Project Simbolon

under the Memorandum of Understanding
between the Deutsche Bundesbank
and Monetary Authority of Singapore

Cross-Border FX Settlement Connectivity Across Independent Digital Infrastructures

Project Report











Table of Contents

Executive Summary **4**
Foreword **7**
1 Introduction & Motivation **12**
1.1 Challenges in Cross-Border FX Settlement 12
1.2 Lessons from Earlier Work 12
1.3 Problem Statement, Objectives and Approach 14
1.4 Project Setup and Scope 15
2 Use Cases and Relevance **17**
2.1 Use Case 1: Overnight EUR/SGD PvP for T+1 securities funding 17
2.2 Use Case 2: Intraday EUR/SGD FX swap to bridge an SGD shortfall 20
3 Proof-of-Concept Setup, Testing & Validation **23**
3.1 Setup and Scope of Experimentation 23
3.2 Settlement Logic: Atomic PvP via ZK proofs 24
3.3 Scenarios covered and test results 28
4 Key Findings from Technical Proof-of-Concept **30**
Finding 1: Atomic PvP settlement can be coordinated across independent ledgers 30
Finding 2: Proof generation was the main contributor to settlement time 30
Finding 3: Finality is not solely determined by the technical design of the ledger 30
Finding 4: The proof-based approach retains key operational dependencies 31
5 Conclusion and Next Steps **33**
5.1 Summary of Insights 33
5.2 Areas for Further Research 33
1: Complementing common platforms 33
2: Assessing alternative operating models 34
3: Improving settlement performance 34
4: Establishing legal settlement finality 34
5: Exploring applications beyond FX PvP 35
6: Leveraging a common technology base 35
Appendix A Survey of Prior Experiments **37**
Appendix B Technical Appendix: Experiment Set-up, Testing and Validation **41**
B.1 Message Transport and Verification 41
B.2 The Two Logical Proofs by Source Ledger 43
B.3 Proof Programs 43
B.4 Three-Ledger Design and Trust Boundaries 44

B.5 Settlement State Machine, Timeouts and Edge Cases 46
B.6 Scope and Test Environment 48
B.7 What Drives Settlement Time 50
B.8 Scalability 50
B.9 Verification across multiple networks 51
Appendix C Settlement Finality and Scheme Considerations 54
C.1 Finality in the Proof-Based Settlement Model 54
C.2 Illustrative Arrangements for Establishing End-to-End Finality 56
C.3 Risks in a Future Settlement Arrangement 57
Appendix D Considerations for Further Development 60
Liquidity, Accounts and Wallet Arrangements 60
Systems Integration and Operational Visibility 60
Treasury, Liquidity and Funding Operations 61
Client and Market Benefits 61
Legal, Regulatory and Prudential Considerations 61
Operational Resilience and Recovery 61
Appendix E Limitations 64
Appendix F Glossary of Terms 67
References 71

List of Figures

Figure 1: Use Case 1: T+1 securities funding through overnight EUR/SGD PvP 19
Figure 2: Use Case 2: Intraday EUR/SGD FX swap to bridge an SGD shortfall 20
Figure 3: High-level solution architecture 25
Figure 4: Component architecture and settlement flow 42
Figure 5: ZK proof model by source ledger 43

List of Tables

Table 1: Ledgers and roles 24
Table 2: Test Scenarios 28
Table 3: Selected prior experiments and their settlement models 37
Table 4: ZK proof relay paths 42
Table 5: Ledgers and their roles 44
Table 6: Verification and trust boundaries 45
Table 7: Settlement state machine 46
Table 8: Test environment configuration 49
Table 9: Illustrative, untested scalability scenarios 51
Table 10: Technical and legal elements of finality 55
Table 11: Key risks in a future settlement arrangement 57

Executive Summary

Cross-border foreign exchange (FX) settlement takes place across currencies, jurisdictions and financial infrastructures with different operating hours and settlement arrangements. Payment-versus-payment (PvP) arrangements reduce settlement risk by making final settlement of one currency conditional on settlement of the other, but existing arrangements do not cover all currencies, participants or transaction types. The need for more efficient cross-border settlement is becoming more pronounced as shorter securities settlement cycles compress the time available for FX execution, settlement and liquidity mobilisation, particularly across time zones, while differences in operating hours can create funding and liquidity gaps.

Under Project Simbolon, the Deutsche Bundesbank (Bundesbank) and Monetary Authority of Singapore (MAS), together with DBS and Deutsche Bank (DB) as participating commercial banks and Partior as their technology provider, set out to test whether zero-knowledge (ZK) proofs could support atomic PvP settlement using wholesale central bank digital currencies (CBDCs) across independent distributed ledger technology (DLT)-based settlement environments, without requiring a shared ledger or direct technical integration between the central bank ledgers.[1] Supporting atomic PvP settlement across independent settlement infrastructures could strengthen the financial connectivity underpinning trade and investment flows between Singapore and Germany.

The proof-of-concept simulated the PvP settlement of EUR/SGD FX transactions using wholesale CBDCs across the respective central banks' DLT-based test environments. Following the matching of settlement instructions, simulated EUR and SGD wholesale CBDC tokens were conditionally locked on their respective infrastructures. ZK proofs were generated from the relevant settlement state of each test environment, allowing the corresponding settlement environment to verify that the required conditions had been met before proceeding with settlement. This enabled the two settlement legs to reach a common settlement outcome without requiring the ledgers to connect directly.

The project also considered how these capabilities could apply to practical cross-border capital-market and liquidity needs. Two illustrative use cases examined securities-related funding across time zones and intraday liquidity management, exploring how financial institutions could obtain and deploy cross-currency liquidity closer

1 Unless otherwise stated, references to central bank ledgers and wholesale CBDC test environments in this report refer to the technical setup developed specifically for this proof-of-concept.

to when it is required while settling the corresponding FX transactions on a PvP basis. These use cases illustrate the potential business applications of the capabilities tested. Further work would be required to validate their commercial benefits.

Key findings

- **Atomic PvP settlement across independent DLT-based test environments.** The experiment demonstrated that two wholesale CBDC settlement legs could be coordinated across separate central bank test environments while maintaining a single settlement outcome.
- **Proof generation was the main contributor to settlement time.** In the test environment, the generation of ZK proofs accounted for most of the end-to-end settlement time. Optimising proof generation could materially reduce settlement time in future implementations.
- **Finality is not solely determined by the technical design of the ledger.** The basis for determining finality on each ledger also depends on the requirements of each central bank. Any future implementation would need to establish how the settlement outcome is recognised as final under the applicable legal frameworks.
- **The proof-based approach retains key operational dependencies.** Relayers and provers remain necessary to generate and transmit proofs, while proof generation depends on access to relevant ledger data. Any future implementation would require appropriate governance and operating arrangements for these functions and data access.

The proof-of-concept was conducted in test environments with simulated wholesale CBDC tokens. It does not establish legal settlement finality, production readiness or production-scale performance.

The report sets out the business problem and illustrative use cases, the technical solution, proof-of-concept testing undertaken and key findings. It concludes with identifying areas for further exploration in subsequent phases of the collaboration.

Foreword

Foreword

Germany and Singapore are major financial centres connecting markets in Asia and Europe. Financial institutions operating across these markets support trade, investment, treasury and securities activity across currencies, infrastructures and time zones. As market operating hours extend and settlement cycles shorten, the ability to complete cross-border transactions with certainty and to mobilise liquidity when and where it is needed is becoming increasingly important.

Against this backdrop, the objective is not simply to move money faster. It is to provide greater certainty in settlement, manage settlement risk effectively and enable liquidity to be positioned more precisely across markets and time zones. More effective cross-border settlement arrangements could help financial institutions reduce the frictions arising from differences in operating hours and settlement timelines, while supporting the financial flows underpinning trade and investment between Germany and Singapore.

Delivering these outcomes requires interoperability across a global financial system comprising different forms of money, technologies and institutional arrangements. Central bank settlement systems, commercial bank liquidity and other financial market infrastructures will not necessarily develop on a common architecture or under a single rulebook. Interoperability will therefore be important to enable transactions to take place across these infrastructures while accommodating their different rules, liquidity and operating models.

Project Simbolon is a proof-of-concept jointly conducted by the Deutsche Bundesbank, the Monetary Authority of Singapore, DBS, Deutsche Bank, and Partior. The project has combined the perspectives of central banks responsible for settlement infrastructures, commercial banks managing foreign-exchange settlement and liquidity, and a technology provider supporting the experiment. This allowed the project to assess the technical feasibility of the settlement arrangement alongside the practical requirements of financial institutions operating across markets.

The name Simbolon draws on the ancient Greek word “Symbolon”, a token of recognition formed by two matching pieces. The analogy reflects the project’s use of cryptographic proofs to verify and enable the coordination of the two settlement legs across independent central bank ledgers.

We thank the teams from Deutsche Bundesbank, MAS, Deutsche Bank, DBS and Partior for the expertise and commitment they brought to this work.

Deutsche Bundesbank

"This joint work successfully explored a pathway to achieving greater efficiency in payment and settlement processes, as well as more precise liquidity management across currencies and time zones. This effort was made possible by bringing together the expertise of central banks, commercial banks and technology providers. It paves the way for eliminating settlement risk in global foreign exchange transactions. At its core, this initiative is about leveraging purposeful innovation for a strong financial system and more liquid markets. We extend our gratitude to our partners and all colleagues involved for their expertise, commitment and close collaboration in making Project Simbolon a success."

Dr. Sabine Mauderer
First Deputy Governor, Deutsche Bundesbank

Monetary Authority of Singapore

"Bringing together public and private sector perspectives, we examined how new settlement arrangements could better serve financial institutions operating across markets and time zones. Through this collaboration, we aim to strengthen settlement connectivity between Singapore and Germany in ways that better support cross-border financial and real economy flows. We are grateful to all project partners for their contributions towards making this publication possible."

Leong Sing Chiong
Deputy Managing Director, Monetary Authority of Singapore

DBS Bank

"As money and assets move on-chain, liquidity must keep pace with markets that operate around the clock. This collaboration with MAS, the Deutsche Bundesbank and our industry partners enables seamless access to on-demand funding across time zones and currencies, while expanding our digital asset ecosystem. Ultimately, harmonising traditional and on-chain market infrastructures underscores our commitment to purposeful innovation and building a more resilient global financial ecosystem. This will enable us to deliver tangible, long-term value to our clients."

Jacky Tai
Deputy Head of Global Financial Markets, DBS Bank

Deutsche Bank

"The significance of this collaboration goes beyond connecting two ledgers. It is about how we can strengthen the financial connection between Singapore and Germany and support clients operating across Asia and Europe. Together, we have explored a potential route towards new payment and settlement efficiency and more precise use of liquidity across currencies and time zones. I am grateful to Deutsche Bundesbank, Monetary Authority of Singapore, DBS and Partior, and to the colleagues across our organisations who brought their expertise to this work. Ultimately, this is about applying innovation with purpose: strengthening the financial system and creating lasting value for clients and markets."

Gerald Podobnik
Co-Head of Corporate Bank, Deutsche Bank

Partior

"For over two decades, multilateral net PvP settlement has substantially reduced systemic risk and increased liquidity efficiency in global FX markets. The task now is to extend those trusted PvP principles to a world of many ledgers, making settlement across them as safe as settlement within them. This project demonstrated how the independent Deutsche Bundesbank and MAS DLT-based settlement environments could each participate in a orchestration protocol through ZK proof verification to solve intraday FX use cases, without bilateral integration or a shared ledger. This points to a network of digital networks, anchored in central-bank money and regulated financial market infrastructures, that extends PvP protection to new settlement windows, currencies and forms of money. It complements existing arrangements and, for banks like Deutsche Bank and DBS, unlocks the next frontier of liquidity efficiency: global, just-in-time liquidity."

Humphrey Valenbreder
Chief Executive Officer, Partior

Chapter 1

Introduction & Motivation

1 Introduction & Motivation

1.1 Challenges in Cross-Border FX Settlement

Cross-border FX settlement remains fragmented across jurisdictions and financial infrastructures. Different legal frameworks, reliance on correspondent banking chains, and differences in operating hours and settlement calendars continue to create processing delays and funding uncertainty before final settlement.[2] Cross-border FX transactions can also leave parties exposed to settlement risk, where one party delivers the currency it sold but does not receive the currency it bought.[3]

PvP arrangements such as Continuous Linked Settlement (CLS) mitigate settlement risk by making settlement of one currency conditional on settlement of the other. Existing arrangements, however, do not cover all currencies, participants or transaction types.[4] Neither do they cover all the prescribed currencies in full.

These gaps are becoming more consequential as securities settlement cycles shorten across multiple jurisdictions with more countries exploring or bringing in shorter settlement timelines. Under a T+1 cycle, post-trade activities that were previously completed over two business days must be completed within a compressed timeframe.[5] Where a cross-border securities transaction requires an associated FX transaction, investors and intermediaries may have less time to execute and settle the FX transaction and mobilise the required settlement currency, particularly across markets in different time zones. The challenge is to obtain and position the required settlement currency within the applicable timeframe while settling the associated FX transaction on a PvP basis.

1.2 Lessons from Earlier Work

Earlier central bank experiments have examined different approaches to atomic cross-border settlement using wholesale CBDC, RTGS and DLT-based infrastructures.[6] For the purposes of this report, we distinguish between two broad approaches: common platforms, where settlement assets and transaction processes are brought onto a single shared infrastructure; and interlinking arrangements,

2 CPMI 2022
3 BIS 2022
4 CPMI 2023
5 DTCC 2024 and GFXC 2025
6 CPMI et al 2022

which coordinate settlement across separate ledgers through a bilateral link, a bridge or a coordinating hub.[7]

Common platform designs have been tested in projects such as mBridge, which placed participating currencies on a shared ledger governed by a common rulebook[8], Dunbar, which experimented with a multi-CBDC common platform for cross-border payments[9], and Agorá, which keeps central bank money on jurisdictional ledgers while bringing commercial bank money and settlement logic together on a shared platform.[10] These models require participating institutions to agree on the governance, rules, access arrangements and operating model for the shared infrastructure. Depending on the design and governance of the platform, this could constrain the extent to which each central bank can retain its own rules and technical development path.

Interlinking arrangements have taken different forms. Project Jasper-Ubin explored atomic cross-border transfers across separate DLT networks using hashed time-locked contracts.[11] Project Mariana used bridges to transfer simulated wholesale CBDCs from domestic networks to a transnational network hosting an automated market-maker for FX trading and settlement.[12] Project Meridian FX tested a synchronisation operator that coordinated PvP settlement across RTGS systems and between RTGS and DLT-based settlement environments.[13]

Interlinking arrangements preserve the autonomy of the underlying ledgers, but each ledger still requires assurance that the conditions for settlement have been met before acting. Earlier projects addressed this through different protocol, bridge and synchronisation arrangements.

Project Simbolon examined whether cryptographic verification could provide such assurance for settlement condition fulfilment, without requiring a direct bilateral link between the two central bank ledgers, thereby adopting an interlinking approach instead of a common platform approach.

---

7 CPMI et al 2022. The three options for interoperability of CBDC systems were set out in the joint report to the G20 by the BIS Committee on Payments and Market Infrastructures, the BIS Innovation Hub, the International Monetary Fund and the World Bank. These were the compatible model, where individual CBDC systems use common standards to reduce the operational burden on PSPs for participating in multiple systems; the interlinked model, where CBDC systems are linked with a set of technical and contractual agreements; and the single system model, where different CBDCs use a single common technical infrastructure and potentially a common rulebook. The latter two models have been referenced in this report.
8 BIS Innovation Hub 2024a
9 BIS 2022
10 BIS Innovation Hub 2026
11 Bank of Canada and Monetary Authority of Singapore 2019
12 BIS Innovation Hub 2023
13 BIS Innovation Hub 2025

1.3 Problem Statement, Objectives and Approach

Project Simbolon is a joint proof-of-concept involving Deutsche Bundesbank, MAS, Deutsche Bank, DBS and Partior. Building on earlier work, the project examined whether cryptographic verification could support atomic EUR/SGD PvP settlement using wholesale CBDCs across independently operated DLT-based settlement environments, while allowing each central bank to retain control of its own settlement infrastructure, currency and acceptance rules.

Problem Statement

How can EUR and SGD be settled safely across separate central bank systems and different operating hours, while ensuring that one currency is paid only if the other is received?

Project Simbolon examined whether ZK proofs could support this outcome across independently operated central bank DLT environments, without requiring a shared ledger or direct bilateral link between the two ledgers.

The project considered three related dimensions:

1. the technical feasibility of atomic PvP settlement across independently operated DLT-based settlement environments;
2. the implications of accelerated securities settlement and extended operating hours for funding, intraday liquidity and treasury operations; and
3. the legal, governance and operational considerations relevant to any potential future implementation.

Under the approach tested, simulated EUR and SGD wholesale CBDC tokens remained within their respective central bank test environments. Following the matching of settlement instructions, each currency leg was conditionally locked on its respective central bank ledger. Cryptographic proofs enabled the coordination layer to verify that both legs had been locked before recording whether settlement should proceed. Each central bank ledger then verified proof of that decision before releasing or refunding its respective leg.

Atomicity was supported by the overall settlement process, combining matching, conditional locking, orchestration and cryptographic verification. The detailed settlement model and proof mechanics are set out in Section 3.

1.4 Project Setup and Scope

This project was established under the Memorandum of Understanding signed by Deutsche Bundesbank and the Monetary Authority of Singapore at the Singapore FinTech Festival in November 2025, under which both institutions agreed to collaborate on new settlement solutions for cross-border transfers and on common standards for tokenised assets.[14]

Deutsche Bundesbank and MAS operated the central bank test environments while Deutsche Bank and DBS contributed their business perspectives as participating commercial banks. Partior provided the technology for the coordination layer and operated the orchestration, relayer and prover services used in the proof-of-concept.

The project ran for twelve weeks, from 10 August to 30 October 2026, across three test environments. It used simulated tokens and did not involve production systems or real money. Legal settlement finality and legal enforceability were outside the scope of the experiment.

The experiment demonstrated the technical feasibility of atomic EUR/SGD PvP settlement across independent central bank ledgers, with each ledger verifying the relevant cryptographic proofs before releasing or refunding its respective settlement leg.

The remainder of this report is structured as follows. Section 2 presents two illustrative use cases. Section 3 describes the proof-of-concept, its scope and the test results. Section 4 sets out the key technical findings. Section 5 presents the conclusions and identifies areas for further examination.

14 MAS 2025. "MAS and Deutsche Bundesbank sign MoU on tokenisation and cross-border settlement". November 13, 2025.

Chapter 2

Use Cases and Relevance

2 Use Cases and Relevance

Project Simbolon considered two illustrative use cases to examine how the settlement approach tested could support the cross-border funding and liquidity needs of financial institutions operating across different markets and time zones. Although FX markets operate across time zones, liquidity conditions and settlement windows vary throughout the operating day. The timing of settlement can therefore affect when financial institutions need to source, position and commit liquidity.

Section 2.1 considers overnight EUR/SGD PvP settlement in support of a potential future T+1 securities-funding journey. Section 2.2 considers an intraday EUR/SGD FX swap used to meet a temporary SGD liquidity need. The two use cases examine cross-currency liquidity needs over different time horizons while providing for the corresponding FX transactions to be settled on a PvP basis.

The use cases are illustrative. The proof-of-concept tested the interbank EUR/SGD PvP settlement component and did not assess the use cases as complete production, commercial or regulatory propositions.

2.1 Use Case 1: Overnight EUR/SGD PvP for T+1 securities funding

Business challenge: A European institutional investor purchasing Singapore-listed securities under a potential future T+1 securities settlement cycle would need to obtain and position SGD in time to meet its settlement obligation. The investment decision may be made in Europe, while trade execution, FX conversion, cash funding, local custody, reporting and securities settlement take place across multiple intermediaries and time zones.

Under a T+1 securities settlement cycle, post-trade activities previously conducted over two business days would need to be completed within a compressed timeframe. This could leave a narrow window to execute and settle the associated EUR/SGD FX transaction and make the SGD available for securities settlement. Depending on their arrangements, investors and intermediaries may therefore need to rely on earlier pre-funding, correspondent balances, intraday credit or operational buffers to manage the timing difference.

Potential commercial approach: The settlement approach addresses this timing challenge by allowing the EUR/SGD transaction to settle across different operating windows, so that SGD could be committed closer to when it is needed for securities settlement. The underlying FX transaction would continue to be agreed and executed through existing processes. The coordination layer would ensure the PvP settlement of the EUR and SGD payments on the Deutsche Bundesbank and MAS ledgers so that either both payments settle or neither does.

Figure 1 shows how this could work within a potential future T+1 securities-funding journey, focusing on the interbank EUR/SGD settlement that supports the subsequent securities settlement. Following the matching of the FX settlement instructions, the corresponding EUR and SGD funds would be conditionally locked on the respective ledgers. Cryptographic proofs would enable the coordination layer to verify that both currency legs had been locked before determining whether PvP settlement should proceed. Each central bank ledger would then verify proof of that decision before releasing or refunding its respective currency leg. Each currency would remain on its respective central bank ledger throughout.

The timings shown in Figure 1 are illustrative and assume that the securities allocation is confirmed after the assumed end of the MAS ledger's operating window on the trade date. The settlement model and underlying technology are described in more detail in Section 3.

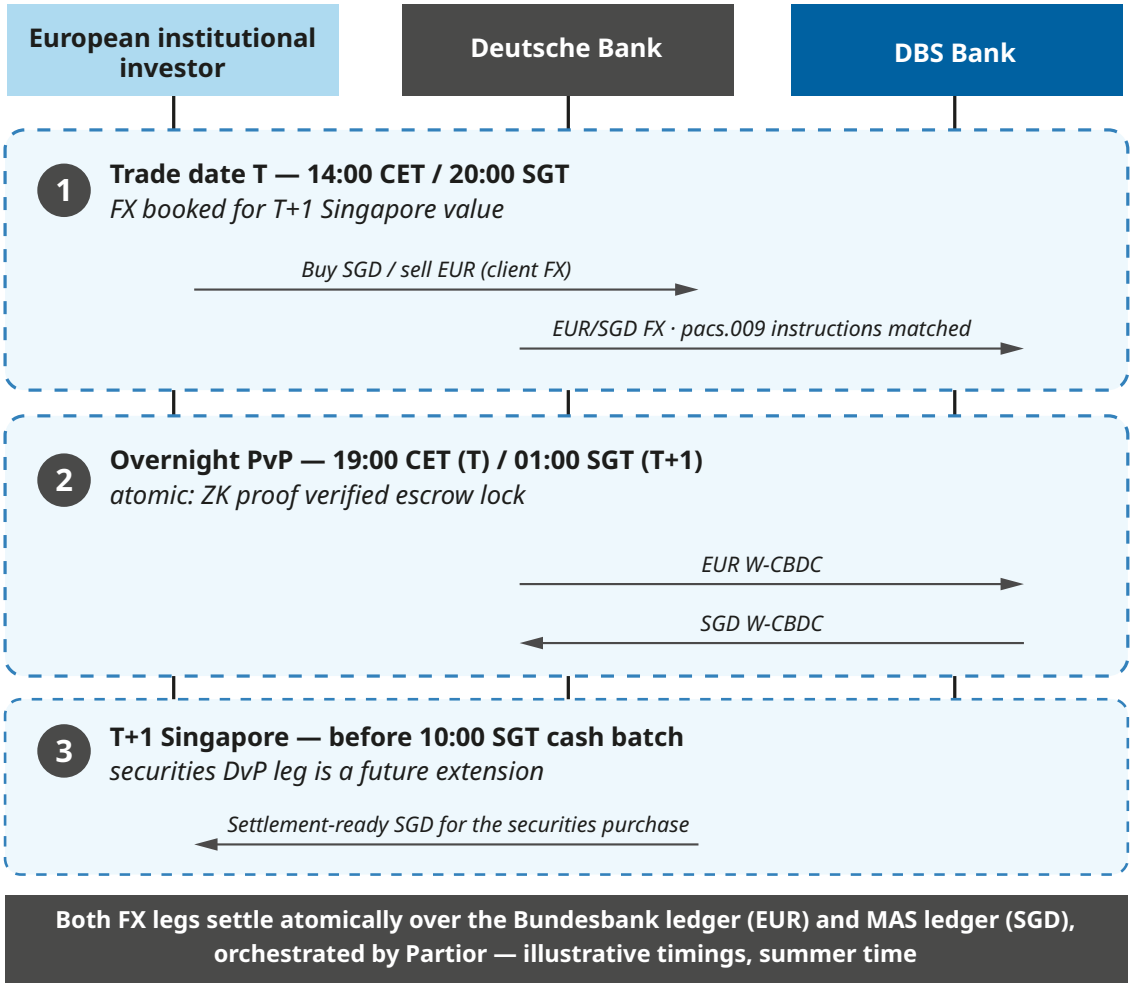


Figure 1: Use Case 1: T+1 securities funding through overnight EUR/SGD PvP

Note: The proof-of-concept tested only the interbank EUR/SGD PvP transaction between Deutsche Bank and DBS (shown in Step 2). The client FX transaction, movement of SGD to the investor's account and securities delivery-versus-payment leg were outside the scope of the experiment.

Potential value: For European investors and their intermediaries, this approach could reduce reliance on early, unconditional SGD pre-funding and precautionary liquidity buffers by allowing funds to be committed closer to when SGD is required for securities settlement. This could shorten the period for which liquidity is reserved. Settling the associated FX transaction on a PvP basis could also reduce the risk of paying one currency without receiving the other.

For Singapore, this approach could support overseas investors' access to the securities market should Singapore transition to a shorter settlement cycle, by facilitating the associated cross-border FX settlement within the compressed timeframe.

2.2 Use Case 2: Intraday EUR/SGD FX swap to bridge an SGD shortfall

Business challenge: As payment, settlement and financial market infrastructures move towards longer operating hours, liquidity needs arise intraday rather than only at end-of-day. A financial institution may require additional liquidity in a particular currency for only a few hours before returning to a surplus position later that same day. The challenge is not simply to obtain liquidity, but to ensure that it is available in the required currency, location and timeframe. Traditional treasury-management tools such as correspondent-bank liquidity, committed facilities and overnight funding remain effective, but may require liquidity to be obtained or held for longer than the underlying need.

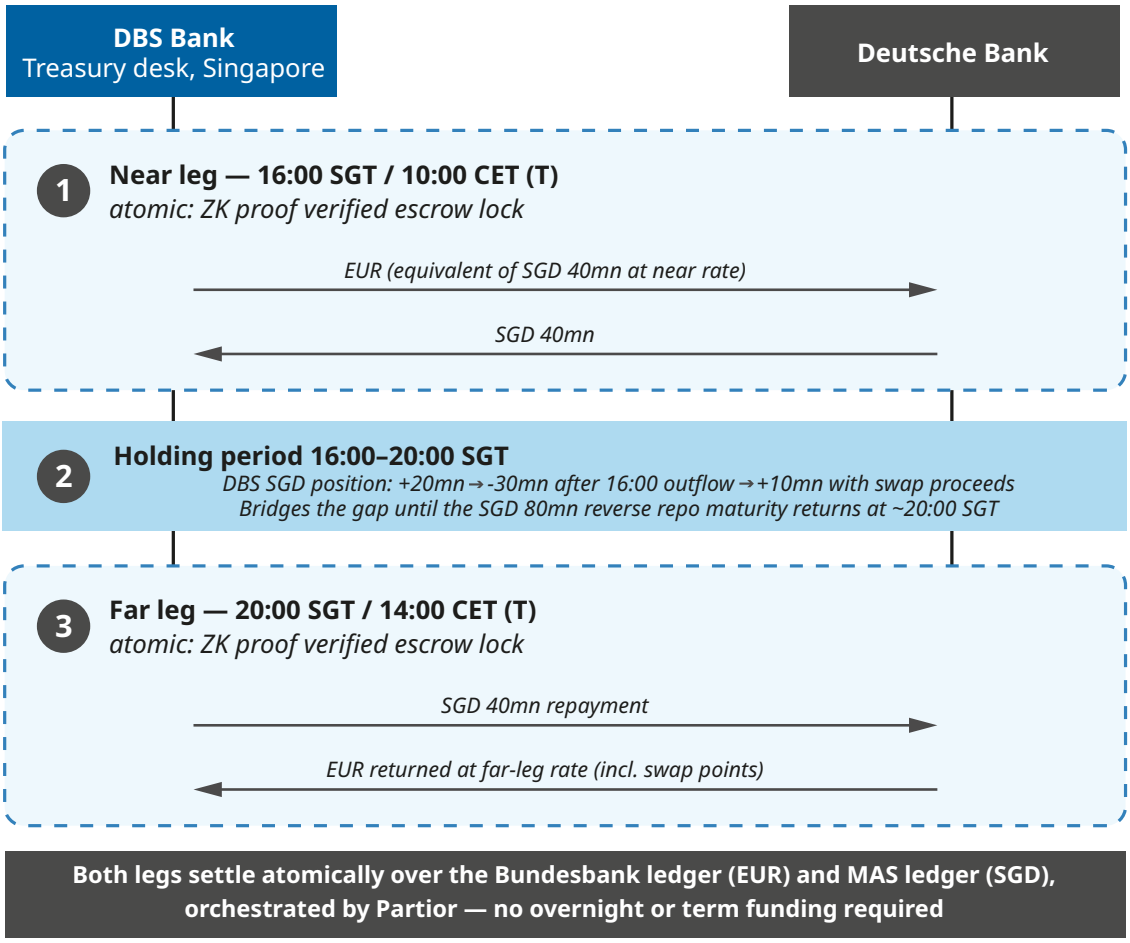


Figure 2: Use Case 2: Intraday EUR/SGD FX swap to bridge an SGD shortfall

Potential commercial approach: An intraday FX swap is one potential mechanism for meeting a temporary cross-currency liquidity need. Two counterparties exchange currencies for a defined period and reverse the transaction later the same day, as shown in Figure 2. The objective is not to take a directional FX position, but to obtain

temporary access to liquidity in the required currency while concurrently holding surplus pools of liquidity in another currency and not expanding the balance sheet by borrowing outright in the needed currency.

The settlement approach considers how each exchange under the intraday FX swap could be settled on a PvP basis across the Deutsche Bundesbank and MAS ledgers. Commercial banks remain responsible for sourcing liquidity, negotiating pricing and executing the underlying FX transaction.

Potential value: The settlement approach could give institutions more precise control over liquidity timing, allowing funds to be obtained closer to the point of need and returned when the requirement has passed. It could reduce idle balances and funding costs by shortening the period for which funds are committed. At each settlement point, PvP would ensure that either both currency legs settle or neither does, reducing principal risk.

Chapter 3

Proof-of-Concept Setup, Testing & Validation

3 Proof-of-Concept Setup, Testing & Validation

The illustrative use cases in Section 2 share a common settlement pattern: two parties need to exchange EUR and SGD atomically across two independently operated central bank ledgers in different jurisdictions and time zones. The proof-of-concept tested whether this could be achieved through cryptographic verification, without a shared ledger or a direct bilateral link between the two central bank ledgers.

The experiment simulated the settlement of a EUR/SGD FX transaction between Deutsche Bank and DBS using wholesale CBDC tokens across the Deutsche Bundesbank and MAS test environments. Partior provided an orchestration service, which operated on Partior's separate third ledger and coordinated settlement without holding either currency. In a future implementation, such a service would need to operate within an appropriate legal, governance and operational framework.

The experiment tested whether ZK proofs could enable relevant settlement states and outcomes to be independently verified across the two ledgers, without requiring either ledger to rely solely on assertions from the orchestration service about the state of the other ledger. The orchestration service verified proofs that the two currency legs had been locked before recording the settlement outcome. Each central bank ledger only released funds after verifying the ZK proof of the settlement outcome. Legal settlement finality, and the governance and operating arrangements required for any future implementation are considered in Appendix C.

Section 3.1 describes the setup and scope of the experiment, Section 3.2 illustrates the settlement process and Section 3.3 sets out the scenarios tested and their results. Section 4 then discusses the findings arising from those results.

3.1 Setup and Scope of Experimentation

The experiment ran for twelve weeks, from 10 August to 30 October 2026. It involved three independently operated ledgers. Each ledger was operated by a different institution and was compatible with the Ethereum Virtual Machine (EVM). The technical setups described in this report were developed and used specifically for the purposes of this proof-of-concept. Their use should not be interpreted as an endorsement or

preference by any participating institution for any particular technology, product or protocol, nor as indicating the technology used or intended to be used in any production system.

Table 1: Ledgers and roles

Ledger and Operator	Technology	Role
Deutsche Bundesbank	zkStack Prividium Layer 2 on a private EVM Layer 1	Holds and conditionally locks the simulated EUR wholesale CBDC tokens. Releases or refunds the EUR leg.
MAS	Hyperledger Besu	Holds and conditionally locks the simulated SGD wholesale CBDC tokens. Releases or refunds the SGD leg.
Partior	Hyperledger Besu	Supports the orchestration service, including instruction matching and recording the settlement outcome.

The proof-of-concept tested simulated EUR/SGD FX transactions between Deutsche Bank and DBS using simulated wholesale CBDC tokens in the test environments. Each transaction was processed separately on a gross PvP basis, without netting. Multilateral net settlement was not tested. Its possible application is discussed in Appendix C.

The settlement process was tested against defined pass-or-fail criteria. Performance was observed on an indicative basis without predetermined targets. Legal settlement finality and production resilience were outside the scope of the experiment. The proof-of-concept did not use production systems or real money. Appendix B sets out the detailed scope and test environments of the experiment; limitations are set out in Appendix E.

3.2 Settlement Logic: Atomic PvP via ZK proofs

In the proof-of-concept, simulated EUR/SGD FX transactions between Deutsche Bank and DBS were recorded with an agreed value date, settlement time, amount and FX rate. The experiment focused on the settlement of the two currency legs in central bank money across the two central bank ledgers. ZK proofs were used to verify the relevant lock states and settlement outcome before the central bank ledgers released any funds.

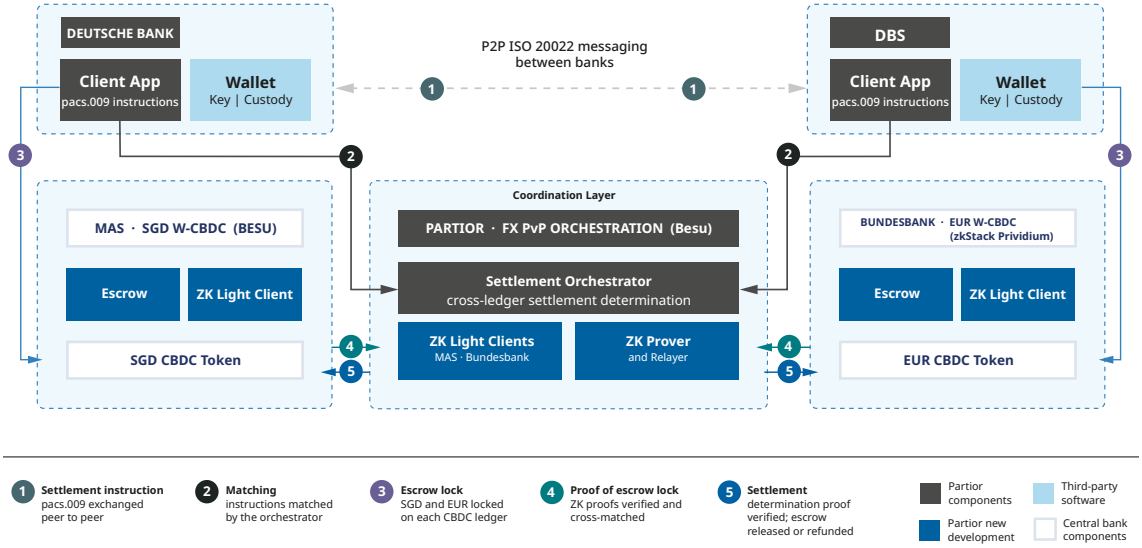


Figure 3: High-level solution architecture

The main components shown in the diagram are:

- **CBDC token:** A simulated representation of wholesale central bank money. SGD tokens were recorded on the MAS ledger and EUR tokens on the Deutsche Bundesbank ledger.
- **Escrow:** A smart contract on each CBDC network that conditionally locks a bank's tokens for a transaction. It releases or refunds the locked tokens after verifying the relevant settlement or refund outcome.
- **ZK prover:** Generates a compact cryptographic proof of a specified ledger state, such as the existence of an escrow lock. The proof allows the relevant condition to be verified without requiring the receiving ledger to maintain the source ledger's full history.
- **Relayer:** Carries proofs and messages between ledgers. It holds no assets and cannot alter a proof without causing verification to fail. It can therefore be run by any authorised party.
- **ZK light client:** A smart contract that verifies proofs from other ledgers. In the proof-of-concept, ZK light clients supported verification of the currency-lock states and the recorded settlement outcome.
- **Settlement orchestrator:** Offers orchestration service, including matching the two banks' settlement instructions and coordinating the lock and release steps across both ledgers.
- **Wallet infrastructure:** Holds each participant's keys and authorisations required for interacting with the central bank ledgers.
- **P2P messaging (ISO 20022):** Enables banks to exchange settlement instructions directly, separately from the ledger-based settlement process.

Settlement follows five steps across the three ledgers. The proofs are generated off chain by a prover and carried between ledgers by a relayer. In the proof-of-concept, both services were operated by Partior.

- **Instruction and matching (Steps 1–2).** Each bank submits a pacs.009[15] settlement instruction through its client application. The instructions are exchanged on a peer-to-peer basis between the banks and matched by the orchestration service before any funds are locked.
- **Locking (Step 3).** Once Deutsche Bank's and DBS's ISO 20022 (pacs.009) instructions have been submitted and matched, each bank locks the currency it is paying in an escrow on the respective central bank ledger: EUR on the Deutsche Bundesbank ledger and SGD on the MAS ledger. The funds remain locked and have yet to be transferred to the beneficiaries.
- **Proof of escrow lock (Step 4).** A ZK proof (Proof A) is generated for each escrow lock and transmitted to the orchestration service on the Partior ledger. Each proof demonstrates that the escrow lock exists in a finalised state on the source ledger.
- **Determine settlement outcome (Settlement Part A, Step 5).** The orchestration service verifies the ZK proofs for both escrow locks and cross-matches them against the corresponding settlement instructions to confirm that the EUR and SGD locks relate to the same FX transaction. If both proofs are verified and successfully cross-matched, the orchestration service records that settlement should proceed and a ZK proof (Proof B) of the settlement outcome is generated. If the required conditions are not met, for example because an escrow lock is missing, does not correspond to the matched transaction or is not received before the applicable deadline, a negative proof is generated to enable the funds to be refunded.
- **Execute settlement (Settlement Part B, Step 5).** The proof of the recorded settlement outcome is transmitted to each central bank ledger. Each ledger verifies the ZK proof and either releases the locked tokens to the beneficiary or refunds them to the payer.

This process resembled a two-phase commit pattern used in distributed systems. Locking represents the preparation phase, and determining settlement represents the commit-or-abort phase. Unlike a conventional two-phase commit, each central bank ledger verified a proof of the settlement outcome before acting, in the proof-of-concept.

15 ISO 20022 pacs.009 standardizes financial institutions' credit transfer message, used in the proof-of-concept at a functional level for settlement instruction initiation between the commercial banks and Partior.

As both central bank ledgers acted on the verified proofs of the same recorded outcome, both legs either settled or both were refunded. Simulated tokens remained on their respective central bank ledger, and the orchestration service did not hold either currency.

Messages between the ledgers used the Inter-Blockchain Communication (IBC) protocol. The proof-of-concept implemented a ZK-based version of IBC. Each message carried two compact proofs — Proof A established that the source ledger has finalised the relevant state and Proof B established that the message was included in that state. The receiving ledger's ZK light client verified both proofs on chain.

Off-chain relayers and provers supported proof generation and message delivery, but neither can cause settlement to take place. Each receiving ledger acts only after independently verifying a valid proof that the required settlement conditions have been met.

ZK proofs

A ZK proof is a cryptographic method that allows one party, known as the prover, to demonstrate to another party, known as the verifier, that a specified statement is true without revealing the private information used to prove it.

ZK proofs have three core properties. First, a valid proof for a true statement can be successfully verified. Second, a false statement cannot produce an accepted proof except with negligible probability. Third, the proof reveals no information about the private inputs beyond what follows from the statement itself. Together, these properties allow the verifier to establish that a condition has been met without relying solely on the prover's assertion or examining the underlying private information.

In financial workflows, for example, a party could prove that it has sufficient funds for a transaction without disclosing its account balance. Other potential applications include demonstrating control of an asset, verifying that transaction conditions have been met, or showing compliance with predefined identity, know-your-customer, or anti-money-laundering requirements.

This project leveraged the verifiability of ZK proofs, enabling specified ledger states to be verified through cryptographic evidence rather than relying solely on assertions from the party communicating that information. It did not separately test the broader privacy and confidentiality applications of ZK technology.

3.3 Scenarios covered and test results

Several functional scenarios were tested end to end across all three ledgers. These included a successful settlement and an abort in which both currency legs were refunded.

The scenarios also covered the rejection of invalid, stale, replayed or misrouted proofs, the rejection of duplicate messages, and recovery following the interruption and restart of the supporting services. All functional scenarios produced the expected results.

Table 2: Test Scenarios

Scenario	What was checked?	Result
Successful settlement	Both currency legs were released to the intended beneficiaries.	Passed
Abort	Both locked currency legs were refunded.	Passed
Invalid proof	Invalid, stale, replayed or misrouted proofs were rejected.	Passed
Duplicate message	A repeated message did not result in a duplicate settlement.	Passed
Recovery	Settlement processing resumed correctly following the restart of a supporting service.	Passed

Table 2 summarises the main end-to-end scenarios tested. The experiment also examined more granular failure conditions that could arise at different stages of the settlement process, including undelivered messages, missing locks, and partial release. These conditions are described in Appendix B. Under the scenarios tested, none resulted in a loss of simulated principal.

Most failures delayed settlement or temporarily locked liquidity until the funds were released or refunded. One scenario involved a partial release, where one currency leg had been released while the other remained locked. Once the settlement outcome had been recorded, it could no longer be reversed. The remaining locked leg could therefore only be released to the beneficiary and could not be refunded to the payer. This prevented the transaction from ending with one currency leg settled and the other refunded.

Settlement and proof-generation times were recorded in the test environment and are discussed in Section 4.

Chapter 4

Key Findings from Technical Proof-of-Concept

4 Key Findings from Technical Proof-of-Concept

The proof-of-concept demonstrated the technical feasibility of coordinating atomic EUR/SGD PvP settlement across independently operated central bank test environments using cryptographic verification. It also identified the principal considerations for any future implementation, including settlement performance, the basis for finality, the operational dependencies of the proof-based approach and the controls required by the participating central banks. This section sets out four key findings.

Finding 1: Atomic PvP settlement can be coordinated across independent ledgers
The experiment demonstrated that two wholesale CBDC settlement legs could reach a common settlement outcome while remaining on their respective central bank test environments. Each central bank retained control of its own ledger and the conditions it accepts for settlement. The settlement process did not require two currencies to be held on a shared ledger or the two central bank ledgers to be directly connected.

Finding 2: Proof generation was the main contributor to settlement time
In testing, end-to-end settlement took approximately 5 minutes. Proof generation accounted for most of this time. Optimising proof generation could materially reduce settlement time in future implementations.

Other potential improvements include running provers in parallel, reusing finality proofs, and batching transactions. These were not tested in the proof-of-concept and would require further examination to assess their effect on settlement time and throughput. Further details are set out in Appendix B.

Finding 3: Finality is not solely determined by the technical design of the ledger
The proof-of-concept demonstrated how two currency legs could be coordinated to a consistent technical outcome. Once the orchestration service recorded that settlement should proceed, each currency leg could only proceed to release funds. If one leg had already been released while the other remained locked, the remaining leg could not be refunded. This prevented the transaction from concluding with one currency leg settled and the other refunded.

This consistent technical outcome does not establish legal settlement finality. Any future implementation would need to determine when the transfer of each currency

becomes legally final and irrevocable, taking into account the conditions of settlement of each central bank and the applicable legal framework.

Finding 4: The proof-based approach retains key operational dependencies

The proof-based approach reduces reliance on provers and relayers as sources of truth as each receiving ledger verifies a valid proof before acting. However, the approach continues to depend on provers to generate proofs and relayers to transmit proofs and messages between ledgers. A failure or delay affecting these services could delay settlement and temporarily lock liquidity.

Proof generation also requires access to ledger data. A ZK proof limits the information disclosed to the receiving ledger, but the prover still requires access to data to generate the proof. Any future implementation would need to determine which entities may perform these functions, what ledger data they may access, and how continuity, recovery and oversight would be managed.

Each central bank would also need to authorise the relevant settlement contracts on its ledger and determine which checkpoints and programme keys those contracts may accept. Each central bank would retain control over access to its ledger data and the circumstances in which that access could be changed or revoked.

One possible operating model could be for each central bank to run provers and relayers within its own environment. This could allow the relevant ledger data to remain under the central bank's control while the proofs are provided for verification by participating ledgers. This arrangement was not tested in the proof-of-concept and would require further examination.

Chapter 5

Conclusion and Next Steps

5 Conclusion and Next Steps

This section draws together insights from the proof-of-concept against the problem statement set out in Section 1. Section 5.1 summarises the key insights, while Section 5.2 identifies the areas for further examination and considerations for future implementation.

5.1 Summary of Insights

The proof-of-concept demonstrated the technical feasibility of using cryptographic proofs to support atomic cross-border wholesale CBDC settlement across independent central bank test environments. The detailed experimental setup is set out in Appendix B and the test results in Section 3.3.

The two use cases illustrated how the settlement approach could potentially support securities-related funding across time zones and temporary intraday liquidity needs. The proof-of-concept only tested the interbank EUR/SGD PvP component and did not test the use cases as complete commercial or regulatory propositions. The relevant business and legal considerations are discussed in Appendices C and D.

The experiment also identified areas requiring further examination before any future implementation. These include improving proof-generation performance, establishing legal settlement finality, determining the governance and operating arrangements for provers and relayers, and governing access to the ledger data required for proof generation. Production readiness, production-scale performance and the operating model for a future implementation were outside the scope of the proof-of-concept. The detailed limitations are set out in Appendix E.

5.2 Areas for Further Research

Building on the results of the proof-of-concept, six areas merit further examination in considering any future implementation of the settlement approach.

1: Complementing common platforms

Proof-based verification could complement, rather than replace, common-platform approaches. A common platform, such as in Project Agorá, brings participating institutions, assets and settlement processes closely within a shared environment.

Proof-based verification could potentially support connectivity with infrastructures outside that environment, while allowing those infrastructures to retain their own rules and technology.

Project Agorá identified interoperability with infrastructures outside the platform as an important consideration.[16] Further work could examine whether the proof-based settlement approach could support such interoperability, in collaboration with the relevant platform operators.

2: Assessing alternative operating models

In the proof-of-concept, a single provider operated the orchestration service, prover and relayer services and the coordination ledger. As each receiving ledger independently verifies proofs before acting, the off-chain services could, in principle, be operated by multiple providers or by the participating central banks. These alternative arrangements were not tested in the proof-of-concept.

Future work could examine alternative arrangements for operating the coordination ledger, including its validator set. Any multi-provider model would require common standards for proof formats, light clients and messaging, together with clear governance, accountability, continuity and recovery arrangements.

3: Improving settlement performance

Proof generation accounted for most of the approximately 5-minute settlement time observed in the test environment. Developments such as dedicated proof circuits, improvements in cryptographic techniques, hardware acceleration and the reusability of finality proofs could further reduce proof-generation time. These were not tested in the proof-of-concept and their effect on settlement time, throughput and resilience would need to be measured through further testing.

4: Establishing legal settlement finality

The proof-of-concept demonstrated a consistent technical settlement outcome, but legal settlement finality was outside the of scope of the experiment. Any future implementation would need to determine when each currency transfer becomes legally final and irrevocable, and how the linkage between the two currency legs would be recognised across the participating jurisdictions.

Further work is needed to consider the legal treatment of conditionally locked funds and partial-release scenarios, together with the applicable legal and operating

16 BIS Innovation Hub 2026, p. 86

frameworks. Possible arrangements are discussed in Appendix C, but would require further assessment by the relevant central banks.

5: Exploring applications beyond FX PvP

The settlement process tested in the proof-of-concept, comprising conditional locking, proof generation, determination of the settlement outcome and execution on the relevant ledgers, is not specific to FX transactions. The same broad process could potentially support other forms of conditional settlement, including delivery-versus-payment involving tokenised securities and settlement involving tokenised deposits, with each asset remaining on its respective ledger.

More broadly, the proof-based settlement approach could provide a basis for interoperability across different types of ledgers operated by public and private organisations. These applications were not tested in the proof-of-concept and would require separate technical, legal, operational and commercial assessment.

6: Leveraging a common technology base

The three ledgers used in the proof-of-concept were EVM-compatible. This common technology base facilitated development, integration and testing across the different ledgers.

Future work could examine whether reusable standards, libraries and tools could reduce the platform-specific adaptations required to connect additional ledgers. It would also need to consider how this settlement approach could accommodate infrastructures based on different technologies.

The proof-based settlement approach should be considered as one option within the broader design space for cross-border settlement, alongside common-platform approaches and other interlinking models. Its potential value lies in enabling connectivity across independently operated ledgers while allowing each participating institution or jurisdiction to retain control over its own infrastructure and acceptance requirements.

Appendix A

Survey of Prior Experiments

Appendix A
Survey of Prior Experiments

Earlier work on cross-border settlement in central bank money has followed three broad models: connecting systems directly, building a shared platform, or coordinating independent systems through an operator. The initiatives below are those most relevant to the design choices made in this project.

Table 3: Selected prior experiments and their settlement models

Initiative	Approach	Settlement model	Key result
Jasper-Ubin (Bank of Canada and Monetary Authority of Singapore, 2019)	The Jasper and Ubin platforms of the two central banks were linked using Hashed Time-Locked Contracts, allowing payments to settle without a third-party intermediary.	Direct bilateral link between two ledgers	The proof-of-concept successfully implemented and demonstrated the use of Hashed Time-Locked Contracts to perform atomic transactions between two different DLT-based networks.
Project Dunbar (BIS Innovation Hub 2022)	Two prototypes of a shared multi-CBDC (m-CBDC) platform for direct cross-border payments and settlements, built on Corda and Quorum DLT platforms.	Shared ledger	The project demonstrated the technical viability of the concept of a multi-CBDC common platform by validating technical prototypes which posed practicable solutions to key design challenges of implementing multi-CBDC platforms, relating to access, jurisdictional boundaries and governance.
mBridge (BIS Innovation Hub 2024a)	A multi-CBDC platform shared among participating central banks and commercial banks, built on a new blockchain for real-time cross-border payments and FX. The platform allows local and foreign financial institutions to directly hold and transact in CBDCs issued by central banks, irrespective of jurisdiction.	Shared ledger	The platform reached minimum viable product stage in mid-2024. The steering committee created a bespoke governance and legal framework, including a rulebook.

Initiative	Approach	Settlement model	Key result
Project Mariana (BIS Innovation Hub, 2023)	A proof-of-concept consisting of three wCBDC platforms and a transnational network which hosts the AMM, where individual domestic platforms are connected to the transnational network via bridges. wCBDCs circulate on domestic platforms and bridges move them onto a transnational network that hosts the market maker. The bridging technologies allow for transfers between networks, and an automated market maker allows for pricing, execution and settlement of spot FX, on a public blockchain.	Common transnational platform with bridges to individual domestic platforms	The project demonstrated the technical feasibility of using automated market makers for cross-border exchange of wCBDCs, while fulfilling central bank requirements and broader principles set by the FX Global Code.
Meridian FX (BIS Innovation Hub 2025)	A technology-neutral synchronisation operator that coordinates the simultaneous exchange of assets across payment systems.	Operator coordinating independent systems	The project demonstrated that a synchronisation operator could settle PvP FX atomically between wholesale payment infrastructures in different jurisdictions and between a DLT-based platform and non-DLT systems.
Project Agorá (BIS Innovation Hub 2026)	A shared platform with a two-layer architecture where tokenised central bank reserves are issued on jurisdictional ledgers (known as the jurisdictional layer) and where tokenised commercial bank deposits are issued on a shared ledger (known as the unifying layer).	Jurisdictional central bank ledgers as the jurisdictional layer plus a single shared ledger as the unifying layer	The prototype demonstrated that a shared DLT platform can support safe settlement in a tokenized environment, enabling multi-currency, cross-border settlement and allowing participants to execute payments through smart contracts. The project has also proceeded to conduct real-value testing in currencies totaling approximately CHF 800,000.
Project Nexus (BIS Innovation Hub n.d)	A single standardised connection through which each domestic instant payment system can reach all others on the network.	Hub-and-spoke (retail instant payments, not wCBDC)	The first-mover central banks incorporated Nexus Global Payments in 2025 to operate the multilateral scheme.

Initiative	Approach	Settlement model	Key result
Project Mandala (BIS Innovation Hub 2024b)	Jurisdiction-specific compliance requirements embedded in a peer-to-peer protocol that generates a cryptographic proof of compliance.	Not a settlement model; a ZK precedent	The project showed potential of the Mandala proof-of-concept to automate compliance while improving data privacy using ZK proofs, multi-party computation and digital signatures. Mandala was announced to be moving into phase 2, which extends its work on streamlining cross-border compliance and further explore programmable compliance for digital assets, expanding to broader use cases and utility to other platforms and projects.

Appendix B

Technical Appendix: Experiment Set-up, Testing and Validation

Appendix B
Technical Appendix: Experiment Set-up, Testing and Validation

This appendix sets out the technical details supporting Sections 3 and 4. It examines the settlement approach and the conditions under which the results were observed.

B.1 Message Transport and Verification

Messages between ledgers use the Inter-Blockchain Communication (IBC) packet model, with all project-specific verification within light-client and application contracts on each ledger. Off-chain services observe settlement events, gather the required ledger data and request proofs from a prover cluster. Appendix B.3 describes the proof programs used.

The proof-of-concept implemented a ZK-based version of IBC. A message was accepted only if two logical proofs passed. Proof A established that the source ledger had finalised the relevant state, and Proof B established that the message was included in that state. The receiving ledger's ZK light client verified both proofs on chain.

The relayer and prover supported proof generation and message delivery, but neither could independently cause settlement to take place. Every proof was checked on chain against the expected route, previous trusted state, height, state root, router, storage path, value and approved program version, and anything else was rejected.

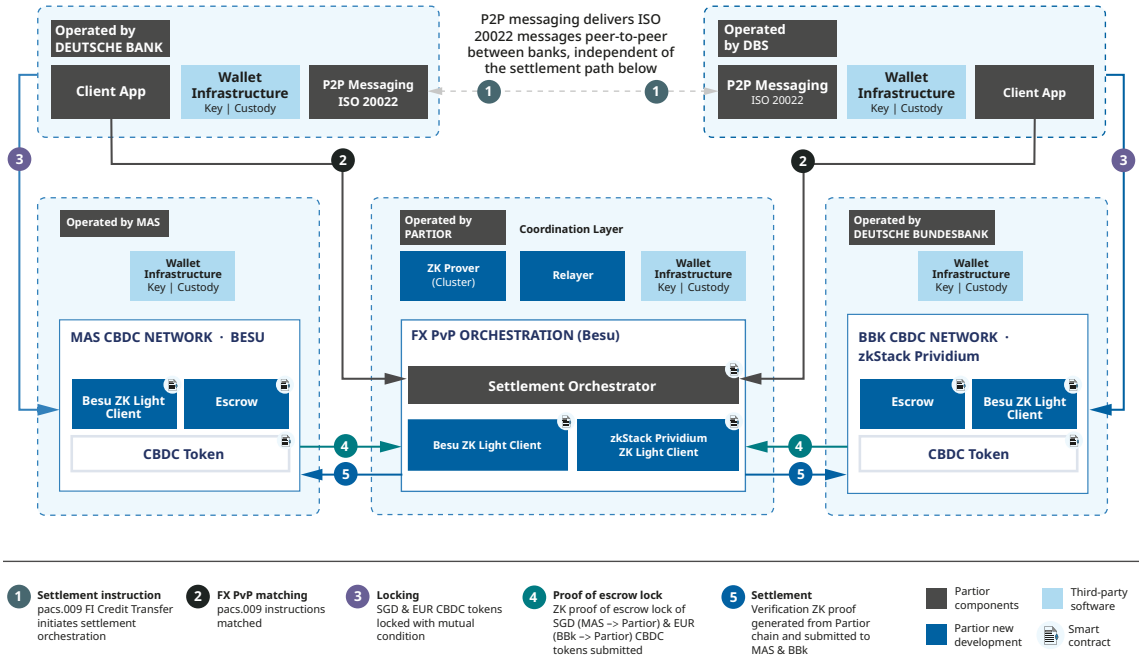


Figure 4: Component architecture and settlement flow

Figure 4 shows the components deployed. Bank-to-bank ISO 20022 messages travel peer to peer, independently of the ledger path. The numbered steps in the figure correspond to instruction, matching, locking, proof of lock and settlement. Table 4 lists the relay paths. Each central bank ledger connected only to the Partior ledger, where the orchestration service ran. There was no relay path between the MAS and Bundesbank ledgers.

Table 4: ZK proof relay paths

Route	Messages carried	Proof family	Verified by
MAS ledger to Partior ledger	SGD lock (prepared leg); acknowledgements	Besu: QBFT finality and Merkle-Patricia-Trie state proof	Besu ZK light client on the Partior ledger
Bundesbank ledger to Partior ledger	EUR lock (prepared leg); acknowledgements	zkStack Prividium: Layer 1 finality and settlement update, then native Layer 2 state proof	zkStack Prividium ZK light client on the Partior ledger
Partior ledger to MAS ledger	Settlement determination proof, or negative proof	Besu	Besu light client on the MAS ledger
Partior ledger to Bundesbank ledger	Settlement determination proof, or negative proof	Besu	Besu light client on the Bundesbank ledger

B.2 The Two Logical Proofs by Source Ledger

Every message was accepted only when two logical proofs passed. **Proof A** established that the source ledger had finalised a particular state. **Proof B** established that the exact message (a lock, an outcome, an acknowledgement) existed in that finalised state. The form of Proof A depends on the source ledger:

- **Besu-origin messages (MAS and Partior ledgers).** Proof A verifies the QBFT validator signatures that finalise the block. Proof B is a Merkle-Patricia-Trie proof of the message in the finalised state. One reusable implementation served both the MAS and Partior ledgers.
- **Prividium-origin messages (Bundesbank ledger).** Proof A verified finality on the Bundesbank private Ethereum proof-of-stake Layer 1 and authenticated the Prividium Layer 2 root, height and timestamp recorded in the rollup settlement contract. Proof B is a native Layer 2 state proof of the message under that root.

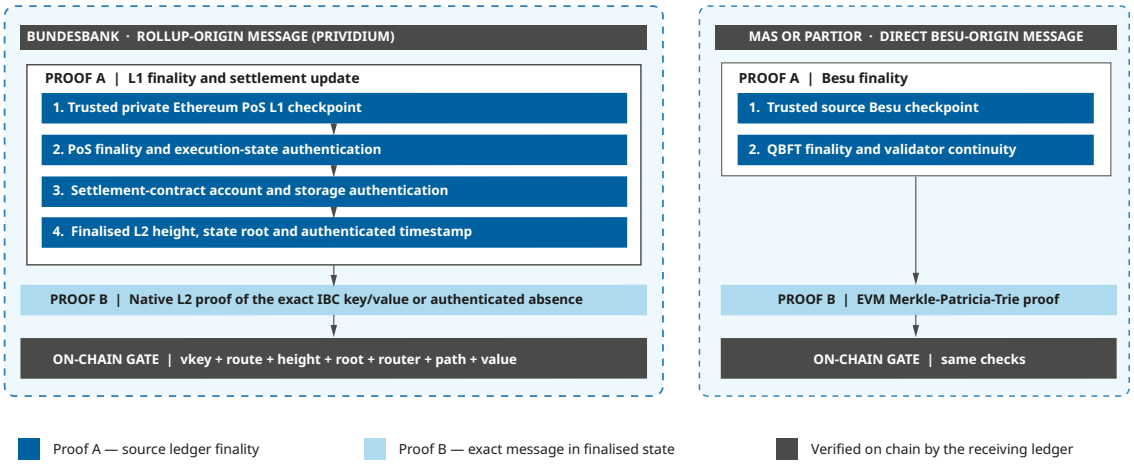


Figure 5: ZK proof model by source ledger

B.3 Proof Programs

In this proof-of-concept, proofs were generated in the SP1 ZK virtual machine and wrapped as Groth16 proofs for low-cost on-chain verification. Finding 2 in Section 4 sets out the timing implications.

B.4 Three-Ledger Design and Trust Boundaries

The technical setups described in this report were developed and used specifically for the purposes of this proof-of-concept. Their use should not be interpreted as an endorsement or preference by any participating institution for any particular technology, product or protocol, nor as indicating the technology used or intended to be used in any production system.

Table 5: Ledgers and their roles

Ledger	Technology	Role in the experiment	Verifies proofs from
MAS	Hyperledger Besu, QBFT consensus	Holds and conditionally locks the simulated SGD wholesale CBDC tokens. Releases or refunds the SGD leg.	Partior ledger (settlement outcome)
Deutsche Bundesbank	zkStack Prividium Layer 2 settling to a private Ethereum proof-of-stake Layer 1	Holds and conditionally locks the simulated EUR wholesale CBDC tokens. Releases or refunds the EUR leg.	Partior ledger (settlement outcome)
Partior	Hyperledger Besu (QBFT) Layer 1	Supports the orchestration service, including instruction matching and recording the settlement outcome. Does not hold any simulated wholesale CBDC token.	MAS ledger and Bundesbank ledger (escrow locks)

The two central bank ledgers were not directly connected. Each connected only to the Partior ledger, and each receiving ledger acted only on proofs that it verified.

Table 6 sets out which components are relied on for correctness, i.e. where a failure or compromise could result in an incorrect settlement outcome, and which are relied on for liveness, i.e. where a failure could prevent or delay an otherwise valid settlement from completing.

Table 6: Verification and trust boundaries

Component	Where it runs	Relied on for correctness	Relied on for liveness
ZK light clients and IBC gate	On chain, all ledgers	Yes: a message is accepted only when Proof A and Proof B verify against the approved program key (i.e. the fingerprint of the specific proof program a ledger has agreed to accept proofs from), route, height, root, router, path and value	Yes
Escrow contracts	On chain, MAS and Bundesbank ledgers	Yes: one terminal state per leg	Yes
Orchestration service	On chain, Partior ledger	Yes: matching, cross-matching of escrow lock proofs and one settlement determination	Yes
Relayer and proof API	Off chain	No: cannot cause an incorrect settlement	Yes
Prover cluster	Off chain	No: an invalid proof is rejected on chain	Yes
RPC	Off chain	No	Yes; also controls who can read ledger data
Trusted checkpoints and approved program keys	Governance of each ledger	Yes: set and updated under each operator's governance	No

Trust assumptions. A receiving ledger relies on the source ledger's consensus (e.g., the QBFT validator set, or the private proof-of-stake Layer 1 and the rollup settlement contract), the soundness of the proof system and its Groth16 setup, and the correctness of the trusted checkpoint and program key it holds. It does not rely on the relayer, prover or any intermediary to attest to the state of another ledger.

Information exposed. A proof shows the receiving ledger only the specific IBC commitment it proves (a lock, an outcome, an acknowledgement or the absence of a receipt) and the header data needed to authenticate it. It does not disclose balances and other transactions on the source ledger to the receiving ledger. The prover and RPC services nevertheless require access to the source ledger data that is needed to generate the proof. The proof-of-concept used ZK proofs mainly for succinct on-chain verification, while privacy and confidentiality were available on the Bundesbank's

zkStack Prividium ledger, the confidentiality of the settlement message contents across ledgers was not separately assessed.

Jurisdictional autonomy. Each central bank deploys and governs the light client on its own ledger and decides which proof programs and checkpoints it accepts. No other party can change what its ledger treats as a valid proof.

B.5 Settlement State Machine, Timeouts and Edge Cases

Each settlement moves through the states in Table 7. Matching on the Partior ledger precedes any lock. The two locks proceed in parallel on the MAS and Bundesbank ledgers. The settlement outcome is recorded only on the Partior ledger, and proof of that outcome is transmitted to both central bank ledgers, which then act independently on it.

Table 7: Settlement state machine

State	Recorded on	Entered when	Next states
INSTRUCTED	Partior	A pacs.009 instruction is submitted and validated	MATCHED, REJECTED
MATCHED	Partior	Corresponding instructions from both banks are matched	PREPARED, ABORT
PREPARED	MAS or Bundesbank escrow	The payer locks wholesale CBDC and the prepared-leg packet is sent	LEG VERIFIED; REFUNDED after timeout
LEG VERIFIED	Partior	The lock proof verifies and the leg passes application validation	COMMIT, ABORT
COMMIT or ABORT	Partior	Both legs verified (COMMIT), or validation failure, cancellation or timeout (ABORT); a one-time transition	RELEASED or REFUNDED
RELEASED or REFUNDED	MAS and Bundesbank escrows	The outcome proof verifies; terminal and idempotent per settlement and leg	SETTLEMENT COMPLETE
SETTLEMENT COMPLETE	Partior	Release or refund results for both legs are verified	CLOSED
CLOSED	Partior	Both banks confirm receipt of the funds credited to them.	–

Timing and timeouts. Timeout cases were not functionally tested as part of this proof-of-concept, but this paragraph sets out the steps that would occur in the case of a timeout. Each settlement carries a deadline. The timeout must exceed the

worst-case proving and relay time for the agreed finality basis. Otherwise, valid settlements could abort before the required proofs and messages are received.

Before the settlement outcome is recorded, a timeout may lead to a refund. Once the workflow has entered the release phase, however, the settlement outcome can no longer be reversed. A timeout on a release message will trigger a retry of the release rather than a refund. This prevents one currency leg from being released while the other is refunded. In the proof-of-concept, refunds were initiated manually.

Failure conditions. The design addresses the following failure conditions.

Abort:

- Application validation failure. If a proven lock does not satisfy the required transaction-level checks, the lock is rejected and the settlement is refunded.
- Contradicted lock result after release has been initiated. A later message reporting a different result is rejected. This prevents the settlement outcome from changing after one or both currency legs have released.

Timeout:

- Counterparty fails to lock. The one-sided lock is refunded from the workflow contract.
- Lock packet not delivered. An IBC timeout provides evidence of non-receipt. The packet is resent if the settlement deadline has not passed. Otherwise, both locks are refunded. A late lock confirmation received after a refund cannot trigger a release.

Invalid proof:

- Invalid proof. A proof is rejected on chain, and the settlement state remains unchanged.

Duplicate message:

- Duplicate instruction, packet or result. If the same instruction, packet or result is received more than once, only the first instance will be processed. A repeated identical result has no effect and a conflicting one is rejected. A duplicate cannot trigger a second lock, release or refund.

Recovery:

- Release not completed. Once the release phase has started, an undelivered or failed release message is retried, never refunded.
- Partial release. If one currency leg has been released but the release of the other has not been completed, the release message for the remaining leg is sent again. The remaining leg cannot be refunded because the counterparty has already been paid and the settlement outcome cannot be reversed.

B.6 Scope and Test Environment

The experiment ran on three independently operated ledgers. Table 8 sets out the details of the configuration of the three test environments and supporting components. The experiment tested EUR/SGD PvP settlement between Deutsche Bank and DBS using simulated wholesale CBDC test tokens in the test environments. Each transaction was processed separately on a gross PvP basis, without netting.

The settlement process was assessed against defined pass-or-fail criteria. Settlement and proof-generation times were recorded to understand the principal contributors to processing time. No performance or throughput targets were set.

In scope

The experiment implemented or tested the following:

- Settlement instructions and matching. Deutsche Bank and DBS initiated settlement instructions by submitting ISO 20022 pacs.009 messages. Corresponding instructions were matched before either currency leg was locked.
- Conditional locking of the currency legs. Simulated EUR and SGD wholesale CBDC tokens were locked in escrow contracts on the respective central bank ledgers. Depending on the recorded settlement outcome, the locked funds could be released to the beneficiary or refunded to the payer.
- ZK proof-based settlement orchestration. The orchestration service coordinated the settlement process by verifying and cross-matching the proofs associated with the two currency locks before recording the settlement outcome.

- Cross-ledger proof generation and verification. Off-chain services generated and relayed proofs and messages between the ledgers. ZK light clients and application contracts on the receiving ledgers performed the relevant on-chain verification.
- Functional and recovery scenarios. Testing covered successful settlement, abort, duplicate message, invalid proof and recovery following the interruption and restart of supporting services. Some recovery actions, including the refund of a one-sided lock, were initiated manually, as described in Appendix B.5.

Out of scope

The experiment did not assess or establish:

- Legal settlement finality, legal enforceability or the legal status of any wholesale CBDC or tokenised asset.
- Production-ready security, resilience or operational certification.
- Production-scale performance, throughput, capacity or cost benchmarking.
- The commercial benefits of the illustrative use cases in Section 2.

The design of production-ready wholesale CBDC token formats, ledger configurations and access arrangements were also outside the scope of the experiment.

The proof-of-concept used simulated tokens in test environments. It did not involve production systems, real money, customer funds or live FX transactions.

Table 8: Test environment configuration

Environment or component	Configuration in the proof-of-concept
MAS SGD wholesale CBDC test environment	Hyperledger Besu with QBFT consensus; simulated SGD wholesale CBDC token; escrow and settlement application contracts; IBC router; ZK light client for the Partior ledger
Bundesbank EUR wholesale CBDC sandbox	zkStack Prividium Layer 2 settling to a private Ethereum proof-of-stake Layer 1; simulated EUR wholesale CBDC test token; escrow and settlement application contracts; IBC router; ZK light client for the Partior ledger
Partior settlement sandbox	Hyperledger Besu with QBFT consensus; settlement orchestrator; network directory; IBC router; ZK light clients for the MAS and Bundesbank ledgers

Environment or component	Configuration in the proof-of-concept
Off-chain services	Relayer, proof API service and prover cluster on a dedicated proving virtual machine (additional computing resources were added during the development and testing); containerised Docker deployment
Participant applications	Prototype client application, operational UI and wallet infrastructure (key custody and signing) for Deutsche Bank and DBS; peer-to-peer ISO 20022 messaging client between the banks

Experiment constraints. The testing period ran for twelve weeks from 10 August to 30 October 2026. The ledger versions, contract interfaces and packet formats were fixed during the experiment to provide a stable basis for testing. The proof-of-concept depended on access to the relevant test environments, historical ledger data and interfaces required for proof generation.

B.7 What Drives Settlement Time

Settlement and proof-generation times were recorded during the experiment. No predetermined performance targets were set, and the results should not be interpreted as production-scale benchmarks.

- **Proof-generation time.** Proof generation accounted for most of the approximately 5-minute end-to-end settlement time observed in the proof-of-concept. The performance implications are discussed in Finding 2 of Section 4.
- **Finality basis.** The proof-of-concept accepted Layer 2 inclusion for the euro leg. Requiring Layer 1 finality would lengthen settlement time. Any future implementation would need to determine the appropriate basis, taking into account the relevant central bank requirements and legal framework.
- **Throughput.** Throughput was not measured in the proof-of-concept. Appendix B.8 considers potential ways to increase processing capacity.

B.8 Scalability

Throughput was not measured in the proof-of-concept. The approximately five-minute end-to-end settlement time was observed for individual settlements processed in the test environment and should not be interpreted as a demonstrated sustained processing rate.

The design could potentially support greater processing capacity through parallel proof generation, additional proof resources, optimisation of proof generation, and batching. Table 9 projects the number of settlements completed per hour based on the configurations and illustrative assumptions stated. Processing settlements sequentially at an assumed rate of 5 minutes per settlement equates to approximately 12 settlements completed per hour. These projections were not tested or benchmarked, and do not represent production performance.

Table 9: Illustrative, untested scalability scenarios

Configuration	Illustrative assumption	Projected settlements per hour
Sequential processing based on observed settlement time in proof-of-concept	One settlement completed every 5 minutes	About 12
Prover per central bank	Proof generation for both currency legs take place concurrently, reducing the processing time to 2.5 minutes per settlement	About 24
Algorithm optimisation	Optimised proof generation reduces processing time to about 2 minutes per settlement	About 30
Parallel provers	10 settlements processed concurrently and reduced processing time to about 2 minutes per settlement	About 300
Batch settlement	Batch of approximately 1,000 settlements processed every 2 to 10 minutes	About 6,000 to 30,000

Batching could increase processing capacity by sharing proof-generation work across multiple settlements. However, individual settlements may take longer because they may need to wait for a batch to be formed and processed. The achievable processing capacity would also depend on the capacity of the participating ledgers and the number of settlements that could be included in each batch. These factors were not measured in the proof-of-concept. Additionally, any batching design would need to preserve atomicity and the appropriate settlement and recovery treatment for each individual transaction.

B.9 Verification across multiple networks

Regulated digital money and assets are likely to be recorded across multiple infrastructures rather than on a single ledger. Connecting these infrastructures requires approaches to verify relevant states and outcomes across them while accommodating differences in technology, governance and operating arrangements.

Connecting independently operated networks. Differences in ledger design and institutional requirements are likely to result in multiple co-existing networks. A recent BIS Bulletin[17] explains how differences in the design of permissionless blockchains have contributed to fragmentation across networks. It also notes that mechanisms used to connect these networks can introduce new trust, governance and operational dependencies. Although Project Simbolon involved permissioned test environments, these considerations remain relevant when assessing how independently operated ledgers could be connected.

Potential application by settlement scheme operators. A settlement scheme operator could use proof-based verification to coordinate conditional settlement across participating ledgers. The operator could verify the relevant states before recording the settlement outcome, while each participating ledger retains control over the proofs it verifies and the actions taken on that ledger. The same approach could support settlement involving tokenised deposits or tokenised securities, with each asset remaining on its respective ledger. These applications were not tested in the proof-of-concept.

Governance and oversight. The BIS Bulletin notes that shared cross-ledger services increasingly perform functions comparable to those of financial market infrastructures and may therefore warrant corresponding governance arrangements, resilience standards and supervision. Any future implementation would similarly need clear accountability for the operation of the proof-based settlement process, including the controls governing proof verification, access to ledger data and recovery from service disruptions. Each participating central bank would continue to retain control over the proof programs, trusted checkpoints and verification rules applied on its own ledger. Appendix C considers how the legal and operating arrangements of linked settlement schemes might interact.

17 Eidan et al., 2026, BIS Bulletin

Appendix C

Settlement Finality and Scheme Considerations

Appendix C
Settlement Finality and Scheme Considerations

The proof-of-concept demonstrated that the two currency legs could be coordinated to a consistent technical outcome. Following verification of the cross-ledger settlement outcome, both currency legs were released or both were refunded. This technical outcome did not establish when either currency transfer became legally final and irrevocable, or how the linkage between the two currency legs should be recognised across jurisdictions.

This appendix identified the legal, governance and operating considerations that would need to be addressed in any future settlement arrangement. These considerations were not tested in the proof-of-concept and remain subject to assessment by the relevant central banks and participating financial institutions.

C.1 Finality in the Proof-Based Settlement Model

Final settlement is the irrevocable and unconditional discharge of an obligation in accordance with the terms of the underlying contract.[18] In a cross-ledger PvP arrangement, the two currency transfers occur on separate ledgers and may be governed by different legal frameworks, system rules and institutional arrangements.

In the proof-of-concept, each currency leg was settled on its respective central bank test ledger. The orchestration service recorded the cross-ledger settlement outcome, and each central bank ledger acted only after verifying the proof of that outcome.

Any future arrangement would therefore need to align the technical settlement process with the applicable legal and operating arrangements. Table 10 distinguishes what was demonstrated in the proof-of-concept from the issues that require further examination.

18 CPMI-IOSCO, 2012, Principle 8

Table 10: Technical and legal elements of finality

Element	What the proof-of-concept demonstrated	What remains to be established
Ledger finality basis	Each receiving ledger verified the relevant proof against the technical finality basis applied in the test environment.	Whether that technical basis corresponds to the point at which the applicable law and the relevant central bank or system rules recognise the currency transfer as final and irrevocable.
Legal finality	Not assessed.	When release or refund of each currency leg becomes final and irrevocable, including the treatment of conditionally locked funds.
Proof verification	Each central bank test ledger verified proof of the relevant state or settlement outcome before releasing or refunding its currency leg.	The rules under which a verified proof authorises the release or refund of conditionally locked funds.
Cross-ledger settlement outcome	The orchestration service recorded one cross-ledger settlement outcome, and both central bank test ledgers verified proof of that outcome before acting.	How the linkage between the two currency legs would be recognised across jurisdictions, including the treatment of insolvency or disruption between the finality points of the two transfers.

Legal basis for settlement finality. The legal basis for finality would depend on the design of any future arrangement and the laws and system rules applicable in each jurisdiction. Contractual or scheme rules could define when transfer instructions become irrevocable, the conditions for releasing or refunding locked funds, and the rights and obligations of participating financial institutions. They would also need to specify the legal effect of the cross-ledger settlement outcome and how it relates to the finality of each currency transfer. Whether applicable statutory regimes would extend to this settlement approach would depend on the legal and operational structure of any future implementation.

Alignment of technical and legal finality. Technical and legal finality may not arise at the same point. CPMI and IOSCO have noted that a system relying on a probabilistic settlement mechanism may not provide a definitive point of technical settlement, even when the legal framework and system rules define the point at which settlement is final.[19] Any future arrangement would need to determine whether the technical state treated as final on each ledger corresponds with the point at which the applicable law and system rules recognise the relevant currency transfer as final and irrevocable.

19 CPMI–IOSCO 2022

C.2 Illustrative Arrangements for Establishing End-to-End Finality

Any future arrangement would need to assign responsibility for the orchestration function and establish the rules under which the cross-ledger settlement outcome is given effect on each participating ledger. The appropriate structure would depend on the applicable legal frameworks, the roles of the participating central banks and financial institutions, and whether the arrangement falls within an existing regulatory, supervisory or oversight framework.

The following arrangements are illustrative. They were not assessed in the proof-of-concept and are not presented as exhaustive or preferred options.

- **A. Contractual settlement scheme.** Participating financial institutions and a scheme operator could establish contractual rules governing matching, conditional locking, the cross-ledger settlement outcome, timeouts and refunds. Each central bank would separately determine the conditions under which its ledger acts on a verified proof. The legal enforceability of the linkage between the two currency transfers would depend on the applicable laws, system rules and contractual arrangements.
- **B. Central bank-governed arrangement.** The participating central banks could establish the rules governing the orchestration function and the conditions under which their respective ledgers act on a verified cross-ledger settlement outcome. The orchestration function could be operated by the central banks or provided by a third party. This approach would require agreement on governance, operational responsibilities and the legal treatment of the settlement outcome in each jurisdiction.
- **C. FMI-operated settlement arrangement.** A financial market infrastructure (FMI) could operate the scheme and coordinate settlement across the respective central bank ledgers. Depending on the design, the FMI could also have responsibilities relating to liquidity provision and participant default. Its rulebook would need to establish the conditions under which the cross-ledger settlement outcome authorises the release or refund of each currency leg, while each central bank would determine the conditions under which its ledger acts on a verified proof. The legal and regulatory feasibility of this arrangement, including the FMI's ability to perform these functions in each jurisdiction, would require further assessment.

Under any of these arrangements, the scheme or its operator could potentially be subject to designation, regulation or oversight. Whether an existing statutory

settlement-finality regime could apply would depend on the legal and operational structure of the arrangement and would require assessment in each relevant jurisdiction. Where more than one authority has responsibilities for the arrangement, arrangements for cooperation among the relevant authorities would also need to be established.[20]

Responsibility for operating or overseeing the orchestration function would need to be clearly allocated. Where an FMI relies on a third party to provide a function critical to its operations, the FMI would remain responsible for managing the associated operational risks. Relevant authorities may also apply the oversight expectations in Annex F of the Principles of Financial Market Infrastructures (PFMI) to a critical service provider.[21]

Under each arrangement, the participating central banks would retain responsibility for determining the conditions under which their respective settlement assets and ledgers participate, including the conditions under which each ledger acts on a verified proof.

C.3 Risks in a Future Settlement Arrangement

The arrangements described in Appendix C.2 would need to address the legal and operational risks arising from the cross-ledger settlement process. Table 11 summarises the principal risks and the matters requiring further consideration. The corresponding arrangements were not assessed in the proof-of-concept unless otherwise stated.

Table 11: Key risks in a future settlement arrangement

Risk	Description	Matters to be addressed
Timeout calibration	Insufficient time for proof generation, transmission or verification could interrupt settlement.	Set and coordinate deadlines across the participating ledgers. Distinguish between expiry before a settlement outcome, which may result in refund, and interruption after a commit outcome, which requires the outstanding release to be retried.
Insolvency challenge	The treatment of a conditional lock, release, refund or cross-ledger settlement outcome could be challenged in an insolvency.	Determine the legal enforceability of each settlement state under the applicable laws, system rules and contractual arrangements.

20 CPMI-IOSCO, Principles for Financial Market Infrastructures, 2012, Responsibility E, "Cooperation with other authorities"
21 CPMI-IOSCO, Principles for Financial Market Infrastructures, 2012, Principle 17 and Annex F.

Risk	Description	Matters to be addressed
Failure to fund or lock	A participant fails to fund or conditionally lock its currency leg.	Define the treatment of incomplete or one-sided locks, including cancellation, refund and operational responsibility.
Proof and verification failure	A defect in the proof program or verifier could cause an invalid proof to be accepted or a valid proof to be rejected.	Establish appropriate assurance, testing and change-control arrangements for proof generation and verification.
Prover and relayer liveness	An outage affecting the off-chain services could delay proof generation or message delivery.	Establish resilience, monitoring and recovery arrangements, including resubmission of proofs or messages.
Ledger upgrades	A ledger or interface change could prevent proofs from being generated or verified using the existing configuration.	Coordinate testing and implementation of changes affecting interfaces, data structures and verification.
Operator failure	Failure of the scheme operator or orchestration service could prevent an outcome from being recorded or communicated.	Establish continuity, recovery and wind-down arrangements. Where a commit outcome has already been recorded, recovery must preserve that outcome and enable any outstanding release to be completed.
Conflict of laws	Different laws and system rules may apply to the currency legs and their cross-ledger linkage.	Determine the law and jurisdiction governing the linkage and its interaction with the laws and system rules applicable to each currency transfer.

Appendix D

Considerations for Further Development

Appendix D
Considerations for Further Development

The proof-of-concept demonstrated the technical feasibility of the settlement approach in test environments. Further work would be required to determine how that approach could operate within existing banking, treasury, legal, regulatory and financial-market-infrastructure arrangements.

The considerations below apply across the two illustrative use cases in Section 2. They identify the principal areas that would need to be examined before progressing to a controlled pilot. They do not represent requirements validated by the proof-of-concept.

Liquidity, Accounts and Wallet Arrangements

Further work would be needed to determine where settlement funds are held and how they would be funded, reserved, transferred, released and reconciled across participating infrastructures. This includes assessing the necessity and role of wallets, settlement accounts, nostro arrangements, pre-funding requirements and any additional components needed to support the ZK proof-based settlement approach.

It would also be necessary to examine whether liquidity becomes trapped, reserved for prolonged periods or fragmented across multiple infrastructures. Liquidity timing, wallet balances and liquidity efficiency would need to be considered for both illustrative use cases.

Systems Integration and Operational Visibility

The orchestration service would need to connect with existing FX, treasury, banking, confirmation, middle-office, custody, risk and reporting systems. Settlement outcomes records on the ledgers would need to be reflected promptly and consistently across these systems. This would be particularly relevant where batch-based processes create a delay between the settlement on the ledgers and updates to internal records. Appropriate controls would also be needed to prevent duplicate processing and support the timely identification and resolution of discrepancies.

The proof-of-concept used pacs.009 messages at a functional level only. A pilot would need full ISO 20022 usage guidelines and standardised status reporting, potentially using pacs.002 messages.

Treasury, Liquidity and Funding Operations

Treasury functions in financial institutions would need to evaluate how liquidity would be sourced, priced and positioned across currencies, jurisdictions, holidays and operating windows. The potential benefits illustrated in Section 2, such as more precise funding, temporary intraday FX liquidity, and support across extended operating hours, would need to be weighed against any increase in gross funding requirements, loss of netting benefits or operational constraints associated with maintaining balances across multiple settlement arrangements.

The assessment should also consider how readily liquidity could be reallocated when funding needs or market conditions change, and whether the settlement approach would reduce or create additional operational demands for treasury functions.

Client and Market Benefits

The value of the settlement approach would depend on whether it offers material improvements over existing arrangements. Potential benefits include greater certainty over settlement timing, more flexible access to liquidity across operating hours and time zones, shorter periods for which funds must be committed and more reliable cross-border settlement. Native programmability could further these benefits by enhancing flexibility in payment and FX settlement arrangements while retaining the benefits of standardised ISO messaging. This could enable connectivity across conventional and DLT-based infrastructures and support emerging cross-border and on-chain operating models.

Legal, Regulatory and Prudential Considerations

Any future implementation would need clarity on when each currency transfer becomes legally final and irrevocable, how linkage between the two currency legs is recognised across jurisdictions, and the rights of participants in conditionally locked funds. The legal treatment of the digital settlement assets and any contractual or scheme rules governing the settlement process would also need to be established.

Relevant regulatory and prudential considerations include reporting obligations, regulatory treatment of locked funds, cross-border data transfers, confidentiality arrangements, and applicable AML/CFT and sanctions requirements.

Operational Resilience and Recovery

Service outages, participant failures, cyber incidents and loss of data access could interrupt settlement at different stages. Continuity and recovery arrangements would need to preserve the recorded settlement outcome, prevent duplicate or inconsistent

processing, and avoid funds remaining locked indefinitely. Any fallback to existing settlement processes would need to be designed and tested to ensure that it does not result in duplicate transactions or outcomes that conflict with those already recorded on the ledgers.

Appendix E

Limitations

Appendix E
Limitations

The proof-of-concept was conducted within the scope and test conditions described in Sections 3.1 and 3.3, and Appendix B. The following limitations should be considered when interpreting its results.

- **Use of test environments and simulated assets.** The experiment used simulated wholesale CBDC tokens in test environments. It did not establish legal settlement finality, legal enforceability or the legal status of the simulated assets.
- **Indicative performance observations.** The approximately five-minute end-to-end settlement time was observed in the test environment. No performance targets were set, throughput was not measured, and the results should not be interpreted as production-scale benchmarks.
- **Dependence on ledger-specific configurations.** The proof profile for Bundesbank's test environment was developed for a specific ledger architecture and settlement contract, including how the relevant settlement data was structured and stored. Changes to the ledger or its contracts could require corresponding changes to the proof profile. Proof profiles for other ledgers would similarly need to reflect their respective technical configurations.
- **Operation of off-chain services.** Partior operated the relayer, proof API and prover cluster using a single proving environment. The experiment did not test whether settlement could continue during a sustained service outage or under an operating model involving multiple service providers.
- **Limited transaction and participant scope.** The experiment covered one currency pair, two commercial banks and simulated wholesale CBDC tokens using an escrow-based model. Other token models, currencies and participants were not covered.
- **No independent technical assurance.** The smart contracts, proof programs and off-chain services were not subject to an independent security audit, formal verification, penetration testing or a production-resilience assessment. Governance arrangements for trusted checkpoints, approved program keys and any required trusted setup were outside the scope of the experiment.
- **Manual recovery.** Certain recovery actions, including refunds of one-sided or stalled locks, were initiated manually. Automated recovery following a failed release-initiation transaction was not tested.

- **No testing beyond FX PvP.** The approach was not tested for settlement involving tokenised deposits or delivery-versus-payment tokenised securities transaction.
- **Gross settlement only.** Each FX transaction was settled individually at its gross value. Netting or other liquidity-savings arrangements were not tested.
- **Access to central bank test environments.** Deutsche Bank and DBS each used wallets on both central bank test environments for the purposes of this experiment. Participation in any future settlement arrangement, including access to wholesale central bank settlement assets, would depend on the eligibility and participation rules established by the relevant central bank.

Appendix F

Glossary of Terms

Appendix F
Glossary of Terms

Term	Definition
AML/CFT	Anti-money laundering and countering the financing of terrorism requirements.
Atomic settlement	Settlement in which all linked transaction legs are completed together or none is completed.
CBDC	Central bank digital currency: a digital form of central bank money issued by a central bank.
CBDC ledger	A ledger operated or authorised by a central bank on which wholesale CBDC transactions are recorded and settled. In the proof-of-concept, the central bank test ledgers recorded transfers of simulated wholesale CBDC tokens.
Circom	A language and toolchain used to define arithmetic circuits for zero-knowledge ZK proofs.
CLS	Continuous Linked Settlement: a payment-versus-payment service that settles certain foreign-exchange transactions by linking the payment of both currency legs.
Coordination ledger	A ledger used to coordinate settlement instructions and outcomes without holding the wholesale CBDC being exchanged.
DLT	Distributed ledger technology: technology that records and synchronises transactions across multiple participating nodes or institutions.
DvP	Delivery versus payment: a settlement mechanism in which delivery of an asset occurs only if payment occurs.
Escrow	A mechanism that temporarily locks funds until specified conditions for release or refund are met.
Escrow lock	Funds locked in an escrow contract on a central bank ledger, pending escrow release or refund.
EVM	Ethereum Virtual Machine: a software environment that executes smart contracts compatible with Ethereum-based networks.
Finality	The point at which a ledger transaction or state change is considered irrevocable under the relevant technical or legal framework.
FMI	Financial market infrastructure: a system or arrangement that facilitates the clearing, settlement or recording of financial transactions.
FX	Foreign exchange: the exchange of one currency for another.
Groth16	A succinct zero-knowledge ZK proof system that enables computationally efficient verification of proofs on chain.
IBC	Inter-Blockchain Communication protocol: a protocol for exchanging authenticated messages between independent blockchains or ledgers.
ISO 20022	An international standard for financial messages and data formats.

Term	Definition
Layer 1	The base ledger or blockchain on which transactions are recorded and finalised.
Layer 2	A secondary network or ledger built on or connected to a Layer 1 system, generally to improve scalability or provide additional functionality.
Legal settlement finality	The point at which a settlement is legally irrevocable and enforceable, including in the event of insolvency.
Light client	A component that verifies selected information from a ledger without storing or processing the ledger's complete history.
Merkle-Patricia Trie	A cryptographic data structure used by Ethereum-compatible systems to organise and prove the inclusion of data in a ledger state.
Orchestration layer	A system that matches the two currency legs, determines whether settlement should proceed or abort, and communicates the outcome to the participating ledgers.
Orchestration service	The software component that, in the proof-of-concept, matched instructions, verified and cross-matched escrow lock proofs and recorded the settlement determination on the Partior ledger.
pacs.002	An ISO 20022 message used to communicate payment or settlement status.
pacs.009	An ISO 20022 message used for financial-institution credit transfers.
PFMI	Principles for Financial Market Infrastructures: international standards issued by CPMI and IOSCO for the safety and resilience of FMIs.
PoS	Proof-of-Stake: a consensus mechanism in which designated validators help secure and finalise a ledger based on staked value or an equivalent authority structure.
Prover	An off-chain service that generates cryptographic proofs for verification by a ledger or smart contract.
PvP	Payment versus payment: a settlement mechanism in which one currency leg is settled only if the other currency leg is also settled.
QBFT	Quorum Byzantine Fault Tolerance: a permissioned consensus mechanism in which a defined set of validators agree on the order and finality of transactions.
RBAC	Role-based access control: a method of restricting system access according to the roles and permissions assigned to users or services.
Relayer	An off-chain service that transports messages or proofs between ledgers.
RPC	Remote procedure call: a method that allows one system or application to request data or services from another system.
Settlement determination outcome	The cryptographically verifiable outcome determination recorded by the orchestration service as to whether the two currency legs should be released or refunded. Each central bank ledger acts only after independently verifying proof of that determination. that instructs each ledger either to release the locked funds or to refund them.

Term	Definition
Settlement scheme operator	The legal entity that would run a settlement scheme in production: it sets the rulebook, admits participants and is responsible for finality and risk management.
T+1	A settlement cycle in which a transaction is settled one business day after the trade date.
Technical finality	The point at which a ledger's consensus mechanism treats a transaction or state as irreversible within the technical system.
Trusted setup	A one-time ceremony or process used to generate cryptographic parameters for certain proof systems.
wCBDC	Wholesale central bank digital currency intended for use by financial institutions rather than the general public.
ZK interoperability	An interoperability model in which ledgers verify cryptographic proofs of events or states on another ledger.
ZK light client	A light-client component that verifies cryptographic proofs about another ledger without maintaining the other ledger's full history.
ZK proof	Zero-knowledge proof: a cryptographic proof that allows one party to demonstrate that a statement is true without revealing the underlying information.
zkVM	Zero-knowledge (ZK) virtual machine that generates a ZK proof that the program was executed correctly.

References

References

Bank of Canada and Monetary Authority of Singapore. 2019. *Jasper-Ubin Design Paper: Enabling Cross-Border High Value Transfer Using Distributed Ledger Technologies*. May 2019, https://www.mas.gov.sg/-/media/jasper-ubin-design-paper.pdf.

BIS (Bank for International Settlements). 2022. "FX Settlement Risk: An Unsettled Issue." *BIS Quarterly Review,* December 2022. https://www.bis.org/publ/qtrpdf/r_qt2212i.htm.

BIS (Bank for International Settlements). 2025. "The next generation monetary and financial system", *Annual Economic Report*, June 2025, https://www.bis.org/publications/aer-2025.pdf.

BIS (Bank for International Settlements). 2026. "Digital Innovation and the quest for new forms of money", *Annual Economic Report*, June 2026, https://www.bis.org/publications/aer-2026_0.pdf.

BIS Innovation Hub. 2022. *Project Dunbar: International Settlements Using Multi-CBDCs*. March 2022. https://www.bis.org/publ/othp47.htm.

———. 2023. *Project Mariana: Cross-Border Exchange of Wholesale CBDCs Using Automated Market-Makers—Final Report.* https://www.bis.org/publications/project-mariana-cross-border-exchange-wholesale-cbdcs-using-automated-market-makers-final-report.

———. 2024a. *"Project mBridge Reached Minimum Viable Product Stage."* Updated November 11, 2024. https://www.bis.org/about/bisih/topics/cbdc/mcbdc_bridge.htm.

———. 2024b. *Project Mandala: Streamlining Cross-Border Transaction Compliance.* October 2024. https://www.bis.org/publ/othp87.pdf.

———. 2025. *Project Meridian FX: Exploring Synchronised Settlement in FX.* April 24, 2025. https://www.bis.org/publ/othp94.pdf.

———. 2026. *Project Agorá: A Shared Programmable Platform for Wholesale Cross-Border Payments.* May 27, 2026. https://www.bis.org/publ/othp110.pdf.

———. n.d. *"Project Nexus: Enabling Instant Cross-Border Payments."* Accessed October 28, 2026. https://www.bis.org/project/nexus.

CPMI (Committee on Payments and Market Infrastructures). 2022. *Extending and Aligning Payment System Operating Hours for Cross-Border Payments: Final Report.* CPMI Papers no. 203, May 2022. https://www.bis.org/cpmi/publ/d203.pdf.

———. 2023. *Facilitating Increased Adoption of Payment versus Payment (PvP): Final Report.* March 2023. https://www.bis.org/cpmi/publ/d216.pdf.

CPMI, BIS Innovation Hub, International Monetary Fund, and World Bank. 2022. *Options for Access to and Interoperability of CBDCs for Cross-Border Payments.* Report to the G20, July 2022. https://www.bis.org/publ/othp52.htm.

CPMI–IOSCO (Committee on Payments and Market Infrastructures and International Organization of Securities Commissions). 2012. *Principles for Financial Market Infrastructures.* April 2012. https://www.bis.org/pages/principles-financial-market-infrastructures/d101a.pdf.

CPMI–IOSCO (Committee on Payments and Market Infrastructures and International Organization of Securities Commissions). 2022. Application of the *Principles for Financial Market Infrastructures to stablecoin arrangements.* July 2022, https://www.bis.org/publications/application-principles-financial-market-infrastructures-stablecoin-arrangements-final-version.pdf

DTCC (Depository Trust & Clearing Corporation). 2024. *Managing the FX Challenge for T+1.* White paper, March 2024. https://www.dtcc.com/insights/2024/managing-the-fx-challenge-for-t1.

Eidan, Daniel, Jon Frost, Rudraksh Kansal, Ulf Lewrick, Sang Hyuk Lim, and Tomasz Rybarczyk. 2026. "Blockchain Consensus Mechanisms and Fragmentation." BIS Bulletin no. 126, July 6, 2026. https://www.bis.org/publ/bisbull126.htm.

GFXC (Global Foreign Exchange Committee). 2025. *FX Market Preparedness for the UK, EU, Switzerland and Liechtenstein Move to T+1 Securities Settlement.* December 2025. https://www.globalfxc.org/uploads/fx_market_preparedness_UK_EU_move_t1_securities_settlement.pdf.