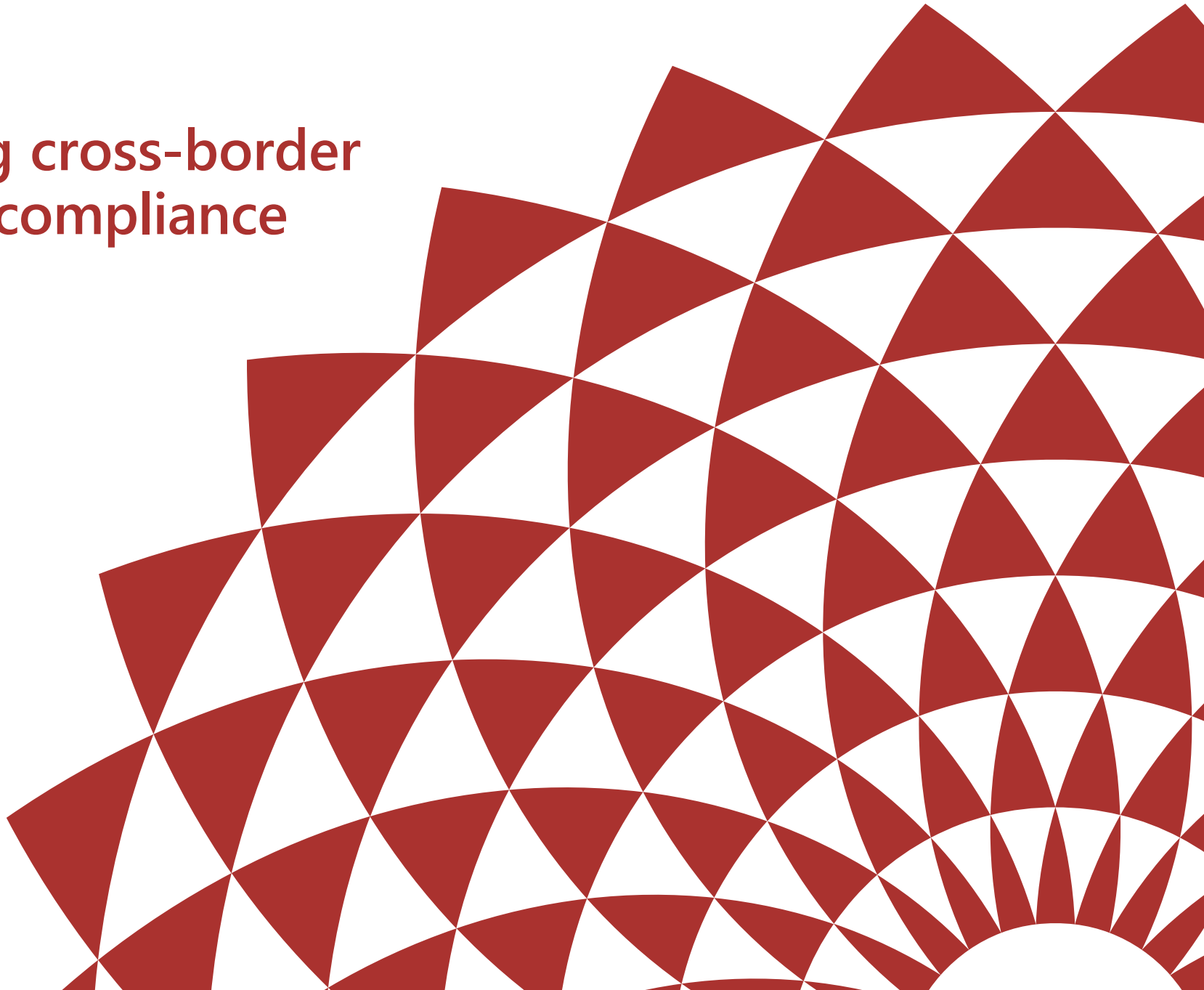
BIS Innovation Hub

October 2024

Project Mandala

Streamlining cross-border transaction compliance



Project Mandala

Streamlining cross-border transaction compliance

Publication date: 28 October 2024

ISBN 978-92-9259-798-6 (online)

Contents

Executive summary

Project Mandala uses a compliance-by-design approach to streamline cross-border compliance processes for financial institutions and explores real-time policy and regulatory compliance monitoring for central banks and other regulators.

The integrity of the financial system is key to a well functioning financial market. To protect the international financial system from illicit finance, regulators and policymakers around the globe have been increasing the regulatory requirements they impose on cross-border transactions. These measures reduce risk, increase transparency and enhance trust in the international payment system. However, as regulatory requirements have increased, so have the costs of compliance and risk mitigation for financial institutions.

Objective

Project Mandala's overarching objective is to increase the efficiency, transparency and speed of large-value cross-border transactions without compromising the quality and soundness of regulatory checks. The project explores a technological solution to automate compliance procedures, enhance transparency on country-specific policies, and provide real-time reporting and monitoring for regulators and supervisors. The project develops a system that allows each party to a transaction to easily conduct checks before funds are released.

Compliance by design

Project Mandala uses a compliance by design approach to streamline cross-border compliance processes for financial institutions and explores real-time policy and regulatory compliance monitoring for central banks and other regulators. The project preserves the existing regulatory framework whereby it encodes existing jurisdiction-specific regulatory requirements such as sanctions screening and capital flow management (CFM) measures into the system. Moreover, it maintains the current model, in which financial institutions are responsible for interpreting and applying official regulatory measures on their own accord.

The architecture of Mandala accommodates the different regulatory measures and risk profiles of participating financial institutions and their clients. The Project Mandala solutions architecture: (i) facilitates secure peer-to-peer communication between parties, without intermediaries; (ii) standardises regulatory inputs and outputs; and (iii) automatically generates cryptographic proofs of compliance. These compliance proofs can be attached to a digital settlement asset such as wholesale central bank digital currency (wCBDC) or to a Society for Worldwide Interbank Financial Telecommunication (Swift) credit transfer instruction. The proof ensures that compliance with relevant measures is achieved before the funds are released. Hence, the project demonstrates the technical feasibility of integrating with both nascent wholesale CBDC systems and existing payment messaging systems.

Project Mandala's system is tested on two use cases of cross-border transactions which were selected in consultation with the project partners and participating commercial banks. The use cases demonstrate how the system can adapt to different regulatory requirements within the four participating jurisdictions for cross-border lending and investment purposes.

Observed benefits

The Mandala system introduces several efficiency gains that are beneficial to commercial banks and regulators alike. First, the system reduces the likelihood of failed transactions, as compliance checks are moved into the pre-validation stage. Second, the project increases the efficiency and speed of compliance processes by introducing straight through processing and decreasing the number of intermediaries. Third, the project introduces transparency around country-specific policies and regulations, and transaction-specific information such as originator and beneficiary details. Finally, Project Mandala has the potential to improve user privacy as no unencrypted data are shared outside the bank environment, while ensuring compliance with pertinent financial integrity standards.

These benefits allow Project Mandala to support the G20 roadmap for enhancing cross-border payments by enhancing the efficiency, transparency and speed of cross-border transactions, while also safeguarding user privacy and promoting transparency around country-specific regulatory measures. There is potential for the Mandala system to reduce compliance costs, but more analysis is needed to substantiate this hypothesis. The project's compliance by design approach aligns with international regulatory priorities. These priorities include promoting the alignment and interoperability of regulatory and data requirements outlined by the Financial Stability Board (FSB) and improving payment transparency and data quality as proposed by the Financial Action Task Force (FATF).

Mandala is designed as a modular system that can integrate with different types of payment systems and supports interoperability, thereby preventing fragmentation and enabling compliance across different financial infrastructures. In the long term, Mandala's approach could enable seamless interoperability across regional payment systems, contributing to a more unified and efficient global financial market infrastructure.

Our partners

Project Mandala is a collaboration between the BIS Innovation Hub, Reserve Bank of Australia, Bank of Korea, Bank Negara Malaysia and Monetary Authority of Singapore with significant contributions from the Bank of France. The project is purely experimental and does not indicate that any of the involved commercial or central banks intend to deploy the Mandala system or endorse a particular technological solution. While Project Mandala does not imply a commitment by participating central banks to adopt these technologies, it offers valuable insights into the future of cross-border compliance and programmable compliance. The project's success in automating compliance procedures, increasing efficiency and enhancing privacy highlights its potential to reshape international financial transactions. Further research is needed to fully assess its legal, technical and commercial viability.

"In the long term, Mandala's approach could enable seamless interoperability across regional payment systems, contributing to a more unified and efficient global financial market infrastructure."

Acronyms, abbreviations and definitions

AML	Anti-money laundering
API	Application programming interface
BB	Beneficiary bank
BNM	Bank Negara Malaysia
BOK	Bank of Korea
CB	Central bank
CBDC	Central bank digital currency
CFM	Capital flow management
CFT	Countering the financing of terrorism
CPMI	Committee on Payments and Markets Infrastructure
CPU	Central processing unit
DLT	Distributed ledger technology
EVM	Ethereum Virtual Machine
FATF	Financial Action Task Force
FPGA	Field-programmable gate array
FSB	Financial Stability Board
GLEIF	Global Legal Entity Identifier Foundation
GPU	Graphics processing unit
HE	Homomorphic encryption
ISO	International Organization for Standardization
LEI	Legal entity identifier
MAS	Monetary Authority of Singapore
MPC	Multi-party computation
MYR	Malaysian ringgit
OB	Originating bank
P2P	Peer to peer
PETs	Privacy-enhancing technologies
PJC	Private join and compute
PSI	Private set intersection
RBA	Reserve Bank of Australia
RFI	Request for information
RTGS	Real-time gross settlement
Swift	Society for worldwide interbank financial telecommunication
SGD	Singapore dollar
wCBDC	Wholesale central bank digital currency
ZKP	Zero-knowledge proof
ZK-SNARK	Zero-knowledge succinct non-interactive argument of knowledge
ZK-STARK	Zero-knowledge scalable transparent argument of knowledge

1 Introduction

Integrity of the financial system

As the main gatekeepers of the financial system, financial institutions are on the front line in the battle against financial crime, and must prevent and detect illicit activities. As regulatory requirements have increased (Thomson Reuters (2020)), so have the costs for financial institutions of compliance and risk mitigation for any payment corridor they are sending payments through. The high cost of compliance has led to a reduction in correspondents (Borchert et al (2024)), resulting in less competition and higher fees for consumers. Moreover, the efficacy of the existing compliance process in the cross-border transaction context is marred by a lack of transparency, data standardisation, data quality issues, manual interventions and duplicative checks. Geopolitical tensions have resulted in additional complexity and the fragmentation of compliance requirements specifically around sanctions screening. The global surge in the adoption of comprehensive data protection laws and regulations, such as the General Data Protection Regulation, presents additional challenges. These regulations strictly limit the use of personal data, while financial institutions often collect more information than necessary upfront to mitigate the risks of penalties associated with non-compliance with anti-money laundering and countering the financing of terrorism (AML/CFT) requirements. This practice can strain customer trust and complicate data-sharing between entities in different countries.

National regulators and supervisors play a key role in compliance monitoring but often rely on manual, risk-based and ex post checks. Compliance monitoring is further aggravated in the cross-border context as divergent national approaches hamper effective cross-border collaboration. In the absence of a global supervisory mechanism and considering their limited resources, national supervisory and regulatory agencies could consider potential technological solutions that would support their efforts in compliance monitoring related to cross-border transactions, particularly in achieving a proactive approach to supervision and oversight.

To manage economic and financial stability, some jurisdictions put capital flow management (CFM) measures in place that regulate certain aspects of foreign exchange and currency inflow and outflow activity. This has further increased the compliance burden for cross-border transactions.

Project Mandala aims at streamlining cross-border compliance processes for financial institutions, while offering real-time compliance monitoring functionalities for central banks. To do this, the project deploys compliance by design, which is a systematic approach to integrating regulatory requirements into automated tasks and processes. Following this approach, the project encodes jurisdiction-specific regulatory requirements into a protocol. This protocol can be used for large-value cross-border transaction use cases selected for Project Mandala such as foreign investment, borrowing and payments. Should the Project Mandala solution prove to be a useful tool for supervision, compliance monitoring and reporting, it could enhance mutual reliance on compliance checks performed by participating commercial banks – reducing the need for duplicate checks and enhancing trust. Hence, the project depends on both public and private sector participants unlocking its full potential for enhancing cross-border payments compliance.

Mandala complements current work aimed at detecting and monitoring illicit financial activities such as Project Aurora (BISIH (2023a)) and Project Hertha (BISIH (2024b)). These projects support the detection of money laundering and financial crime patterns ex post. Project Mandala's compliance by design approach seeks to ensure compliance with pertinent measures ex ante.

This report describes the experimental setup of Project Mandala, its findings, as well as operational, policy and regulatory considerations for commercial and central banks. The remainder of the report is structured as follows. Section 2 provides a high-level project overview. Section 3 details the project's solution design including its core components. Section 4 describes the project's use cases. Section 5 discusses the results and key efficiency gains of the experiment. Section 6 lays out key considerations for policymakers, regulators and supervisors. Section 7 sets out potential areas of future work and Section 8 concludes.

2 Background

Disparate regulatory and policy frameworks across jurisdictions affect the ease of cross-border payments; they introduce uncertainties among stakeholders and slow down transaction speed.

Illicit financial activities such as money laundering and the financing of terrorism have been on the rise. Large sums of money are laundered every year. According to estimates, more than a $3.1 trillion in money laundering and terrorist financing flowed through the global financial system in 2023 alone.[1] The amount of money laundered globally is estimated to be between 2 and 5% of global GDP, and only a fraction of that is seized annually – between $20 billion and $50 billion (BISIH (2023a)). Moreover, jurisdiction-specific CFM measures impose additional considerations into cross-border compliance processes.

In response, there has been a 15% annualised growth rate in regulations over the last decade (Thomson Reuters (2020)) and banks have augmented their investments in programmes to combat financial crime and meet regulatory obligations. Banks consider the escalation of financial crime regulations and regulatory expectations as the primary factor driving increases in compliance costs (Forrester (2023)). Complicating the compliance burden is the disparity across jurisdictions of AML/CFT and other regulatory obligations and expectations. This is further aggravated by a range of laws, rules and regulatory requirements related to the collection, storage and management of data, which are also jurisdiction-specific. These disparate regulatory and policy frameworks across jurisdictions affect the ease of cross-border payments, introduce uncertainties among stakeholders and slow transaction speeds.

These issues are a focus area of the G20 roadmap for enhancing cross-border payments, which was developed to address the four challenges faced by cross-border payments of high costs, low speed, limited access and insufficient transparency. Specifically, improving the interaction between data frameworks and cross-border payments has been identified as a priority action in the G20 roadmap. In support of this, the Financial Stability Board (FSB) and its partner institutions are working to develop recommendations to address data-related frictions arising in cross-border payments, including promoting the alignment and interoperability of regulatory and data requirements, as well as promoting their consistent and widespread implementation (FSB (2024b)).

2.1 Intended outcomes

Project Mandala seeks to address some of the identified challenges, thereby supporting the G20 roadmap's objectives in cross-border payments. The project streamlines and automates several compliance procedures that are under disparate regulatory frameworks, a challenge identified in Project Dunbar (BISIH et al (2022)).

Project Mandala tests the hypothesis that embedding policy measures into a common protocol would automate compliance procedures and increase transparency and visibility around country-specific policies for financial institutions, while providing real-time compliance monitoring capabilities for central banks and other regulators. The most suitable policies and regulations for testing this hypothesis is a subset of measures that are quantifiable and configurable while respecting their jurisdiction-specific variations. These measures include controls designed to implement sanctions screening requirements and quantifiable CFM measures such as thresholds or limits that require approvals or reporting, as illustrated in Section 4.

Extensive consultation with commercial banks from participating jurisdictions confirmed that the most complex compliance obligations are related to sanctions checks using public and private lists, and compliance with pertinent CFMs.[2] Understanding and addressing those complexities would support the overarching objectives of cheaper, faster and safer cross-border payments.

Key intended outcomes

The first intended outcome is for Mandala to reduce regulatory uncertainties related to cross-border payments. To increase straight through processing, automated reconciliation and effective AML/CFT controls, which are stated G20 objectives for cross-border payment messages, Mandala extends the payment chain to include the pre-validation phase, closing the information gap on the originating entity. As part of the pre-validation process, financial institutions receive a compliance checklist, as detailed in Section 3.2. This checklist provides banks with information on applicable regulatory measures, based on the transaction inputs, before the payment can occur. By allowing compliance to be validated before clearing and settlement, Project Mandala aims to reduce the risk of payment delays due to request for information (RFI) processes, or payment reversals due to failed downstream compliance checks.

The second intended outcome is the standardisation of formats for the regulatory and policy requirements that are included in the Mandala proof of concept (PoC). For this purpose, the PoC develops templates included in the underlying rules engine (Section 3.2). This standardisation will form the basis of Mandala's modular compliance system, allowing for any new regulatory measures to be included or existing ones to be amended depending on the payment corridor or use case.

The third intended outcome for Mandala is modularity so that its components can be easily interchangeable and deployable across existing and nascent digital asset systems, with a strong focus on privacy preservation and operational efficiency.

The intended outcomes of Project Mandala align with the FSB's 2023 priority actions for achieving the G20 targets for enhancing cross-border payments in promoting an efficient legal, regulatory and supervisory environment for cross-border payments while maintaining their safety, security and integrity. For example, the FSB has issued a consultation containing recommendations for a range of policies to strengthen consistency in the regulation of payment service provision (FSB (2024a)). Project Mandala also aims to support the FSB and Bank for International Settlements' Committee on Payments and Markets Infrastructure's (CPMI) efforts to promote the use of global digital unique identifiers such as the legal entity identifier (LEI) (FSB (2022) and CPMI (2023)). The project also supports the objectives of the Financial Action Task Force's (FATF) proposed revisions to Recommendation 16, such as enhancing payment transparency, preserving the singleness of the payments chain and improving data quality (Section 6.3). Finally, there is potential for Mandala to support the Organisation for Economic Cooperation and Development's "data free flow with trust" initiative that aims to promote free data flow while ensuring privacy, oversight and protection.[3]

2.2 Project scope

Project Mandala uses a compliance by design approach to streamline cross-border compliance processes for commercial banks and explores real-time policy and regulatory compliance monitoring for central banks and other regulators.

The Mandala system retrieves and applies pertinent regulatory requirements into tasks and processes through the rules and proof engine (Sections 3.2 and 3.3). This approach introduces efficiencies and streamlines compliance processes as rules are automatically applied based on parameters entered through the messaging system (Section 3.1).

The relevant regulatory requirements related to compliance burdens in cross-border transactions have been determined based on two use cases deemed most relevant by the project partners and financial industry representatives from participating jurisdictions. These use cases help determine the project scope.[4] The selected use cases do not cover regulatory measures of specific jurisdictions exhaustively. Instead, they focus on the most relevant measures in the AML/CFT and CFM domains. The Project Mandala solution can be applied to both retail and wholesale cross-border transactions. The project focuses on large-value wholesale cross-border transactions for the selected use cases, in view of the potentially higher compliance burden as compared with retail transactions.

Based on industry consultations, Project Mandala included sanctions screening within the project scope, as well as compliance with selected CFM requirements, and their real-time compliance monitoring by central banks and other regulators. Analysis revealed that the most suitable candidates for Project Mandala are measures that are quantifiable, as they can be easily encoded and converted into a machine-readable format. Project Mandala deploys the two use cases to illustrate how the solutions architecture could address existing challenges related to regulatory compliance with the selected measures and introduce efficiency gains compared with the status quo.

"Based on industry consultations, Project Mandala included sanctions screening within the project scope, as well as compliance with selected CFM requirements, and their real-time compliance monitoring by central banks and other regulators."

- Use case 1 focuses on *compliance processes around cross-border lending from an entity located in Singapore to an entity located in Malaysia* and examines how Project Mandala can facilitate compliance checks by enabling provable sanctions screening and CFM measures to be conducted during the pre-validation phase. As an extension of use case 1, Mandala illustrates how central banks could deploy the developed solution for their CFM compliance monitoring.
- Use case 2 investigates *streamlining compliance processes related to the cross-border financing of capital investments involving corporations in Korea and Australia*. In this use case, a South Korea-based entity finances a capital investment by an Australia-based entity through the acquisition of its unlisted debt securities, and the payment for the securities involves a cross-border transfer and netting of existing obligations. This transaction could trigger CFM and netting notification requirements, subject to thresholds. As such, in addition to the concepts tested in use case 1, use case 2 addresses the challenges associated with the manual verification process of applicable CFM measures and netting reporting requirements.

To achieve the intended outcomes within the project timelines, several aspects were scoped out at this phase including identity solutions, customer onboarding, beneficial ownership information and enhanced due diligence for clients or correspondent financial institutions (eg the Correspondent Banking Due Diligence Questionnaire published by the Wolfsberg Group). Governance models, certain non-functional aspects (eg cybersecurity), full-fledged integration with existing systems and processes (eg real-time gross settlement (RTGS) or commercial bank systems), legal liability aspects and commercial viability considerations (eg cost of setup and maintenance) are also out of scope.

2.3 Overview of high-level system architecture

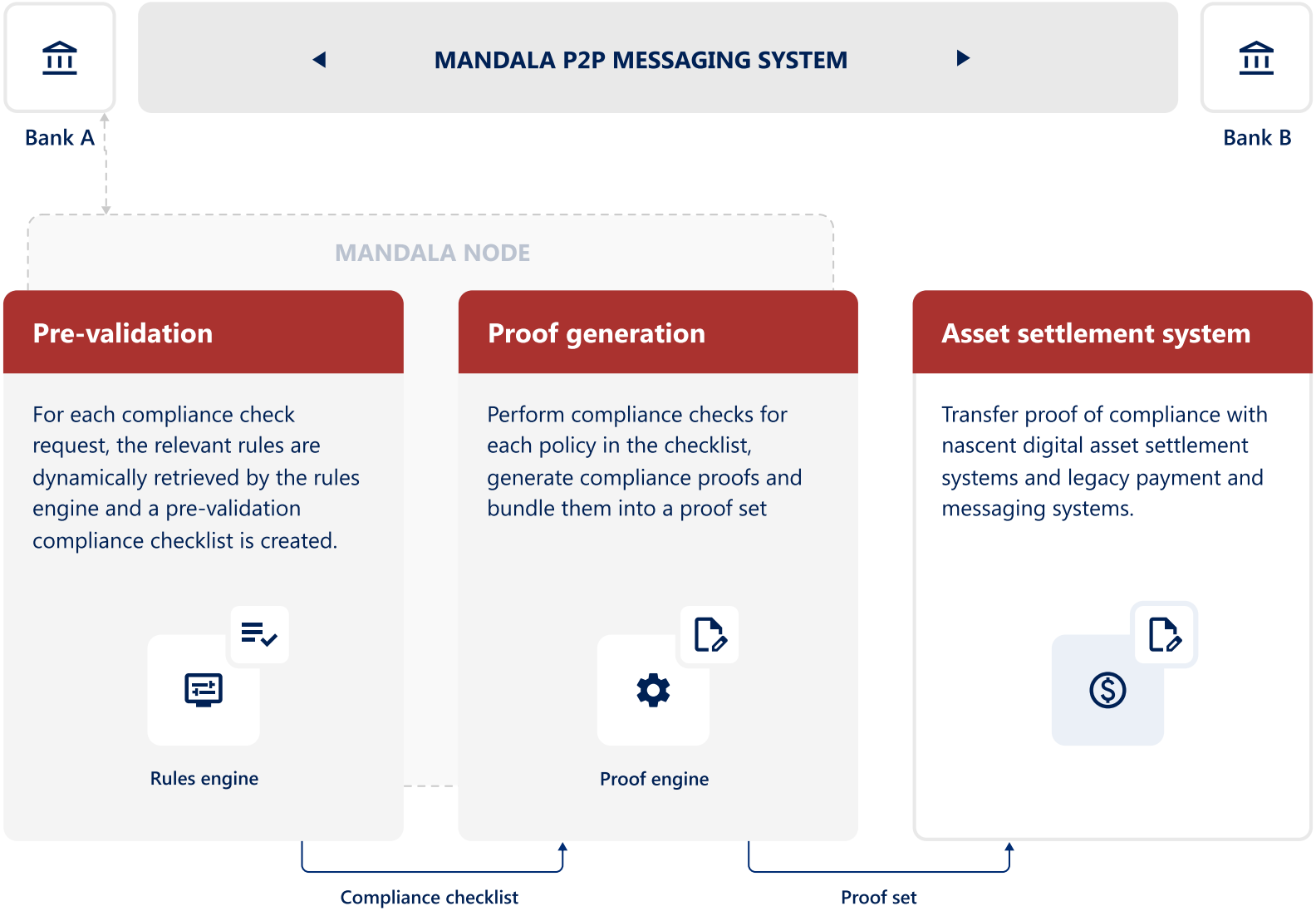
Mandala operates as a decentralised network of interconnected nodes, collectively known as the Mandala network. All participant institutions, including commercial banks, central banks and other regulated financial entities, operate a Mandala node. A node consists of three core components – a peer-to-peer (P2P) messaging element, the rules engine and the proof engine.

The nodes communicate directly via a P2P messaging system, eliminating the need for intermediaries. The P2P messaging system uses encrypted communication between nodes, ensuring data confidentiality. This messaging system facilitates the transmission of data necessary for generating proofs of compliance, sharing generated proofs and handling other essential communication tasks for automated compliance checks. Another core component of Project Mandala is the rules engine. Following the compliance by design approach, each Mandala node hosts a comprehensive policy library that standardises the representation of regulatory measures across various jurisdictions. This library includes templates for ingesting new policies and regulations, which are then converted into machine-readable instructions. The standardisation process enables the encoding of different measures from various jurisdictions as rules within the system.

The originator bank sends a compliance check request to the beneficiary bank (BB) before the transaction. After the request has been sent, the relevant rules are retrieved, and a pre-validation checklist with applicable rules for the transaction is created. For each rule in the checklist, the proof engine, another core component of the Mandala system, checks whether the rule has been met using client and transaction data, or, if required, by communicating with other commercial bank or central bank nodes to gather the information needed. The proof engine does so without sharing client data and generates the evidence (or proof) of compliance for each of these checks (see Sections 3.2 and 3.3).

These compliance proofs are then integrated into the asset transfer system or payment messaging system, providing evidence that all necessary compliance checks have been completed, and ensuring seamless and expedited value transfers (Graph 1).

Graph 1 – Mandala high-level architecture



3 Solution design

This section describes the solution design of the Mandala PoC based on the three core components – the P2P messaging system, the rules engine and the proof engine.

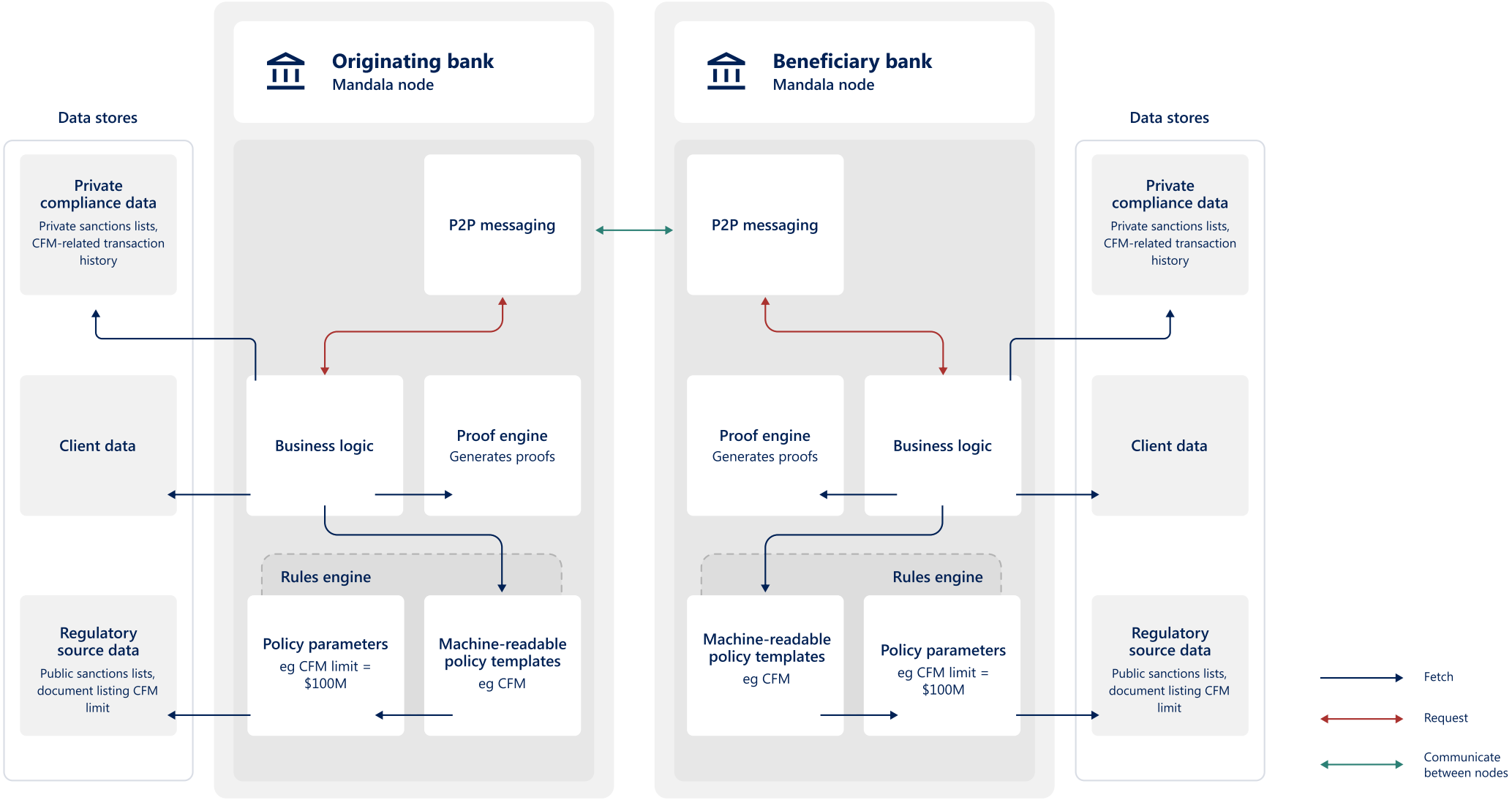
Mandala preserves the existing model in which financial institutions independently interpret and apply official regulatory measures.

In alignment with this approach, each participating financial institution is responsible for the proper functioning of its node, including maintaining the code and updating databases to ensure the accuracy and currentness of the applicable measures.

The P2P messaging system enables banks to exchange instructions related to compliance checks without the need for an intermediary. The rules engine determines the applicable regulations, and the proof engine generates compliance proofs in a privacy-preserving manner using secure multi-party computation (MPC),[5] zero-knowledge proofs (ZKP)[6] and digital signatures. The full stack of the Mandala components are referred to as nodes, and each participant in the Mandala system runs their own node.

The PoC also provides implementations for both local verification of compliance proofs at the node level to support existing payment flows using ISO20022 messages, as shown in Section 5.2, and DLT verification implemented as Ethereum Virtual Machine (EVM)-compatible smart contracts to support digital asset transactions. The full solution design is shown in Graph 2, and the full transaction flow with Mandala in place is described in Section 4.

Graph 2 – Mandala solution design



Business logic orchestrates the functions of various components within the Mandala node

3.1 Peer-to-peer messaging system

Project Mandala uses a P2P network allowing for compliance checks to be coordinated directly between banks rather than through a centralised intermediary.

The network facilitates direct encrypted communication between participants without exposing any data to third parties or intermediaries.

Mandala's P2P network is made up of nodes running in the system of participating central and commercial banks. Each node is assigned a unique identifier when it joins the network. Nodes in the P2P network define and perform pieces of work collaboratively in the form of tasks. These tasks include listing known peers in the network, coordinating interactive compliance checks and communicating local compliance policies to other nodes attempting to perform a compliance check.[7]

Message fields and codes were designed to align with the ISO 20022 standard, where feasible, to simplify adoption. However, the Mandala P2P messaging system requires less data than ISO20022 messages in the existing transaction context.

3.2 Rules engine

The rules engine in Mandala converts regulations into a machine-readable format and determines the regulations that the proof engine must check for each specific transaction.

Translating rulesets to computational operations

By translating the rulesets from the rules repository into code, the PoC established general computational operations for compliance checks in the proof engine. These operations establish a standard pattern for compliance checks which can be applied to a wide array of regulatory measures. They also specify the information necessary for applying the rules, which typically includes client and transaction details. The identified computational operations are checks related to public and/or private sanctions lists and regulatory thresholds.

Ruleset gathering and application

When initiating a compliance check, the originating bank (OB) node may not know all relevant policies and regulations. The OB node can query the BB or the regulatory node through the P2P messaging system to gather transaction-relevant regulatory measures. For example, in use case 1, as described in Section 4.1, the Bank Negara Malaysia (BNM) imposes a policy obligation relating to CFMs for borrowing from a non-resident entity. Although Project Mandala created the rules for an originating and BB and a central bank for use case 1 (Section 4), any intermediary in the payment chain can define their own specific rules.

For each incoming compliance check, the rules engine matches compliance check parameters with encoded policies and regulations. These parameters are transaction details which the OB inputs at the start of a compliance check. The key parameters required to trigger the relevant measures that are considered in the PoC are:

- from jurisdiction;
- to jurisdiction;
- transaction type (eg loan drawdown, loan repayment and acquisition of unlisted securities); and
- transaction amount.

Once all relevant rules from the database and those obtained from the beneficiary bank node are identified, they are passed to the proof engine for execution.

Policy and regulatory repository

The internal policy and regulatory repository standardises how applicable cross-border payment regulations are integrated into the system. It focuses on quantifiable, machine-readable rules. The repository organises rules based on standardised templates, enabling seamless input and output interactions with the rules and proof engines. On the input side, the rules cover numerical and categorical data such as thresholds and sanctions list checks. On the output side, it supports binary decisions or notifications. These standardised templates ensure efficient rule management, allowing easy creation, modification and testing of compliance measures while maintaining the integrity of the overall framework.

3.3 Proof engine

The proof engine is a core element of the Mandala system that automatically carries out compliance checks and generates cryptographic compliance proofs. Each compliance check validates against existing regulatory requirements that apply for a particular transaction.

The proofs are aggregated into a proof set that is mapped to a unique identifier called a compliance check identifier (CCID). The participants along the payment chain may verify each of the proofs in the proof set as an alternative to performing duplicate compliance checks themselves.

Project Mandala defines two types of decentralised compliance checks: non-interactive checks and interactive checks. Both types preserve the privacy of input data from the other participants. In the Project Mandala use cases, it is either the OB and BB; or the BB and the central bank participating in the required checks. There are also local checks which can be performed by the banks themselves using their internal rules.

Non-interactive checks

Project Mandala uses non-interactive checks where one party holds confidential data necessary for a compliance check. A party can prove to another party that it has completed the required check without sharing the underlying data. The non-interactive checks are implemented via ZKPs – cryptographic protocols for proving the validity of a statement without having to share data (Box A). ZKPs generate a shareable proof that the check has been executed correctly.[8] When executed, the proof is produced in the form of a receipt – a list of public outputs of the compliance check and a proof based on ZK-STARK (Box A) that can be verified to show the compliance check was executed correctly.[9]

Non-interactive checks are a good fit for public sanctions list checks because all data needed to perform the check and produce a proof are known by the proof-generating party, ie the OB knows the public sanctions lists, and their client data. In a standard compliance check flow, the OB conducts the public sanctions list check and generates a verifiable proof. The proof includes a hash of the sanctions list to verify that the correct version was used.

"Project Mandala defines two types of decentralised compliance checks: non-interactive checks and interactive checks. Both types preserve the privacy of input data from the other participants."

Box A: Zero-knowledge proofs – a primer

Zero-knowledge proofs (ZKPs) are cryptographic protocols that allow one party (the prover) to demonstrate to another party (the verifier) that they possess certain knowledge or information without revealing the information itself. This method ensures privacy and security by only proving the validity of the information rather than sharing the details. ZKPs are particularly useful in scenarios in which sensitive data need to be verified without exposure.

Two popular ZKPs are:

- **ZK-STARK:** a ZKP system designed to be scalable and transparent. It relies on cryptographic hash functions for security and does not require a trusted setup phase, which enhances transparency and trust. ZK-STARKs can handle large computations efficiently and are well suited to applications needing high scalability and public verifiability such as layer 2 blockchains based on zero-knowledge proofs to scale the Ethereum blockchain, decentralised oracles and verifiable credentials.
- **ZK-SNARK:** a ZKP system that is succinct and non-interactive. This means the proofs are short and the verification process is efficient. They use advanced cryptographic techniques like elliptic curve pairings to achieve compact and quickly verifiable proofs, making them suitable for on-chain verification in blockchain applications in which efficiency and minimal interaction are critical.

Since the generation of ZKPs are computationally intensive, Project Mandala explores ways of using a special type of integrated circuits called field programmable gated arrays (FPGA).[10] By combining the power of existing computer processors with FPGAs, the speed of the end-to-end proof generation would be two to five times faster while reducing the cost by half compared with using the standard graphics processing units (GPUs). The improvements in cost and speed were benchmarked for a specific relevant operation SHA256 hashing which are tabulated in Appendix C.

"Project Mandala uses non-interactive checks where one party holds confidential data necessary for a compliance check."

Interactive checks

Interactive checks are applied where both parties provide data that are commercially sensitive or confidential. Through a multi-party computation (MPC) approach (Box B), both parties collaboratively compute the result of the check without revealing their individual inputs.

In the Mandala use cases described in Section 4, interactive checks were implemented for private sanctions lists and CFM checks. For private sanctions list checks in the Mandala PoC, the OB holds the client data, and the BB has a private list. The Mandala protocol allows them to perform a set intersection check without the other party gaining insights into the input data. For CFM checks, the OB holds the client data along with the transaction details and the central bank maintains a database with records of CFM approvals and outstanding loans.

Using the Mandala protocol, the parties perform arithmetic checks that ensure no CFM limits are exceeded, without letting the other party know the exact data inputs. Upon completing these interactive checks, the involved parties sign a message with their private keys,[11] confirming that their checks have been finalised. This signature serves as a verifiable proof in the proof set.

Two MPC frameworks are deployed for the interactive checks within the Mandala PoC, as laid out below.[12] The first MPC implementation, private join and compute (PJC),[13] is employed to securely check whether client details appear in the private sanctions list of the BB, without sharing the client's details or the content of the BB's list. PJC implements private set intersection and homomorphic encryption, as described in Box B.

In the context of Mandala, the PJC framework does not completely prevent the risk of participants, such as commercial banks, violating the protocol's rules. This could lead to exposure of private data, for example. To mitigate these risks, the project adopted a second, more robust MPC implementation to ensure that the MPC execution is immediately halted, and the data are kept secure, in case of suspected malicious behaviour. This approach is more reliable where complete trust in the participating parties cannot be assumed, which could be the case in the Mandala system.

"Interactive checks are applied where both parties provide data that are commercially sensitive or confidential."

Box B: Multi-party computation – a primer

Secure multi-party computation (MPC) enables a group of independent data owners, who do not trust each other or any common third party, to jointly compute a function that depends on all their private inputs. There are various types and implementations of MPC to suit different use cases. Project Mandala uses MPC for private sanctions list checks and capital flow management measures, as detailed in Appendix A.

Key MPC concepts:

- **Private set intersection (PSI):** allows a group of parties to jointly compute the intersection of their input sets without revealing any information related to those sets.
- **Homomorphic encryption:** a form of encryption that permits computations to be performed on encrypted data without the need for decryption. The results remain in an encrypted form and, when decrypted, yield an output identical to that produced if the operations were performed on unencrypted data.
- **Cryptographic hash functions:** hash functions transform input data into fixed-size hash values that appear random and unique for different inputs, ensuring data integrity and security. They are used in various security protocols to verify data authenticity and integrity without exposing the actual data. In MPC, hash functions are vital for creating hashes of data that allow for secure comparison without revealing the data.
- **Oblivious pseudo-random function (OPRF):** an OPRF allows one party to compute a pseudo-random function on an input, with the help of another party, without learning anything about the input or the output. This is crucial for secure multi-party protocols where function evaluations need to be hidden. OPRFs are often used in conjunction with PSI to enhance privacy.

Local checks

The proof engine can also perform local checks that neither require generating an actual proof nor communication with other nodes. These checks are internal compliance measures that commercial banks wish to perform based on their specific risk profiles.

Compliance proof verification

Proof verification allows the party that is verifying the proof, ie the verifier (the BB node), to ensure that the prover's (the OB node) check was completed successfully, and the outputs are truthful. Proof verification happens instantly and requires relatively little compute resources compared with the proof generation.

In a digital asset system, a smart contract verifies the proof set, including both non-interactive and interactive proofs. The smart contract verifies the proof set, ensuring the hash of the public sanctions list matches the latest version. Additionally, it validates the signatures by checking that the content of the signed message is correct and the signatories are authorised. The transaction receipt from the smart contract acts as a log of the proof verification. Automatic proof verification through smart contracts introduces programmable compliance for digital assets, as laid out in Section 5.1.

In the existing payment system flow, the BB node verifies the validity of the compliance proof. Depending on regulatory requirements, the BB node may log that it has performed the verification. For auditing purposes, a cryptographically valid proof is sufficient to verify compliance with all relevant measures. Nevertheless, the BB may also conduct its own public sanctions check upon receiving the payment initiation message.

4 Use cases and process flows

This section presents an overview of the selected use cases. Participating commercial banks identified several mandatory regulatory checks as the most challenging aspects of transaction processing.

Although there are common regulatory challenges for all cross-border payments, such as sanctions screening, there are also obligations that are transaction-specific and jurisdiction-specific including the payment corridor, amount, purpose of the transfer and location of the final beneficiary.

The project selected two use cases illustrating how Project Mandala can address regulatory compliance challenges faced by institutions processing high-value cross-border payments. The two use cases focus on commercial bank operations: Singapore-Malaysia lending operations and South Korea-Australia cross-border financing. Additionally, the first use case includes the central bank's role in monitoring compliance with CFM measures. Appendix E lays out the full list of regulatory and policy obligations. The common regulatory and policy compliance challenges addressed in both use cases include managing divergent regulatory frameworks across jurisdictions, conducting post-transaction regulatory verifications and eliminating duplicate regulatory checks.

"The project selected two use cases illustrating how Project Mandala can address regulatory compliance challenges faced by institutions processing high-value cross-border payments."

4.1 Use case 1: cross-border lending between Singapore and Malaysia

This use case examines how Project Mandala can facilitate compliance checks for cross-border lending from a Singapore-based entity to a Malaysia-based entity by enabling provable sanctions screening and CFM measures to be conducted during the pre-validation phase.

In addition, Project Mandala explores the potential to streamline selected CFM processes, such as reducing the need for self-declaration forms from the borrowing entity for transaction amounts that exceed the stipulated threshold as well as duplicate checks at the repayment leg.

To illustrate the use case further, Malaysia currently implements macroprudential measures whereby Malaysian resident entities are subject to an outstanding limit of MYR 100 million equivalent for foreign currency-denominated external borrowing obtained from non-residents that are not related parties, such as overseas banks or private equity firms.[14] External borrowing above the limit would require prior approval from BNM before drawdown. In facilitating resident client's inbound payments arising from drawdown of external borrowing, compliance checks by Malaysian commercial banks typically involve obtaining a declaration from clients on the outstanding borrowing amount and an approval letter from the central bank (if there is one). This could result in delayed crediting of the payment. Furthermore, the subsequent repayment leg is subject to a similar process of compliance checks, before the commercial bank will allow the repayment to go through, to ensure that the earlier loan drawdown was compliant. The detailed process steps of the loan repayment flow before and with Mandala are explained in Appendix E.

Currently, the loan drawdown process involves several steps included below and further illustrated in Graph 3.[15]

1. If the new foreign currency loan brings the borrower's outstanding external borrowing above MYR 100 million equivalent on a cumulative basis, the borrower seeks an approval from BNM prior to drawdown.
2. The BNM provides the necessary approval to the borrower for this loan drawdown.
3. The borrower submits the approval letter to the Malaysian commercial bank which is the beneficiary bank (BB) and holds the borrower's crediting bank account.
4. Upon notification by the borrower, the lender initiates the loan disbursement process to the borrower through the originating bank (OB).
5. The OB receives the lender's request and performs the necessary AML/CFT checks, such as sanctions screening.

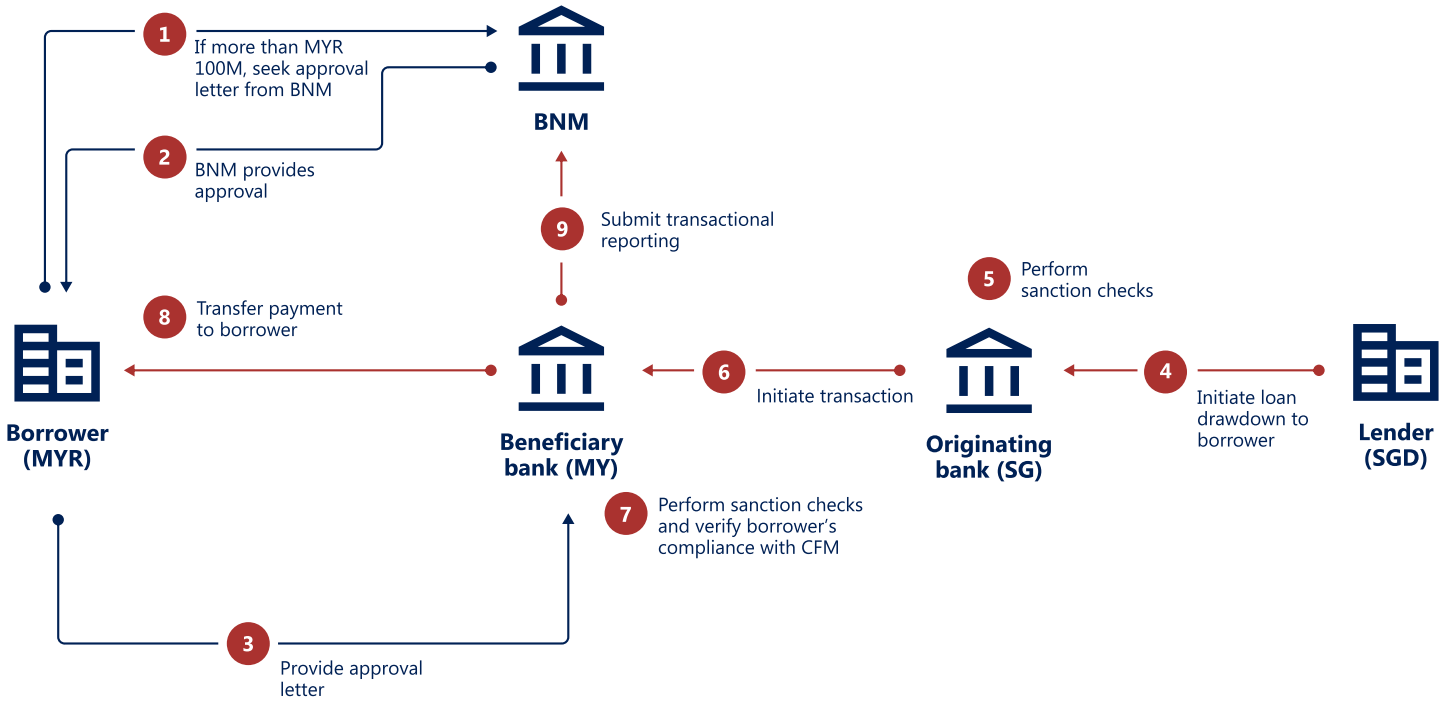
6. After these checks, the OB initiates the transfer to the BB.

7. Upon receiving the transfer request, the BB conducts AML/CFT checks and requests a confirmation from the borrower to verify their cumulative outstanding borrowing with the addition of the new loan drawdown. If the cumulative outstanding borrowing exceeds MYR 100 million equivalent, the borrower provides the approval letter to the BB (if not already done in step 1).

8. After receiving either the confirmation or approval letter, the BB releases the funds to the borrower. If the borrower failed to obtain prior approval from BNM, the BB rejects the payment and returns the funds to OB.

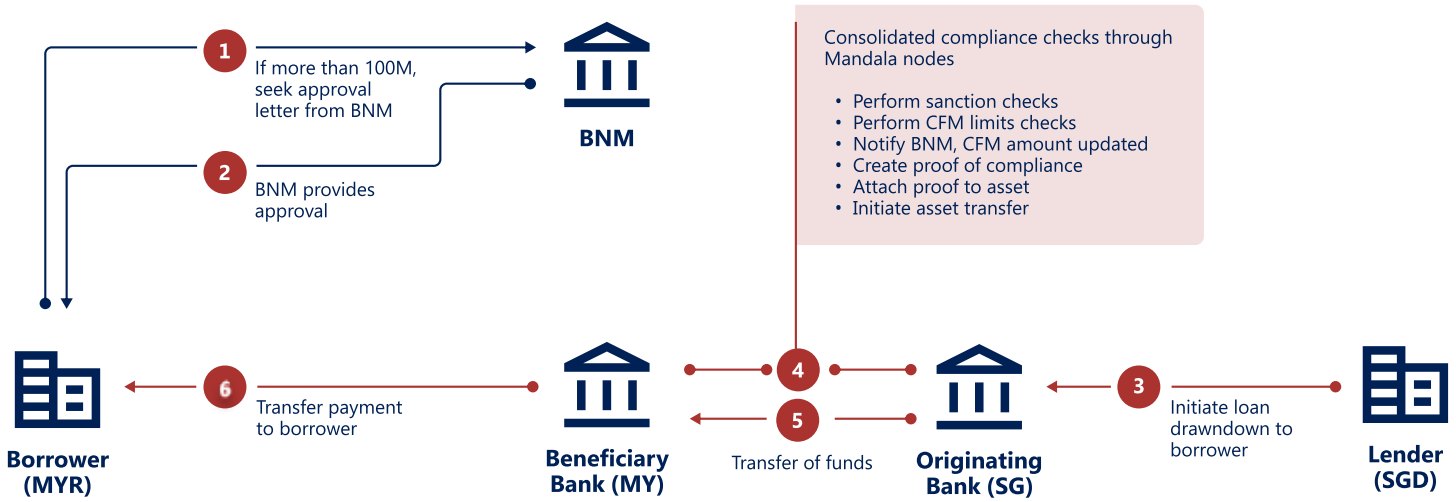
9. Finally, the BB submits transactional reporting to BNM on the completed loan drawdown for CFM compliance monitoring.

Graph 3 – Loan drawdown process before Mandala



Project Mandala introduces transparency, efficiency and privacy into the existing cross-border lending process depicted in use case 1. First, the OB will know all compliance requirements ex ante in the pre-validation phase via the rules engine, as laid out in Section 3.2. Second, the proof engine consolidates all required checks, such as sanctions screening and CFM checks, into one single action removing sequencing and truncation of the process flow, as illustrated in Graph 4.[16] Third, the verification of any central bank approval records can also be performed concurrently via the central bank node that is connected to an internal database, eliminating the need for manual sighting of the approval letter by the BB. Fourth, each loan drawdown receives a unique identifier, which is used to identify associated loan repayments, removing the need for additional supporting documents such as the BNM approval letter, as described above. Finally, Project Mandala enables provable checks while preserving privacy related to commercially sensitive data such as private sanctions lists.

Graph 4 – Loan drawdown process with Mandala



Central bank CFM compliance monitoring use case

Due to the limited availability of real-time data, central banks face challenges in monitoring compliance with CFM requirements. For example, current inefficiencies in the monitoring process in relation to use case 1 include:

1. The central bank would process applications from a borrower seeking to undertake external borrowing above the permissible threshold or borrowing limit. After an approval is granted, the central bank manually tracks and reconciles the payment flows of loan disbursements and repayments reported by commercial banks to ensure external borrowing is within the resident's permissible limit or scope of the approval granted.
2. The manual process for tracking payment flows can be time-consuming and inefficient for effective monitoring of external borrowing activities. Ideally, the central bank should have real-time access to such data and information.[17]
3. Central banks also have limited real-time visibility on cases of non-compliance, ie when borrowers attempt to drawdown an external loans without obtaining prior approval. BBs in Malaysia typically handle these checks and report non-compliance cases ex post.

Project Mandala demonstrates the potential to simplify the CFM reporting and monitoring process, eliminating the need for central banks to track and reconcile transactions manually. Commercial banks notify the BNM of the transfer and the CFM utilisation amount immediately through the Mandala protocol. This automation streamlines the compliance monitoring process as outstanding loan amounts are tracked and updated automatically. Moreover, the Mandala protocol automatically verifies that the transaction details match the previously approved loan drawdown, removing the need for human verification. The Mandala system enables central banks to monitor CFM compliance in real time through a designated central bank dashboard.

"Project Mandala demonstrates the potential to simplify the CFM reporting and monitoring process, eliminating the need for central banks to track and reconcile transactions manually."

4.2 Use case 2: cross-border financing for capital investments between South Korea and Australia

Use case 2 explores the use of Project Mandala in streamlining compliance obligations associated with a cross-border financing transaction.

In this use case, a South Korea-based entity seeks to finance a capital investment by an Australia-based entity through the acquisition of its unlisted debt securities. The originating (South Korean) bank covers the payment for the securities partially by a credit transfer and partially by netting of existing obligations. Prevailing South Korean regulations classify this as a capital transaction.

The Korean CFM framework requires commercial banks to verify whether a payment instruction requested by a client is subject to reporting under CFM, based on factors such as transaction type (capital or current), payment type (gross or net), total investment or any offsetting of the payment amount. A significant challenge in this framework is manually checking whether a transaction is subject to CFM and netting reporting. Korean commercial banks currently perform manual verification of transaction details to ensure compliance with the CFM reporting requirements (Box C).

Use case 2 expands the concepts tested in use case 1 to address the challenges associated with the manual verification process of applicable CFM measures and netting reporting requirements. The steps involved in establishing the netting requirements are:

1. Identifying and verifying specific transaction amounts:
   - securities acquisition amount [A]: the total value of securities being acquired;
   - offset amount [B]: the portion of the transaction amount that is offset against existing obligations; and
   - transaction amount [C]: the net amount to be transferred after accounting for offsets (C = A – B).
2. Verifying if the amounts meet the thresholds included in Box C.

Box C: Summary of Korean capital flow management measures

Amount type	**≤ US$5,000**	**US$5,000 < amount ≤ US$100,000**	**≤ US$100,000**
Securities acquisition amount (A)	No reporting required	No reporting required; unless cumulative amount above US$100,000*	Reporting to Bank of Korea (BOK)
Offset amount (B)	No reporting required	Bilateral offset: reporting to foreign exchange banks (FEB) Multilateral offset: reporting to BOK[1]	
Transaction amount (C)	No reporting required	FEB to verify the purpose of the transfer	

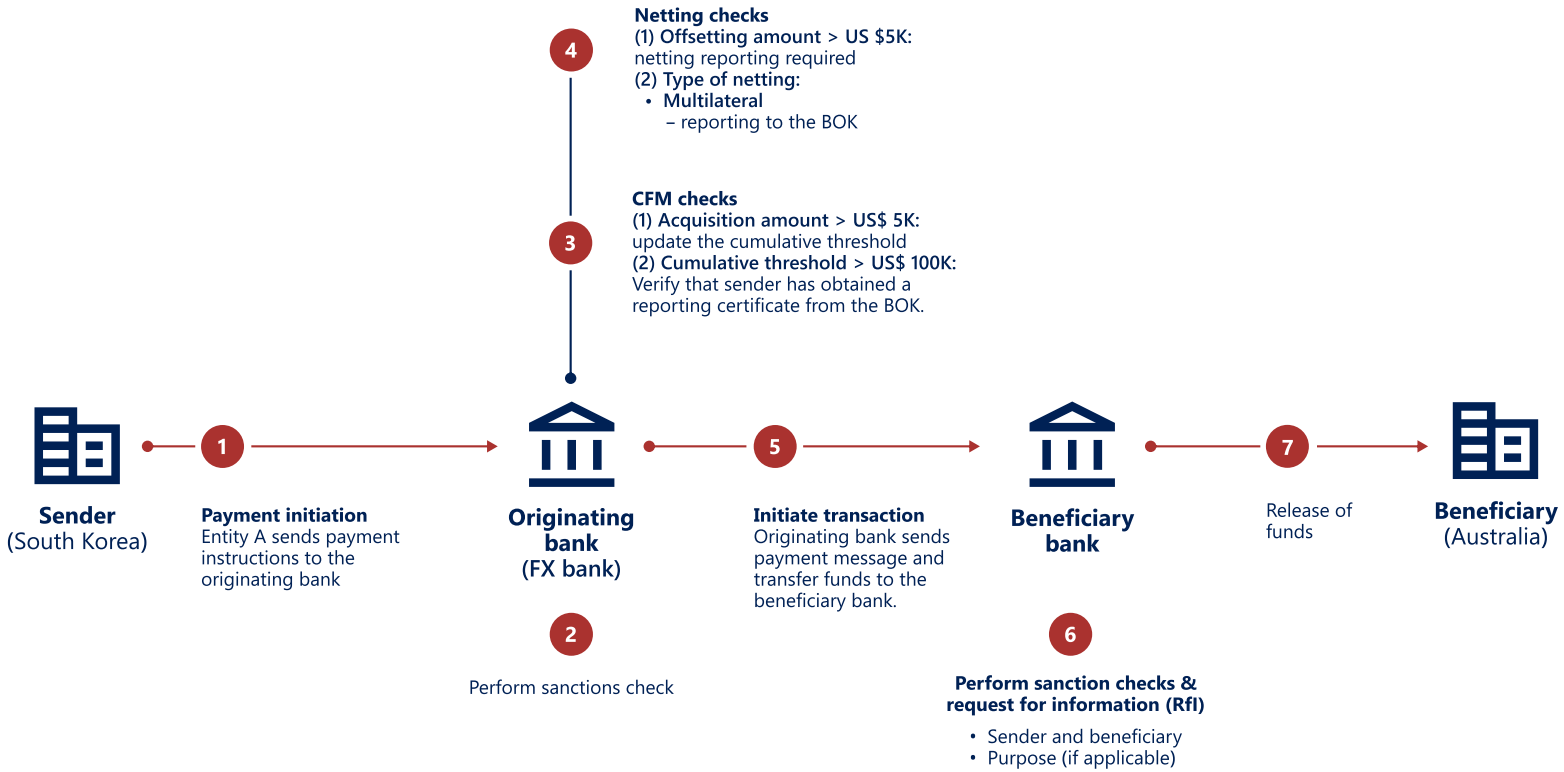
* Cumulative amount = ∑Ti where Ti are the transactions exceeding US$5,000. The cumulative amount is reset on 1 January each year.

The current process for acquiring unlisted debt securities involves several steps as described below and illustrated in Graph 5.[18]

1. The originator company initiates the payment process by sending the payment instructions to the originating bank (OB).
2. The OB receives the payment instructions and performs the necessary AML/CFT checks, such as sanctions screening.
3. The OB also performs CFM checks to verify the purpose of the transfer and ensure that the transaction amounts (eg securities acquisition amount, offset amount and transaction amount) fall within the thresholds. If the securities acquisition amount exceeds US$5,000, the OB updates the cumulative amount. If the securities acquisition amount exceeds US$100,000, or when the cumulative amount exceeds US$100,000, the OB must ensure that the originator has obtained the necessary reporting certificate from the Bank of Korea (BOK).
4. The OB then checks if the offset amount exceeds US$5,000 and, if it does, determines whether the transaction falls under a bilateral or multilateral netting arrangement. For multilateral netting, the OB is also required to verify that the originator has obtained the necessary reporting certificate from BOK before proceeding.
5. After completing these checks, the OB transfers the payment to the beneficiary bank (BB).
6. The BB receives the payment notification and performs the necessary AML/CFT checks. The BB requests any required information from the OB if needed.
7. Once all checks are completed, the BB releases the funds to the beneficiary. However, if AML/CFM checks fail on the BB side or the OB cannot provide additional information requested by the BB, the payment will be reversed.

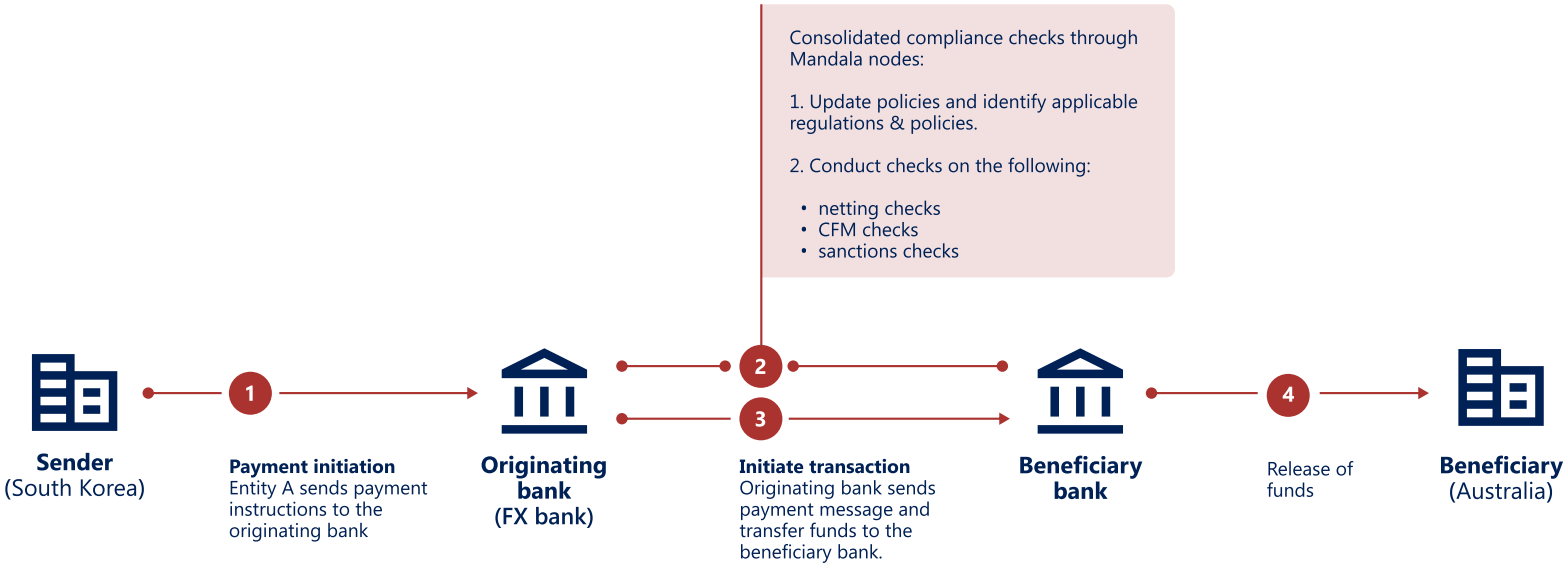
Finally, upon receipt of the unlisted debt securities, the originator is required to notify the Australian Transaction Reports and Analysis Centre (AUSTRAC) within 10 days of the transfer.

Graph 5 – Acquisition of unlisted debt securities before Mandala



In addition to the benefits associated with the consolidation of required sanctions and CFM checks and the privacy preservation demonstrated in use case 1 (Section 4.1), use case 2 presents additional potential for streamlining cross-border compliance processes, as shown in Graph 5.[19] First, the use case can streamline the verification of required reports that need to be submitted to relevant authorities for capital transactions conducted via netting arrangements such as BOK and the foreign exchange bank (FXB). Second, the proof engine automatically verifies if the amounts meet the thresholds, streamlining the process as detailed in steps 3 and 4 of the current process flow described above. Third, if a transaction exceeds the prevailing CFM thresholds, the OB node will automatically notify the relevant authorities, eliminating additional reporting requirements ex post. Although use case 2 does not include a full-fledged central bank node, such a capability can be enabled in future phases (Section 7).

Graph 6 – Acquisition of unlisted debt securities with Mandala



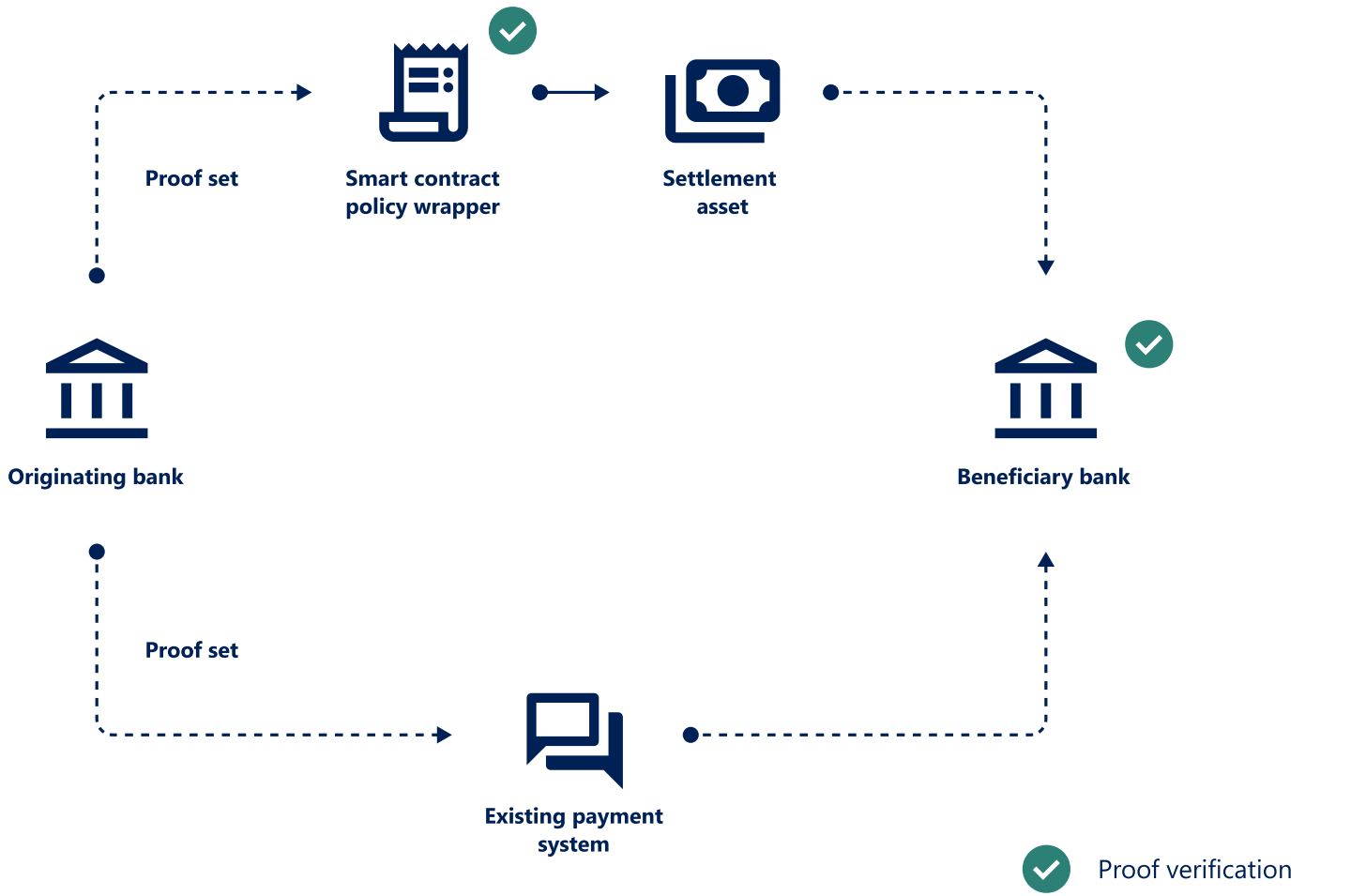
5 Integration with asset settlement systems and key findings

As part of Project Mandala, the compliance proof was successfully integrated with the wCBDC originally developed within Project Mariana (BISIH et al (2023)). It was also integrated with Swift, the most widely used messaging system.

The wCBDC integration required a special policy wrapper designed to facilitate proof verifications and programmable on-chain compliance, as described in Section 5.1.

Integration with Swift was achieved by including the compliance proof within a field in a credit transfer message, as detailed in Section 5.2. Project Mandala demonstrates the wCBDC integration based on use case 1 and the Swift integration for use case 2. A simple process overview for both integration approaches is shown in Graph 7.

Graph 7 – Asset settlement system



5.1 Integration with digital asset settlement systems

The proof set was designed to be verifiable in smart contracts and hence enable digital asset systems to use Mandala as a modular compliance component that allows for programmable compliance – embedding policy requirements directly into the core logic of an asset or a policy wrapper.

Conceptually, Mandala can be used with various forms of tokenised central bank money, tokenised commercial bank deposits, regulated stablecoins and other tokenised assets.

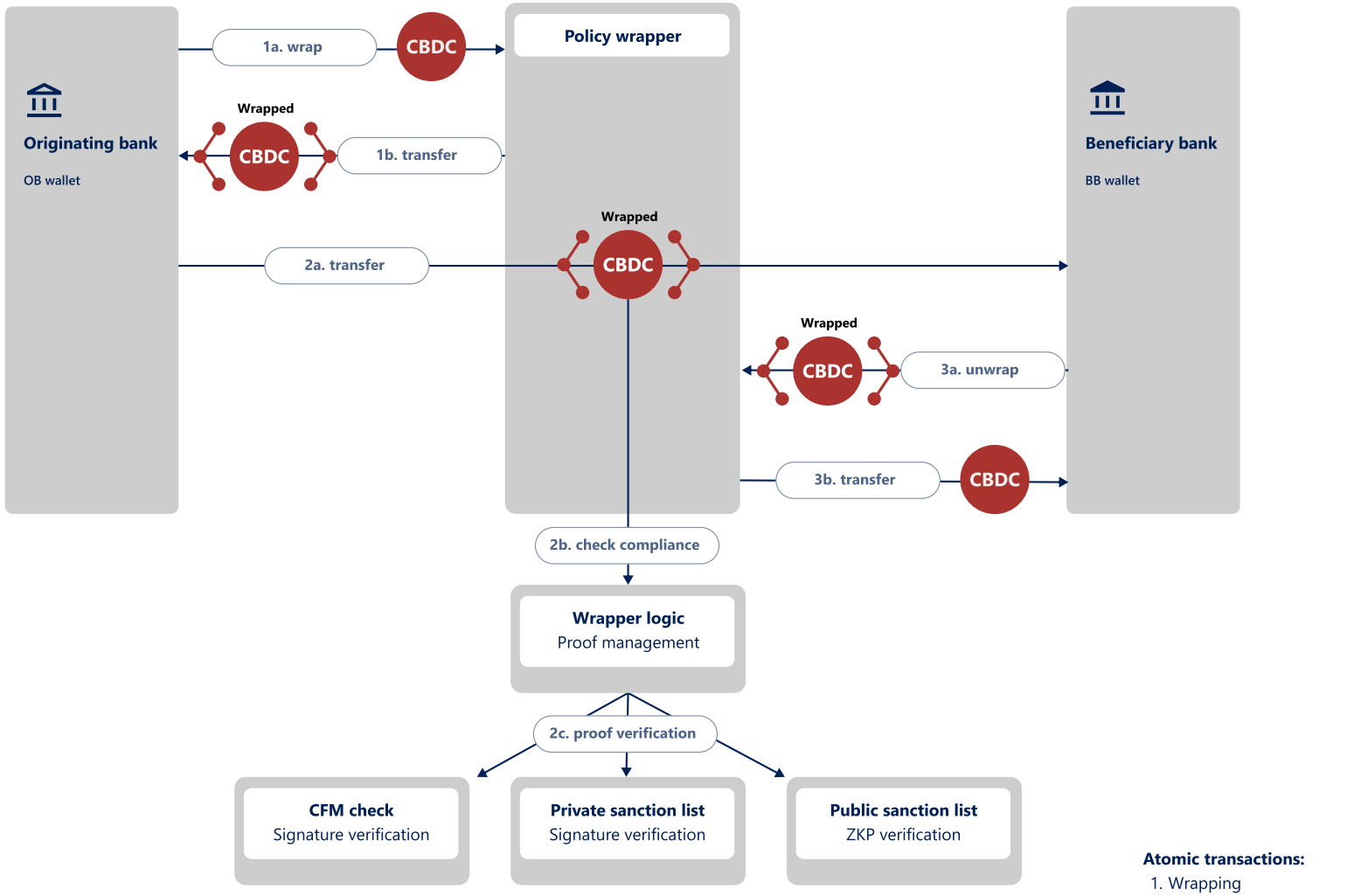
The OB wraps the wCBDC into a pre-deployed policy wrapper contract – the wCBDC tokens are locked in the policy wrapper and the same amount of wrapped wCBDC tokens are minted to the OB's account in return. The OB then calls the transfer function which sends the wrapped wCBDC to the BB. The transfer function of the policy wrapper requires a valid proof set. Each proof in the set has a specific verifier contract, so the transfer only succeeds if each verifier confirms the validity of the respective proof in the proof set. Verifier contracts differ depending on the nature of the underlying proof to adjust to the proof data formats described in Section 3.3. The benefit of supplying proofs of compliance to the smart contract is that most of the compliance checks are performed off-chain, ensuring data privacy and reducing transaction costs.

Once received, the BB can unwrap the wrapped wCBDC. The wrapped tokens are burnt and the same amount of wCBDC is released from the wrapper contract and sent to BB's account. Before unwrapping, the BB has the option to double-check all compliance proofs.

For demonstration purposes, the PoC successfully integrated with project Mariana's wCBDC, deployed on Sepolia testnet (BISIH et al (2023)).[20] This integration leverages MAS's purpose-bound money (PBM) concept (EIP-7291) as a policy wrapper (MAS (2023)). Hence, Project Mandala demonstrates a viable evolution of the MAS PBM concept in the cross-border payments context, as depicted in Graph 8. The Mandala project evaluated compatibility with Project Dunbar's multi-wCBDC prototypes (BISIH et al (2022)). While the integration with EVM-based prototypes is technically feasible through the developed smart contracts, further development is needed for non-EVM digital asset systems.[21]

Integration with other EVM-compatible frameworks, such as the mBridge platform (BISIH (2023b)), is feasible. Currently, the mBridge project maintains compliance checks outside the platform, delegating this responsibility to the participating commercial banks. Establishing a more standardised approach to handling compliance proofs could potentially enhance the mBridge system. The introduction of compliance proofs minimises data-sharing requirements and could lower entry barriers for some central and commercial banks, especially when considering the diverse privacy laws of each country.

Graph 8 – Proof verification using smart contracts



Atomic transactions:

1. Wrapping
2. Transfer from OB to BB
3. Unwrapping

5.2 Integration with Swift

Project Mandala tested integration with the Swift network by utilising the transaction manager simulator in Swift's experimental sandbox environment.

In the PoC, two test bank nodes were created to represent the originating bank (OB) and beneficiary bank (BB) in the Swift test environment, following the process outlined in use case 2 (see Section 4.2).

After the compliance proofs have been generated as outlined in Section 3.3, the OB node forwards the compliance proofs, along with a compliance check ID (CCID), directly to the BB via the P2P messaging system. This means the BB will have access to all the proofs required to verify a compliance check and ultimately approve a payment.

When the OB generates an ISO 20022 payment instruction, such as a pacs.008 customer credit transfer, the CCID is embedded into a data element to be sent as part of the credit transfer instruction. This payment instruction is then securely delivered to the BB by the Swift network.

In the PoC, the existing "InstructionForCreditorAgent" *(InstrForCdtrAgt)* ISO 20022 element is used to carry the CCID, however, a future change request could be submitted to the ISO 20022 Registration Authority for a new element to carry signatures and proofs related to compliance procedures.[22]

Upon receiving the payment instruction, the BB node uses the CCID to retrieve the previously communicated proofs and verifies that all compliance checks have been fulfilled. Although the PoC involves only two test bank nodes, this process can be extended to multiple participants along the payment chain, ensuring scalability in real-world applications. Additionally, banks having the relevant compliance information and proofs available in their node should facilitate automation to enable straight through processing of payment instructions that currently require manual checking.

This integration demonstrates the capability of Project Mandala to work seamlessly with existing financial messaging systems, enhancing compliance and transparency in cross-border transactions. Looking forward, Swift is exploring the potential of network-level validation of compliance proofs to ease the adoption of the Project Mandala concept by the global banking community, preventing tampering and verifying key details including generation date, time and authorisation of signatures.

"This integration demonstrates the capability of Project Mandala to work seamlessly with existing financial messaging systems, enhancing compliance and transparency in cross-border transactions."

5.3 Key efficiency gains

Project Mandala introduces the capability to adapt to evolving regulatory and policy requirements, ensuring compliance with jurisdiction-specific variations and enhancing efficiency in cross-border transactions.

Section 4 describes how the Mandala system would work for the selected use cases and illustrates individual transaction-specific and jurisdiction-specific benefits. While some benefits will remain specific to a particular use case, other benefits can be abstracted into universally applicable advantages. Even if some aspects of KYC/AML processes cannot be automated, there should still be substantial gains from deploying the Mandala system. Box D summarises the key efficiency gains identified by Project Mandala.

Box D: Summary of key benefits

Efficiency gain/benefits	Explainer
1. Reduction of failed transactions	Participants perform compliance checks before initiating transactions. This approach reduces the number of failed transactions.
2. Automation of compliance procedures	By automating the required compliance checks through the proof engine, Project Mandala removes the manual and slow process that currently occurs and increases the likelihood of straight-through processing.
3. Enhanced end-user privacy	Mandala shows that the exchange of information during the compliance check can occur without the need to share unencrypted data outside of bank environment.
4. Reduction of intermediaries and central governing bodies	Mandala is designed as a decentralised P2P system; this eliminates third-party risks related to an intermediary being in charge of the protocol.
5. Transparency around policy and regulatory measures	Central banks and commercial banks can include rules and measures in their rules engine that other participants of the Mandala network can query when initiating a compliance check. This approach enables stakeholders to gain insights into applicable policy and regulatory measures at the pre-validation stage.
6. Programmable compliance for digital assets	Mandala allows a new paradigm for digital assets through the verifiable proof of compliance – the proof can be verified on-chain, allowing for programmable compliance in smart contracts.
7. Consolidation of compliance checks across the payment chain	Originator and beneficiary related compliance checks are consolidated into a verifiable compliance proof to travel the whole length of a cross-border payment from pre-validation to asset settlement.
8. Decreased error resolution costs	Reduced manual interventions result in lower costs related to error resolution.
9. Improved payment data quality	The standardisation of the way policies and regulations are included in the rules engine reduces errors when running a compliance check. The incorporation of global digital unique identifiers such as the LEI also allows for better data quality of identifier information.

6 Policy, regulatory and supervisory considerations

The potential impact of Project Mandala should be considered in the context of the existing national and international regulatory and supervisory environment. This section discusses the extent to which Project Mandala could impact the work of policymakers, regulators and supervisors, while hinting at key signposts for future phases. The section also showcases how Mandala can aid compliance processes by integrating policy databases into the rules engine.

6.1 Integration and management of regulatory measures

The Mandala system has the capability to integrate with internal and external databases to complete relevant compliance checks for the selected use cases.

For the basic identity or KYC requirements, the Mandala PoC uses the LEI database.[23] The LEI data pool can be regarded a global directory with standardised information on legal entities. Each LEI contains key information regarding an entity such as its official name, registered address, country of formation and ownership structure. For Mandala, the use of LEI was key to reducing sender frictions in the input of recipient data (eg by pre-populating recipient details) and to pre-validate or improve the quality of basic originator and recipient data for compliance checks.

Alternatively, the participating banks can enter business contact details of entities manually, to support cases where an LEI is not available. In future iterations. Project Mandala could explore the integration of proxy directories, KYC registries or open ownership databases.

Sanctions screening capabilities are key for Project Mandala. Rather than integrating numerous official public sanctions lists, the project works with the OpenSanctions database, which includes the official sanctions lists of the four participating jurisdictions.[24] OpenSanctions is a curated and easily accessible database of persons and companies of political, criminal or economic interest. The database consolidates data from several hundred global sources on sanctions, politically exposed persons and crime-related entities.

While the project selected OpenSanctions due to its comprehensive coverage, future iterations of Mandala could connect to official sanctions lists directly or any other sanctions-related data sets.

The relevant stakeholders need to carefully weigh the upsides and downsides of a centralised database including all relevant regulatory measures versus a decentralised database structure, in which regulatory measures are hosted in the local regulatory libraries of participating nodes. While a centralised national database could be simpler from a technical integration perspective, it could also become a single point of failure in case of an outage, disruption or cyber attack. Decentralised databases might be complex from an integration perspective but would allow nodes to maintain autonomy in how they store and maintain official rules in conjunction with any internal rules based on their particular risk profile.

6.2 Financial integrity considerations

FATF leads the global action to tackle money laundering, and terrorist and proliferation financing through the promotion of standards to mitigate risks.[25]

There are several FATF recommendations that might be applicable to Project Mandala's use cases involving wholesale cross-border payments. The most pertinent one is Recommendation 16, which outlines the information that should be included in a cross-border transaction and shared with financial institutions and other entities facilitating the transaction. FATF is in the process of reviewing Recommendation 16 with a view to revising it and updating it to be more consistent with the current payments landscape. In this section, the report explores the extent to which Project Mandala supports this recommendation, especially considering the proposed revisions (FATF (2024)).

Project Mandala contributes to **improving the content and quality** of basic originator and beneficiary information in payment messages, including by deploying a global unique identifier such as the LEI wherever available. Including the LEI at the input stage would pre-populate associated originator and beneficiary information such as name and address. Despite operational and governance limitations and low adoption, by encouraging the use of global digital unique identifiers such as the LEI, Project Mandala supports improvements to the overall quality of the data used in the payments chain.

While the compliance checks involve messages with details of intended payments, any messages related to the execution of the payment instruction and clearing and settlement are handled by the payment and asset settlement systems. In future phases, any data relating to the beneficiary[26] could flow from the P2P messaging into the payment messaging system.

Project Mandala **supports the singleness of the payment chain.** Key originator-related and beneficiary-related compliance checks are consolidated into a verifiable compliance proof set that travels the whole length of a cross-border payment from pre-validation to asset settlement.

In the compliance process envisioned for Project Mandala, the payment chain is expected to begin in the pre-validation phase as payments will not be released until the required compliance checks have been completed successfully. Information on the institution and account which is the origin of the funds being transferred is supposed to be populated at the beginning of the pre-validation stage. Although only the compliance proof ID is included in the payment message, Project Mandala could explore including information related to the originating entity in the payment message in the future. As such, Project Mandala could close the information gap on the originating entity that emerges when the payment chain is supposed to begin at the payment instruction stage, as identified in FATF Recommendation 16.

FATF expects to develop future guidance on the implementation of Recommendation 16, and this guidance may explain practices and potential uses of pre-validation systems to enhance payment transparency in support of AML/CFT and sanctions objectives. Project Mandala could be a useful illustrative example of a pre-validation system that complies with FATF Recommendation 16.

More generally, Project Mandala could help balance the need to comply with financial integrity standards such as alignment with the proposed revisions to Recommendation 16 while safeguarding user privacy using privacy-enhancing technologies (PETs) such as MPC and ZKP as described in Section 3. For example, the project could extend the proof of compliance to cover information related to the beneficiary without having to share additional information that might be covered by privacy rules. This aspect of Project Mandala supports the FSB's work under the G20 roadmap to mitigate frictions arising from data frameworks in cross-border payments without compromising on the objectives underlying AML/CFT, sanctions and data protection and privacy rules.

6.3 Supervision, monitoring and reporting

Supervisory authorities such as central banks could benefit from Project Mandala in enhancing their compliance monitoring functions. As an extension to the first use case, the project explores how the pain points outlined in Section 4.1 could be addressed.

The Mandala protocol allows commercial banks to report any relevant data to central banks or other supervisory bodies in real time. The reported data populates databases, which allows central banks to build comprehensive supervision and monitoring dashboards, thus central banks have visibility into compliance checks reported by the commercial banks, including the status of the checks, eg successful or failed CFM checks.

For auditing, central banks would be able to view the details of specific compliance checks including associated policies, originator and beneficiary information, and the history of checks filtered by individual institutions. Auditing will be simplified as central banks can conduct verification of the compliance proofs.

Project Mandala's compliance monitoring capabilities are still limited to meeting the requirements of specific jurisdictions such as Malaysia for the compliance monitoring needs related to use case 1, as described in Section 4.1. For instance, in use case 2, an Australian bank is required to submit a report to AUSTRAC within 10 business days of the date of a transaction. As this reporting occurs after the transaction has taken place, the reporting obligation is excluded from the current project scope. Future phases of the project could be expanded to include additional supervisory and regulatory nodes in the Mandala network.

"Auditing will be simplified as central banks can conduct verification of the compliance proofs."

7 Future areas of work

The Project Mandala PoC could be extended to several different areas. In addition to extending the scope, the next phases of the project could consider technical aspects and legal liability considerations. Before integration in a production environment can be considered, future phases of Project Mandala should factor in the cost and speed of the developed solution within a banking environment.

An important factor moving forward is smooth integration with existing banking systems and any pertinent regulatory and policy databases.

Scope

In a future phase of Project Mandala, additional public sector nodes could benefit from the functionalities for compliance monitoring, supervisory, reporting or law enforcement purposes. For example, use case 2 could include BOK and FXB potentially using Mandala to automate commercial bank reporting of Korea's thresholds or include AUSTRAC for post-settlement reporting on the purchase of unlisted securities. Similarly, BNM could expand Project Mandala for statistical reporting purposes. Further, AML supervisors or law enforcement agencies could consider the project's utility for their oversight of sanctions screening requirements.

In the next iteration, the project could also include non-transaction-specific requirements such as selected questions from the Wolfsberg questionnaire.[27] Future phases could also consider KYC requirements as part of the integration with external databases, as laid out in Section 6.2. Project Mandala could also add new jurisdictions or qualitative regulatory measures.

Integration of Project Mandala with other tokenised and programmable systems such as mBridge (BISIH (2023b)) or Agorá (BISIH (2024a)) on the asset layer and Rialto (BISIH (2024c)) on the protocol layer could enhance cross-border and digital asset transactions. This is also applicable to existing central bank initiatives such as integration of the Mandala components within the Global Layer 1 platform as envisioned by MAS (MAS (2024)).

Legal liability considerations

Legal liability considerations were out of scope of this phase of Project Mandala. An in-depth analysis is needed to determine legal liability associated with the provision, maintenance and operation of different components of the Mandala solutions architecture, ie P2P messaging system, rules engine and proof engine. While each participant in Mandala's decentralised network is responsible for the proper functioning of its node, issues with potential legal liability implications may benefit from greater exploration in subsequent phases of the project.

These include:

- Who is responsible for ensuring the safety, efficiency and reliability of the entire Mandala network including the P2P messaging system?
- With respect to the rules engine, how would the issue of legal liability be dealt with in scenarios in which inaccurate or outdated information is stored in BB or central bank (CB) nodes, resulting in inaccurate or outdated rulesets being applied by the OB for its compliance checks?
- With respect to the proof engine, how would the issue of legal liability be dealt with if, to avoid duplicative compliance checks, a party (eg BB) relies on the check undertaken by another party along the payment chain (eg OB)?

Additionally, there are potential legal liability implications along the payment chain, especially for the designed policy wrapper (Section 5.1). Since the policy wrapper will hold actual monetary value in the form of a digital asset, it would be critical to determine the boundaries of legal liability.

Technical considerations

Future phases could consider the optimal process for OBs to gather rules from other participating commercial banks and regulators, while ensuring that these rules are updated according to the regulatory source data. In a production system, each Mandala node could leverage other technologies such as a rules cache to improve performance. Alternatively, future phases could explore extracting applicable regulatory measures directly from regulatory texts through machine learning techniques.

The Mandala PoC implements policies as custom-built machine-readable rulesets that follow standardised templates (Section 6.1). Further exploration is needed to validate the templates (Section 6.1) and computational categories (Section 3.2) against a range of other compliance use cases. Future iterations of Project Mandala could consider implementing a more flexible rules engine which allows for dynamic and automated invocation of rules, following the format of the standardised templates (Section 6.1). The project could also apply appropriate sequencing of applicable rules in the form of a rule flow builder.

The concept of providing cryptographic proofs of compliance could unlock new methods to provide assurance to regulators. For instance, the inputs to ZKPs produced by Mandala's non-interactive checks could be automatically spot checked by a regulator participating in the network enhancing compliance assurance without compromising user privacy using PETs. Furthermore, the Mandala proof set could include digital certificates that are static, such as compliance with the Wolfsberg questionnaire or successfully completed audits.

Mandala's smart contract integration places the compliance check off-chain, requiring the smart contracts to only verify a cryptographic compliance proof, as initially proposed in Buterin et al (2023). Not having compliance-related data – like sanctions lists – on-chain improves privacy and reduces computational requirements and therefore transaction costs of on-chain transactions.

With growing acceptance from regulators and adoption by the industry, this approach could become the leading paradigm in programmable compliance for digital assets and tokenised money. Future phases could explore incorporating different proof types, governance of the policy wrappers, further transaction cost optimisations, and improved management of disputes and transaction reversals.

Path to production

Project Mandala shows the potential to lower the costs of compliance procedures by removing redundancy, automating policy and regulatory checks, and minimising the need for manual processes such as RFI processes.

For successful integration in a production environment, future iterations should consider integration with commercial bank systems and full-fledged integration with existing systems such as Swift's messaging system.

After the technology solution has been established and firmed up, the legal liability aspects clarified and the usage of cryptographic proofs for compliance verification approved by regulators, the Mandala system could be applied more widely in the industry. The first phase of the project already demonstrates the potential for cost and efficiency gains, which need to be explored further in a near-production setting.

8 Conclusion

Project Mandala deploys a compliance-by-design approach to streamline compliance with regulatory and policy requirements for cross-border transactions.

Given the regulatory complexity, the project selected pertinent regulatory measures based on two use cases involving the four participating jurisdictions.

The selected use cases and regulatory measures, such as sanctions screening and CFM compliance, reflect the outcome of extensive consultation with commercial banks that engage in regional cross-border activities. Use case 1 further extends to central bank' requirements for real-time monitoring of compliance with CFM measures.

The basis of the solutions architecture is a fully decentralised and distributed system that accounts for jurisdiction-specific regulatory disparities and commercial bank risk profiles. The P2P messaging layer enables seamless and secure communication between the nodes without the need for intermediaries. The rules engine standardises the inputs and outputs of regulatory measures to the fullest extent possible, so that participating nodes in the network (central and commercial banks alike) can manage the applicable rules easily. The proof engine automatically carries out compliance checks and generates cryptographic proofs of compliance for each check that can travel with a DLT-based digital settlement asset or can be linked to existing non-DLT-based payment messages. This enables all entities to verify compliance efficiently.

Project Mandala shows that it is possible to apply the designed solutions architecture for a variety of use cases to accommodate requirements of both public and private sector participants. Further, the project has successfully demonstrated the technical feasibility of integrating with nascent digital assets and existing systems. While Project Mandala applied a light touch integration, with existing systems limited to Swift, a specially designed smart contract allows for full-scale integration with a wCBDC system developed as part of Project Mariana. Project Mandala introduces a new paradigm for digital assets – the compliance proof can be verified on-chain, allowing for programmable compliance in smart contracts.

The project introduces several efficiency gains that are beneficial to commercial banks and regulators alike. First, the project contributes to reducing the number of failed transactions as compliance checks need to be completed before any funds can be released. Second, the project increases the efficiency and speed of compliance processes by introducing straight through processing and decreasing the number of intermediaries. Third, the project introduces transparency around country-specific policies and regulations and transaction-specific information such as originator and beneficiary details. Finally, Project Mandala has the potential to improve user privacy as no unencrypted data are shared outside the bank environment, while ensuring compliance with pertinent financial integrity standards.

The identified efficiency gains could actively support the work of international financial institutions and standard-setting bodies. The verifiable compliance proof could support the singleness of payment chain concept as laid out in the proposed revisions to FATF Recommendation 16. Further, Project Mandala could benefit FATF's future guidance on pre-validation systems that would improve payment transparency. Although LEI operational and governance aspects need to be solidified, Project Mandala could support its use – a stated objective of the FSB taskforce on legal, regulatory and supervisory matters and the CPMI. As such, Project Mandala contributes to FSB's efforts to promote the alignment and interoperability of regulatory and data requirements.

There are several future areas of work that the project could focus on such as including new jurisdictions or regulatory measures, improving technical aspects and exploring further integrations with external databases. Project Mandala has shown that the architecture can successfully integrate with external systems including GLEIF and OpenSanctions. This can be expanded to include any other databases such as corporate registries or open ownership databases. For supervisory purposes, the project could also explore integration with pertinent central bank databases. Connecting the Mandala system to commercial bank databases will allow more granular insights on costs, speed and other data in a near-production environment. These insights are important for assessing the commercial viability of Project Mandala.

In the long term, Project Mandala's proof-based approach to programmable compliance could enable interoperability across different cross-border payment arrangements while safeguarding privacy and introducing operational efficiencies with novel smart contract approaches. The project could become the bridge between regional payment systems, pre-empt fragmentation and enable compliance interoperability in a future financial market infrastructure ecosystem.

"There are several future areas of work the project could focus on such as including new jurisdictions or regulatory measures, improving technical aspects and exploring further integrations with external databases."

References

Bank for International Settlements Innovation Hub (BISIH) (2023a): *Project Aurora: the power of data, technology and collaboration to combat money laundering across institutions and borders,* May.

——— (2023b): *Project mBridge update: experimenting with a multi-CBDC platform for cross-border payments*, October.

——— (2024a): *Project Agorá: central banks and banking sector embark on major project to explore tokenisation of cross-border payments*, press release, April.

——— (2024b): *Project Hertha: identifying financial crime patterns while preserving user privacy within a real-time payment system,* April.

——— (2024c): *Project Rialto: improving instant cross-border payments using wholesale CBDC settlement,* July.

BISIH, Reserve Bank of Australia, Bank Negara Malaysia , Monetary Authority of Singapore and South African Reserve Bank (2022): *Project Dunbar: international settlements using multi-CBDCs*, March.

BISIH, Bank of France, Monetary Authority of Singapore and Swiss National Bank (2023): *Project Mariana: cross-border exchange of wholesale CBDCs using automated market-makers*, September.

Borchert, L, R De Haas, K Kirschenmann and A Schultz (2024): "The impact of de-risking by correspondent banks on international trade", *VOXEU*, 18 September.

Buterin, V, J llum, M Nadler, F Schär and A Soleimani (2023): "Blockchain privacy and regulatory compliance: towards a practical equilibrium", *Blockchain: Research and Applications*, vol 5, no 1, March.

Committee on Payments and Market Infrastructures (CPMI) (2023): *Harmonised ISO 20022 data requirements for enhancing cross-border payments,* October.

Financial Action Task Force (FATF) (2024): *Explanatory memorandum and draft revisions to Recommendation 16,* February.

Financial Stability Board (FSB) (2022): *Options to improve adoption of the LEI, in particular for use in cross-border payments,* July.

——— (2024a): *Recommendations for regulating and supervising bank and non-bank payment service providers offering cross-border payment services: consultation report*, July.

——— (2024b): *Recommendations to promote alignment and interoperability across data frameworks related to cross-border payments: consultation report,* July.

Forrester (2023): *True cost of financial crime compliance study, 2023 Asia Pacific.*

Garay J, B Schoenmakers and J Villegas (2007): "Practical and secure solutions for integer comparison", in T Okamoto and X Wang (eds), *Public key cryptography – PKC 2007*, Springer-Verlag, pkc07intcomp.pdf (tue.nl).

Monetary Authority of Singapore (MAS) (2023): *Purpose bound money (PBM), technical whitepaper,* June.

——— (2024): *Global Layer 1 (GL1) whitepaper,* June.

Nasdaq and Verafin (2024): *Global financial crime report: insights at the intersection of financial crime data and real survivor stories*, November.

Thomson Reuters (2020): *Regulatory intelligence desktop*, July.

Appendices

Appendix A – MPC implementation

Google PJC's MPC implementation

The Mandala proof of concept (PoC) utilises private join and compute (PJC).[28] PJC combines private set intersection (PSI) and homomorphic encryption to compute the intersection of two users' data sets.

1. **Data ownership:** the originating bank (OB) retains ownership of its customer data, which needs to be checked against the beneficiary bank's (BB) private sanctions list.
2. **Encryption:** both the OB and the BB use their private keys to encrypt their respective data. The OB encrypts the customer data, while the BB encrypts the private sanctions list, ensuring the data remain secure and indecipherable to others.
3. **Data exchange:** the OB and BB exchange their encrypted data with each other.
4. **Double encryption:** upon receiving the data, both the OB and BB further encrypt the already encrypted data using their own private keys. This results in data that are doubly encrypted, preventing either party from decrypting it individually. PJC uses a deterministic commutative cipher that enables the doubly encrypted values to be compared securely.
5. **Comparison:** the OB sends the doubly encrypted data back to the BB in a randomised order. The BB then compares the double-encrypted data sets to identify any overlaps, ensuring secure and private compliance checks.

Silence Laboratories' MPC implementation

Private sanctions list check

This protocol allows the OB to check if a customer is present in the BB's private sanctions list without revealing the customer data to BB or having the sanctions list revealed by BB. Both the hash functions $H1$ and $H2$ are known to OB and BB and they are agreed upon initially.

OB prepares the blinded customer data:

1. OB has customer data x which needs to be checked against BB's sanctions list.
2. OB selects a random number r from a large set of possible values.
3. OB computes $A = r \cdot H1(x)$, where $H1$ is a cryptographic hash function, that hashes x to a point on the elliptic curve.
4. OB sends A to BB.

BB processes the blinded data:

1. BB receives the blinded customer data A from OB.
2. BB selects a random number k from a large set of possible values
3. BB computes $B = k \cdot A$
4. BB generates an encoded list $encoded(Y)$ by hashing each entry in its private sanctions list Y with $H1$ and then applying another hash with k $encoded(Y) = \{H2(H1(y), k \cdot H1(y)) \,|y \in Y|\}$ where $H2$ is another cryptographic hash function.
5. BB sends the $encoded(Y)$ and the blinded data B back to OB.

OB unblinds and checks the result:

1. OB receives the encoded list $encoded(Y)$ and the blinded data B from BB.
2. OB computes encoded(x) = $H2(H1(x), r^{-1} \cdot B)$, where r^{-1} is the multiplicative inverse of r.
3. The computation is:

a. Since $A = r \cdot H1(x)$ and $B = k \cdot A$, we have $B = k \cdot r \cdot H1(x)$

b. OB computes $r^{-1} \cdot B = r^{-1} \cdot 6k \,.\, r \,.\, H1(x)9 = k \cdot H1(x)$

c. OB then computes $encoded(x) = H2(H1(x), k \cdot H1(x))$

4. OB checks if $encoded(x)$ is present in the encoded list $encoded(Y)$
5. OB outputs the result b which is a boolean with value 1, if there is a match for x in the private sanctions list, and 0 otherwise.

Capital flow management (CFM):

The CFM check is performed between the originating bank (OB) that holds the details of a proposed transaction for a company C for an amount X, and the central bank (CB) that holds the list of the current capital flows(CFL) for a range of companies. The mechanism of this check check discloses whether the amount X, in combination with the existing capital flow $CFL[C]$ exceeds a specified capital limit L, while maintaining privacy – a party does not have sight of the private data inputs of the other party.

1. Masking the values (phase 1):

- The CB starts by **masking** the values in CFL using a **one-time integer pad** i.e. **a secret random value** (ZCB) is added to all the entries in CFL. This masked value hides the true value of $CFL[C]$ from anyone who does not know ZCB.
- Through a secure protocol (such as private set intersection), the OB learns only the masked value $MaskedCFL[C]$ for C. OB does not learn the actual value $CFL[C]$ or the masking value ZCB; it only knows the sum$MaskedCFL[C]$.

2. Transforming the comparison problem (phase 2):

- The original goal is to determine whether $X + CFL[C] < L$, where X is the transaction amount known to OB, and $CFL[C]$ is the existing capital flow known to CB.
- To preserve privacy, instead of comparing $X + CFL[C]$ directly with L, both parties compare $X + MaskedCFL[C]$ with $L + ZCB$. This transformation works because adding the same random value ZCB to both sides of the inequality does not change the truth of the comparison. This ensures that the comparison can be carried out without revealing the actual values of $CFL[C]$ or ZCB.

3. Bitwise decomposition (phase 3):

- OB computes the left-hand side (LHS) of the inequality as $LHS = X + MaskedCFL[C]$. This value is then broken down into its individual bits (bitwise decomposition). For example, if **LHS** is an n-bit number, it would be decomposed into bits **LHS0, LHS1, …,LHSn**, where **LHS0** is the least significant bit and **LHSn** is the most significant bit.
- Similarly, CB computes the right-hand side (RHS) of the inequality as $RHS = L + ZCB$ and also decomposes it into bits **RHS0, RHS1, …, RHSn**.
- This bitwise decomposition is crucial because it allows the comparison to be performed bit by bit, which is a mode of operation that is native to most secure comparison protocols.

4. Secure comparison protocol (phase 4):

- OB and CB then engage in a secure comparison protocol that compares the bits of **LHS** and **RHS** one by one, starting from the most significant bit. The protocol used for this comparison is based on the technique by Garay et al (2007), which recursively decomposes the comparison operation into a series of additions and multiplications on the bits of the operands.
- The key here is that neither OB nor CB learns the actual bit values of the other party's input. Instead, they only learn the final result of the comparison: whether **LHS** < **RHS** or not. In terms of the original values, this determines whether $X + CFL[C] < L$.

The protocol is designed to be secure against malicious parties who might try to deviate from the protocol. Multiple safeguards are in place to detect and prevent cheating. For instance, the protocol ensures that the inputs X and $CFL[C]$ are positive integers and that the bitwise decompositions are correctly formatted boolean values. These security measures are important because if a party provides invalid inputs or manipulates the data in an attempt to cheat, the protocol will detect this behaviour and halt the execution, ensuring no sensitive information is leaked.

In the actual implementation, the transaction details are shared by OB with BB, and the computation is performed between BB and CB. This mirrors the real-world scenario in which OB does not interact directly with BB's CB. However, depending on future developments, this could be extended to a direct check between OB and BB's CB, as outlined in the original explanation.

Appendix B – P2P network: technical implementation details

The Mandala demo implementation is built in Rust and uses Celery to define tasks. A node which wants to produce a task can add it to the queue of tasks for the network using RabbitMQ. Additional information about each task, such as its identifier, status and payload, is stored using Redis. Once a task has been defined and queued, it can then be worked on by other nodes.

Each node also runs an HTTP server so that it can communicate with servers outside the P2P network, including APIs internal and external to the bank running the Mandala node. For example, as part of use case 2 (Section 4.2) the originating bank (OB) has to check with the central bank and its own systems to ensure that netting and capital flow reports have been received from the sender. To automate this process the OB's Mandala node uses its HTTP server to communicate with APIs at the central bank and in its own systems.

In addition to the core functionalities, the Mandala P2P network leverages advanced libp2p features such as QUIC and Kademlia. QUIC, a modern transport protocol, enhances the network's performance by providing low-latency, reliable, and secure connections.

Kademlia, a distributed hash table, is used for efficient peer discovery and routing, enabling nodes to locate each other and exchange information quickly within the network. This decentralised approach ensures robustness and scalability.

These features collectively improve the overall efficiency and reliability of the Mandala P2P network, making it well-suited for high-performance, distributed applications.

Appendix C – Benchmark tests for SHA256 using FPGA

The table below presents the cost and time required to perform SHA256 hashing across five different instance types.

The first three rows correspond to GPU variants, while the last two demonstrate the efficiency gained by pipelining CPUs with FPGAs, showcasing an alternative approach that optimises both proof time and cost.

Instance Type	Data Size	VM Config	Segment Size	Proof Time (Sec)	Price (cents)
g4dn.xlarge	32768	r0	20	213.101	1.96
g6.16xlarge	32768	r0	21	81.654	5.02
g6.xlarge	32768	r0	21	91.092	1.33
8 vCPU + u55c	32768	r0	21	30	0.75
16 vCPU + u55c	32768	r0	21	18	0.6

Appendix D – Overview of applicable regulatory measures

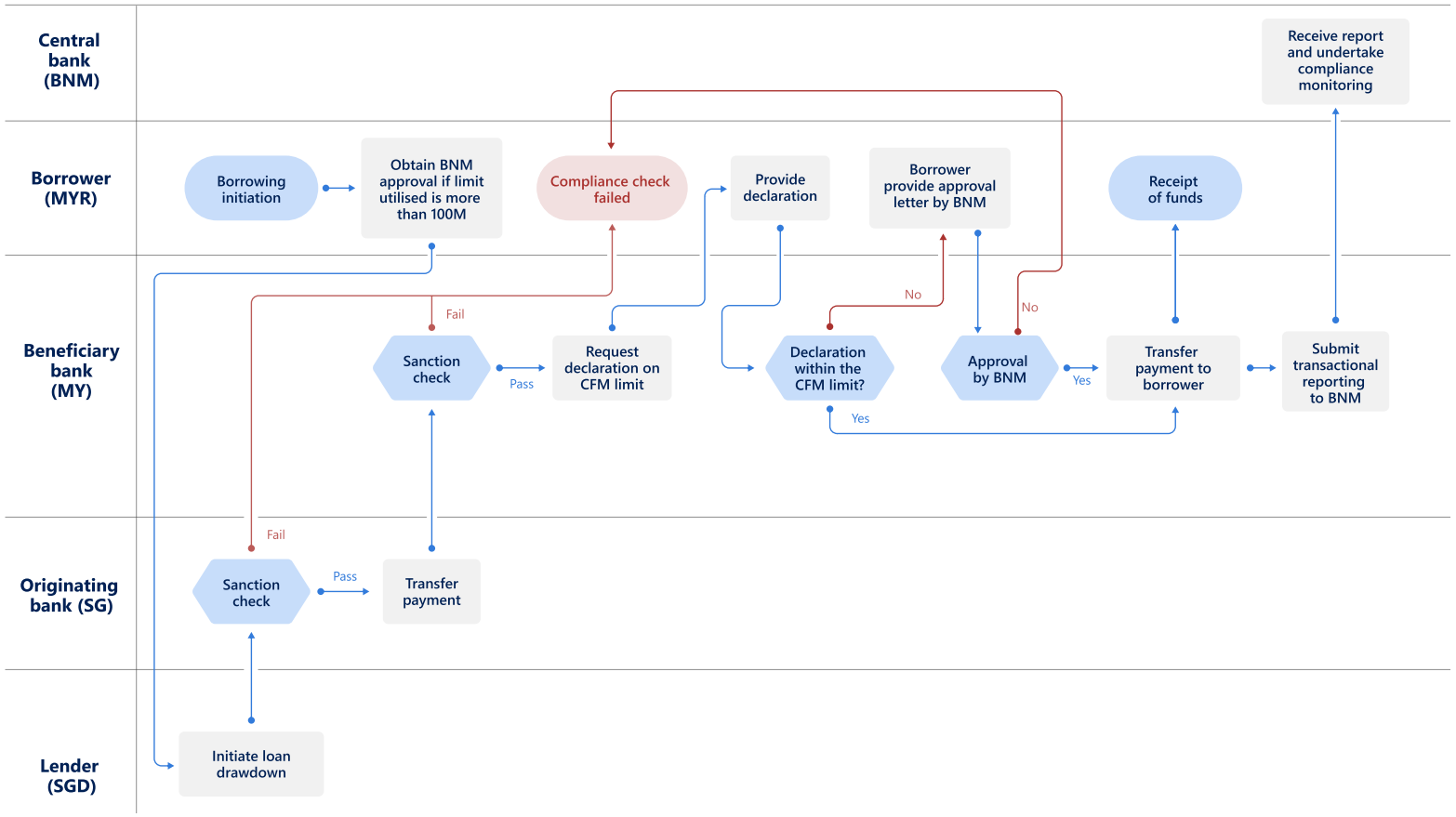
Relevant policy/ ruleset	Computational operation	Inputs	Proof of compliance	Benefits
AML	**Provable blacklist check**	Target, list	Zero-knowledge proof	OB fulfils their sanctions obligations by performing the check. Other banks in the payment chain can choose to verify the sanctions check instead of performing the check themselves.
Commercial bank policies	**Private blacklist check**	Target, list	Commercial bank signature	OB has assurance that any private sanctions list checks at the BB will pass. BB can choose to use the sanctions check result from Mandala. If receiving a payment message, BB may optionally run the check again.
Korean Netting	**Centralised threshold check:** OB compares number of parties to the threshold limit.	Threshold	N/A	
Korean CFM	**Centralised threshold check:** OB calculates cumulative amount locally (since it maintains a database of this information) and compares it to the threshold limit.	Threshold, amount, transfer amount, input currency, existing amount (number or array)	N/A	OB can choose to notify the CB upon transfer in asset system.
Malaysian CFM	**Option 1 Centralised threshold check:** Regulator calculates cumulative amount locally (since it maintains a database of this information) and compares it to threshold limit. **Option 2 – MPC threshold check:** OB and regulator calculate cumulative amount and compare it to the limit using MPC.	Threshold, amount, transfer amount, input currency, existing amount (number or array)	Regulator signature	Regulator that holds CFM data performs the check before the transfer. Regulator can receive a notification upon transfer. Option 2 allows for privacy preserving CFM checks in real-time

Appendix E – Use case diagrams

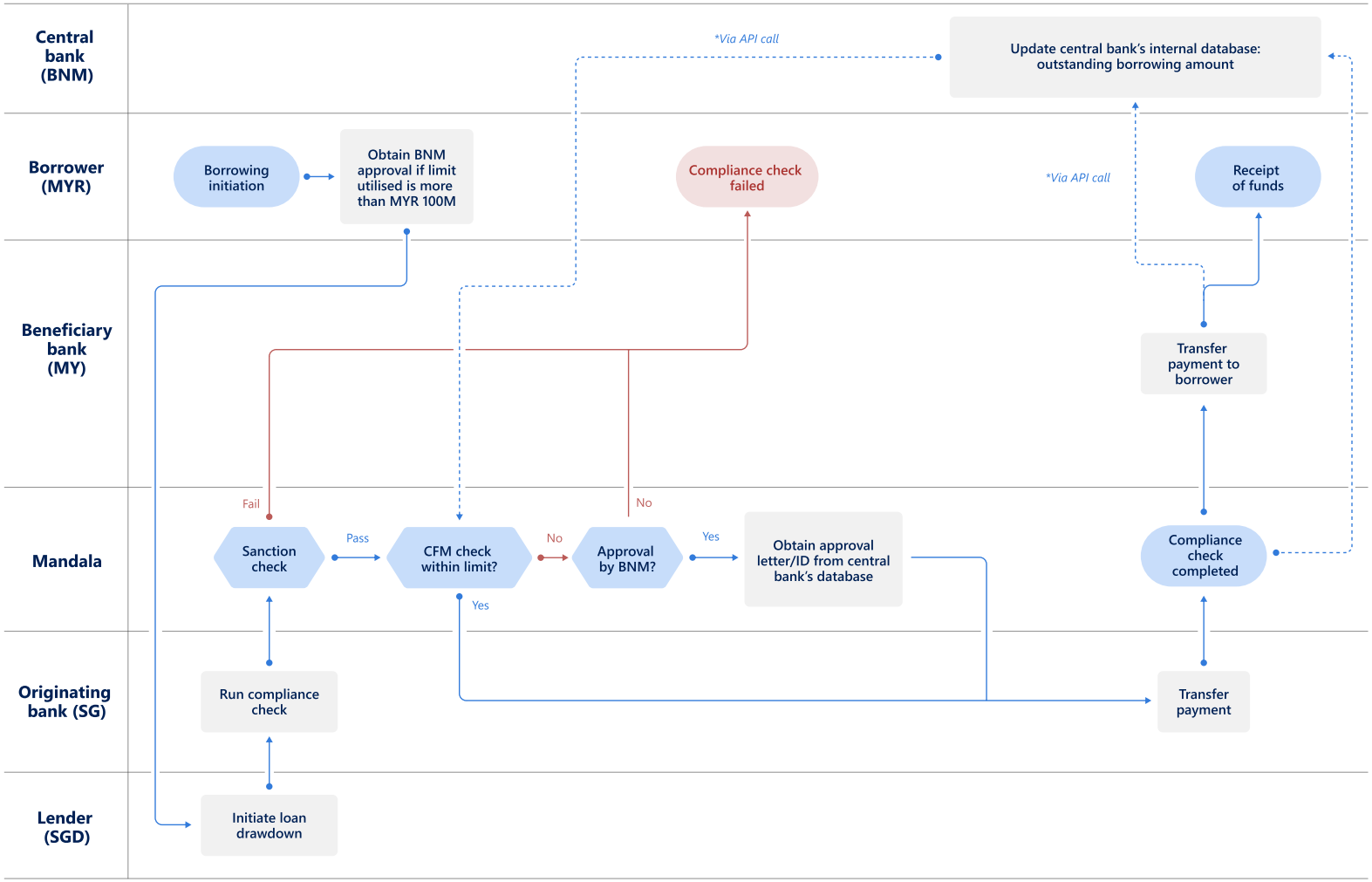
Use case 1: Loan drawdown

Graph 9 depicts the loan drawdown process between a Singapore-based lender and a Malaysia-based borrower, both before and after the implementation of the Mandala system. These graphs also show the involvement of key entities such as Bank Negara Malaysia (BNM), the originating bank (OB) in Singapore and the beneficiary bank (BB) in Malaysia.

Graph 9.A – Loan drawdown – before Mandala



Graph 9.B – Loan drawdown – with Mandala

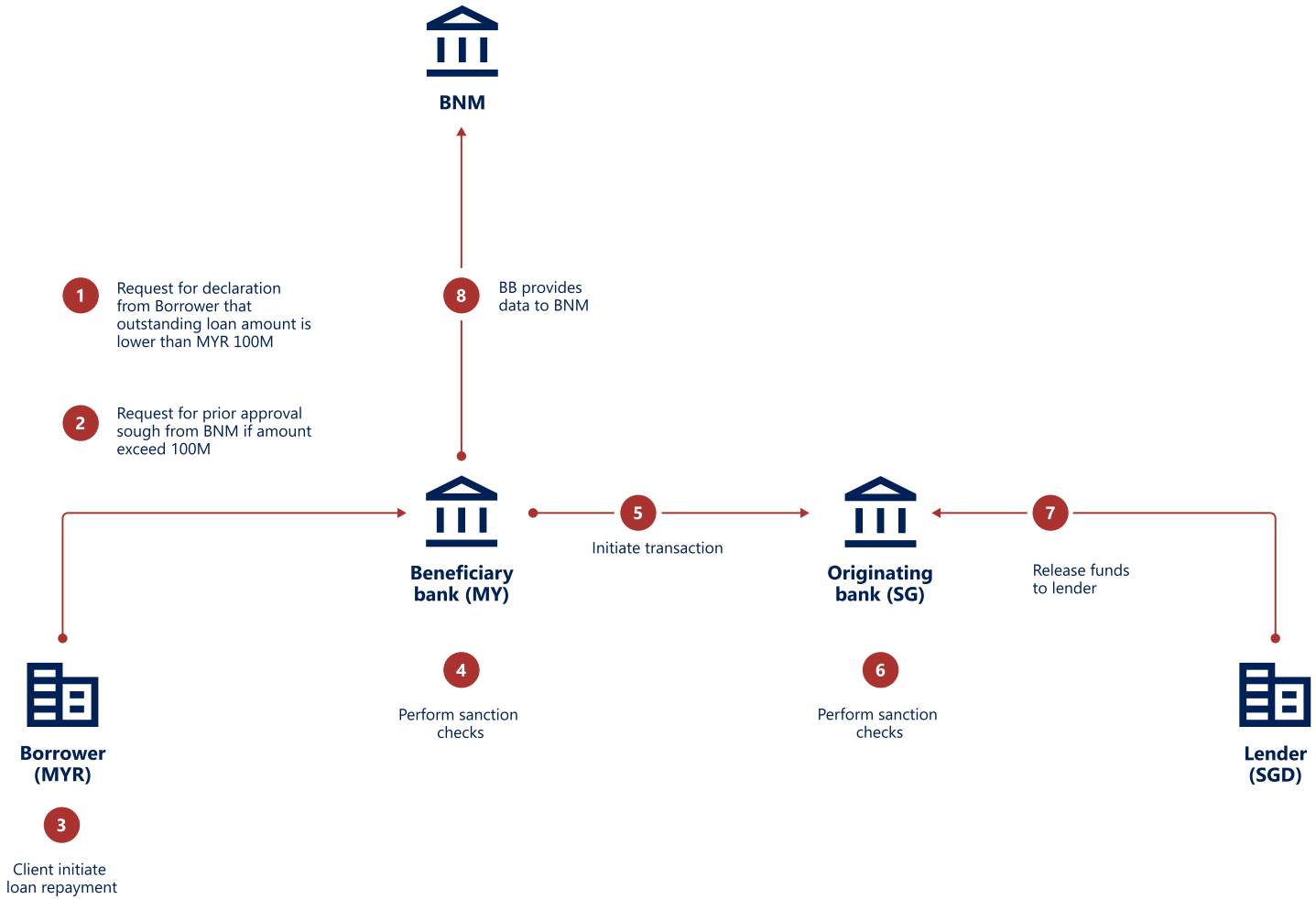


Use case 1: Loan repayment

The current loan repayment process involves the following steps:[29]

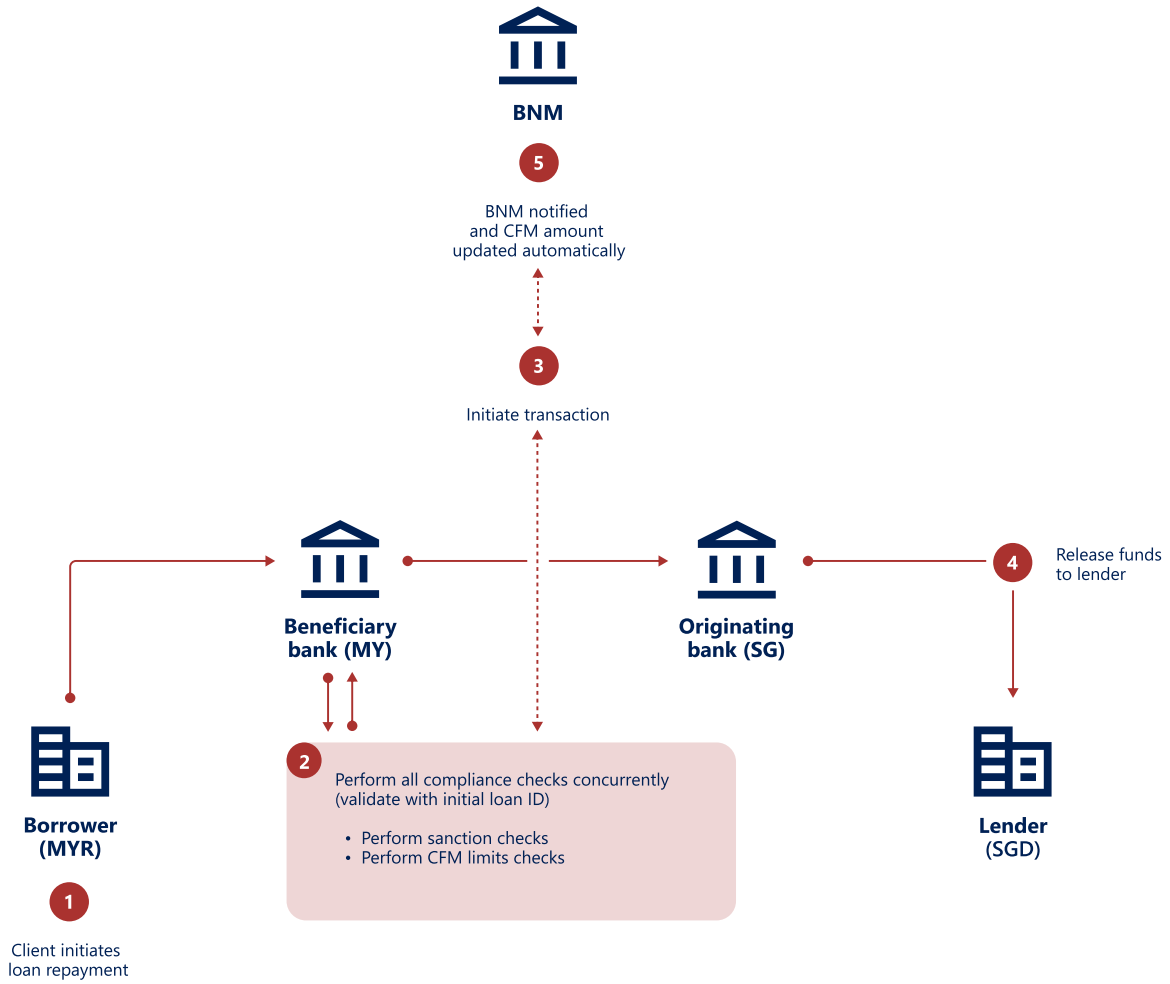
1. The Malaysian commercial bank, ie the BB [30] (the borrower's bank in this context) requests a confirmation from the borrower that the repayment is for an outstanding loan that the borrower had previously drawn down within the permissible limit or has approval from BNM.
2. Where necessary, the borrower needs to provide the initial approval letter obtained during the loan drawdown as proof for loan repayment.
3. Next, the borrower initiates the loan repayment process to the lender through the BB.
4. The BB receives the repayment request and performs the necessary AML/CFT checks, such as sanctions screening.

Graph 10 – Loan repayment flow before Mandala



5. After completing these checks, the BB transfers the payment to the OB, which is the lender's bank in this context.
6. Upon receiving the payment, the OB conducts its own AML/CFT checks.
7. Once these checks are completed, the OB releases the funds to the lender.
8. Finally, the BB submits transactional reporting to BNM on the completed loan repayment for CFM compliance monitoring purposes.

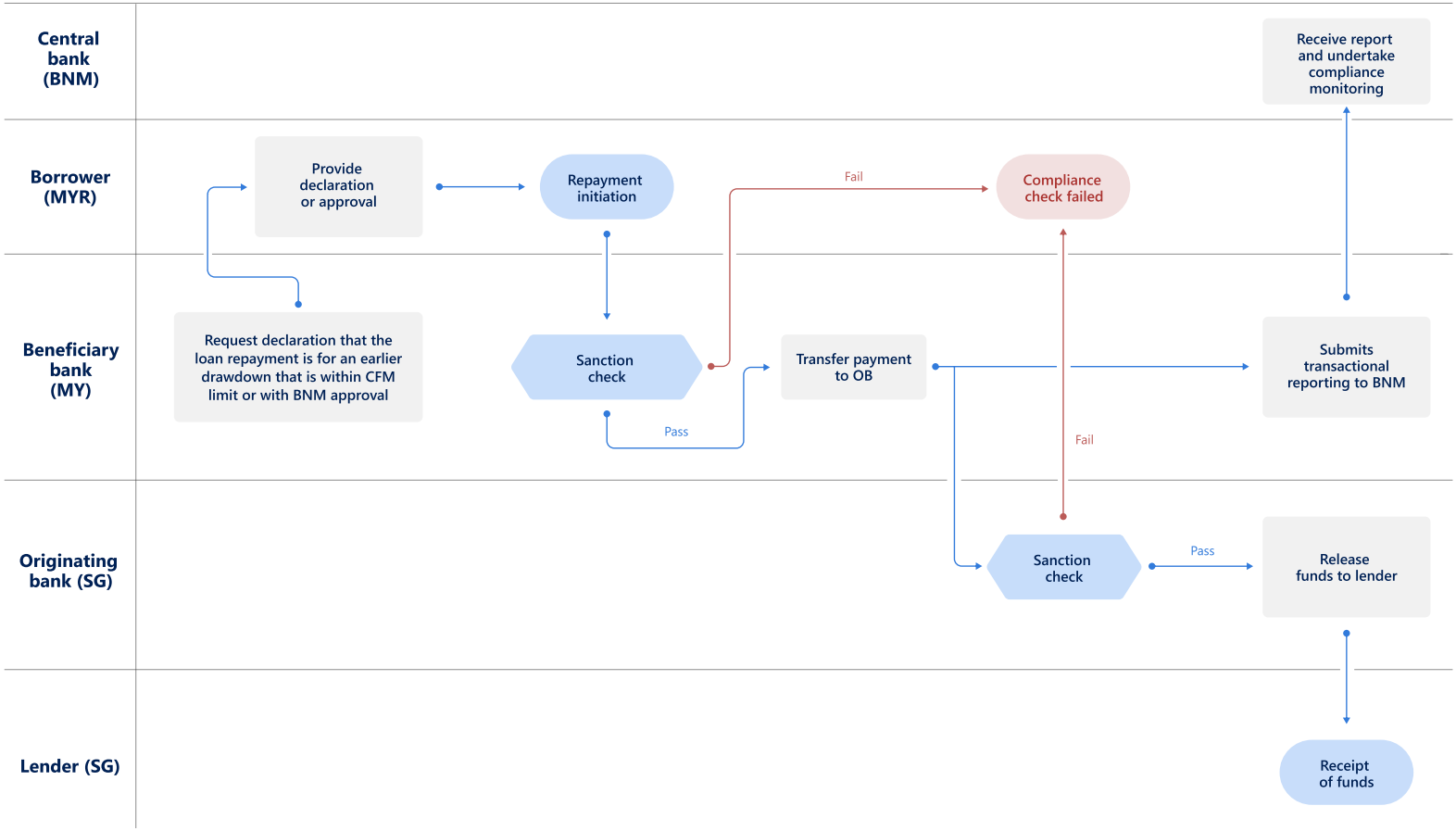
Graph 11 – Loan repayment process with Mandala



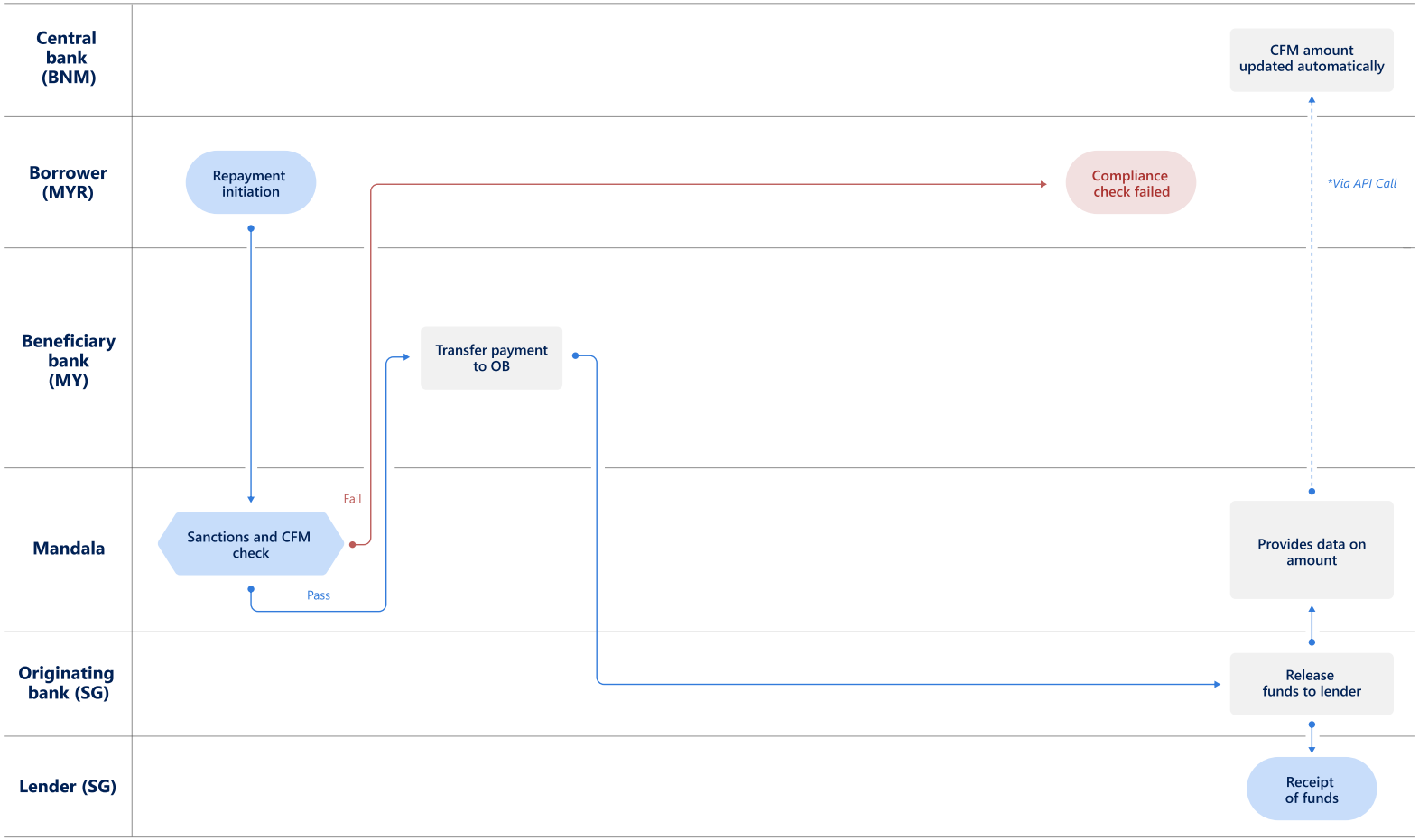
Use case 1: Loan repayment

Graph 12 illustrates the loan repayment process from the Malaysia-based entity (borrower) to the Singapore-based entity (lender).

Graph 12.A – Loan repayment – before Mandala



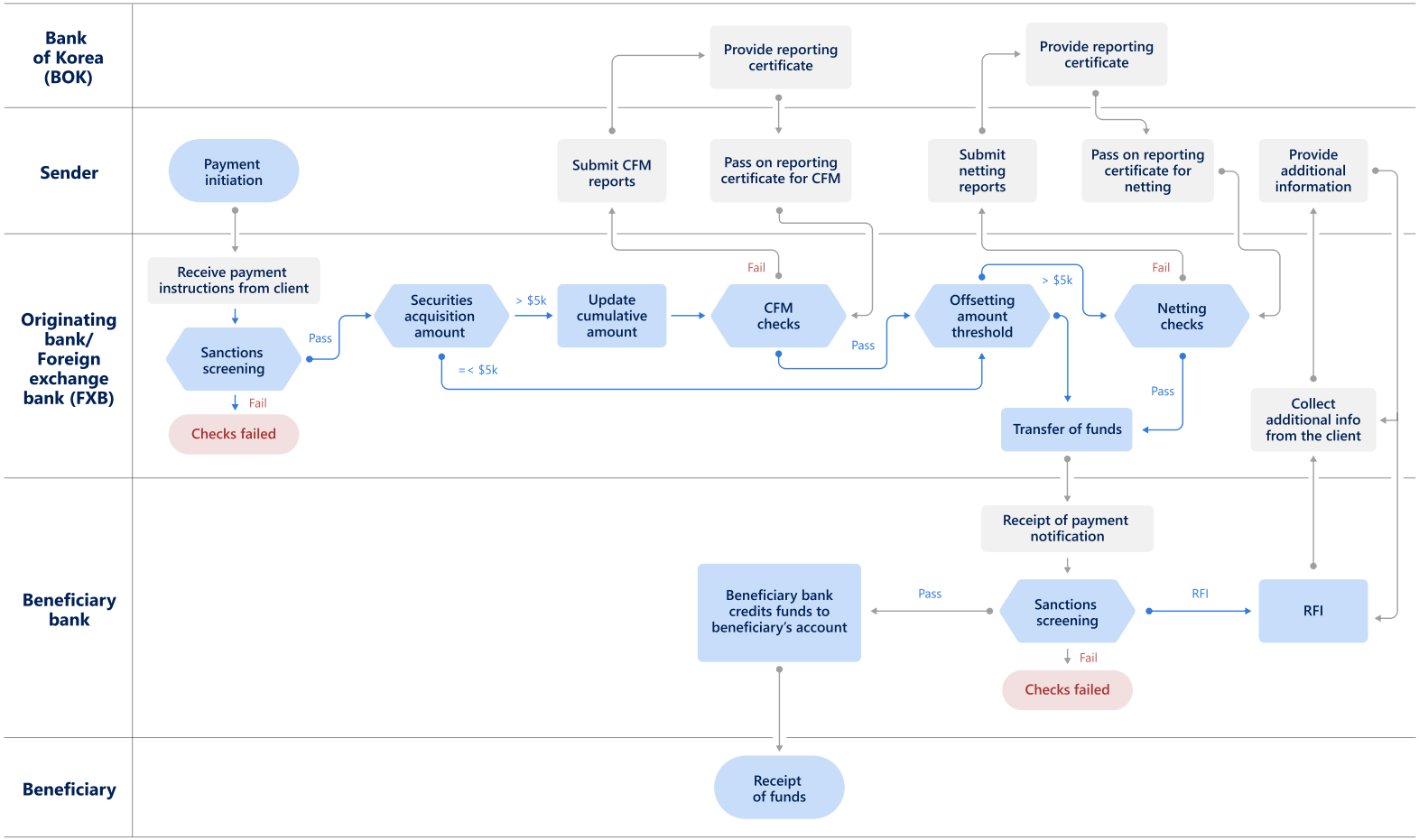
Graph 12.B – Loan repayment – with Mandala



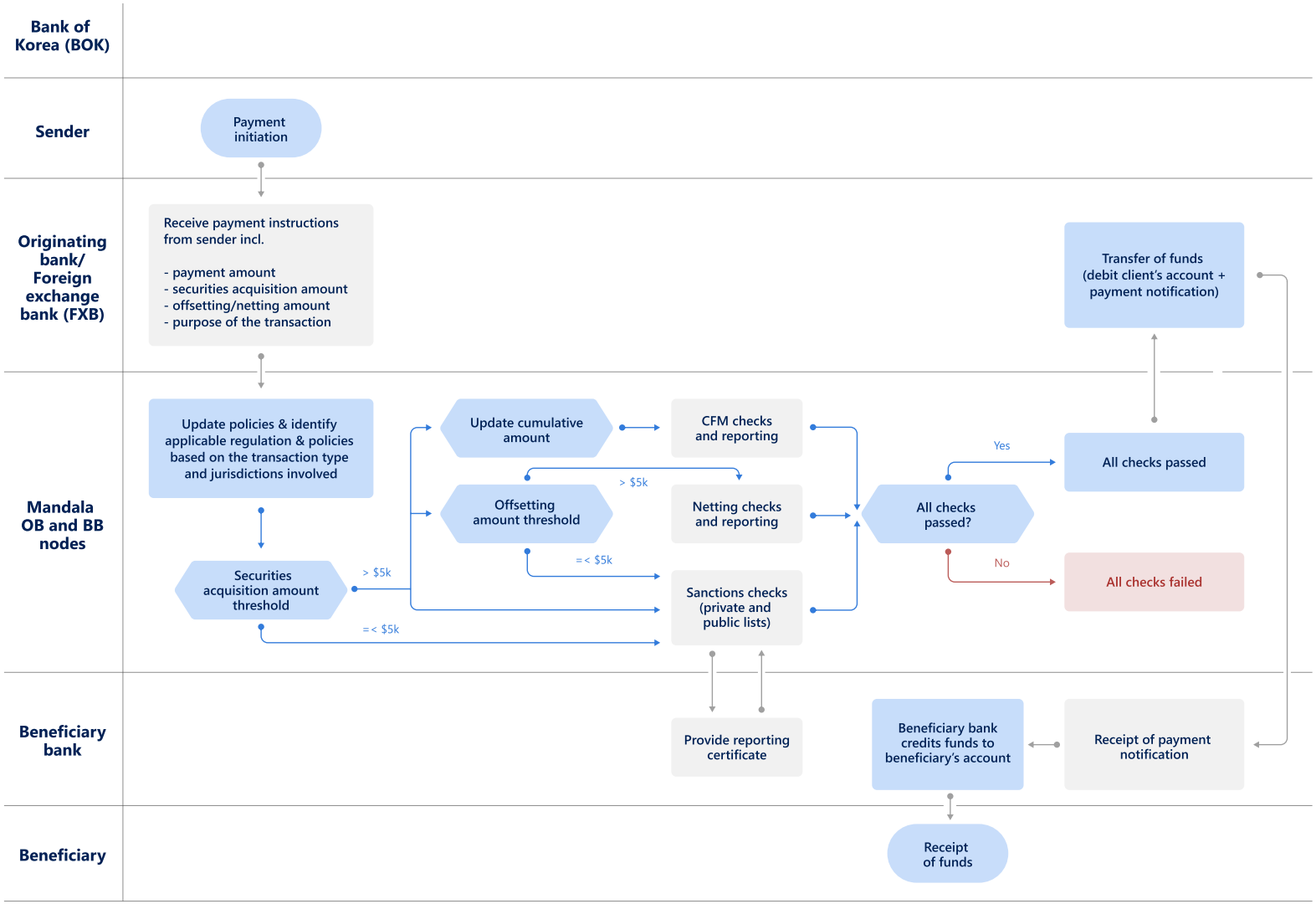
Use case 2: Acquisition of unlisted debt securities

Graph 13 illustrates the acquisition process of unlisted debt securities between a South Korea-based originator and an Australia-based beneficiary, both before and after the implementation of the Mandala system. Graph 13 also details the involvement of key entities, including the Bank of Korea (central bank), the foreign exchange bank (FXB)[31] – which also acts as the OB – and the Australian commercial bank.

Graph 13.A – Acquisition of unlisted debt securities before Mandala



Graph 13.B – Acquisition of unlisted debt securities with Mandala



Contributors

Steering group

BIS Innovation Hub	Maha El Dimachki, Head, Singapore Centre (from October 2023)
	Benjamin Lee, Acting Head, Singapore Centre (August-October 2023)
Reserve Bank of Australia	Chris Thompson, Deputy Head, Payments Policy Department
Bank of Korea	Sung Hwan Shin, Team Lead, Digital Currency Analysis Team (from February 2024)
	Teuk Rok Kang, Team Lead, Digital Currency Analysis Team (August 2023-February 2024)
Bank Negara Malaysia	Qaiser Iskandar bin Anwarudin, Director, Payments Services Policy Department
Monetary Authority of Singapore	Alan Lim, Director, Financial Technology and Innovation Group

Project group

BIS Innovation Hub	Sonja Davidovic, Adviser
	Friedrich Klinger, Adviser
	Kah Kit Yip, Adviser
	Balu Babu, Intern
Reserve Bank of Australia	Rochelle Guttmann, Senior Manager, Payments Policy Department (from February 2024)
	Cameron Dark, Manager, Payments Policy Department (August 2023-February 2023)
	Tatiana Moiseeva, Lead Analyst, Payments Policy Department
	James MacNaughton, Senior Developer, Payments Policy Department
Bank of Korea	Duck Hyung Kim, Manager, Payment and Settlement Systems Department
	Hyung Jin Cho, Manager, International Department (from March 2024)
	Sungki Kim, Manager, International Department (from March 2024)

Bank Negara Malaysia	Norasyikin Mohamad Razali, Deputy Director, Payments Services Policy Department
	Nur Liyana Abd Rahim, Manager, Payments Services Policy Department
	Charmaine Tew Shu Yi, Senior Analyst, Foreign Exchange Policy Department
	Amalina Nabilah Rozlan, Analyst, Payments Services Policy Department
	Basyirah Mohd Khairi, Analyst, Payments Services Policy Department
	Chew Ming Heong, Principle, Business Technology Department
Monetary Authority of Singapore	Jaelyn Teo, Assistant Director, FinTech Infrastructure and Innovation Group (from January 2024)
	Emilia Lee, Assistant Director, FinTech Infrastructure and Innovation Group (August-April 2024)
	Vincent Pek, Deputy Director, FinTech Infrastructure and Innovation Group
Bank of France	Cédric Coiquaud, Business Analyst, Innovation and Support for Euro Infrastructure Payment Products (from March 2024)
	Clément Delaneau, Blockchain Engineer, Blockchain Division (from March 2024)
	Khai Uy Pham, Adviser, Innovation and Financial Market Infrastructures (from March 2024)

Acknowledgments

Public sector partners

Bank of Thailand

Financial Action Task Force (FATF)

Financial Stability Board (FSB)

International Monetary Fund (IMF)

Project advisers

Mojaloop

Silence Laboratories

Swift

Commercial banks

AmBank

ANZ

Hong Leong Bank

OCBC

Onyx JP Morgan

Hana Bank

KB Kookmin Bank

Shinhan Bank

Woori Bank

Endnotes

1 See Nasdaq and Verafin (2024) for statistics on global financial crime.

2 The consultation was conducted during the period September 2023–March 2024 with commercial banks from the four participating jurisdictions. A full list of the banks can be found in the acknowledgments section.

3 www.oecd.org/en/about/programmes/data-free-flow-with-trust.html.

4 The project team engaged several financial institutions in bilateral conversations and online surveys during the period August 2023–January 2024 to solicit which regulatory measures are considered most complex from a compliance perspective.

5 Based on Google's private join and compute and Silence Laboratories' libraries. See Annex A for details.

6 Based on RISC Zero.

7 For more technical details on the P2P network see Appendix B.

8 The proof is generated through the open-source ZKP framework RISC Zero, which generates proofs of the correct execution of arbitrary code. This means compliance check logic can be written in more commonly used programming languages.

9 To facilitate verification of the ZK-STARK on-chain, Mandala converts it to a ZK-SNARK Groth16 proof.

10 FPGAs are integrated circuits that can be configured by the user after manufacturing. They offer flexibility and high performance for specific tasks, making them ideal for applications requiring parallel processing and low latency.

11 A private key, also known as a secret key, is a variable in cryptography that is used with an algorithm to encrypt and decrypt data.

12 For a technical overview of the workings of private join and compute and Silence Laboratories' implementation of MPC for the private sanctions list and the CFM check, refer to Appendix A.

13 PJC is an open software MPC developed by Google.

14 A more detailed swimlane diagram for the loan drawdown process can be found in Appendix E, Graph 11.

15 The detailed illustration of the loan repayment process is shown in the swimlane diagram which can be found in Appendix E, Graph 12.

16 A more detailed view of compliance processes with Mandala for the loan drawdown and repayment can be found in Appendix E, Graphs 11 and 12.

17 While non-financial corporates submit statistical reporting on external liabilities as part of the International Investment Position (IIP) statistics, such data are received on a lagged basis at the end of each quarter.

18 A more detailed swimlane diagram depicting the compliance process for use case 2 is depicted in Appendix E, Graph 13.

19 A more detailed swimlane diagram for use case 2 can be found in Appendix E, Graph 12.

20 On Sepolia, all transactions are public. For real-world implementations, more work on settlement layer privacy is needed.

21 The project evaluated compatibility with both prototypes built by Partior and R3 as part of Project Dunbar.

22 The Mojaloop Foundation has submitted a change request (CR1357) for the inclusion of a new element, "VerificationOfTerms," within ISO 20022 messages that could potentially be used to carry the compliance check ID/signature.

23 The LEI is a 20-character, alphanumeric code based on the ISO 17442 standard developed by the International Organization for Standardization (ISO) and the Global Legal Entity Identifier Foundation (GLEIF).

24 www.opensanctions.org.

25 Financial Action Task Force, https://www.fatf-gafi.org/en/the-fatf/what-we-do.html

26 In the context of this report, beneficiary refers to the entity that receives the funds.

27 The commercial banks that contributed to Project Mandala stated that there is an increased workload related to responding to and fielding questionnaires about their correspondent banking relations. The Correspondent Banking Due Diligence Questionnaire covers a wide range of financial crime risks and is the successor to the Wolfsberg AML questionnaire which was first issued in 2004. It is revised and updated periodically on an as-needed basis.

28 PJC is an open source project developed by Google.

29 The detailed illustration of the loan repayment process is shown in the swimlane diagram which can be found in Appendix E, Graph 12.

30 In this context, the borrower's bank is referred to as the BB and the lender's bank as the OB to maintain consistency with the loan drawdown process terminology.

31 The Foreign Exchange Bank is a bank designated to handle foreign exchange transactions in accordance with the Foreign Exchange Transaction Act. These banks are authorised to process cross-border payments, conduct foreign currency exchange, and manage related regulatory compliance and reporting to the Bank of Korea.

BIS Innovation Hub

RESERVE BANK OF AUSTRALIA

BANK OF KOREA

BANK NEGARA MALAYSIA
CENTRAL BANK OF MALAYSIA

MAS
Monetary Authority of Singapore

Project Mandala
Streamlining cross-border transaction compliance

ISBN 978-92-9259-798-6 (online)
bis.org