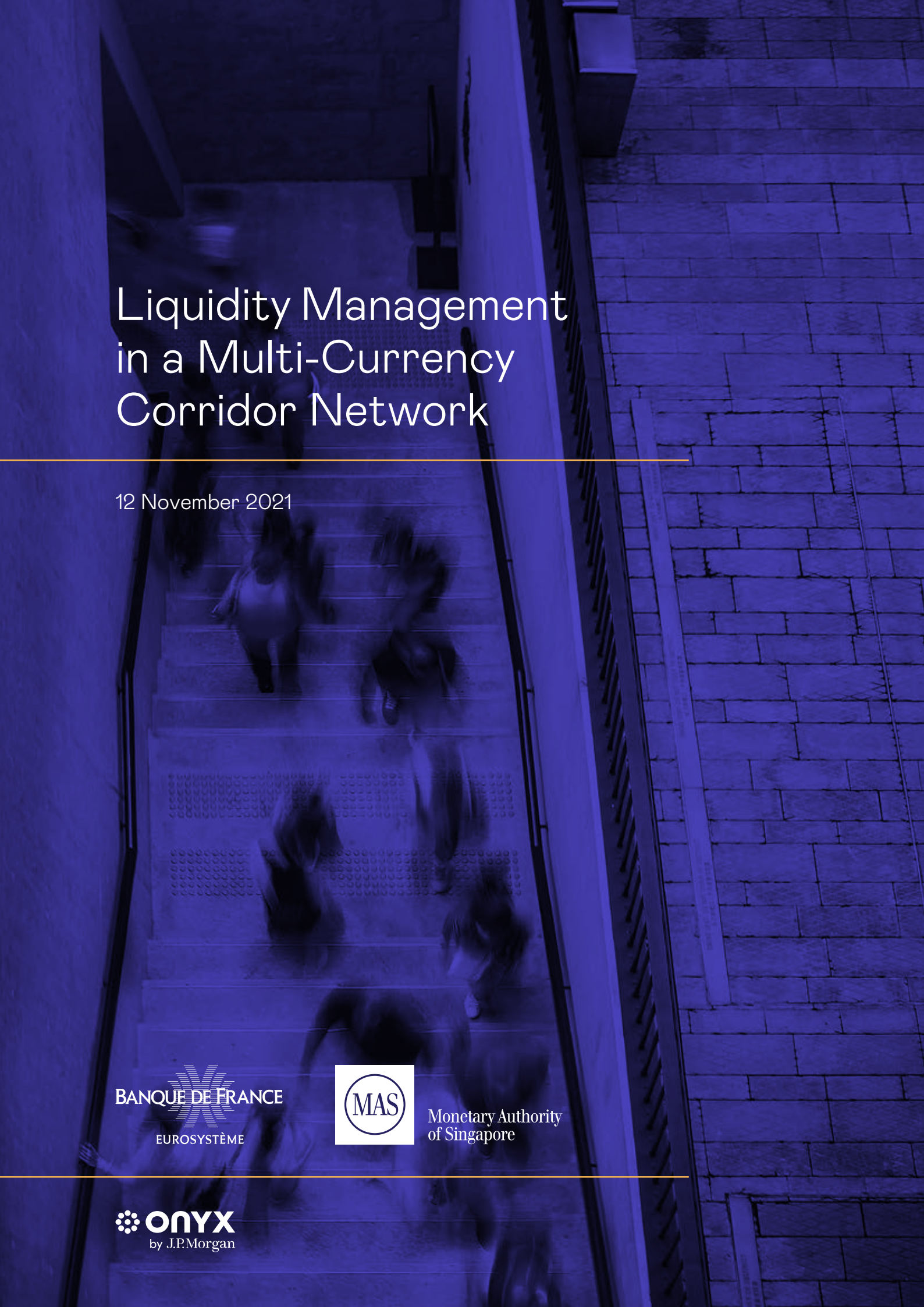


Liquidity Management in a Multi-Currency Corridor Network

12 November 2021

BANQUE DE FRANCE
EUROSYSTÈME

MAS
Monetary Authority of Singapore

onyx by J.P.Morgan

Contents

01 Executive summary

Cross-border payments are frequently criticized due to issues such as their slow speed, relatively high costs and lack of transparency. Cross-border payments currently rely on arrangements which may also be subjected to limited transparency on foreign exchange rates, restricted operating hours of payment infrastructure and currency settlement delays due to differences in time zones. An emerging priority for policymakers is the need to address the frictions associated with cross-border payments. To address these challenges, the Monetary Authority of Singapore ("MAS") and Banque de France ("BdF"), supported by J.P. Morgan's Onyx, simulated an experiment, held on 30th June 2021, using a common multi-CBDC (mCBDC) network to facilitate cross-border payments.

The experiment simulated cross-border and cross-currency transactions for Singapore Dollar (SGD) CBDC and €uro (EUR) CBDC, and was conducted using a permissioned, privacy-enabled blockchain based on Quorum® permissioned DLT network. Four key outcomes were achieved:

1. The demonstration of interoperability across different types of cloud infrastructure. Blockchain nodes were set up across private and public cloud infrastructures in both Singapore and France.
2. The design of a common mCBDC network that enabled MAS and BdF to have visibility on cross-border payments, while retaining independent control over the issuance and distribution of their respective CBDC.
3. The setup of an experimental mCBDC network that incorporated automated liquidity pool and market-making service for EUR/SGD currency pairs. Smart contracts were used to manage the EUR/SGD currency exchange daily rate.
4. The simulation of an experimental mCBDC network that showed that the number of correspondent banking parties involved in the payment chain for cross-border transactions can be optimised. Consequently, the number of contractual arrangements, the Know-Your-Customer (("KYC") burden as well as the associated costs could be more efficient.

While the simulation was limited to two central banks, the design of the mCBDC network enables it to be scaled up to support the participation of multiple central banks and commercial banks located in different jurisdictions. This offers great potential to simplify integration and significantly reduce costs, since a single connection to a common platform driven by a common governance is used in place of multiple connections to different and specific information systems.

02 Introduction

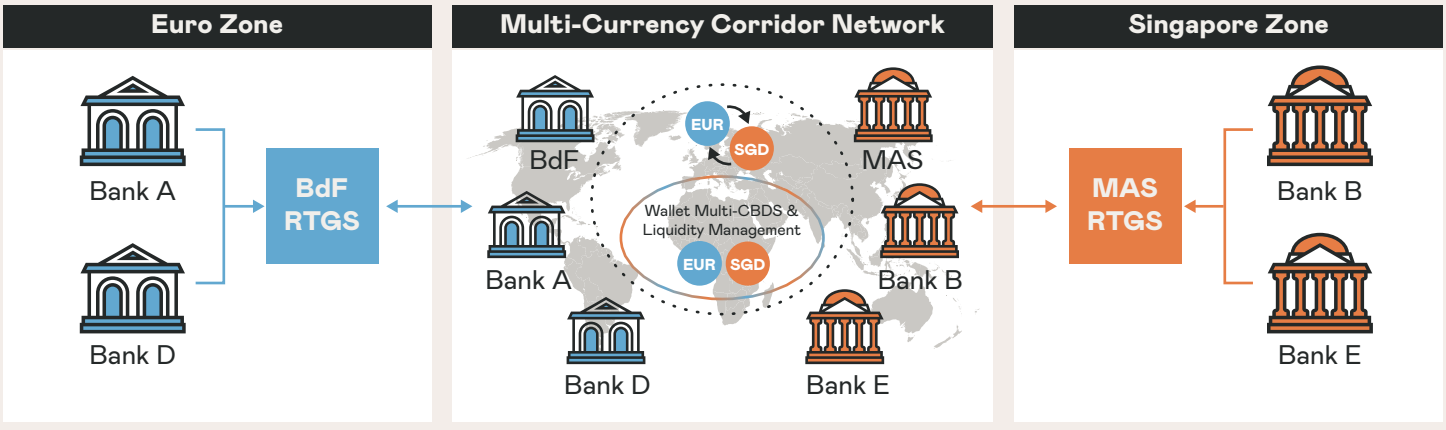
The design and implication of Central Bank Digital Currencies ("CBDCs") is being explored by Central Banks around the world. A survey[1] by the Bank for International Settlement ("BIS") reflected that more than 80% of those surveyed were conducting CBDC experiments or pilots. Most of the respondents also stated that they were undecided on whether any CBDC issued could be used in other jurisdictions.

Nevertheless, there is a momentum at international level to further enhance cross-border payments. The Financial Stability Board (FSB), in coordination with the Committee on Payments and Market Infrastructures (CPMI), has developed a roadmap comprising a set of 19 building blocks designed to address some of the challenges. This roadmap identifies the issuance of CBDC as a possible way forward to improve cross-border payments (building block 19 of the roadmap).[2] The possibility of forming multi-CBDC ("mCBDC") arrangements to establish interoperability between national CBDCs and thus improve the cross-border payment rails is also being examined.

Three interoperability arrangements have been suggested by the BIS. In the first, billed Enhanced Compatibility, each jurisdiction maintains their own complete CBDC systems. Interoperability is mainly achieved through compatible technical and regulatory standards. In the second model, termed Interlinking, siloed CBDC systems are interlinked through shared technical interfaces or by using a centralized or decentralized common clearing mechanism.

In the third model, known as the Integration, into a single system arrangement, multiple CBDCs can be run on a single platform.

This report discusses the set-up and findings of a simulation using the third type of arrangement, which is technology-agnostic and where a single CBDC system is set up, on which currency pairs can be exchanged. For this simulation, commercial banks perform (i) cross-border payment and (ii) cross-currency Payment versus Payment (PvP) transactions in EUR CBDC and SGD CBDC. These functions are performed between the simulated commercial banks established in different countries. The simulation posits a shared governance and a shared rulebook (e.g., payment rules, fees) agreed upon by the participating entities. Meanwhile, a key design principle of the simulation is that each central bank retained its independence over the control of their respective currencies. Privacy of transactions is preserved, and central banks have full control and the ability to define which participants can use its CBDC token. A shared distributed ledger system acts as a corridor between two central banks' Real Time Gross Settlement ("RTGS") system, offering a multi-currency environment including a liquidity pool facility service (see below). This setup, through its relative openness, offers a governance framework where wholesale CBDC can be used by design for a large pool of currencies with the option to onboard other central banks, currency types and market participants.



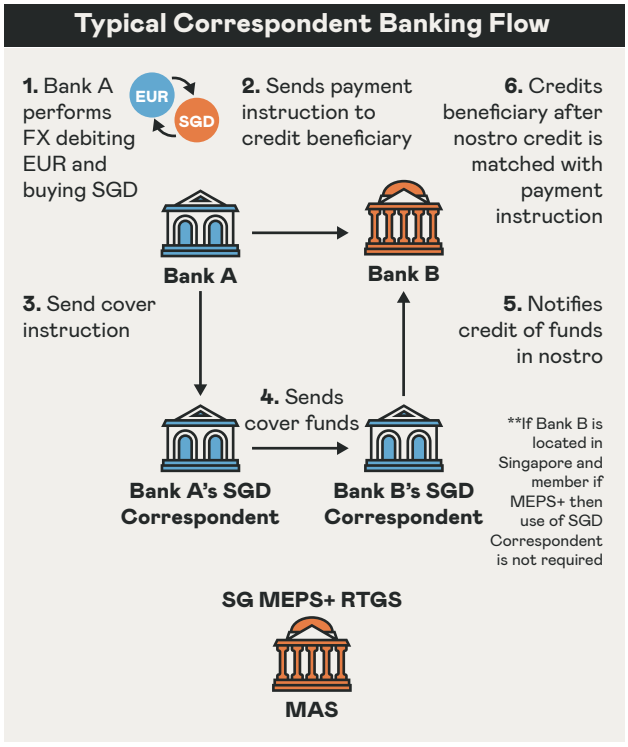
1. BIS, August 2020, 'Rise of the central bank digital currencies: drivers, approaches and technologies.' Available at: www.bis.org/publ/work880.htm. Accessed October 2021.
2. BIS, July 2020. 'Enhancing cross-border payments: building blocks of a global roadmap.' Avilable at: www.bis.org/cpmi/publ/d193.htm. Accessed October 2021.

02 The need to facilitate cross-border payments

While cross-border payments continue to evolve, slow speed, high costs and the lack of transparency are often cited as frictions. These inefficiencies can be attributed to the primary mechanism for cross-border wholesale payments today- involving several intermediaries, governed by several jurisdictions, different operational processes and specific trading hours. As a result, the underlying lack of interoperability, availability across time zones and standardisation are the root causes of the frictions to cross-border payments.

An example of the type of banking flows involved in these cross-border payments is shown in Figure 1 below, where a customer of Bank A holding a EUR account is making a SGD payment to Bank B's customer.

FIGURE 1: TYPICAL CORRESPONDENT BANKING FLOW FOR A CROSS-BORDER SGD SETTLEMENT



As a result, there is a need to improve cross-border payments and make them faster, cheaper, safer and more inclusive. Some of the potential benefits include:

1. Increased transparency
The correspondent banking model could be optimized by improving transparency and reducing the need for reconciliation, and thus reducing both processing time and costs.

2. Increased availability across time zones
Time zones affect cross-border payments. Most banks typically only support processing during business hours. For cross-border payments spanning different time zones, limited overlapping business hours constrain the availability of a common transacting window. This in turns prevents same day payments processing. Additionally, a bank's internal treasury management processes typically provide funding coverage during business hours only. A currency cut-off time may be defined after which payments can only be processed the following business day. Finally, cross-border payments often get settled between intermediary banks through the domestic RTGS system of the payment currency. Many of these RTGS systems have defined operating hours, outside of which banks will need to withhold the payment until the next business day. A key improvement would be to increase the number of cutoffs per day to increase settlement speed.

3. Reducing FX settlement risk for new and emerging markets
There is a positive evolution in emerging markets implying an evolution in the demand for FX in these markets which today do not benefit from the same security as the major currencies. This implies that many emerging markets that are experiencing increasing capital flows and thus greater cross-border payments needs, do not benefit from the same level of safety in settlement. According to the BIS, the proportion of FX settlements with PvP protection appears to have fallen from 50% in 2013 to 40% in 2019 due to greater transactions in trading currencies not supported by CLS.[3] An inclusive solution is required to cover currencies especially those from emerging markets.

3. BIS. "BIS Quarterly Review, December 2019". Available at: www.bis.org/publ/qtrpdf/r_qt1912x.htm. Accessed September 2021.

03 The Simulation

This simulation investigates the viability of cross-border payments through a mCBDC shared corridor network using distributed ledger technology ("DLT"). The use of a shared corridor network resolves the issue of reconciling disparate ledgers thereby creating process efficiency and opens the possibility for improved supervision by central banks on their respective CBDC movements. Enabling and ensuring privacy is also one of the critical success factors for such a shared network.

Objectives

The objectives this simulation seeks to achieve include:

- **Real Time processing**
  Technical mechanisms to support processing cross-border payments involving CBDC exchange in real-time and 24 by 7 basis;
- **Liquidity Management**
  Test the use of automated liquidity pool and market-making service to automatically manage the currency exchange rate in line with real-time market transactions and demands without a central order book;
- **Efficiency**
  An approach whereby PvP can be executed atomically and autonomously on a single technical environment for a large subset of currencies;
- **Multi-cloud/Hybrid-Cloud**
  Demonstrate that the platform provides flexibility to operate in private and public cloud infrastructures across jurisdictions;
- **Monitoring**
  Enable central banks to issue their respective CBDCs into the share corridor network and to track the circulation of CBDCs in real-time while retaining independent control over the issuance and distribution of their own CBDC;
- **Privacy**
  Support for private transactions on a DLT such that central banks and commercial banks are only privy to their own CBDC transactions and positions.

Scope

This simulation involved setting up a common mCBDC shared corridor network (based on a permissioned Consensys Quorum® DLT network) that would support the following use cases:

a. A Liquidity Pool Manager ("LPM") that allows financial institutions to stake liquidity to enable transfers;

b. Cross-border payment using the established liquidity pool as the CBDC exchange;

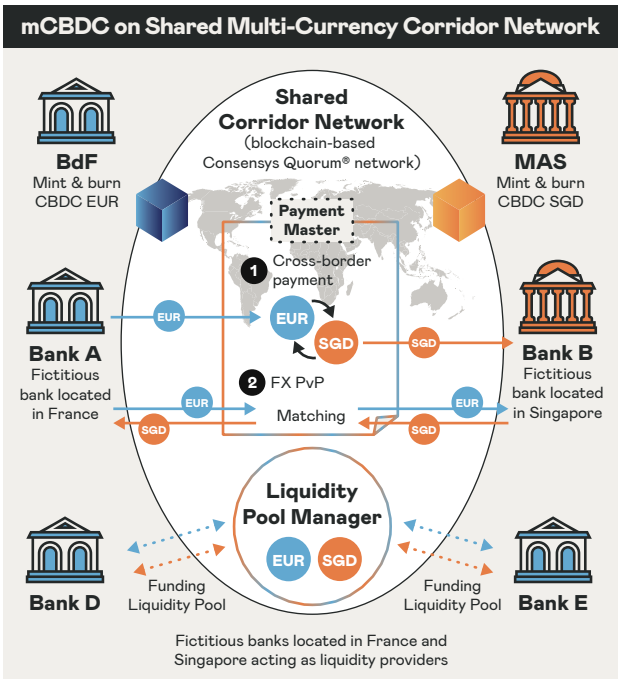
c. Payment versus Payment ("PvP") matching in a gross settlement mechanism;

Simulated participants in this shared corridor network were:

- **Banque de France** (BdF) and **Monetary Authority of Singapore** (MAS), each owning their CBDC smart contracts for issuance and tracking of CBDC EUR and CBDC SGD respectively;
- **Bank A** and **Bank B** as transacting parties for both cross-border payment and PvP use-cases; and
- **Bank D** and **Bank E** as liquidity providers to the LPM.

A high-level schematic of the simulation is provided in Figure 2.

FIGURE 2: DESIGN OF THE mCBDC NETWORK



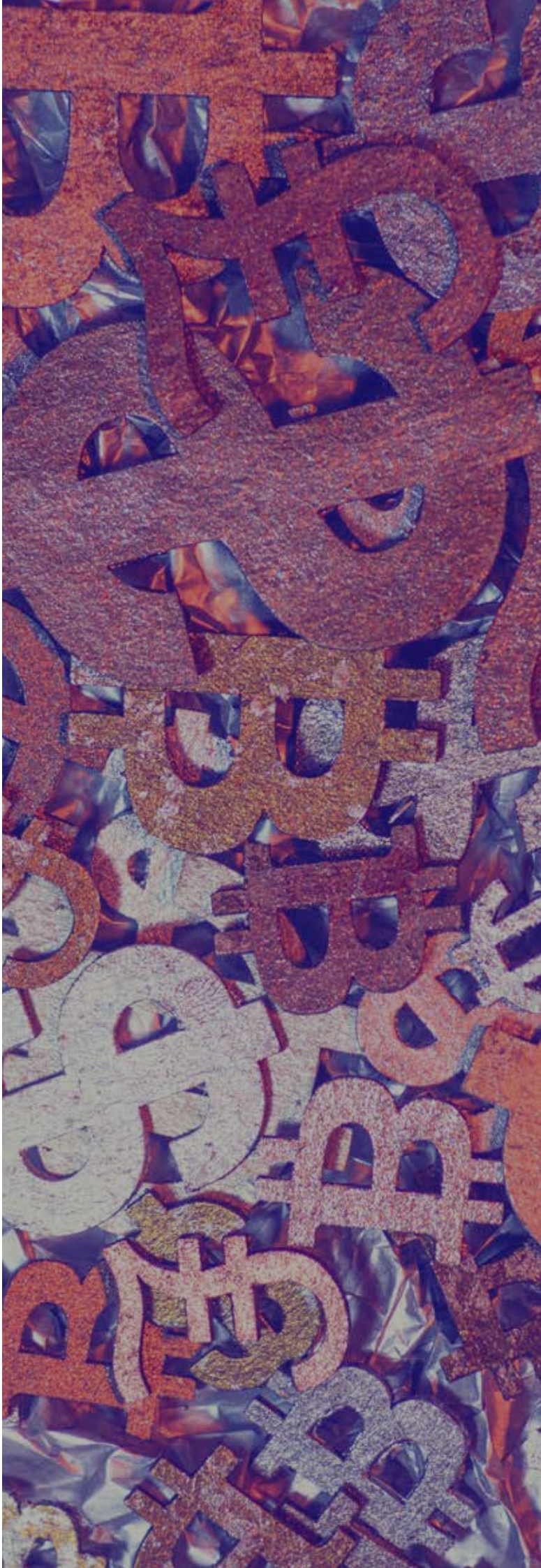
03

The simulation assumed that the shared corridor network was jointly controlled and operated by both central banks through a consortium arrangement ("Consortium"), under a mutually agreed rulebook and governance model. Additionally, as part of the simulation, four fictitious commercial banks were admitted to the network as participants to support cross-border payments and PvP settlements.

Expected Benefits

We began the simulation with the expectation that we would demonstrate that a mCBDC arrangement based on a single DLT platform would reduce complexity of bank-to-bank integration and would simplify the business process through a single standardized governing rulebook. Consequently, it results in a more efficient payments infrastructure yielding benefits that can be passed on to key participants and end customers. Other benefits include:

- A shared platform and common rulebook as a mechanism for a standard-based infrastructure that provides a **level playing field for market participants** to offer competitive and innovative products on the shared corridor network;
- A decentralized liquidity pool mechanism provides FX **pricing transparency** to all participants and supports immediate and atomic settlements; an efficient payments infrastructure will also translate to **operating cost savings** through a higher degree of automation;
- Providing **secure settlement in emerging FX markets**. Emerging markets investments have significantly increased in the last decade. DLT mitigates against settlement failure as smart contracts are programmed to ensure that PvP settlement happens only if both wallets are sufficiently provisioned, removing counterparty risks;
- Allowing flexibility for **24x7 real-time gross settlements for a larger set of currencies** complementary to the daily netted settlement mechanism provided. It is also possible that netting solutions be implemented in smart contracts on the shared corridor network to support autonomous matching and settlement, while providing liquidity optimization benefits for all currencies in the network.



04 Simulation Design

A high-level overview of this simulation involves the respective central banks issuing CBDC EUR and CBDC SGD tokens to the commercial banks' wallets. The central banks are also responsible for the destruction of these tokens at the end of the simulation. The commercial banks could initiate transactions on the network if they have the sufficient CBDC tokens required for such transactions. The simulation does not consider a credit facility.

Scalability beyond the initial two participating jurisdictions is also factored in. Instead of having multiple bilateral connections between each country and network, this simulation envisages that each country will need to maintain only a single connection to this multilateral platform[4].

4. To illustrate, bilateral point-to-point connections between 20 different entities would result in 190 connections. Alternatively, in a model where a shared common platform is used, just 20 connections would be required.

Structure of DLT Accounts

In this simulation, two central bank DLT accounts and two consortium DLT accounts are created on the shared corridor network. The consortium accounts are created to deploy smart contracts recognizing the consortium's role as the network operator. For simplicity of setup, each of the central banks will be responsible for one of the two consortium accounts. In terms of permissions,

- The BdF account has permissions to deploy the CBDC EUR smart contract using the BdF private key;
- The MAS account has permission to deploy the CBDC SGD smart contract using the MAS private key;
- The BdF-owned Consortium account has permission to deploy the Liquidity Pool Manager ("LPM") smart contract using the BdF-owned Consortium account private key;
- The MAS-owned Consortium account has permission to deploy the Payment Master smart contract using the MAS-owned Consortium account private key.

There are also four DLT accounts created for the fictitious commercial banks – Bank A, Bank B, Bank D and Bank E (see Figure 2). Both central banks will grant the rights to each of these commercial banks' DLT accounts to receive their respective CBDC tokens. In addition, Bank D and Bank E are granted permission to stake CBDC tokens to the LPM.

CBDC Smart Contract

For this simulation, the CBDC smart contract is an ERC20 contract[5] with extensions to support role-based permissions. The same smart contract code is deployed twice, once by MAS for CBDC SGD and again by BdF for CBDC EUR. The same CBDC smart contract source code is used for convenience. Any CBDC smart contract that conforms to the ERC20 standard can interoperate in this network.

5. ERC20 has emerged as the technical standard used in smart contracts on the Ethereum blockchain for token implementation.

04

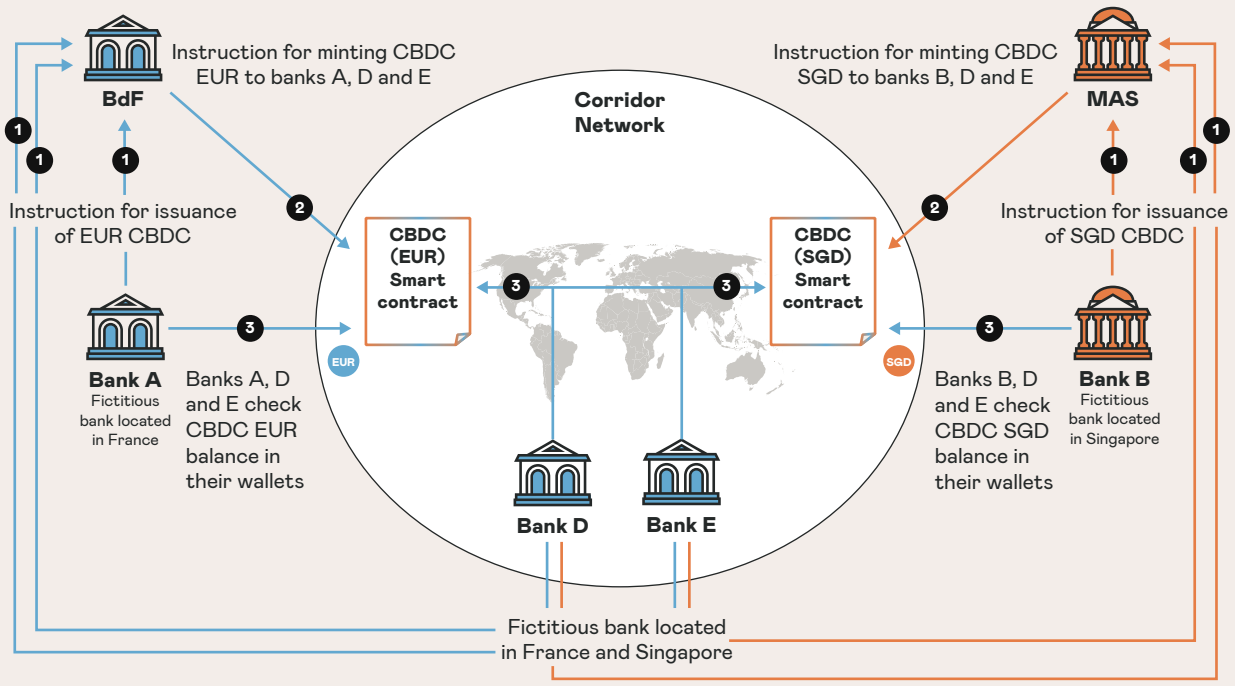
The sequence for CBDC token issuance is described below and reflected in schematic form in Figure 3.

1. Commercial banks outside the shared corridor network **initiate requests** for CBDC token issuance. For this simulation, successful debiting of commercial banks' funds from their central bank deposits will be initiated.

2. The central banks instruct their CBDC smart contracts to **transfer an equivalent amount of CBDC tokens to the commercial bank's balance**. The respective CBDC smart contracts track the total supply and circulation of tokens, and the balance held by each commercial bank in their wallet.

3. Commercial banks can **directly query** the CBDC smart contracts to check their balances. The CBDC smart contract has an ERC20 approve function for commercial banks to preauthorize the Payment Master smart contract to debit their balance for the purpose of making a payment, or for staking tokens to the LPM.

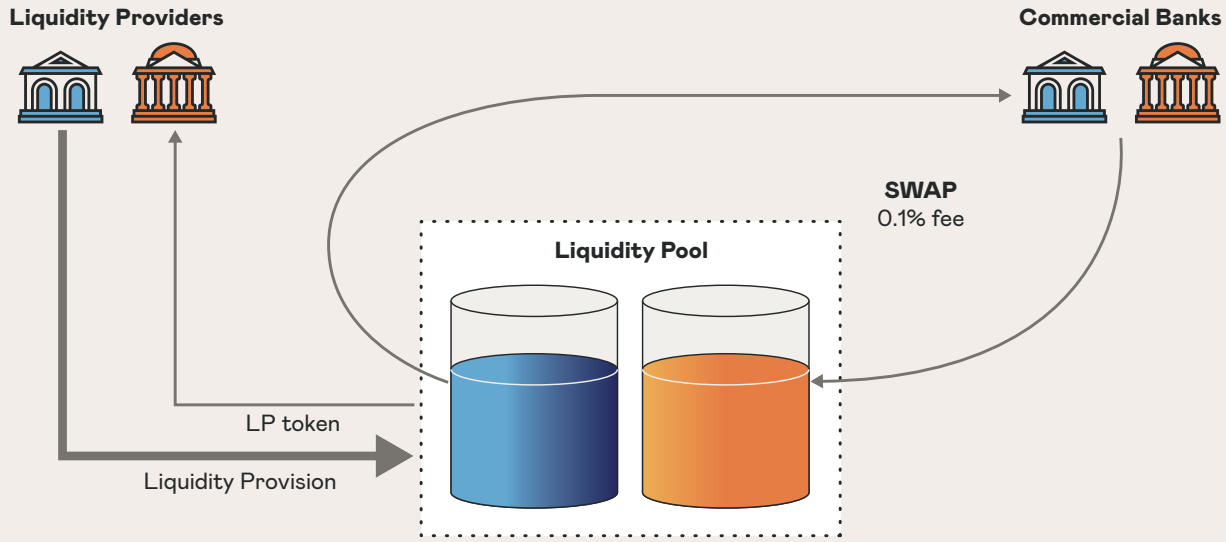
FIGURE 3: CBDC TOKEN SEQUENCE SCHEMATIC



Liquidity Pool Manager ("LPM") Smart Contract

For this simulation, automated market making ("AMM") and liquidity management capabilities are incorporated into its overall design. Bank D and Bank E act as liquidity providers to the LPM through staking of CBDCs from their wallets into the pool. When a currency exchange is required for a cross-border payment, the LPM will levy a ten-basis point exchange fee computed over the payment amount to be debited from the payer bank's wallet. This exchange fee is kept by the LPM and accrued to the liquidity providers, based on their contributing proportion to the overall pool.

FIGURE 4: PROVISION OF LIQUIDITY FOR CBDC EXCHANGE



For simplicity, a fixed daily exchange rate is established, and this daily rate is configured in the LPM per calendar day. For this simulation, the daily rate is set at

$$1\ CBDC\ EUR = 1.6\ CBDC\ SGD$$

When staking tokens to the LPM, liquidity providers need to stake both CBDC EUR and CBDC SGD in proportion to the exchange rate. Using the established exchange rate, this means that for every 100 CBDC EUR staked, 160 CBDC SGD is staked at the same time. For future phases of this simulation, AMM strategies such as the Constant Product Market Maker formula will be trialed.

For tracking contributions to the liquidity pool, an internal Liquidity Pool Token ("LPT") is used, with 1 LPT equivalent to 1 CBDC EUR plus 1.6 CBDC SGD. Hence, if the liquidity provider stakes 100 CBDC EUR and 160 CBDC SGD, they will be allocated 100 LPT.

A liquidity pool provider can withdraw all or part of their LPT at any time, subject to the availability of CBDC tokens in the Liquidity Pool Manager. The CBDC EUR to CBDC SGD rate used to settle will be the same as the rate established when LPT was allocated.

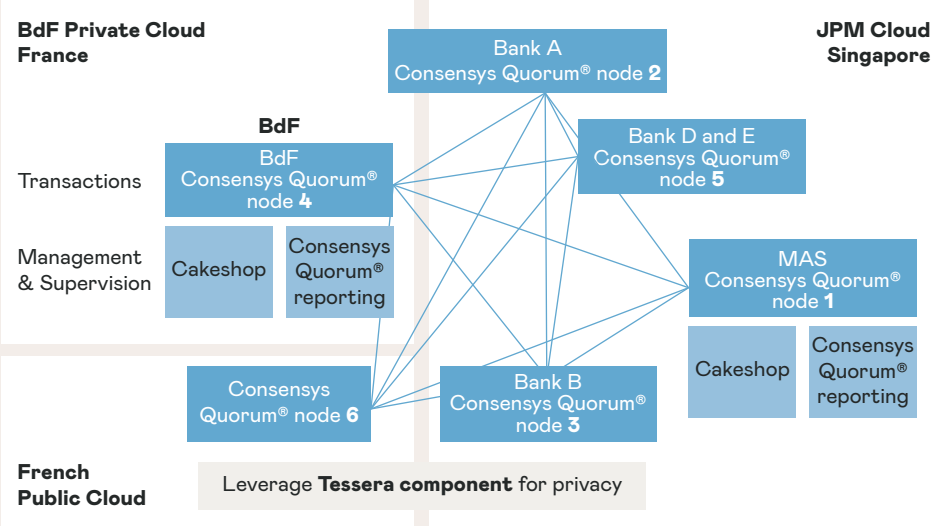
Network Topology

Consensys Quorum® is used for this test network as the permissioned blockchain implementation with support for private transactions. All nodes are set up as validator nodes using the Istanbul-Byzantine Fault Tolerant ("IBFT") consensus algorithm, which caters for F faulty nodes in a N validator network, where N = 3F + 1. Hence, under a six-node configuration, the system will still continue to operate even if one of the nodes goes down, or starts acting maliciously. For private transactions, the additional Tessera component in every Consensys Quorum® node orchestrates the sharing, securing and storage of the private data. Tessera implements its own peer-to-peer communication protocol outside of the blockchain.

This simulation also demonstrates the viability of deploying nodes across different regions and cloud providers. We used two industry-standard cloud environments in Singapore and France. In addition, we also used BdF Private Cloud in France.

Figure 5 represents a high-level schematic of the network topology.

FIGURE 5: NETWORK TOPOLOGY



Node 1 and Node 4 represent the respective central banks with additional monitoring and reporting tools installed:

- **Cakeshop** – An explorer tool that supports viewing of transactions, blocks and contracts on the blockchain.
- **Consensys Quorum® Reporting** – A tool that indexes blocks and transactions in the network and generates reports of smart contract states, events and changes.

Node 2 and Node 3 represent nodes of Bank A and Bank B where cross-border payment and PvP transactions are being initiated. Bank D and Bank E nodes are hosted on node 5 for the staking and withdrawal of the liquidity pool. Node 6 is used as a negative test node for privacy to demonstrate that transactions between the commercial banks are not visible to non-stakeholder nodes, even when node 6 is actively participating in the consensus algorithm.

For this simulation, the private keys of each participant are stored on the file system of their respective node. To elaborate,

- Node 4 stores the BdF key for deploying the CBDC EUR smart contract. It also stores BdF's consortium key for deploying the LPM smart contract.
- Node 1 stores the MAS key for deploying CBDC SGD smart contract. It also stores the consortium key for deploying the Payment Master smart contract.
- Node 2 and Node 3 store the keys for Bank A and Bank B respectively.
- Node 5 stores the keys for both Bank D and Bank E, which act as the liquidity providers on the network.
- Node 6 does not have any keys to transact on the network.
- Since all the nodes are validators, an additional validator key is stored in the file system of each node.

04

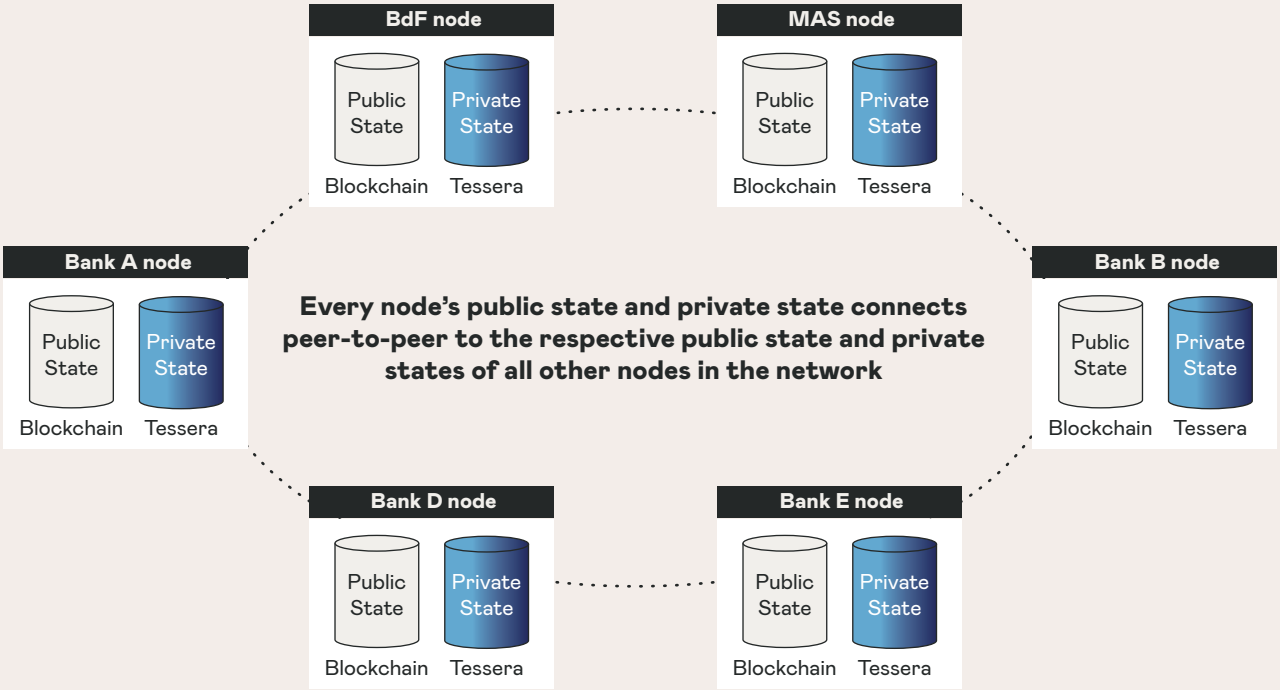
Privacy Mechanism

One of the simulation's considerations is to ensure that the CBDC balances of each commercial bank is known only to itself and the central bank issuing the CBDC token, in line with the principle of sharing data on a need-to-know basis.

Consensys Quorum® private transaction capability has been used in the simulation to fulfill this requirement. Consensys Quorum® private transactions ensure that the transaction payload is visible only to the parties of the transactions. Only a hash on the blockchain is visible to the rest of the network.

To achieve this, at the Consensys Quorum® node level, the state database is split into a public state and a private state. A public state is always in sync across the network through the IBFT consensus algorithm. The private state is updated based on the private transactions that a node is part of, and thus is unique only to that node. This also means that the private state will be divergent across nodes. Tessera is the private transaction manager for Consensys Quorum® and manages the encrypted payload exchange between other Tessera nodes in the network.

FIGURE 6: CONSENSYS QUORUM® PRIVATE AND PUBLIC STATES



When a node receives a transaction to publish, it first checks if the transaction is private. If the transaction is private, the node forwards the transaction to its linked Tessera module, which shares the encrypted transaction payload securely with the other parties of the transaction and waits for confirmation. Upon confirmation, the node replaces the original transaction payload with a hash from the Tessera module and submits the transaction to the blockchain, which is then propagated to all the nodes in the network. At the time of block minting, each node checks if the transaction is a private transaction. If the transaction is private and the payload is available in its linked Tessera node, it gets decrypted and passed back to the node to be executed and the private state of the node is updated. If the payload is unavailable in Tessera, the node skips the transaction. However, the transaction is included in the block.

04

Based on the network topology established in Figure 5, the data privacy design implemented for the simulation is reflected in the table below.

Data Type	Node 1 (MAS)	Node 2 (Bank A)	Node 3 (Bank B)	Node 4 (BdF)	Node 5 (Bank D&E)	Node 6
Own balances – EUR	⊘	✓	✓	✓	✓	⊘
Participants balance – EUR	⊘	⊘	⊘	✓	⊘	⊘
Own balance – SGD	✓	✓	✓	⊘	✓	⊘
Participants balance – SGD	✓	⊘	⊘	⊘	⊘	⊘
Liquidity pool balance – EUR & SGD	✓	⊘	⊘	✓	✓	⊘
Liquidity pool token (LPT) balance	✓	⊘	⊘	✓	✓	⊘
Liquidity pool accrued fee – EUR & SGD	✓	⊘	⊘	✓	✓	⊘
					✓ visible	⊘ invisible

(Note: Central Banks are the issuer of their own CBDC but they do not hold other country's CBDC in this simulation)

For example, when BdF sends a transaction in the network to issue CBDC EUR tokens to Bank A's wallet, it will send the transaction private for itself and Bank A's node. The rest of the network (except BdF and Bank A's node) will see that there is a transaction initiated by BdF, but they will not have access to the transaction payload. When the transaction is executed, the change in balance will only be visible on BdF's and Bank A's nodes.

According to the above privacy design, the two central banks issuing the CBDC tokens have complete visibility on the overall distribution of their respective tokens and CBDC balances of the tokens' owners. The participants only see their own balances and do not have any visibility into the balances of other participants.

Based on these privacy design principles, the following challenges were observed during the execution of the simulation:

- The simulation required the central bank node to be part of every transfer transaction happening for the respective CBDCs to ensure that appropriate validations were carried out. In Consensys Quorum®'s privacy model, it is not possible to define a mandatory party at each private contract level. As a result, a transaction may be executed without including the central bank node as a party to the transaction. This may impact the central bank's oversight effectiveness and could lead to balance mismatches[6].
- As the private state is divergent, the same transaction execution may be successful on one node but may fail in another node. For example, if there is an EUR token transfer happening from Bank A to Bank B with the transaction being private for Bank A, Bank B and BdF, the debit balance check will be successful on Bank A's node and BdF's node assuming Bank A has sufficient balance. However, this will fail on Bank B's node as it does not know Bank A's balance. As a workaround, a private validator contract was deployed across the network and inherited in the CBDC contracts. This private contract held the context for each node. The validations at the CBDC contracts were modified to consider the context under which the code is getting executed.

6. For the purpose of this simulation control is implemented at the DApp layer

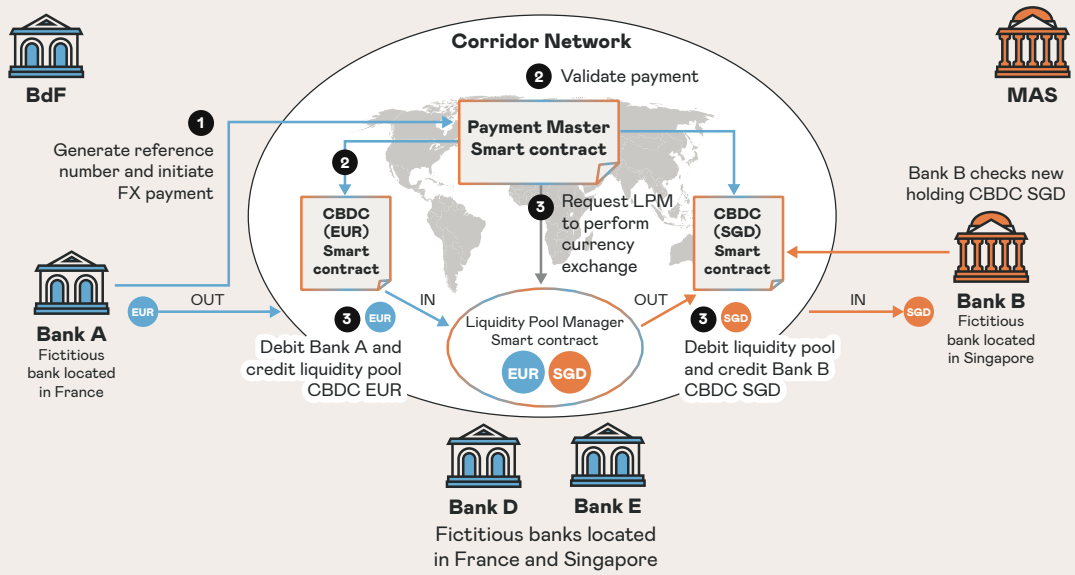
05 Simulation's Use-cases Walk-throughs

In this simulation, commercial banks perform (i) cross-border payment with currency exchange and (ii) cross-currency Payment versus Payment ("PvP") transactions in EUR CBDC and SGD CBDC between commercial banks established in different countries.

Cross-Border Payment with Currency Exchange

A high-level schematic of the execution of this use-case is shown in Figure 7 below.

FIGURE 7: CROSS-BORDER PAYMENT WITH CURRENCY EXCHANGE



The process is:

Step 1 →

Bank A creates a cross-border payment agreement ("the agreement") that contains the details of the payment instruction, calls the CBDC EUR smart contract to preauthorize (i.e., approve) the Payment Master to debit its wallet for the specified amount of CBDC EUR tokens. Bank A then makes a call to the Payment Master smart contract to initiate the cross-border payment by providing the reference to the agreement.

Step 2 →

The Payment Master validates that Bank A has sufficient CBDC EUR tokens in its wallet and that LPM has sufficient CBDC SGD tokens to be exchanged. This includes the LPM fee amount that Bank A must pay for the currency exchange (0.1% of the debit amount). If the validation is successful, the payment will proceed. Otherwise the Payment Master aborts with a failure.

Step 3 →

The Payment Master instructs LPM to proceed to settle the currency exchange by:

- Debiting Bank A's wallet for CBDC EUR for an amount comprising of the payment principle plus the fee, and crediting the total amount to the LPM's wallet; and
- Debiting LPM's wallet for the equivalent of CBDC SGD on the payment principle, and crediting the amount to Bank B's wallet.

This settlement is done atomically on the DLT. Bank A and Bank B can then check the new balances with the respective CBDC smart contracts.

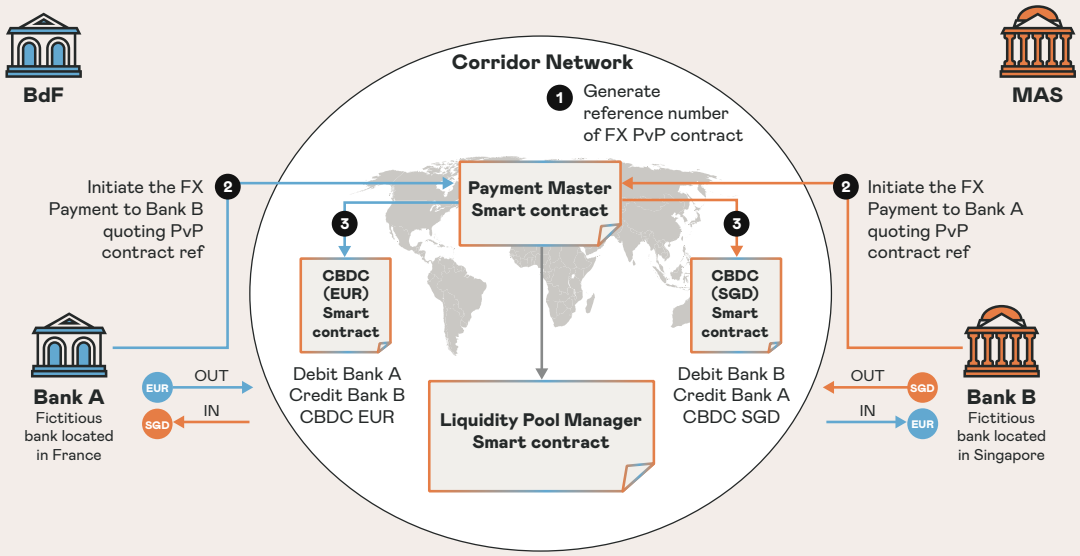
05

Cross-currency Payment versus Payment ("PvP") transactions

PvP is a mechanism in the foreign exchange settlement to ensure that a final transfer of one currency occurs only if a final transfer of another currency also takes place. The PvP process requires both counterparty banks to establish pre-agreed conditions of exchange. Both banks will specify, in their request to the Payment Master, the currency and amount they are sending, and the equivalent currency and amount they are expecting to receive in return. The Payment Master tracks the receipt of both legs of the transaction and when validation and matching are successful, it will atomically settle the exchange of payment to both sides.

A high-level schematic of the execution of this use-case is shown in Figure 8 below.

FIGURE 8: CROSS-CURRENCY PAYMENT VERSUS PAYMENT ("PVP") TRANSACTIONS



To initiate a PvP transaction, one of the commercial banks – Bank A in this example – creates a PvP agreement indicating the following:

- Sender's DLT address
- Sending currency and amount
- Expected currency and amount to receive in return
- Exchange rate used
- Payment date

The process is:

Step 1 → The Payment Master smart contract will generate a PvP reference for the agreement back to Bank A, and Bank A will need to convey the reference to Bank B out of band. Bank B can use the reference to retrieve and validate the agreement with the Payment Master.

Step 2 → Both Banks A and B will initiate respective PvP transaction legs each quoting the same PvP agreement reference. Both banks will preauthorize CBDC smart contracts for the Payment Master to debit their respective wallets for the specified amounts. On receipt of each leg, the Payment Master smart contract checks to ensure that there is sufficient CBDC tokens in the bank's wallet to debit.

Step 3 → When both legs are received and matched, the Payment Master instructs:

- CBDC EUR smart contract to transfer tokens from Bank A to Bank B
- CBDC SGD smart contract to transfer equivalent tokens from Bank B to Bank A

Both these transfers are executed atomically on the DLT. The banks can then query the CBDC smart contracts for their new token balances.

Destruction of the CBDC Tokens

At the end of the simulation, a process is initiated to ensure orderly removal of all CBDCs in circulation, and destruction of the CBDCs token supply. The process is:

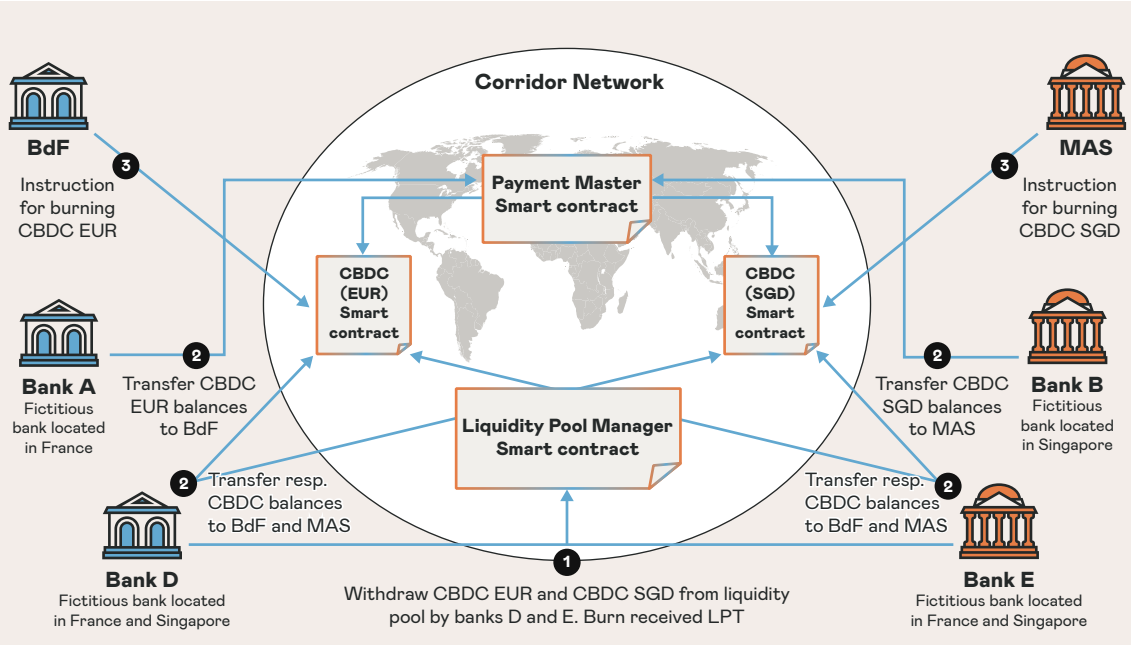
Step 1 → Bank D and Bank E withdraw their contributions from the LPM and receive the accrued exchange fees. The LPT balances of Bank D and Bank E will be reduced to zero as a result, and any LPT balances will be held by the LPM smart contract. The Consortium will instruct LPM to destroy the remaining LPT balance with its private key.

Step 2 → All banks will transfer their remaining CBDC balances back to the respective central banks.

Step 3 → Both central banks initiate destruction of all CBDC in circulation through the respective CBDC smart contracts.

These steps are shown schematically in Figure 9 below.

FIGURE 9: DESTRUCTION OF CBDC TOKENS



06 Lessons Learnt and Recommendations

Multilateral platforms may face technical, legal and regulatory barriers that may hinder their ability to function effectively and efficiently. This chapter discusses some of these barriers as well as recommendations to mitigate against these challenges. Some of these challenges may be addressed in a future phase of this project.

Visibility

Enhanced visibility of the movement of CBDC within the system reduces the dependence for participants to do post facto reporting. However, real time visibility has to be balanced with the need for a degree of privacy. The trade-offs between confidentiality and privacy on one hand and accountability and security on the other were successfully addressed in the simulation through a centralization approach at the application level, where the issuer needs to validate every transfer transaction initiated by a holder. While effective, such intervention of the issuer on the critical path of the transactions may not be the best approach since it puts the availability of the service sorely dependent on the Central Bank's node. This approach removes the decentralization advantage of the network architecture.

Other approaches may enforce transaction visibility by mandatorily including the issuer, or a supervisory party, in the transaction participants' list, effectively building a transaction repository that can be ex-post audited instead of being validated in real time. Additionally, zero-knowledge cryptographic proofs can also help with solving the confidentiality conundrum without compromising decentralization. Whichever solution is employed, there is great potential to improve CBDC circulation monitoring through DLT and shift from a reporting-based supervision to a real-time or almost real-time approach.

Interoperability & Standards/Rulebook

All participants, including the monetary authorities participating in a network dictated by this simulation must accept common terms of use that govern areas such as:

- Transaction finality and irrevocability
- AML/CFT obligations
- Operational requirements
- Minimum service level thresholds
- Investigations and problem resolution
- Transaction fees

Additionally, due consideration must be given to how such a network can integrate with domestic CBDC platforms. Another dimension to consider is how this network would interoperate with existing financial market infrastructure and payments networks.

FX

The use of automated market makers ("AMM") is a seemingly viable alternative to traditional order book infrastructures. AMMs allow permission-less and automatic ways of trading digital assets and use liquidity pools instead of a traditional market with buyers and sellers. However, it is important to consider risks of high slippage and impermanent losses in the use of such liquidity pools and ensure that mitigating measures are in place. The use of AMM, including a brief discussion on the Constant Product Market Marker formula, is covered in Appendix A.

Governance

An acceptable governance model must be established for a common multilateral settlement. Such a model will facilitate the decision-making process for eligibility and onboarding, given that the platform needs to remain open, equitable and inclusive for new participants. In order to ensure a smooth and uninterrupted functioning of the network, participants will need to demonstrate that they can meet a minimum technical standard for key management and cybersecurity controls.

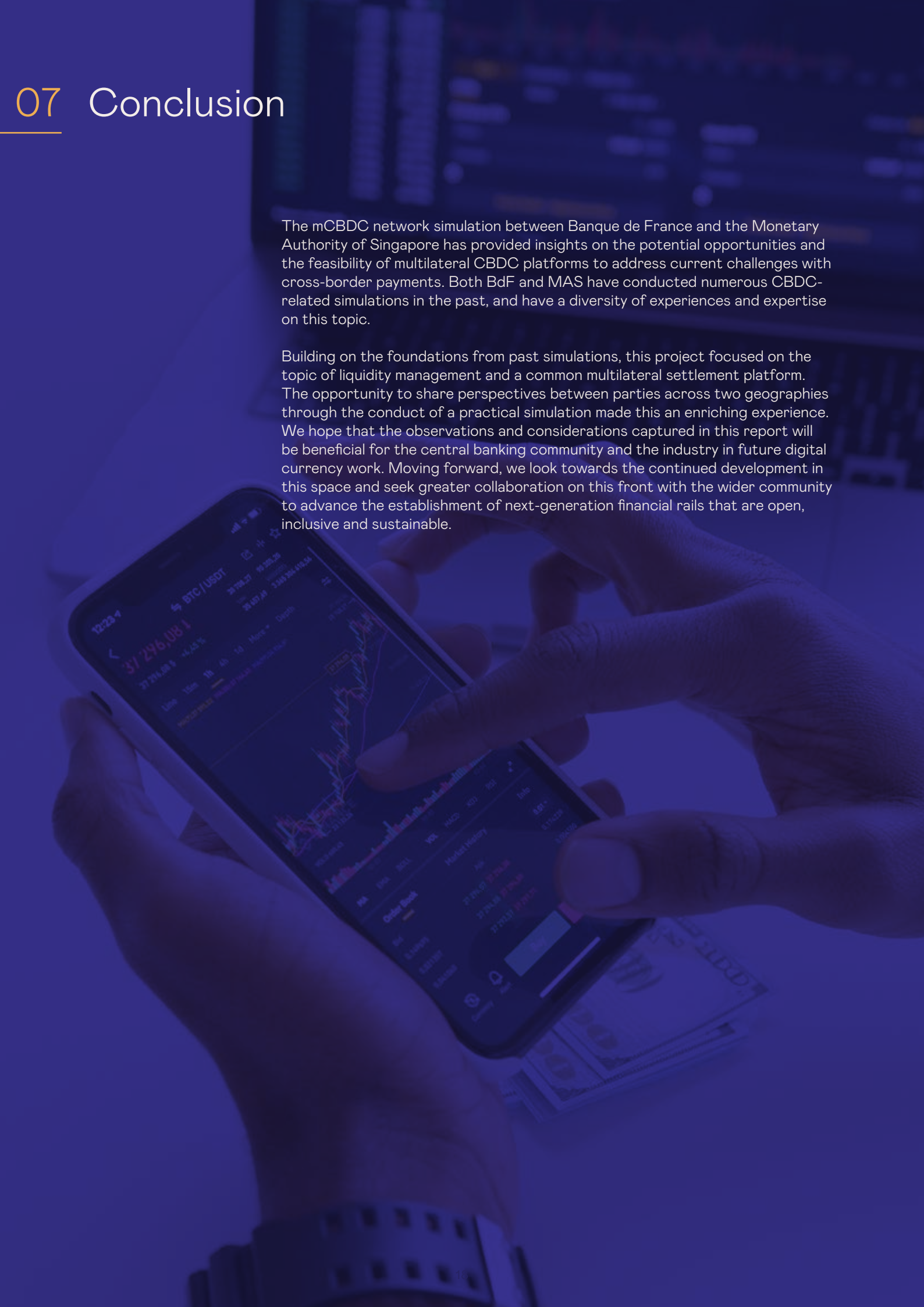
Contrary to domestic, or in some cases regional, platforms, there is no obvious party that is "naturally" entitled to operate such an international network, which can be seen as a common good of their participants. Confidentiality of operations, sovereignty considerations, the decision-making process for onboarding new members and post implementation maintenance matters would pose a significant challenge to operationalize this simulation.

These challenges remain unresolved and there are multilateral projects being conducted to explore various solutions to the governance challenges.

07 Conclusion

The mCBDC network simulation between Banque de France and the Monetary Authority of Singapore has provided insights on the potential opportunities and the feasibility of multilateral CBDC platforms to address current challenges with cross-border payments. Both BdF and MAS have conducted numerous CBDC-related simulations in the past, and have a diversity of experiences and expertise on this topic.

Building on the foundations from past simulations, this project focused on the topic of liquidity management and a common multilateral settlement platform. The opportunity to share perspectives between parties across two geographies through the conduct of a practical simulation made this an enriching experience. We hope that the observations and considerations captured in this report will be beneficial for the central banking community and the industry in future digital currency work. Moving forward, we look towards the continued development in this space and seek greater collaboration on this front with the wider community to advance the establishment of next-generation financial rails that are open, inclusive and sustainable.



08 Acknowledgements

Project Steering Committee

Name	Organization
Valérie Fasquelle	Banque de France
Claudine Hurman	Banque de France
Adeline Bachellerie	Banque de France
Sopnendu Mohanty	Monetary Authority of Singapore
Alan Lim	Monetary Authority of Singapore
Umar Farooq	JP Morgan Onyx
Naveen Mallela	JP Morgan Onyx

Project Management Team

Name	Organization
Khai Uy Pham	Banque de France
Alvinder Singh	Monetary Authority of Singapore
Arun Vignesh Muthiah (until July 2021)	Monetary Authority of Singapore
Lee Muh Hwa	JP Morgan Onyx

Project Working Group

Name	Organization
Monica D'Onofrio	Banque de France
Adrien Delcroix	Banque de France
Anne-Catherine Bohnert	Banque de France
Victor Budau	Banque de France
Florence Saint-Andre	Banque de France
Frederic Riera	Banque de France
Vincent Pek	Monetary Authority of Singapore
Amalraj Mani	JP Morgan Onyx
Hendrik Tan	JP Morgan Onyx
Hitanshi Thaman	JP Morgan Onyx
Sai Valiveti	JP Morgan Onyx

08 Appendix

Appendix A – Automated Market Maker

An automated market marker ("AMM") allows for permission-less and automatic ways of trading digital assets via liquidity pools, eliminating the need for centralized exchanged and related market-making techniques. Liquidity providers are involved in providing liquidity to the pool using a predetermined ratio of currency pairs. Several AMM formulas are utilized to cater to different currency tokens pricing strategies. This section discusses the Constant Product Market Maker formula, a strategy that is used in several decentralized finance exchange protocols because of its relative simplicity.

The Constant Product Market Marker formula is:

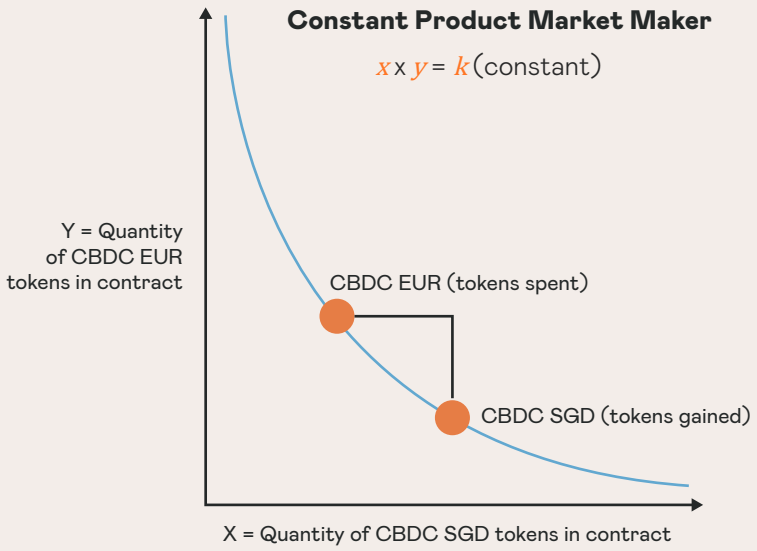
$$x \times y = k$$

where

x represents the value of currency A (EUR CBDC in our simulation),

y represents the value of currency B (SGD CBDC in our simulation), and

k is a constant.



For example, assume a liquidity pool is constituted as follows during its creation:

Let x = 1,500,000

Let y = 2,400,000 [1 SGD CBDC = 1.6 EUR CBDC]

Therefore, k = 1,500,000 × 2,400,000

= 3,600,000,000,000

In the Constant Product Market Marker approach, the value of k shall remain fixed at this constant value. An illustration of the working is as follows:

To swap for EUR CBDC, a participating bank must add SGD CBDC to the system.

Let y' be the amount of SGD CBDC that is added to the pool.

Therefore, total SGD CBDC in the pool is now $y + y'$.

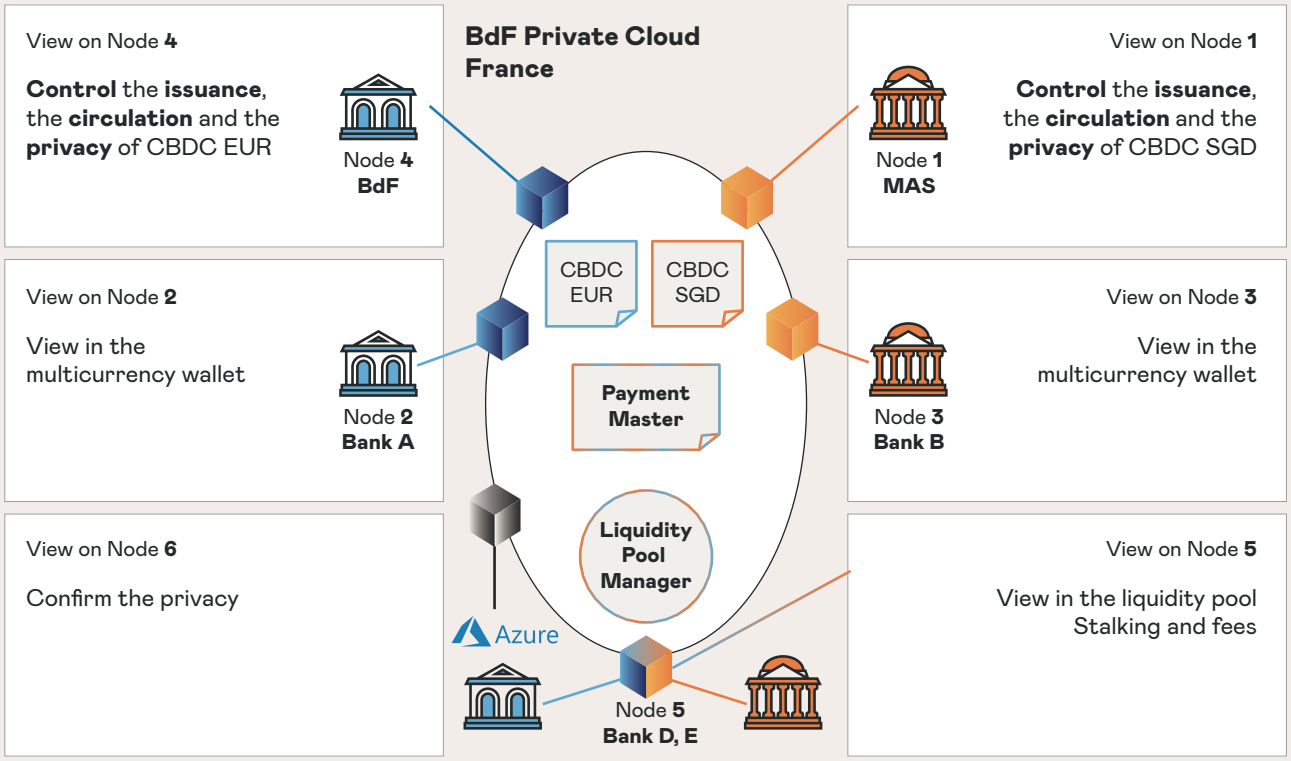
Hence, the total amount of EUR CBDC to be paid out, denoted as x' is given by the formula:

$$(x - x') \times (y + y') = k$$

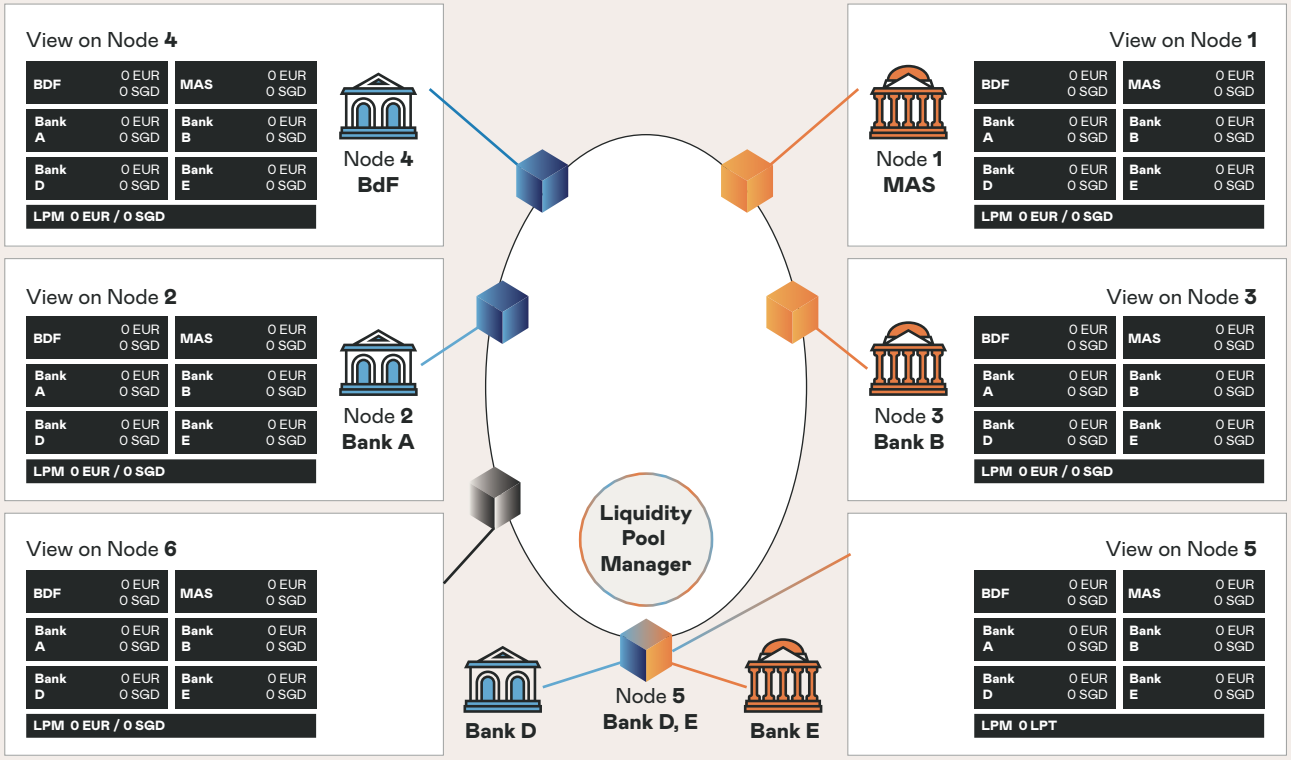
This approach may result in risks such as arbitrage, where the rate the currency is traded on the platform diverges from the established market rate. Other risks include impermanent loss when a liquidity provider might risk withdrawing less of the amount deposited in the pool should the price change significantly. These, and other risks, may be explored in subsequent phases of this simulation.

Appendix B – Simulation Playbook and Results

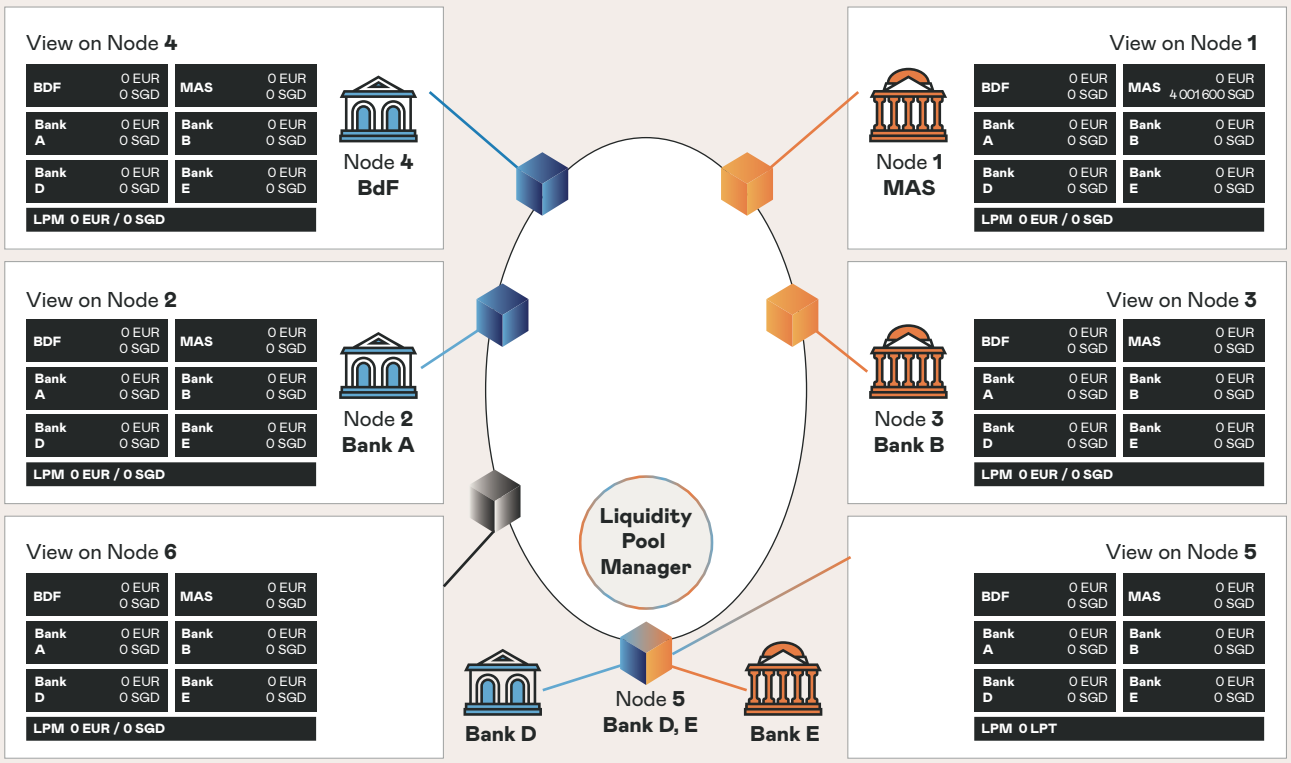
Prior to the execution of the of the simulation held on 30th June 2021, the network was set up with six nodes across the cloud providers and the smart contract up and running in the blockchain. For each step of the playbook, an extract of the view of balances from each node was performed and recorded. Due to the nature of private transactions, all nodes will not have the full view of all balances and they should be treated as relative positions arising from private transactions that the nodes are party to.



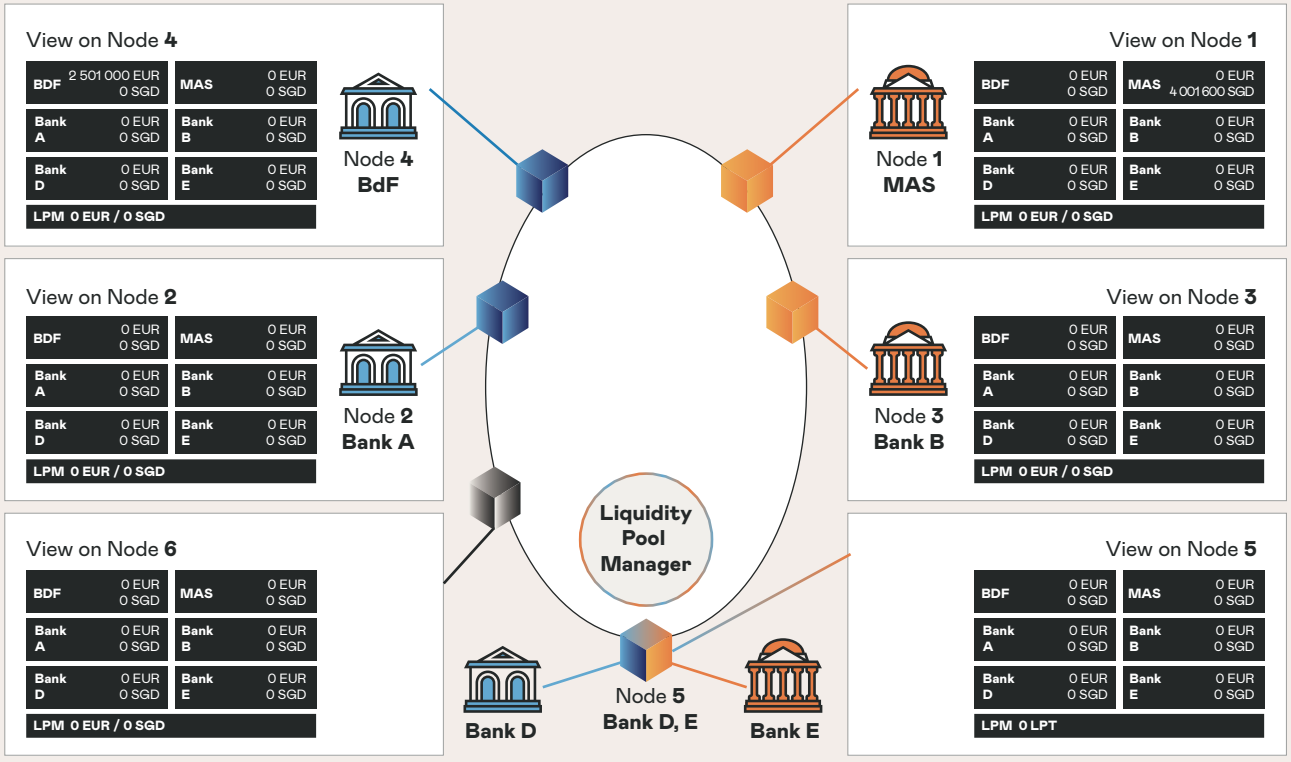
8.1.1 Initialize all CBDC balances to ensure all are zero as starting position



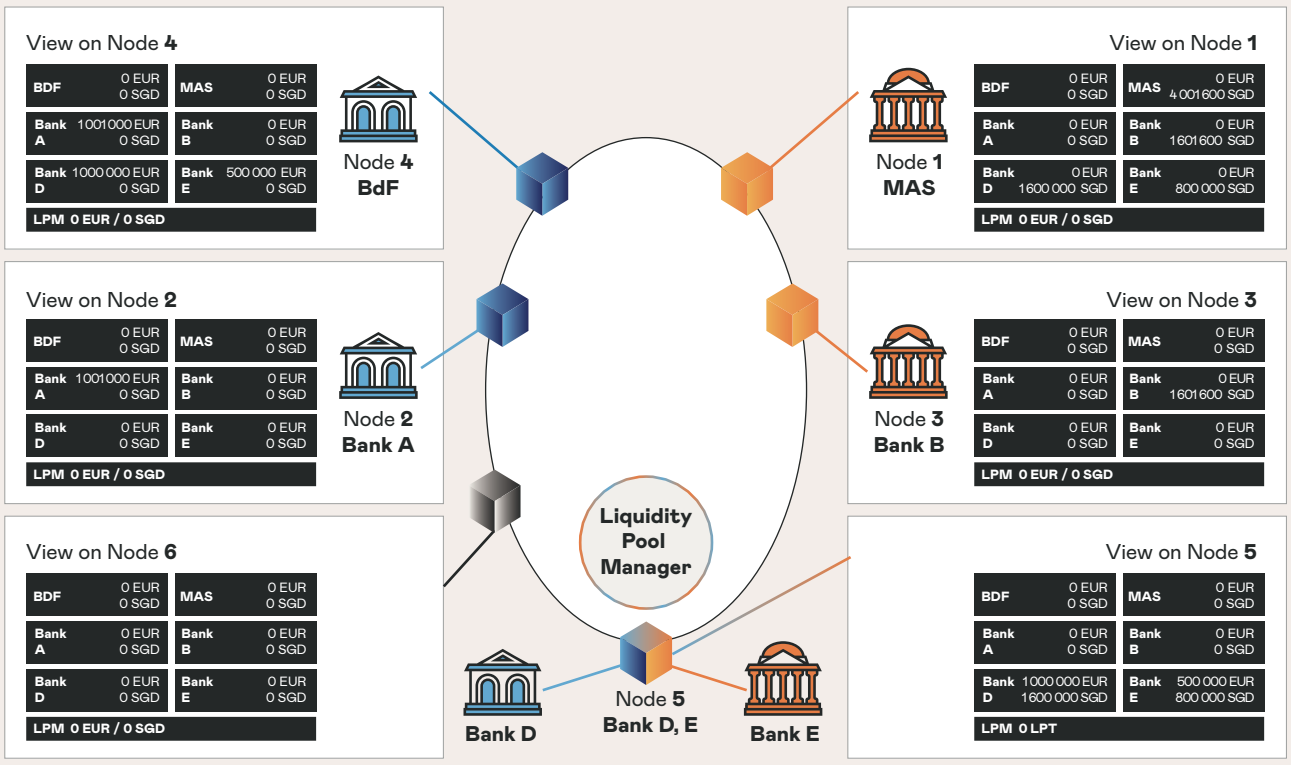
8.1.2 MAS issues CBDC SGD into the shared corridor network for circulation



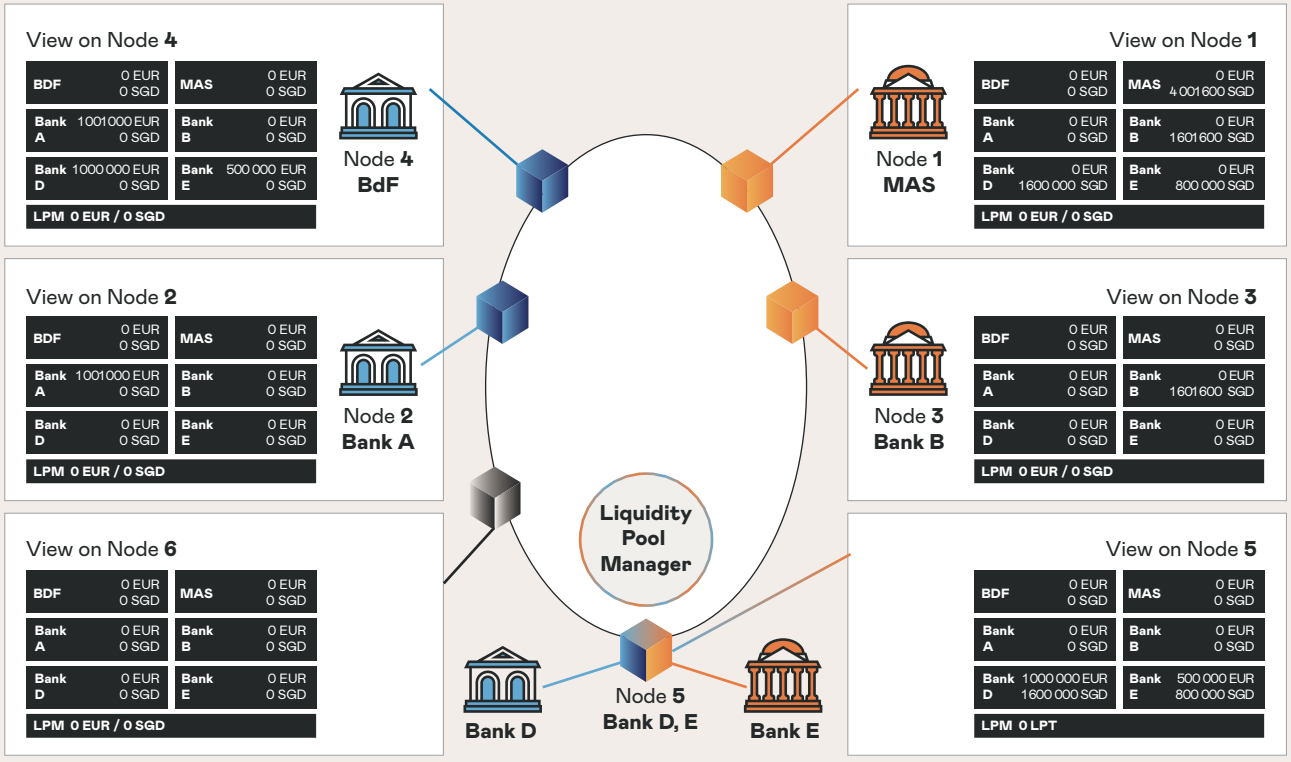
8.1.3 BdF issues CBDC EUR into the shared corridor network for circulation



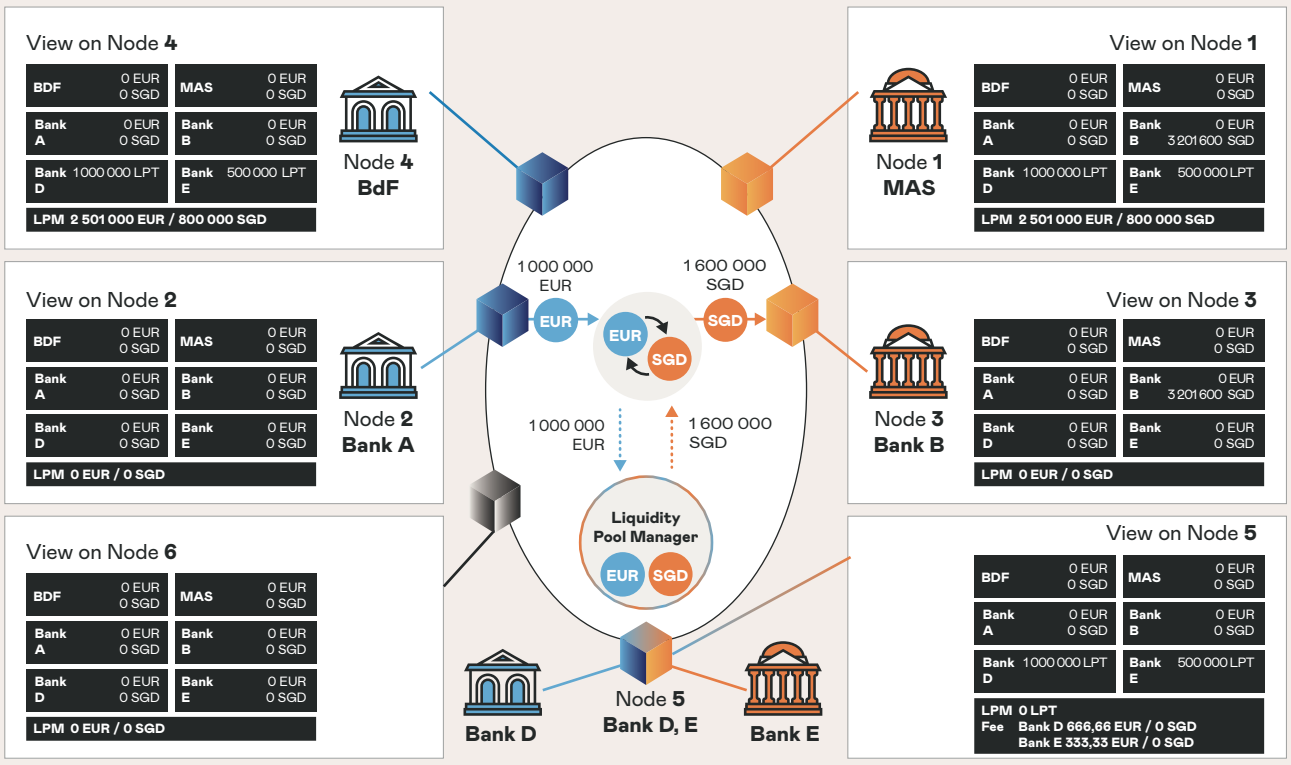
8.1.4 Banks A, B, D and E requests CBDC issuance to their respective wallets



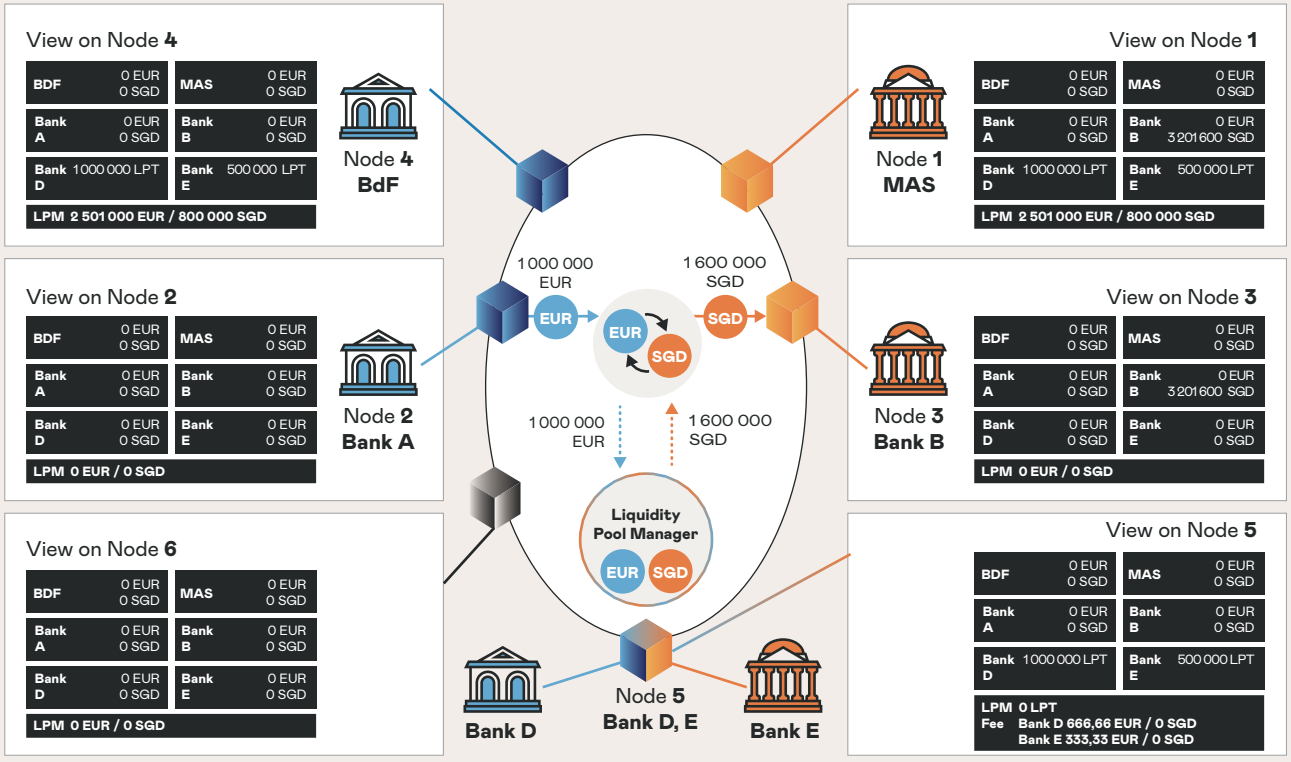
8.1.5 Banks D and E stake CBDCs to the Liquidity Pool



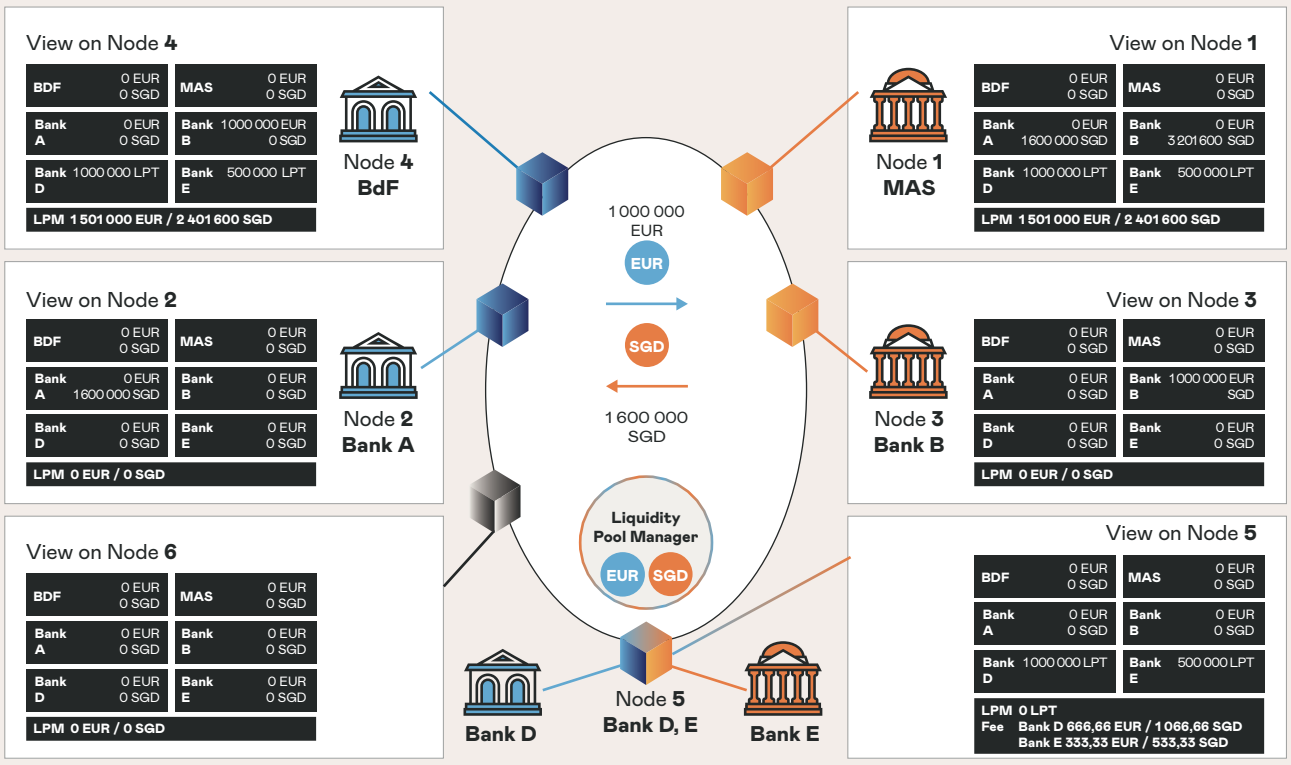
8.1.6 Bank A initiates cross-border payment to Bank B



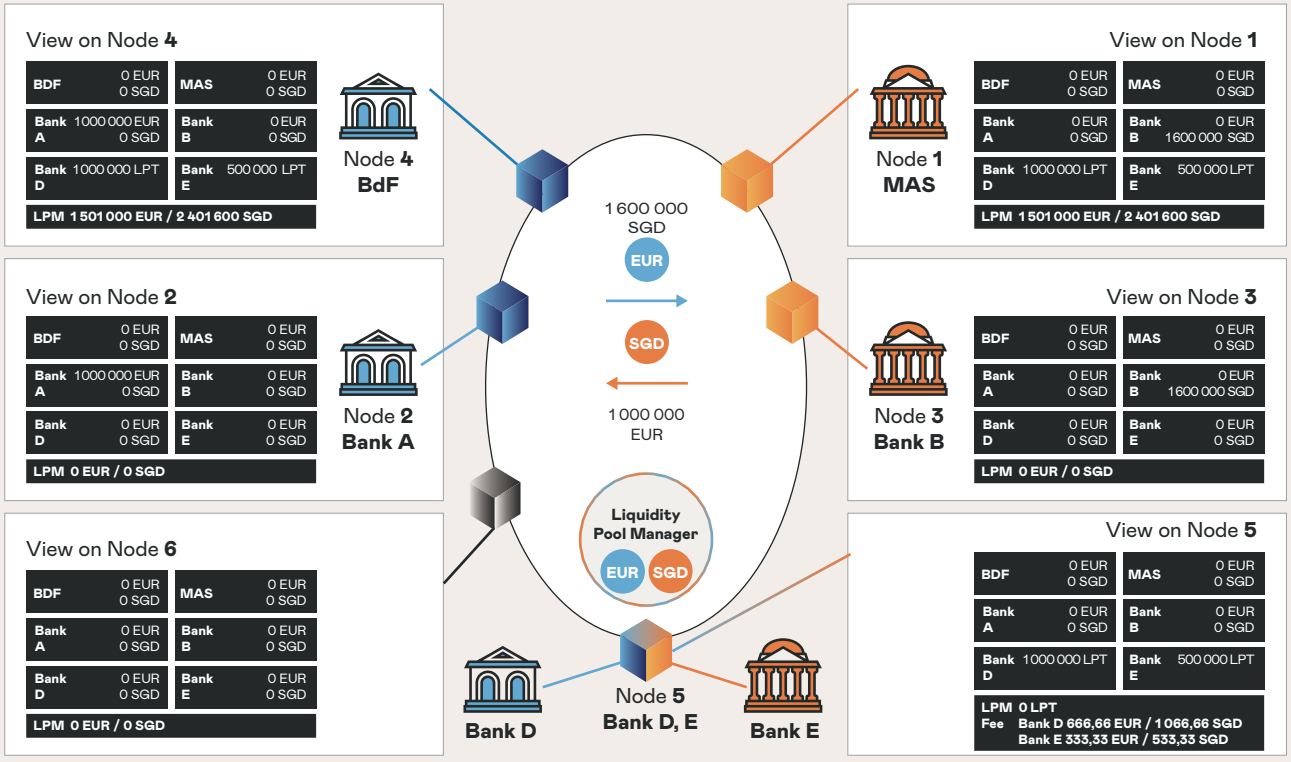
8.1.7 Bank B initiates cross-border payment to Bank A reversing the previous payment



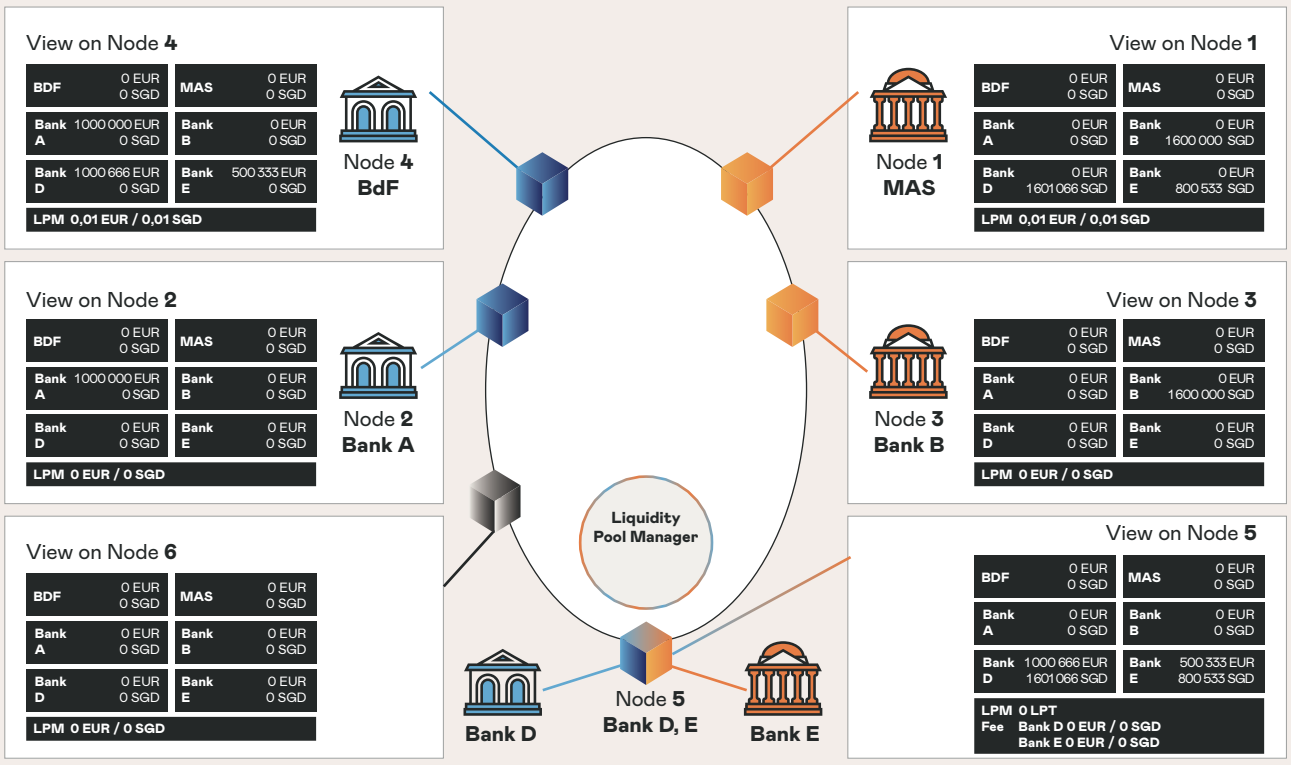
8.1.8 Banks A and B initiate corresponding legs of a PvP transaction for EUR/SGD



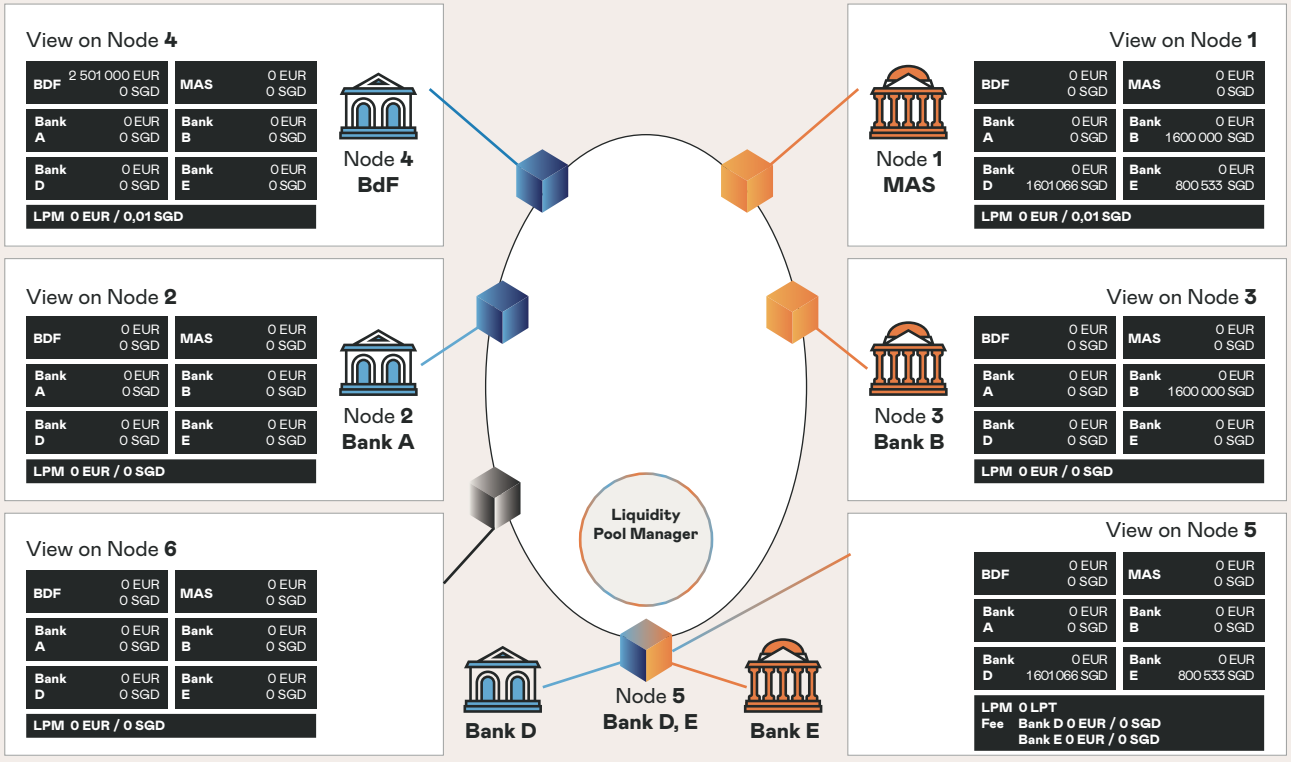
8.1.9 Banks A and B initiate corresponding legs of another PvP transaction for SGD/EUR in reverse



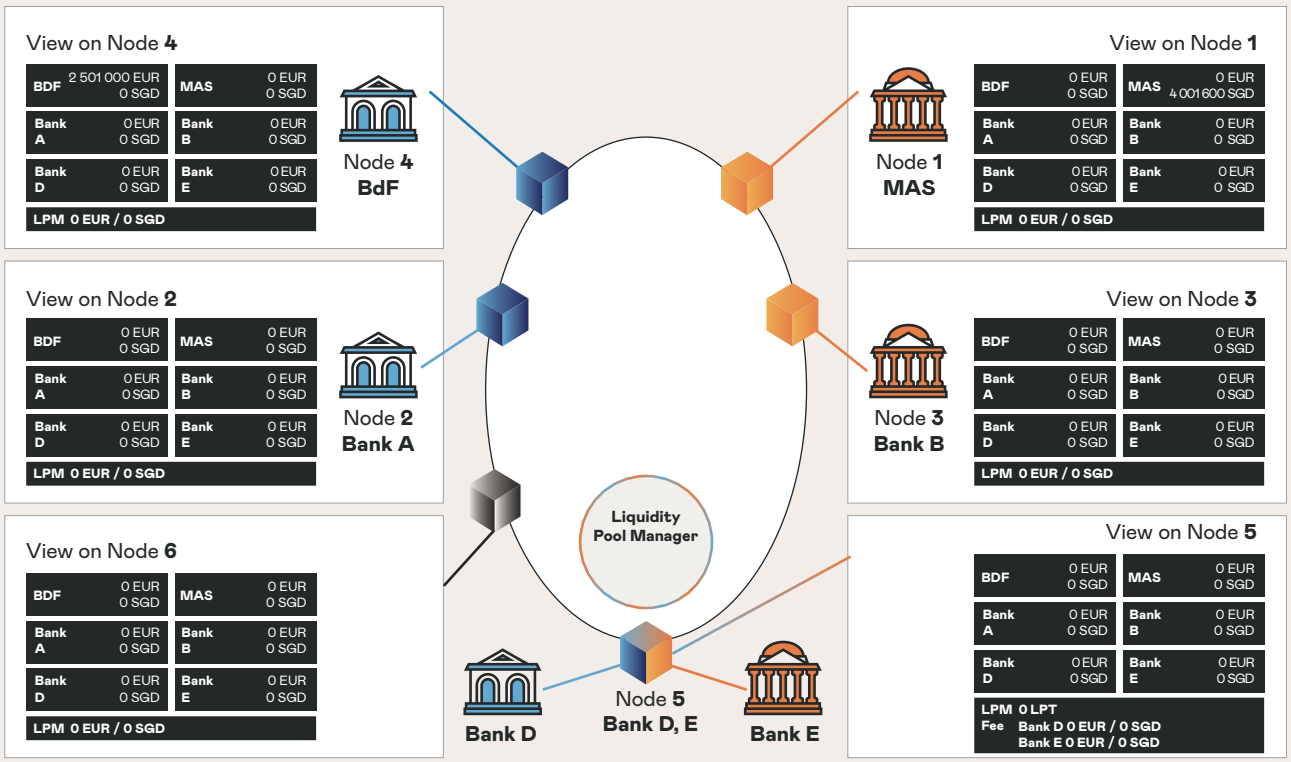
8.1.10 Banks D and E unstake fully from the Liquidity Pool



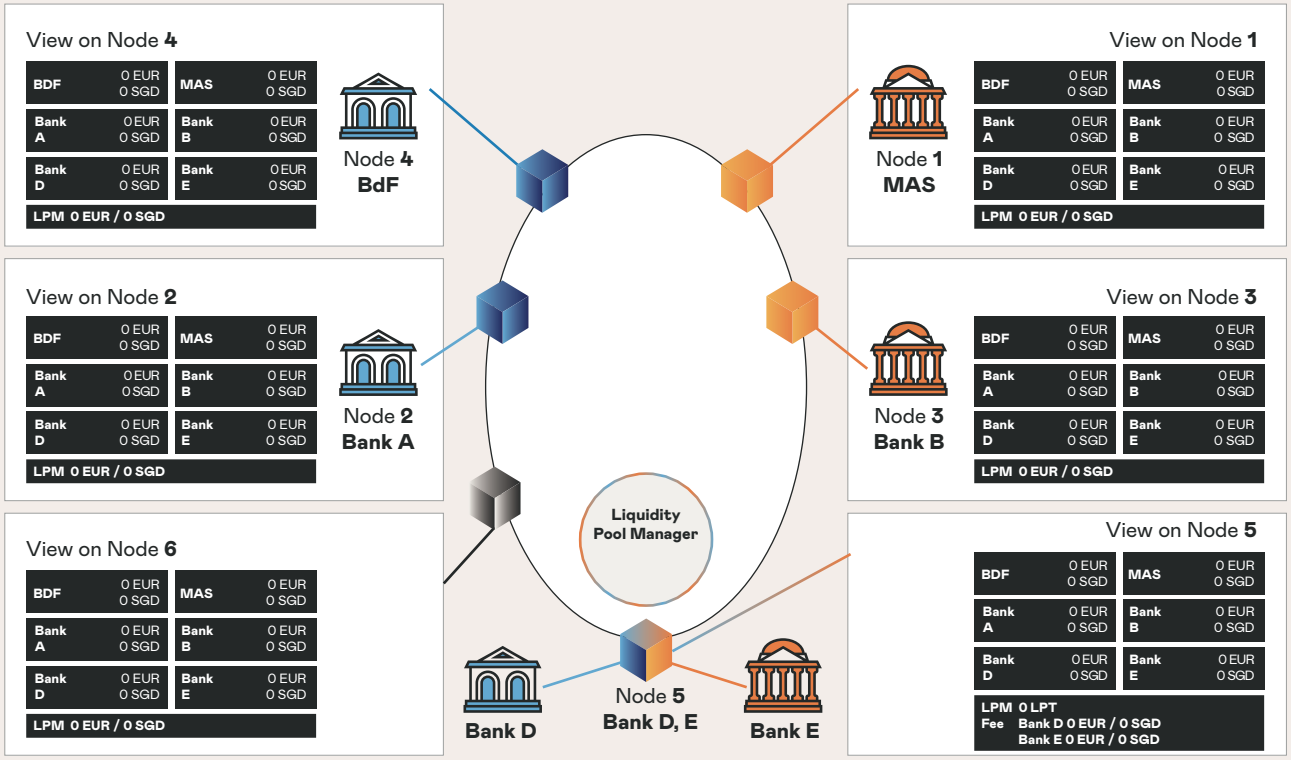
8.1.11 Banks A, B, D and E transfer back all CBDC EUR to BdF



8.1.12 Banks A, B, D and E transfer back all CBDC SGD to MAS



8.1.13 BdF and MAS destroys all CBDCs in circulation



This is the final step of the simulation playbook.

The analysis presented in this report aims at presenting key takeaways from the referenced mCBDC simulation amongst the Report Parties. It does not pre-empt any decisions nor commits the Eurosystem and MAS to provide CBDC, or J.P. Morgan to provide related services. The statements in this report are only working hypotheses. They are neither definitive nor binding for the Report Parties in any respect.

Certain information in this Report, or on which this Report is based, has been obtained from sources that the Report Parties believe to be reliable and accurate. However, such information has not been independently verified and no representation or warranty, express or implied, is made as to the accuracy or completeness of any information obtained from third parties. The information and conclusions are provided as at the date of this Report, the Report Parties undertake no obligation to update or revise any information or conclusions contained herein, whether as a result of new information, future events, or otherwise. The information and conclusions provided in this Report take no account of any relevant persons' individual circumstances, should not be taken as specific advice on the merits of any investment decision, product or service and should not be deemed to be a reasonably sufficient basis upon which to make an investment decision or undertake any product or service. This Report is not intended to provide, and should not be relied on for, accounting, legal or tax advice or investment recommendations. Please consult your own tax, legal, accounting or investment advisor concerning such matters The Report Parties and their respective affiliates accept no liability for any loss arising from any action taken or refrained from as a result of information and conclusions contained in this Report or any reports or sources of information referred to herein, or for any consequential, special or similar damages even if advised of the possibility of such damages.

This Report has been provided solely for information purposes and does not constitute a recommendation, advice or an offer or solicitation to buy or sell any securities or financial instruments or of any product or service. It should not be so construed, nor should it or any part of it form the basis of, or be relied on in connection with, any contract or commitment whatsoever. Further, this Report shall not be considered advice on the merits of acquiring or disposing of any particular investment or as an invitation or inducement to engage in any investment activity or other product or service.

J.P. Morgan is a marketing name for the payments business of JPMorgan Chase Bank, N.A. and its affiliates worldwide. JPMorgan Chase Bank, N.A., organized under the laws of U.S.A. with limited liability.

BANQUE DE FRANCE
EUROSYSTÈME

MAS
Monetary Authority of Singapore

onyx by J.P.Morgan