BIS Innovation Hub

Project Dunbar

International settlements using multi-CBDCs

March 2022

Reserve Bank of Australia

Bank Negara Malaysia
Central Bank of Malaysia

MAS
Monetary Authority of Singapore

South African Reserve Bank

Contents

Appendix

Executive summary

01

Project Dunbar explores how a common platform for multiple central bank digital currencies (multi-CBDCs) could enable cheaper, faster and safer cross-border payments. The project is a collaboration between the Bank for International Settlements (BIS) Innovation Hub Singapore Centre, the Reserve Bank of Australia, Bank Negara Malaysia, the Monetary Authority of Singapore and the South African Reserve Bank.

This initial phase of the project successfully developed working prototypes and demonstrated practicable solutions, achieving its aim of proving that the concept of multi-CBDCs was technically viable. The prototypes validated the design approaches taken to resolve three critical sets of challenges relating to **access, jurisdictional boundaries** and **governance**.

The first part of the report provides a broad overview of the multi-CBDC space, including key benefits and challenges, and would be of interest to policymakers. This starts in Section 2, which explains the motivations for the project and the approach to achieving its objectives. Section 3 elaborates on the expected benefits of a multi-CBDC platform, explaining how cross-border payments can be made faster, cheaper and safer through reduced reliance on intermediaries, simplification of settlement processes, consolidation of common processes and process automation using smart contracts. Section 4 explores three critical challenges of implementing a multi-CBDC platform.

The second part of the report describes the design of a multi-CBDC platform and would be of interest to technologists. An overview of the foundational capabilities required in a multi-CBDC platform is outlined in Section 5, which describes its capabilities across the areas of governance, processes and technology. Each of these is covered in greater depth in Sections 6, 7 and 8. The technical design of the prototypes is summarised in Section 8, with further details of the technical prototypes developed by R3 and Partior available in the appendix.

The final part of the report suggests areas for further exploration and would be of interest to policymakers and technologists. As one of the first technical experiments in the nascent space of multi-CBDCs, Project Dunbar focused as much on identifying problems as on solving them, and ended with more questions than answers – and with more questions than before it started. Open questions and challenges were identified and categorised across the areas of policy, business and technology. Key milestones and next steps were also identified.

This final section describes problem statements that need to be explored in the multi-CBDC space and constitutes an open call for collaboration to the central banking community, banking and payments companies, and the broader blockchain technology ecosystem. Multi-CBDC common platforms could make cross-border payments cheaper, faster and safer – and see them approach the efficiency of domestic payments systems that we are familiar with. However, this is a journey that we must take together.

Introduction

02

Project Dunbar is a collaboration between the Bank for International Settlements (BIS) Innovation Hub Singapore Centre, the Reserve Bank of Australia (RBA), the Bank Negara Malaysia (BNM), the Monetary Authority of Singapore (MAS) and the South African Reserve Bank (SARB) to explore how a common platform for multiple central bank digital currencies (CBDCs) could enable cheaper, faster and safer cross-border payments.

The area of cross-border payments is complex with multiple challenges, although several projects are underway to address them. One key challenge is fragmentation, which Project Dunbar looks to address by exploring a common platform for cross-border settlements that allows participating central banks and financial institutions to transact directly with each other in CBDCs.

2.1 Background

Cross-border payments are fund transfers for which the sender and the recipient are in different jurisdictions.[1] Such payments can be further classified into wholesale and retail payments. Project Dunbar focuses on wholesale payments between banks (interbank payments).

Unlike domestic payments, where banks can pay each other directly on a single national payments platform, there is currently no single international platform for cross-border payments and settlements leveraging CBDCs. Today, the correspondent banking model is used, where banks hold foreign currency accounts with each other. To complete a single cross-border transfer, multiple correspondent banks may be involved, with transactions recorded on multiple ledgers on multiple systems built on different technologies and communicating in different message formats.

2.1.1 Inefficiencies of cross-border payments today

This fragmented network results in cross-border payments being generally slower, opaque and more expensive compared with domestic payments. A single cross-border payment might pass through multiple correspondent banks using the foreign currencies held with them. Each leg of the overall transaction takes time and effort to process, with fees levied that add up quickly and are passed on to customers, resulting in slow and costly cross-border payments.

In addition, there are significant operational processes that are needed to comply with regulations such as foreign exchange controls and anti-money laundering/countering financing of terrorism (AML/CFT) measures. These processes, such as enhanced due diligence (EDD) and know-your-customer (KYC) processes, are often manual and must be performed in each jurisdiction and by multiple parties in order to satisfy the unique requirements imposed by respective regulators.

2.1.2 Global efforts to improve cross-border payments

Globally, cross-border payments lag significantly behind domestic payments in meeting user expectations for services. Faster, cheaper, more transparent and more inclusive cross-border payments could have widespread benefits for citizens and economies worldwide, supporting economic growth, international trade, global development and financial inclusion.

In October 2020, the G20 endorsed an ambitious *roadmap* to enhance cross-border payments around the world.[2] The G20 *roadmap* was developed by the Financial Stability Board (FSB) in coordination with the BIS Committee on Payments and Market Infrastructures (CPMI) and other international bodies. It sets out a five-year programme to address various frictions in retail

[1] See Bank for International Settlements et al, "Central bank digital currencies for cross-border payments", 2021, www.bis.org/publ/othp38.htm.
[2] See Financial Stability Board (2020), Enhancing Cross-border Payments Stage 3 roadmap. https://www.fsb.org/wp-content/uploads/P131020-1.pdf

and wholesale cross-border payment arrangements that contribute to the challenges of high cost, low speed, limited access and insufficient transparency.

The G20 *roadmap* aims to address these interrelated problems through 19 "building blocks" (ie workstreams) that will be run in parallel over the course of the plan by the relevant international organisations and standard-setting bodies (Figure 1).

2.1.3 CBDCs as a potential solution

One focus area of the G20 *roadmap* is in new payments infrastructures and arrangements, which includes CBDCs. CBDCs show great promise in terms of improving payments, and have been the subject of exploration by multiple central banks.

Prior explorations have focused on the use of CBDCs for domestic payments. Examples of projects by our project partners include Project Atom by the RBA, Project Ubin by the MAS and Project Khokha by the SARB. There have also been projects on cross-border payments using CBDCs through bilateral connectivity, such as Jasper-Ubin by the Bank of Canada and the MAS.

Building block 19 of the G20 *roadmap* seeks to "factor an international dimension into CBDC designs", and this has led to growing interest in exploring models through which multiple CBDCs could be used for cross-border payments (so-called multi-CBDC arrangements). Three conceptual models for multi-CBDCs were described in a recent paper by the BIS:[4] compatible CBDC systems (model 1), interlinked CBDC systems (model 2) and a single system with multiple CBDCs (model 3).

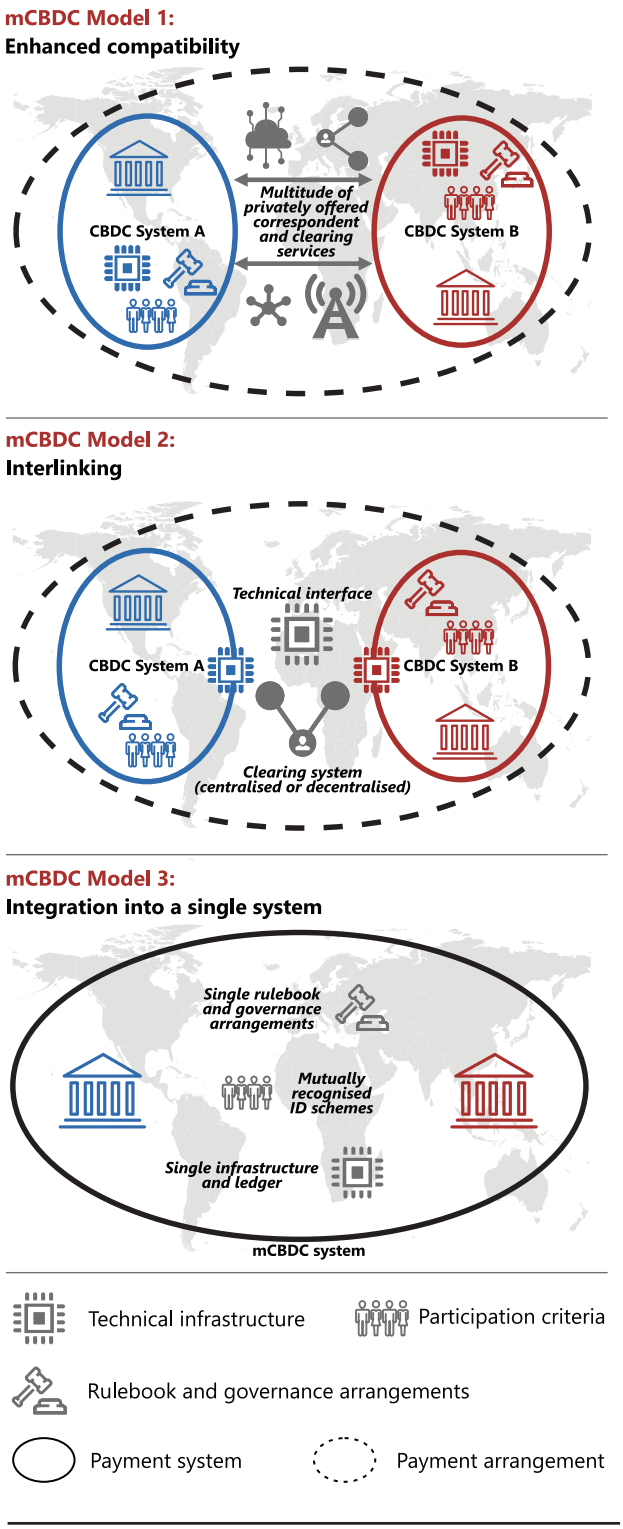
What is a CBDC?

In simple terms, a CBDC is a digital banknote. It could be used by individuals to pay businesses or other individuals (a retail CBDC) or it could be used by financial institutions or other wholesale market participants to settle trades in financial markets or other transactions (a wholesale CBDC).[5]

Figure 1: Overview of the focus areas and associated building blocks[3]

[3] See BIS, "Enhancing cross-border payments: building blocks of a global roadmap", July 2020, p3.
[4] See R Auer et al, "Multi-CBDC arrangements and the future of cross-border payments", BIS Papers, no 115, March 2021.
[5] See BIS, "BIS Innovation Hub work on central bank digital currency (CBDC)", www.bis.org/about/bisih/topics/cbdc.htm.

Figure 2: Multi-CBDC arrangements can facilitate cross-border payments



Model 1 enhances compatibility for CBDCs via similar regulatory frameworks, market practices, messaging formats and data requirements.

Model 2 involves interlinked CBDC systems. This could build on enhanced compatibility while offering additional safety, via PvP settlement. Further, common clearing mechanisms – potentially operated by central banks acting as super-correspondents in cross-currency settings – could enhance efficiency, especially when they are linked with FX trading.

Model 3 involves a jointly operated mCBDC payment system hosting multiple CBDCs. All FX settlements would be PvP by default, rather than requiring routeing or settlement instructions through a specific entity acting as an interface. Trading venues could also be integrated into an mCBDC system, to reduce complexity, fragmentation and concentration.

Source: R Auer, P Haene and H Holden, "Multi-CBDC arrangements and the future of cross-border payments", BIS Papers, no 115, March 2021

2.2 Motivations and objectives

Project Dunbar builds on the prior work and experience of its partnering central banks to explore the development of a common shared settlement platform which connects all participating central and commercial banks. This is aligned with the model 3 arrangement of a single system for multi-CBDCs.

A common platform for international settlements using CBDCs could bring about significant improvements to cross-border payments, much like how national payments systems have made domestic payments seamless, instant and low cost in many countries. At the same time, this new type of arrangement also brings new challenges.

Project Dunbar aims to explore the potential benefits and opportunities of a multi-CBDC platform, understand the critical obstacles and challenges to implementing such a platform, develop design approaches to address them, and prove the viability of the concept through the building and testing of technical prototypes.

2.3 Project methodology

2.3.1 Project partners and structure (workstreams)

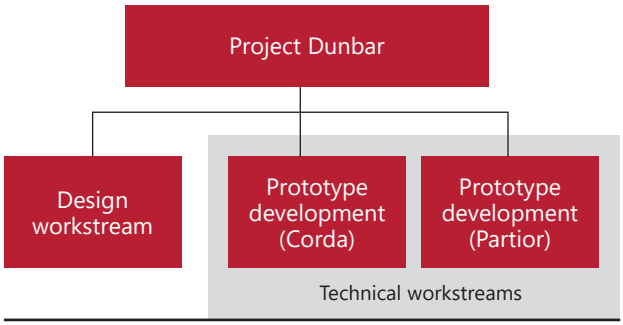
Project Dunbar is a collaboration between the BIS Innovation Hub Singapore Centre and the central banks of Australia, Malaysia, Singapore and South Africa.

The partner central banks have published multiple reports and conducted technical experiments on CBDCs, bringing a wealth of knowledge and expertise to the project. This has helped to generate useful insights during discussion workshops and led the team to develop an appreciation of the complexities involved in building a common platform, as well as on more abstract topics such as governance. There were also two central bank observers of the project, the Bank of France and Hungary's Magyar Nemzeti Bank, which contributed substantially to the discussion, and their support is greatly appreciated.

In addition to the central banks, the project was supported by diverse industry participants from the finance and technology sectors. R3 and Partior, which have been working actively in the area of digital currencies, supported the project as distributed ledger technology (DLT) and platform providers, bringing a deep technical and commercial perspective to the project. Commercial banks also participated in workshops to review and discuss their perspectives on a multi-CBDC platform.

Project Dunbar was organised in three concurrent workstreams to carry out design and technical activities.

Figure 3: Workstreams



The design workstream was led by Accenture with support from Temasek, and focused primarily on developing the high-level functional requirements and design of a shared cross-border payments system. A series of workshops, which were conducted across three sprints with the participating central and commercial banks, utilised a structured design-thinking approach to discuss and develop an innovative yet practical solution.

The goal of the technical workstreams was to develop technical prototypes on two different DLT platforms – Corda and Quorum – to transform the idea of a multi-CBDC platform into working prototypes. The Corda platform development was led by R3 while the Quorum platform development was led by Partior (with support from DBS, J.P. Morgan and Temasek). The two prototypes were developed based on the proposed requirements and designs from the design workstream, while leveraging the existing

foundational features and architecture of their respective platforms. These capabilities and features were enhanced to support the specific needs of a multi-CBDC platform.

2.3.2 Scope of Project Dunbar

Many of the basic functionalities required of a multi-CBDC platform, such as CBDC issuance, transactions and redemption, are similar to those of domestic wholesale CBDC systems. As this area has been the subject of significant global research efforts by central banks and technology providers, many such functionalities have been developed and made available as out-of-the-box aspects of the two DLT platforms. As such, Project Dunbar did not seek to replicate these efforts, but rather to focus on the specific requirements of a multi-CBDC platform.

2.3.3 Approach and sprint structure

As an exploratory project with open-ended questions to be explored within a defined timeframe, the Agile methodology was adopted for the project. Initial scoping workshops were held to define logical groupings of areas to be explored in the project. User inputs were sought through iterative discussions, which also helped to set the direction and scope of subsequent workshops. A total of three sprints were planned over a period of nine weeks with three concurrent workstreams. During each sprint, the design and technical workstreams focused on their sprint objectives which are based on the identified scope and high-level topics listed in figure 4 below.

The sprint order is not a reflection of the importance of the topic. Instead, the order was determined based on the sequence of key information that the technical partners needed in order to develop their prototypes. For example, account structure was discussed in Sprint 1 by the design workstream, and its outputs were used as requirements and specifications for development by the technical workstreams in Sprint 2.

2.3.4 Methodology

Accenture's financial market infrastructure (FMI) capability model was used as a reference to identify key areas for scope discussion within each capability across the three sprints. This was to ensure a structured approach to identifying the scope required for designing a payments settlement platform. Over the course of the project, a proposed capability framework for a multi-CBDC common platform was developed to represent the key topics that were covered. This is covered in greater detail in Section 5 and in the appendix.

Prior to Sprint 1, a Sprint 0 scoping workshop was conducted for the central banks to discuss and agree on the key focus areas. Their inputs were then cross-referenced to the FMI capability model, after which the central banks voted for the five most important capabilities for further exploration and discussion during the sprints. This formed the scope for the three sprints.

At the start of each sprint, key questions were identified to guide discussion throughout. These key questions were first explored from the design perspective, which is elaborated on in Sections 4 to 7. Further discussion on how they were implemented by R3 and Partior on the Corda and Quorum platforms respectively, is detailed in Section 8.

Figure 4: Sprint Objectives

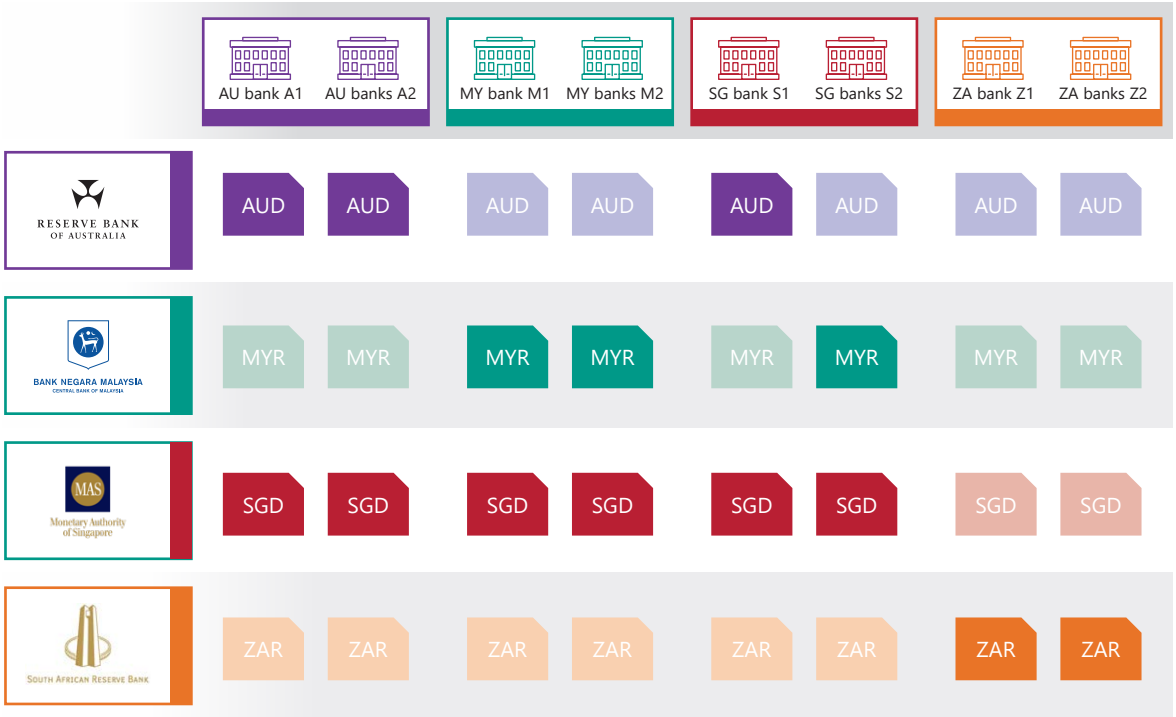
	Sprint 1	Sprint 2	Sprint 3
Design workstream	Define participants and stakeholders, membership structure and onboarding processes	Define processes for FX and settlement services across participant types	Review legal and regulatory policies, and define governance and technical controls
Technical workstream	Enable multiple CBDC issuers and customise base functionality (issue, redeem, transact)	Enable foreign currency (FCY) transactions, with multi-tier account structure and onboarding	Enable new models of FX, and technical controls to support governance models

International settlements with multi-CBDC

03

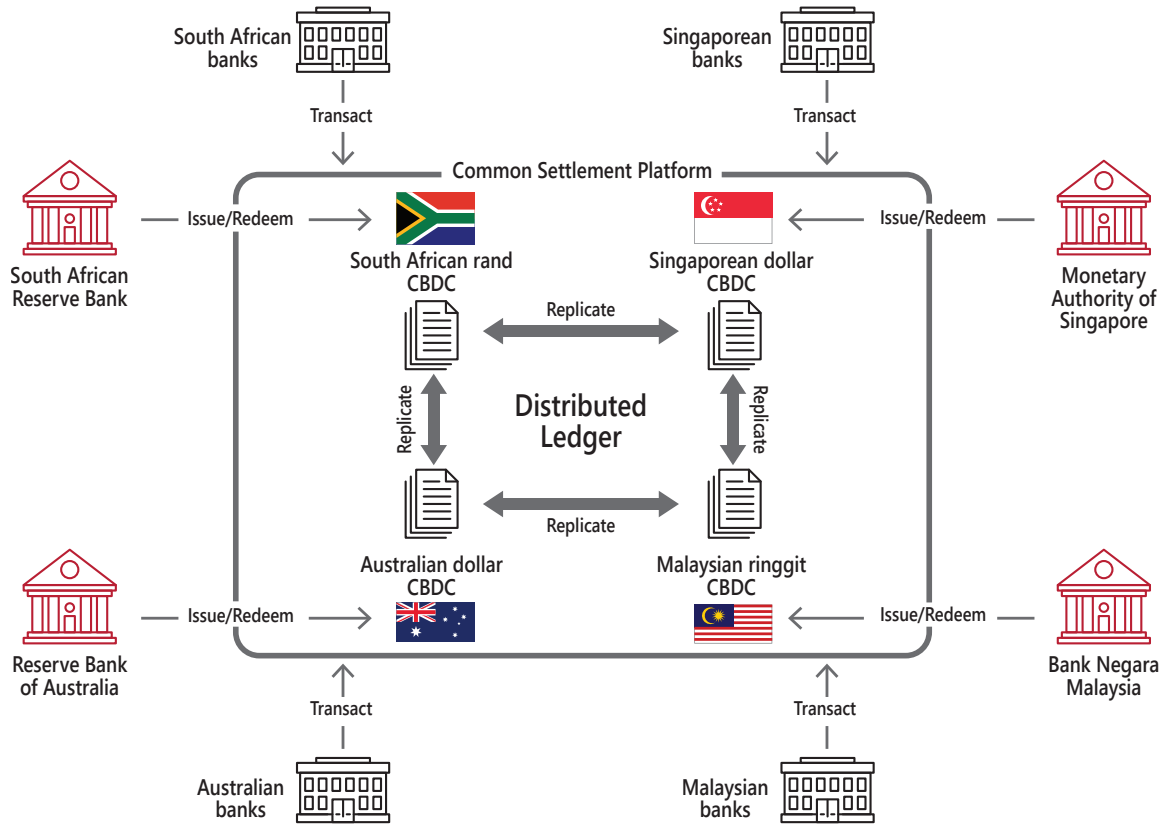
On a multi-CBDC common platform, each participating central bank issues its own CBDC in its own domestic currency. Participating commercial banks are then able to hold these CBDCs directly, gaining access to foreign currencies without the need for accounts with correspondent banks. As all participating banks could potentially hold the different CBDCs directly, they would be able to transact directly with each other in the participating currencies.

Transacting on a multi-CBDC platform



As an example, Singapore-headquartered bank S2 is a banking group with licences to operate in Singapore and Malaysia. It would likely already have access to the national payments systems of both jurisdictions and access to the two currencies (Singaporean dollars and Malaysian ringgit) in central bank money, shown in solid colours. The multi-CBDC platform is intended to allow the bank to hold CBDCs directly even in jurisdictions in which it does not have a presence – such as Australia and South Africa. In this way, it can hold Australian dollars and South African rand issued by the respective central banks, shown in shaded colours. This allows all banks participating in the platform to hold all currencies, enabling them to transact directly with each other. S2 can hold AUD CBDC and use it for payment to South African bank Z1 directly, which was not previously possible.

Figure 5: multi-CBDC platform



3.1 Expected benefits

International settlements on a multi-CBDC common platform could make cross-border payments faster, cheaper and safer. This is achieved through reduced reliance on intermediaries, simplification of settlement processes, efficiency gains through consolidation of common processes, and process automation with programmable money using smart contracts.

3.1.1 Reduced reliance on intermediaries

Cross-border payments today take place through a correspondent banking model in which banks hold foreign currency accounts with other banks (called correspondent banks). A single cross-border transfer may involve one or more correspondent banks using the foreign currencies held with them to settle the transaction. Correspondent banks also perform non-settlement processes such as AML/CFT compliance and foreign exchange controls on the transaction. Each leg of the overall transaction takes time and effort to process, which adds up quickly when multiple correspondent banks are involved.

A multi-CBDC platform would be designed so that participating banks can transact directly with each other using different CBDCs without the need to hold foreign currency accounts with correspondent banks. Instead, CBDCs can be transferred directly from the sender to the recipient bank. However, although reliance on correspondent banks is reduced, it might not be fully eliminated to the extent that correspondent banks are needed for onboarding and transaction approvals – as explained in Section 6.1.

3.1.2 Simplification of settlement processes

With the correspondent banking model, a single cross-border transfer requires multiple ledgers to be updated on different systems. Banks also need

to reconcile their nostro and vostro balances to verify that balances were correctly updated.

On a multi-CBDC common platform, transfers are recorded on a single ledger in one step, and participants have full real-time visibility of their balances. The settlement process is hence simplified and there is no need for reconciliation.

3.1.3 Efficiency gains with common platform processes

The multiple banks involved in a cross-border transfer often perform similar processes individually, such as AML/CFT and sanctions screening. Such processes are similar in nature, with a common aim of verifying the sender and recipient's identities to minimise the risk of transactions facilitating money laundering, terrorist financing or other forms of financial crime.

A common platform creates an opportunity for such processes to be performed centrally. For example, multiple sanctions checks which are performed for the respective jurisdictions could be consolidated into a single check against a common sanctions list that is based on the UN Security Council consolidated list[6] or the FATF recommendations[7].

Differences in regulatory requirements across jurisdictions, however, mean the scope for centralisation of compliance activities may be limited. For example, countries might have domestic watchlists that do not apply to transactions outside their jurisdiction. Centralising common processes might create efficiency gains in reducing duplicative processes, but further exploration is required to ascertain how feasible this is in practice.

3.1.4 Process automation with smart contracts

Other than reducing duplicative processes, there is also the potential for processes to be automated through smart contracts. Business rules or conditions – such as having sufficient liquidity, technical validations and meeting business requirements – could be automated using the smart contract features on a DLT platform.

Smart contracts can also be used for conditional payments, to hold funds and to release payment upon the fulfilment of pre-defined conditions – for example, with payment-versus-payment (PvP) and delivery-versus-payment (DvP) transactions. Where the assets are issued on a common platform, they can be directly managed by smart contracts without the need for a trusted intermediary and coordination across different platforms. Examples include PvP settlement for exchange of CBDCs in different currencies, as well as DvP settlement of tokenised assets with CBDCs if such assets were to be issued on a common platform. Where the assets are issued on different platforms, smart contracts can still be used, but with a higher level of technical complexity due to the need for coordination across platforms.

Automating conditional checks using smart contracts could help ensure each party's obligations are clear and enforced. This could give stakeholders involved in cross-border transactions greater assurance of efficient and equitable processes.

[6] UN Security Council, "UNSC Consolidated List", https://www.un.org/securitycouncil/content/un-sc-consolidated-list
[7] FATF, "FATF recommendations", https://www.fatf-gafi.org/publications/fatfrecommendations/

Critical challenges

04

While there may be significant benefits to conducting settlements on a common platform, success also comes with significant challenges. This project focused on challenges that are distinct to a multi-CBDC common platform. This includes the cross-border and cross-jurisdictional aspects of international payments, and the challenges of managing a multi-central bank shared platform. Many of the general aspects of wholesale CBDC have been addressed in earlier projects by central banks, and were not revisited in detail.

The project identified and focused on three critical sets of challenges, which had a significant impact on the subsequent design. These were access, jurisdictional boundaries and governance.

4.1 Access

As noted earlier, one defining characteristic of a multi-CBDC platform is the ability for participating banks to hold and transact in CBDCs of different currencies. This is critical in reducing the reliance on correspondent banks for cross-border payments. However, there are some key questions to be explored to ensure that this is feasible, such as whether non-resident banks – ie banks which do not have a local presence and are not authorised to operate or provide domestic financial services – can be trusted to access and make payments with CBDCs when they do not have a presence in those jurisdictions?

In designing the access framework, two models were explored: "direct" CBDC access and "hybrid" CBDC access. These access models are described in Section 6.1.

4.2 Jurisdictional boundaries

Payments regulations are different in each country, and participants in a cross-border payment are subject to these different regulatory frameworks. A key challenge is how to simplify the cross-border payments flow while respecting regulatory differences across jurisdictions.

The project took a design approach to differentiate between settlement and non-settlement processes, which enables the clear delineation of jurisdictional boundaries, adherence to regulatory policies of different jurisdictions, and the streamlining of settlement processes. This is explored in detail in Section 7.2 and Section 7.3.

4.3 Governance

Central banks traditionally have a high degree of control over their domestic payments systems. A multi-CBDC platform would serve as an international payments system for, and record the liabilities of, multiple central banks. In such an arrangement, how can multiple central banks share a common platform while addressing the financial system resilience and national security concerns that may arise from sharing such a critical payments infrastructure with other central banks?

A shared platform implies a level of universality – with features and capabilities that are common and available to all participants. At the same time, an adequate level of autonomy and control over each jurisdiction's domain areas is required to build greater confidence among the equal participants of a shared platform.

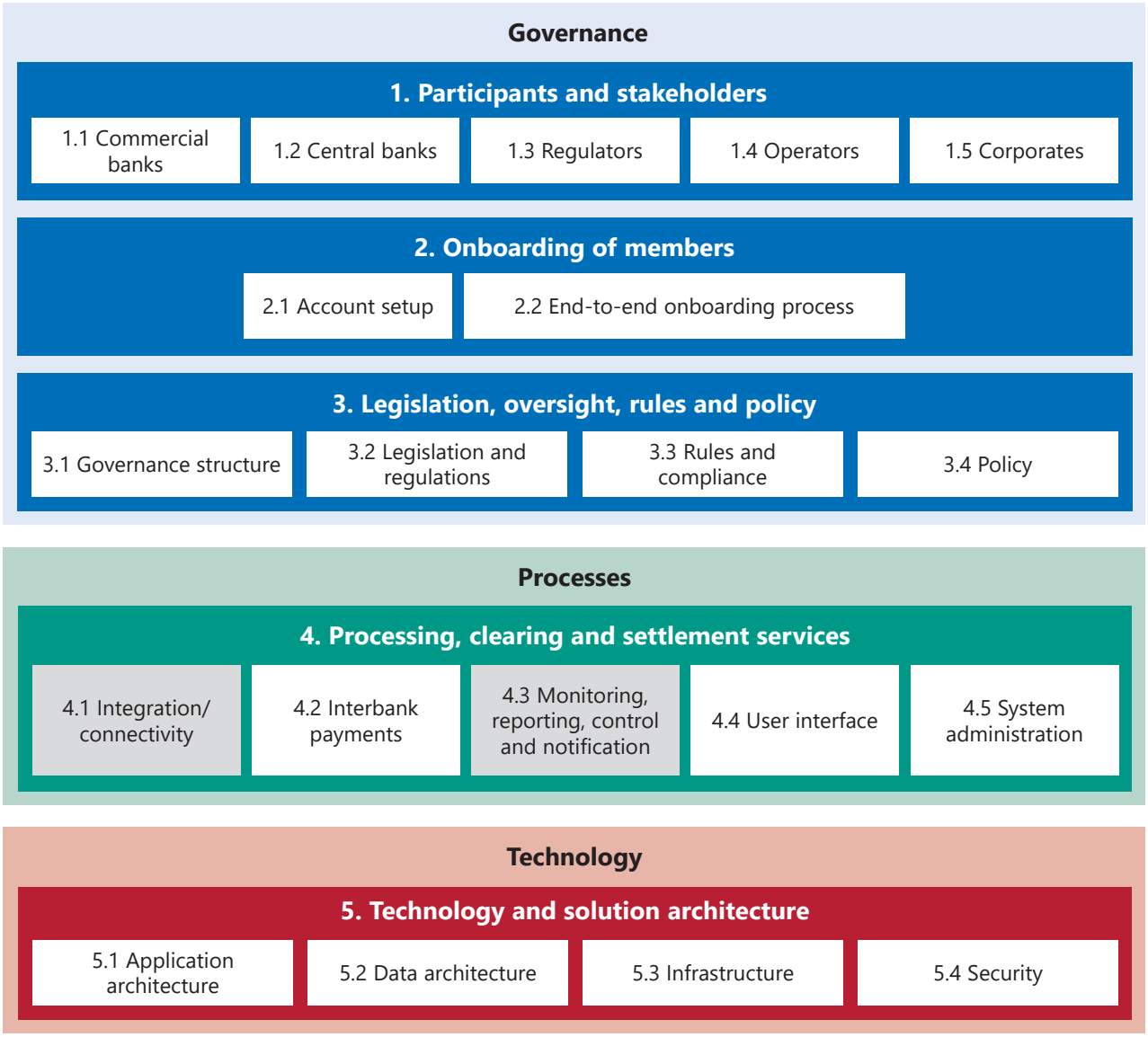
The project took a design approach of optimising universality and autonomy. Governance structures and decision-making authorities are designed to ensure that the diverse stakeholders are represented, and that collective decisions are made fairly and equitably. Central banks are also granted autonomy within the boundaries and parameters of a universal platform-level framework. This is explored in Section 6.3.

05

Designing for a multi-CBDC common platform

A multi-CBDC common platform requires foundational capabilities across the areas of governance, processes and technology. These capabilities are outlined below and covered in greater depth in the subsequent sections.

Figure 6: Capabilities and considerations for a multi-CBDC common platform



Governance capabilities relate to the rules and boundaries for the operations and usage of the platform, and the mechanisms by which decisions are made. Rules include internal rules that are inherent to the platform, as well as the broader legal and regulatory policies that the platform and its participants must adhere to. A key part of governance is about defining participants and stakeholders, and their roles and responsibilities on the platform. Other aspects include access considerations, how members are onboarded, the structures for making decisions, and how rules are developed and applied.

Process capabilities relate to the series of actions taken to complete a payment transaction, and the functionalities required to perform these actions. As this phase of the project focuses on proving the viability of cross-border payments, most of the work centred around interbank payments processes. Capabilities relating to integration and connectivity with central banks' systems, such as those used for pledging assets to back the issuance of CBDCs, were not explored as they have been tested and proven in prior research by central banks. Ancillary capabilities such as monitoring, reporting, control and notification were deemed to be a lower priority and were not explored in the current phase. Similarly, user interfaces and system administration tools were deemed to be a low priority and no further work was conducted on them. However, these are often already available as built-in capabilities of existing platforms, and so were made available for testing by the technology partners.

Technology capabilities refer to the complete solution stack required to enable the technical delivery of the multi-CBDC common platform. Infrastructure includes the servers, network and DLT platform that enables central banks to communicate with each other on a shared platform. Data and application architectures define the CBDC tokens and how they can be used for transactions by participants. Security includes security features and controls that enable central banks to comfortably transact on this shared platform.

Governance

06

Governance is a key consideration for a multi-CBDC platform that is shared by multiple central banks and involves numerous stakeholders across jurisdictional boundaries.

The project identified key participants and stakeholders, and defined their roles and responsibilities, as well as considerations for access to the multi-CBDC platform. Decision-making considerations, including governance structures and framework, were explored to understand how decisions can be made in a manner that ensures representation of diverse stakeholders and is fair and equitable. The project also explored how central banks can be granted autonomy within the boundaries and parameters of a universal platform-level framework.

6.1 Access considerations

Participants must be granted access to transact on the multi-CBDC platform. There are multiple layers of access, each with its own set of considerations, and with different privileges and modes of access for different participants.

First, participants must have access to the platform to use it and communicate with others. This could be directly through the nodes they host, or indirectly through nodes hosted by others. Second, participants must have access to hold the CBDCs as assets representing a legal claim on the issuing central banks. Third, participants must have access to transact with the CBDCs, to initiate and make payments to others. This could be directly between them and their recipients or indirectly where intermediaries play a role in processing the transaction.

6.1.1 Participants and stakeholders

The level of access granted will be different for different participants. Defining the participants and stakeholders is hence an important part of access policies and the broader governance framework. For the project, participants and stakeholders include parties that are directly involved in using the platform, as well as other stakeholders that may have an interest in doing so. In defining the participants, there was a deliberate decision to create granular groups due to their different treatments from policy and technical perspectives. This differentiation at an early stage also allows for a common set of terms to be used across the different workstreams.

Commercial banks were split into three groups. The differentiation of non-resident banks, which do not have a presence in the local jurisdiction, was particularly important from the perspective of access policies. The differentiation of commercial banks into "selected" and "others" was to cater for potential differentiation in the hosting of nodes and direct access to the network, as well as the onboarding processes.

A limited number of large commercial banks of proven financial standing in their respective jurisdiction would be identified as selected commercial banks. They would be provided with additional privileges and may be required to comply with more stringent requirements. Other commercial banks would transact through these selected commercial banks and may have limited privileges on the system and be subject to less stringent requirements.

Central banks, regulators and operators were also split into three distinct roles. In some jurisdictions, a single entity takes on the role of both central bank and financial regulator. Similarly, central banks in some jurisdictions are also operators of the national payment systems. The distinction between central bank and regulator is particularly important in relation to transaction processes, as settlement or the movement of CBDCs is the domain of central banks, while other processes relating to AML/CFT are the domain of regulators. Definitions of the participants are detailed in Appendix 1.1.

Each of the parties has a role which defines their rights and obligations on the platform – it is vital to note that some of these roles apply only to the hybrid CBDC model and are not part of the direct CBDC model.

Figure 7: Participants' roles

		Role
Commercial banks	**Selected commercial banks**	1. Initiate transfer and exchange of CBDCs 2. Perform AML processes on non-local banks 3. On-ramp/Off-ramp of CBDCs 4. Exchange collateral with central bank for CBDC (primary issuance) 5. Onboard other commercial banks/non-local banks
	Other commercial banks	1. Initiate transfer and exchange of CBDCs 2. Perform AML processes on non-local banks
	Non-resident banks	1. Initiate transfer and exchange of CBDCs
Central banks		1. Initiate transfer and exchange of CBDCs 2. Issue/destroy CBDC 3. On-ramp/Off-ramp of CBDCs 4. Onboard selected commercial banks *Including: set up and manage currency controls (if any)*
Regulators		1. Review members of the system (incl. during onboarding) *Including: regulate members of their own jurisdiction*
Operators		1. Onboard central banks *Including: execute operational policies set out for the scheme*
Corporates – Customers of banks		**N/A – Transact only through commercial banks**

6.1.2 Access to platform

Access to platform refers to the ability to use the platform and communicate with others. The primary means of accessing the platform is through hosting a node and connecting to other nodes and components of the network. Participants that host nodes have direct access to the platform, while participants that do not host nodes may access indirectly through nodes hosted by other participants.

Access to the platform is managed through an onboarding (and offboarding) process. This will likely be governed in a federated manner to respect central banks' autonomy within their jurisdictions or domains. For example, while central banks will be onboarded by a central operator, commercial banks will be onboarded by their respective central banks. It should also be noted that there are two perspectives to

onboarding. There is a governance perspective – this is the decision to accept and onboard the participant. There is also a technical and operational perspective of enabling network connectivity of the nodes, and provisioning of network credentials and wallets. For example, technical and operational onboarding of a new central bank will be performed by the operator, following approval by a governance body.

From a technical scalability perspective, there may be a limit to the optimum number of nodes on the network. If so, access to the platform would be implemented as a two-tier model, with only selected commercial banks hosting nodes, and other commercial banks connecting through them. While technical scalability was not tested in the project, access to the platform was still designed for flexibility with this possibility in mind.

Figure 8: Onboarding participants

		Onboarding/off-boarding by		
		Central operator	**Central banks**	**Selected commercial banks**
Commercial banks	**Selected commercial banks**		✓	
	Other commercial banks		✓ (If all banks host nodes)	✓ (If only selected banks host nodes)
Central banks		✓ (With approval of governance body)		

Central banks
The decision to admit new central banks to the scheme would be undertaken by a governance body, based on a variety of factors (see Section 6.3.5).

From a technical and operational perspective, onboarding would be executed by a central operator.

Selected commercial banks
Selected commercial banks could be chosen and technically and operationally onboarded by the central banks in their country of domicile. These would likely be larger banks that are existing participants of other payment schemes.

Other commercial banks
Other commercial banks and non-resident banks could be onboarded by a selected commercial bank for a jurisdiction and may be subject to commercial agreements.

When a new participant is being onboarded onto a platform, it needs to meet two sets of onboarding requirements. The first is a set of common rules at the platform level. The second relates to jurisdiction-specific requirements as mandated by the local central bank.

Non-resident banks
As banks only require a single point of connection to the platform, access to the platform for non-resident banks will be provisioned in their country of domicile.

6.1.3 Access to hold CBDCs

One defining characteristic of a multi-CBDC platform is the ability for participating banks to hold and transact in CBDCs of different currencies. This is a change from conventional models where only banks licensed in a particular jurisdiction are granted access to its national payments system and to central bank money.

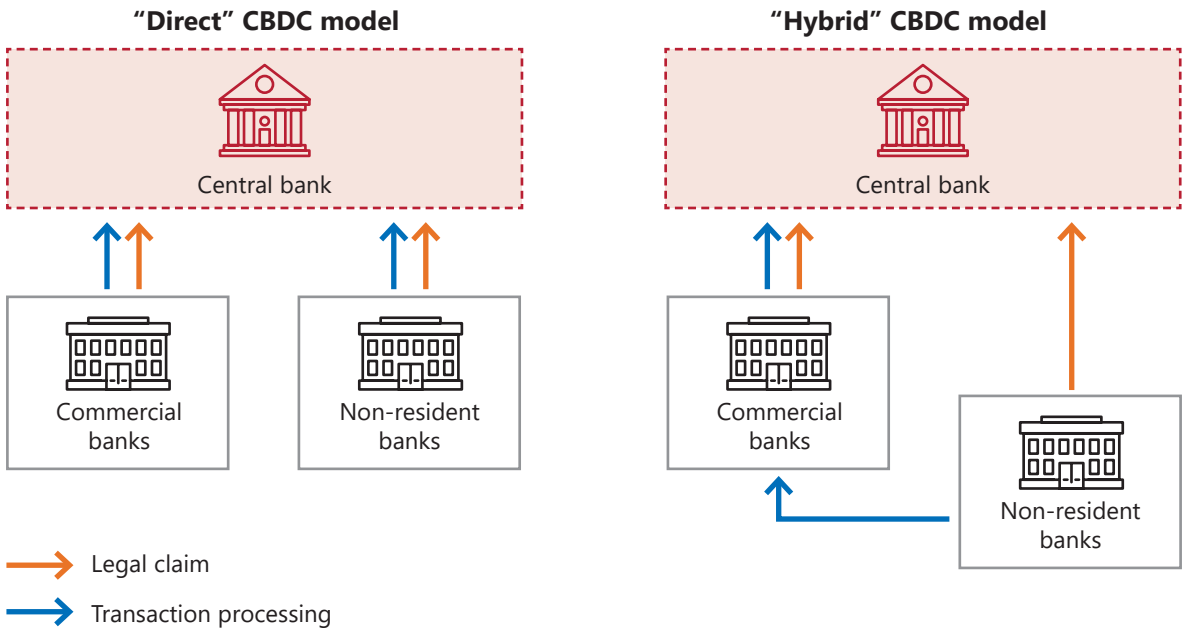
On the platform, all participants can hold CBDCs that represent a direct claim on the central bank. In that regard, there is no intermediation of liability. All digital currencies transacted on the platform are central bank money and are not commercial bank money.

While all participants can hold CBDCs, central banks will likely only issue CBDCs to banks licensed in their jurisdictions. This is because the issuance of CBDCs needs to be backed by a corresponding amount of pledged assets which the central banks receive through their national payment systems. Non-resident banks can receive and hold CBDCs by purchasing them from other banks as a foreign exchange transaction.

6.1.4 Access to transact in CBDCs

In transacting with CBDCs, there is a need for compliance with local regulatory requirements such as AML/CFT and foreign exchange controls. Intermediaries may be required to fulfil these requirements. Two possible models for access were explored: "direct" CBDC access and "hybrid" CBDC access, both of which borrow heavily from the access models for retail CBDC.[8] In a conventional correspondent banking model, non-resident banks typically hold foreign currencies through resident banks in the same way that retail customers hold deposits with their banks. This similarity allows the retail CBDC models to be applied in a similar manner.

Figure 9: Potential access models



[8] See R Auer and R Böhme, "The technology of retail central bank digital currency", BIS Quarterly Review, March 2020, pp 85-100, www.bis.org/publ/qtrpdf/r_qt2003j.pdf.

Direct CBDC access by non-resident banks
With a direct CBDC access model, non-resident banks can hold and transact directly with CBDCs without the need for sponsoring banks. However, an onboarding process will still be required for non-resident banks and they may be subject to the central banks' internal controls and processes. Processes can be further streamlined and made significantly more efficient, but this may require changes to existing regulatory policies and harmonisation across participating central banks. For example, different jurisdictions might have different thresholds to identify significant transactions that require enhanced due diligence. On a common platform, participants may collectively agree to adopt the lowest threshold to comply with the most stringent regulatory requirements.

Hybrid CBDC for access by non-resident banks
With a hybrid CBDC model, non-resident banks hold CBDCs representing a direct claim on the issuing central banks, but they require intermediaries, in the form of "sponsoring" banks, for transaction processing. "Sponsoring" banks are resident banks which are subject to local regulations, and perform customer due diligence processes on behalf of the non-resident banks. This includes onboarding and KYC processes as well as suspicious transaction monitoring and AML/CFT processes. As these control processes continue to be applied in a similar manner, a hybrid CBDC model is unlikely to require significant amendments to existing regulatory policies for implementation. However, this will need to be further validated and may differ across jurisdictions.

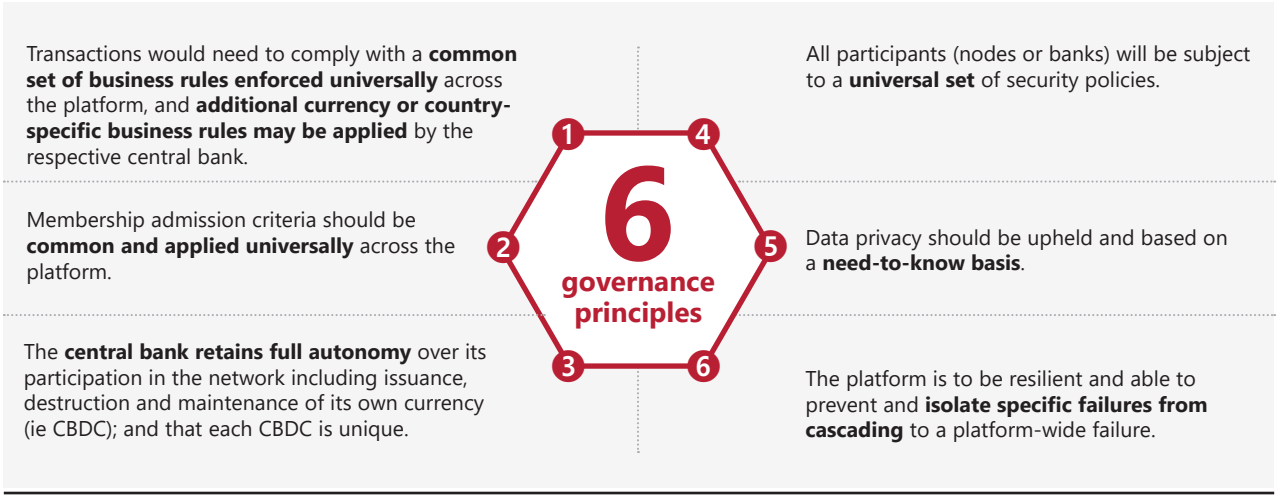
While the need for correspondent banks is eliminated in the settlement process, intermediaries in the form of "sponsoring" banks may continue to play a role in control processes such as KYC and AML/CFT. This limits the efficiency gains of eliminating intermediaries and poses a challenge for commercial models and incentives for banks to play such sponsoring roles. Various possibilities exist, including reciprocal arrangements and obligations imposed as conditions of access and fees, and these need to be evaluated further. For example, one solution could see selected banks agree to sponsor each other's transactions; banks might also charge fees for transactions that they sponsor.

6.2 General principles for shared platform

A multi-central bank common platform would be a shared platform where central banks issue and record their liabilities on a platform over which they do not have full control. This is an unfamiliar concept and there is a need to develop principles that could engender trust and confidence in using the shared platform.

Participating central banks in the project were polled on the considerations that are collectively important in bringing about a high level of comfort in using a shared platform. These inputs were subsequently examined and distilled into six key ideas, which are further refined into general principles that act as a guiding step for the right governance structure to be put in place to maintain assurance for participants.

Figure 10: Six governance principles



6.3 Decision making considerations

A shared platform implies a level of universality – with features and capabilities that are common and available to all participants. Platform rules and policies are applied universally and fairly across participants.

To enable this universality, governance structures and decision-making authorities must be designed to ensure that the diverse stakeholders are represented, and that collective decisions are made fairly and equitably. At the same time, an adequate level of autonomy and control over each jurisdiction's domain areas is required to build greater confidence among the equal participants of a shared platform.

6.3.1 Governance structure

One major consideration is the composition and setup of one or more committees to provide oversight over the various business activities conducted in and for the multi-CBDC platform.

At a conceptual level, the structure for a multi-CBDC platform is comprised of three levels of decision-making: strategic and platform decisions; tactical decisions; and day-to-day operational decisions.

Each level would be deliberated in committees, comprising groups of stakeholders that have a diverse interest in ensuring the platform's extended-term sustainability.

Figure 11: Governance structure

Levels of decision-making	Applicable forums	Relevant parties
Strategic and platform decisions	• Governance bodies	Central banks, the BIS, selected commercial banks, operator
Tactical decisions	• Business management; governance-related bodies • Technology- and architecture-related bodies • Risk- and compliance-related bodies • Innovation- and research & development-related bodies	Central banks, the BIS, selected commercial banks, operator
Day-to-day operational decisions	• Business operations team • Technology team • Risk and compliance team • Innovation and research & development team	Central banks (or their appointed operator), operator

6.3.2 Decision-making framework

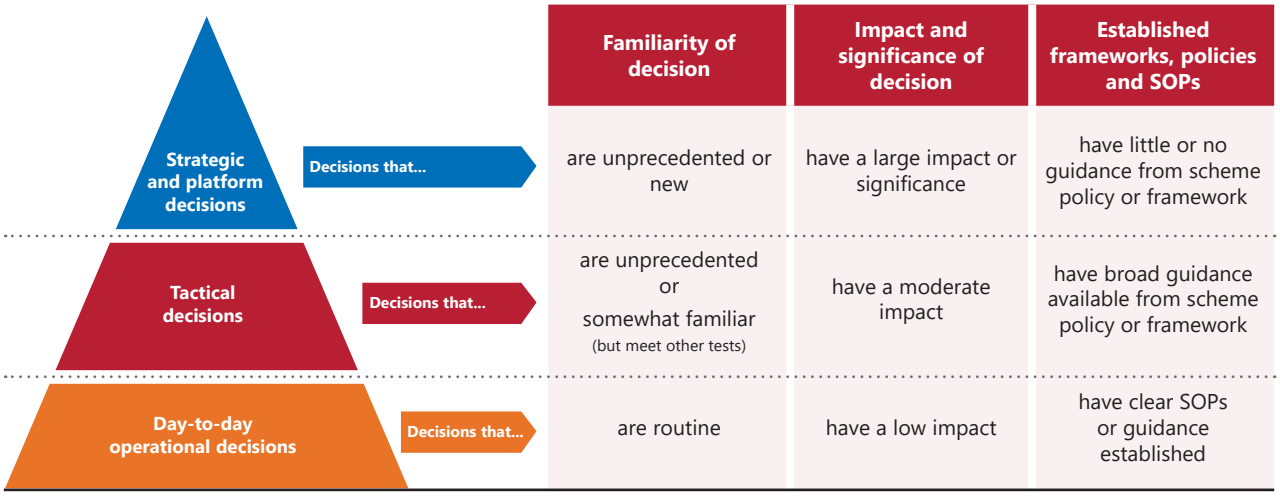
Decision-making on a shared platform involving multiple countries is complex. For this reason, the types of decisions are classified in three categories below. Each category of decision-making may involve different governance.

Strategic and platform decisions – decisions that are unprecedented or require judgment, and which have a large impact or significance with little or no guidance from the scheme's policy/framework. For example, taking a decision on who should operate the multi-CBDC platform, or onboarding a new central bank.

Tactical decisions – decisions that are unprecedented or somewhat familiar, and that have a moderate impact and broad guidance available from the scheme's policy/framework. An example includes the types of services that are available to different members.

Day-to-day operational decisions – decisions that are routine with low impact and have clear standard operating procedures (SOPs)/guidance established. Examples include technical patching or connecting new members to the platform.

Figure 12: Three levels of decisions



6.3.3 Common rules and autonomy

For the consistency of the platform, a set of common rules would be applicable to all participants. Under a consortium structure, these common rules would be established through a consensus of the participating central banks.

At the same time, central banks demand complete sovereignty and autonomy in: (i) areas of critical functions, such as issuance of currency; (ii) the application of "local" rules and regulations at the currency- and jurisdiction-level; (iii) the application and the recognition of the central bank's mandate provided in its national legislation; and (iv) data, including privacy and selective sharing of data.

Rules on the platform are thus designed to be applied in three ways.

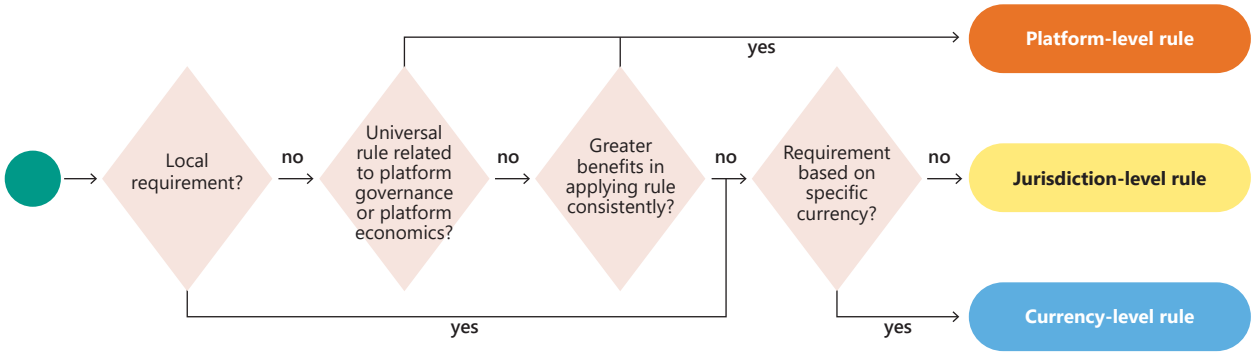
- **Platform-level rules –** universal rules applicable to all that participate in the scheme and applied at the platform level. These rules are maintained centrally by the platform operator. A potential platform-level rule could be managing access to the multi-CBDC platform.

- **Jurisdiction-level rules –** rules specific to a local requirement are applied on a jurisdiction level. These rules can be maintained by each central bank. An example of a potential jurisdiction-level rule could be limitations on members which are allowed to obtain CBDCs directly from the central bank issuing them.

- **Currency-level rules –** rules specific to a currency on the scheme. These apply across different jurisdictions, and are applied on a currency-level. These rules can be maintained by each central bank. Examples include payment transaction restrictions on members, such as setting a maximum threshold for the inflow/outflow of the currency within a specified window and foreign exchange controls.

When a new rule has been enacted, the following flowchart may be used to determine whether the rule will be applied at the platform, jurisdiction or currency level.

Figure 13: Rule-mapping flowchart



Achieving autonomy for central banks

Central banks are responsible for managing and regulating their nation's currency to achieve the objectives (fiscal or otherwise) set by that country. This management of currency would extend to a multi-CBDC platform, where a central bank would need to be able to manage its own CBDC on the platform. This entails not only oversight over usage of its CBDC, but also issuance and redemption of CBDCs.

The prototype platforms are designed to give central banks autonomy within the boundaries and parameters of a universal platform-level framework, such as in the application of jurisdiction- and currency-level rules. Autonomy here is viewed as the ability for central banks to exert control within the boundaries of their scope, as well as the inability of any other party to do so without the consent of the central banks.

Strict technical controls are put in place to guarantee this autonomy such that even a super-user operator of the platform cannot violate it. In addition, the platforms are designed for resilience; this means failures at the individual country level are isolated and therefore do not cascade into platform-wide failures. This ensures that the autonomised regions and components of a central bank on this shared platform are not infringed by the failures of other central banks.

From a technical perspective, both the R3 and Partior sandboxes were able to support the necessary control that central banks require to manage and regulate their own currency. The technical details are elaborated on in Section 8.

Processes

07

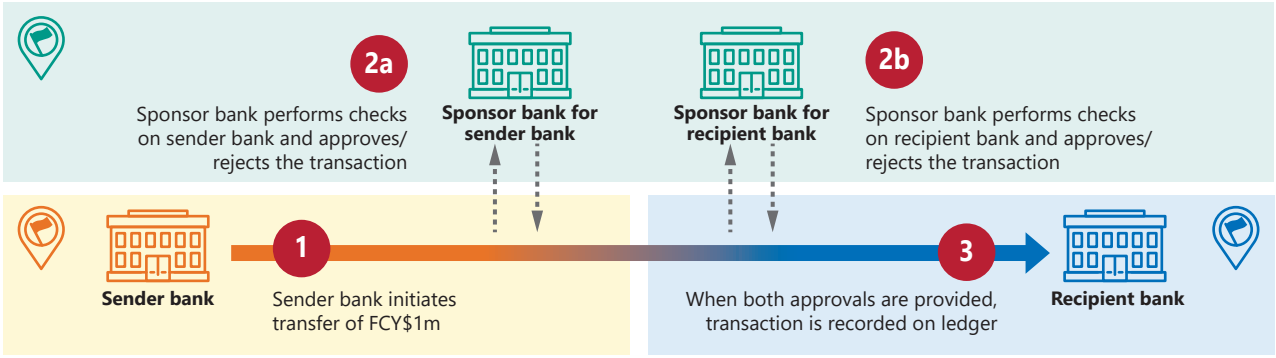
A typical cross-border payment includes multiple steps or sub-processes, including the exchange of local currencies for foreign currencies, transfer of the currencies, as well as other supporting non-settlement processes such as AML/CFT compliance.

7.1 High-level cross-border payments flows

In a conventional cross-border payments flow, multiple steps are often linked and performed as sequential and integral parts of the bigger process. In designing the process flow on the multi-CBDC platform, the steps were split into discrete sub-processes that could be performed separately. The processes are categorised into: foreign exchange, cross-border settlement and non-settlement processes.

As banks can now hold CBDCs in different currencies on the platform, they can perform the foreign currency exchange independently of the transfer, holding the foreign currency until such time as it is used for transfers. The process of exchanging local currency to foreign currency is explained in Section 7.4.

Figure 14: Future payments flow



The diagram describes how a cross-border transfer takes place between a sender and recipient bank in different jurisdictions, using a currency from a third jurisdiction. The cross-border transfer begins with Step 1, with the initiation of a transaction by the sender bank, which results in a debit or deduction of its CBDC balance. After the transfer has been initiated, sponsor banks for both sender and recipient banks are notified in Steps 2(a) and 2(b) and would carry out non-settlement processes such as AML/CFT and other control processes before they approve the transaction. Upon receiving the necessary approval from sponsor banks and fulfilling the obligatory conditions of the smart contract, the CBDCs are credited or added to the balances of the recipient bank in Step 3, which marks completion of the transfer.

Approval routing rules for Steps 2(a) and 2(b) are determined and set by the central bank issuing the CBDC. In this example, the approvals are routed to designated intermediaries as both sender and recipient banks are not in its jurisdiction. If the recipient bank is in the same jurisdiction, the routing rules would skip Step 2(b) as no sponsoring bank is required.

A central bank could also disable the need for Steps 2(a) and 2(b), allowing for a direct transfer from sender to recipient bank, without the need for any intermediaries. Such a payment flow would be akin to the direct CBDC model.

The technical choice of designing the payments flow and the underlying technical architecture

based on the hybrid CBDC model enables the technical flexibility to support different policy choices. Central banks can amend the approval routing rules to switch between the hybrid CBDC and direct CBDC models.

7.2 Cross-border settlement

Transactions that take place "across borders" are subject to the laws of the jurisdictions involved, and hence to a higher level of complexity. To reduce the overall complexity, there is an attempt to differentiate between processes that take place across jurisdictions and those processes that take place within a single jurisdiction, and to minimise the scope of the former.

Cross-border settlement, or the movement of funds between the sending and receiving banks in different jurisdictions, is one that must occur across borders. Ensuring common treatment of such transactions would require common rules agreed by all participants. It is expected that the settlement process will be governed and subject to a common set of platform-level rules. However, there may still be domestic laws that apply, such as laws relating to payment finality, that may require harmonisation across the participating jurisdictions. This is an area that will likely require more in-depth research.

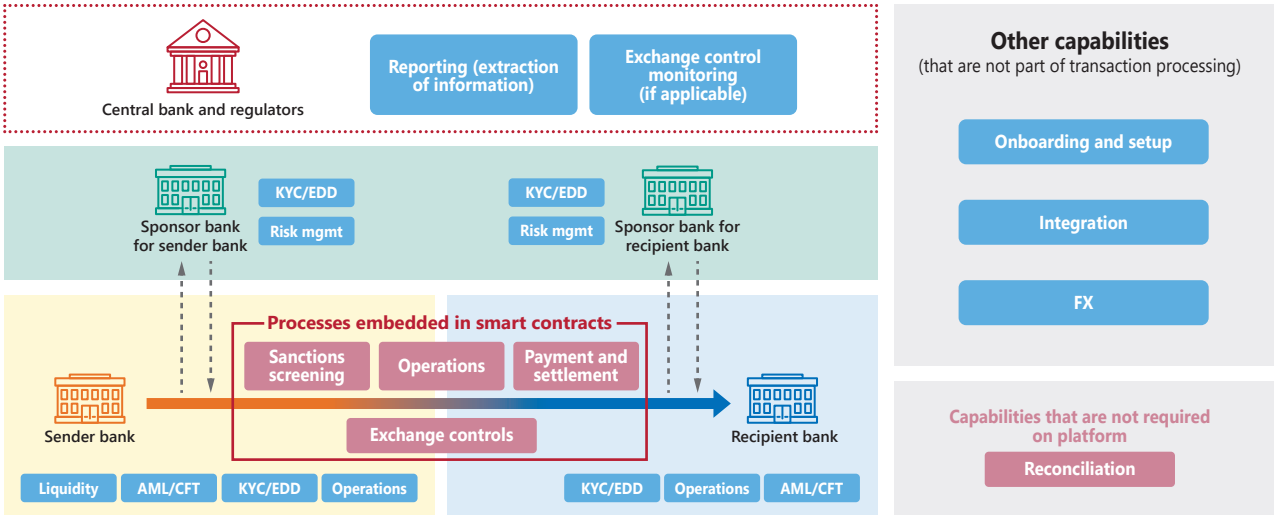
7.3 Non-settlement processes

Differentiating between settlement and non-settlement processes allows non-settlement-processes to be processed in country and subject to the local regulations. Most non-settlement processes such as KYC, AML/CFT and foreign exchange controls are subject to the regulatory policies of the individual countries and fall within this category. This separation of processes enables the clear delineation of jurisdictional boundaries and adherence to regulatory policies of different jurisdictions, while allowing for the streamlining of settlement processes.

Although differentiation between cross-jurisdiction and single-jurisdiction processes is commonly drawn between settlement and non-settlement processes, this may not always be the case. One potential area for efficiency gains is in enabling common processes for control processes like AML/CFT. For example, sanctions screening could be performed once only rather than repeatedly by each bank involved. However, this would place such processes in the category of cross-jurisdiction processes and would likely require the agreement of central banks and relevant regulatory agencies and/or the harmonisation of legal and regulatory policies across participating jurisdictions.

The settlement processes would be handled on the platform while the KYC-related processes would still be handled off the platform, with regulatory requirements performed by sponsor banks subject to their respective jurisdictions. There is a possibility that some processes may be embedded into smart contracts..

Figure 15: Processes in a cross-border payment flow



While settlement processes will be performed on the multi-CBDC platform ("on-platform"), many non-settlement processes may continue to be performed in external systems ("off-platform") due to their nature. One consideration is the availability of data on-platform. For example, exchange controls based on annual limits can be performed on-platform, while exchange controls based on verification of trade documents will require connectivity to a source of trusted data. Certain processes are expected to be eliminated. As cross-border payments are now completed in a single transaction with a single ledger update, and participants have visibility of their transactions and statuses, there is no longer a need for multiple separate confirmations and acknowledgements, and reconciliation across accounts.

Figure 16: Processes in to-be state

Dunbar capabilities	Existing settlement processes	On-platform	Off-platform	Eliminated
2.1 Account setup	Onboarding and setup	✓		
3.2 Rules and compliance	Exchange control	✓		
	Sanction screening	✓	✓	
	AML/CFT		✓	
	KYC/EDD		✓	
4.1 Integration/connectivity	Integration	✓		
4.2.1 Position management, 4.2.6 Payments processing and 4.2.7 Settlement	Payment and settlement	✓ Such as funding, charges (metering, usage reports), account updates, settlement, and warehousing	✓ Such as charges (rate table and billing, interim), and interest calculation	
4.2.4 Risk management	Risk management		✓	
4.2.5 Liquidity management	Liquidity	✓		
4.2.6 Payments processing	Operational considerations	✓		✓ Such as confirmation of receipt of funds for initiator
	FX	✓ Depending on FX model adopted	✓ Depending on FX model adopted	
	Reconciliation			✓
4.3 Monitoring, reporting, control and notification	Reporting		✓	

7.4 Foreign currency exchange

A foreign exchange (FX) transaction can be viewed as two parts: FX trade and FX settlement.

FX trade is the agreement between two counterparties to exchange one currency for another at a specified rate for a specified amount on a specified date. FX settlement is when the obligations by the counterparties are fulfilled and discharged. An example of an FX trade is where a buyer agrees to buy one unit of foreign currency CBDC (FCY) from the seller with two units of local currency CBDCs (LCY). This implies an FX rate (LCY/FCY) of 0.5. The settlement is when the buyer successfully sends two units of LCYs to the seller and receives one unit of FCY in return.

As part of the project, only FX settlement is in scope, and FX trading was taken to be performed outside the platform using existing means. The platform provided interfaces for settlement to take place within the platform on a real-time gross settlement basis. This was tested in the form of an over-the-counter (OTC) transaction where the FX trade has been agreed directly and bilaterally between the transacting parties.

A common theme for FX settlement was the elimination of settlement risk through the provisioning of payment-versus-payment (PvP) mechanisms on the platform. With the transfer of both currencies taking place on a common platform, PvP could be easily implemented as a form of conditional payment. The two linked transactions would either succeed or fail together as a set, eliminating the possibility of one succeeding while the other failed, which could lead to the loss of principal by one of the parties.

Beyond the scope of FX settlement, FX trading was a topic of interest for the central banks, particularly around understanding different FX trading mechanisms, how they might fit into a cross-border payments solution using CBDCs and the opportunities for efficiency gains. Given this potential to streamline the payments process further, performing both FX trading and settlement on the platform was of interest. One specific area of interest is in automated market-making (AMM), in which rates are determined and settled algorithmically.

These areas relating to foreign currency exchange have been of interest for project participants and the commercial banks, and could feature in future phases of the project.

Figure 17: FX models

Model	Who are the counterparties	How are FX rates determined	How is FX trade settled	Connectivity mechanism
1 **FX exchange (and clearing)**	A third-party, such as an exchange operator	Matching of buy/sell orders on the third-party platform	Transfers between the participants and third-party exchange operator/clearing house on multi-CBDC platform	Integration with the third-party platform for settlement on multi-CBDC platform
2 **OTC between participants**	Bilaterally among the participants	Agreed bilaterally between participants	Transfers between the participants on multi-CBDC platform	APIs for PvP settlement to ensure transfers are linked through unique identifiers, and either complete or fail together
3 **Designated market-maker**	Participants who are designated as market-maker(s) for the currency	Set by appointed market-maker(s) quoting bid-ask rates	Foreign currency exchange and settlement could be part of payment flow on multi-CBDC platform	FX bid-ask process incorporated into payment process flow
4 **Automated market-making**	Liquidity pools, with liquidity contributed by participants	Algorithmically	Foreign currency exchange and settlement performed on multi-CBDC platform	Automated market-making protocols deployed on multi-CBDC platform

Technology

08

In this phase of Project Dunbar, prototypes were developed based on the requirements and designs proposed in the design workstreams. The prototypes were developed by the technology providers R3 and Partior, using the distributed ledger technologies of Corda and Quorum respectively.

Both R3 and Partior have done extensive work on digital currency projects and were able to leverage platform functionalities developed previously. The CBDC Accelerator by R3 has been used and tested by multiple central banks over the last few years, with a comprehensive feature set developed which is based on the requirements of central banks. The Partior Sandbox is developed by Partior, which has since built a live platform for multi-currency clearing in Singapore. The Partior platform is being used for USD and SGD payments (with additional currencies and corridors going live in 2022).

As such, many of the basic features of a wholesale digital currency platform are available out-of-the-box (OOTB). This allows the project to focus on a targeted scope of proving the technical feasibility of transacting on a multi-CBDC platform, while leveraging relevant existing functionalities and user interfaces.

This section will describe the infrastructure, application and data architecture of the two prototype platforms, with additional technical details included in the appendix. As the two platforms were built on different distributed ledger technologies, the infrastructure is markedly different. On the other hand, the applications were built to specifications from the design workstream, and hence operate in a similar manner.

8.1 Infrastructure

8.1.1 Cloud infrastructure

Both prototypes were developed in a cloud infrastructure, with R3's deployed on Azure cloud and Partior's deployed on Amazon Web Services (AWS).

Cloud services were ideal for deployment and testing of the prototypes, due to their elastic nature that allows resources to be ramped up or down, or even suspended, depending on usage needs.

For ease of experimentation, a single cloud account was used for each set of deployments. In a live implementation, it is likely that participants would manage their own nodes, either using on-premises or cloud infrastructure.

8.1.2 Network components and services

A typical network for both prototypes would consist primarily of nodes, which are hosted by participants. Both prototypes are built on a permissioned network, with access controlled by the network operator.

A Corda network is made up of nodes, each of which runs an instance of Corda and one or more CorDapps. Communication between nodes is point-to-point and does not rely on global broadcasts. Each node has a certificate that maps its network identity to a real-world legal identity. A Corda network also includes other services such as a **network map service**, which maps each well known node identity to an IP address; an identity manager service, which acts as the gatekeeper to the network; and a **signing service**, which acts as a bridge between the main network map and **identity manager services**, and the public key infrastructure (PKI) and hardware security module (HSM) infrastructure. Additionally, a **notary service** provides **uniqueness consensus** by

attesting that, for a given transaction, it has not already signed other transactions that consume any of the proposed transaction's input states, and an oracle service links the Corda network to the outside world.

The Quorum network used by Partior consists only of Quorum nodes, of which there are two types. **Participant nodes** communicate within the network to share transaction details for processing. Every node in a decentralised system has a copy of the blockchain. **Validator nodes** are responsible for verifying transactions on a blockchain. Once verified, transactions are added to the distributed ledger. The central banks' nodes are configured to be the validator nodes in this setup. Validator nodes are connected to each other in a point-to-point manner. Participant nodes are non-validating nodes and are not required to be interconnected to all nodes in the network.

8.1.3 Nodes

Nodes are key components of a DLT network. A node usually consists of a platform core that manages communications with other nodes, a distributed application that runs the logic of the smart contracts and an internal database for data storage. Typically, there are multiple nodes on a network, with each hosted individually by participants. Integration with external systems, such as integration with central banks' systems for the pledging of assets, is usually performed at the node level.

A Corda node consists of the **Corda Core**, **CorDapps (Corda distributed applications)**, which are distributed applications that run on the Corda platform, and the **Corda vault**, which acts like a database to store on-ledger shared facts for a node. A CorDapp is made of these components: **states**, which define the facts over which agreement is reached; **contracts**, which define what constitutes a valid ledger update; a **legal prose** document, which states the rules governing the evolution of the state over time in a way that is compatible with traditional legal systems; and **flows**, which define a routine for the node to run, usually to update the ledger.

A Quorum node is a minimal fork of Go Ethereum, providing privacy, new consensus mechanisms, network-permissioning and higher throughput. It consists of the core **Quorum platform, dApps**, that act as a middle layer between conventional systems to the DLT and serves as a translator to convert the user's API into the required smart contract format, and **Tessera**, which is a stateless Java application responsible for the encryption/decryption of private transaction data and off-chain private messaging. Tessera consists of the **transaction manager** – which allows access to encrypted transaction data for private transactions, and which also manages the local data store and communications with other transaction managers – and the **Enclave**, which is responsible for private key management and for the encryption and decryption of private transaction data.

8.1.4 Network architecture

The Corda network implemented for Project Dunbar is made up of four logically separated sovereign networks, each representing a country. This enables each domestic sovereign network to be in complete control of its monetary sovereignty, as well as the design and implementation of its own network membership criteria, and governance, policies, regulations and compliance.

A regional platform like this would require a network operator to perform activities such as day-to-day management of the network, managing technical policies around the overall upgrade schedule of the application, its infrastructure and maintenance, and network services that control admission of participants to the Dunbar network.

Figure 20 depicts the multi-CBDC network as a single Corda private network, with the four domestic sovereign networks represented in circles. Each sovereign network is a combination of selected commercial banks, regional commercial banks, global commercial banks and the central bank that represents the current real-world scenario. Participants on the platform will each host a node, and central banks will each host a notary service that is responsible for all transactions in their currency. Network services such as network map, identity manager and signing services will be operated by the network operator.

The Partior network implemented for Project Dunbar consists of four distinct networks logically separated by currencies, with each central bank in control of its own network. A domestic bank that is not a host may engage in transactions on the Dunbar platform by initiating a transaction with its sponsor bank, after which the transaction flows on to the multi-CBDC platform.

The decision on who should host validator and participant nodes depends on several factors, including performance, scalability, costs, resilience and security. It is likely that validator nodes will be hosted by central banks, and that participant nodes will be hosted by commercial banks.

Figure 18: Dunbar network in Corda

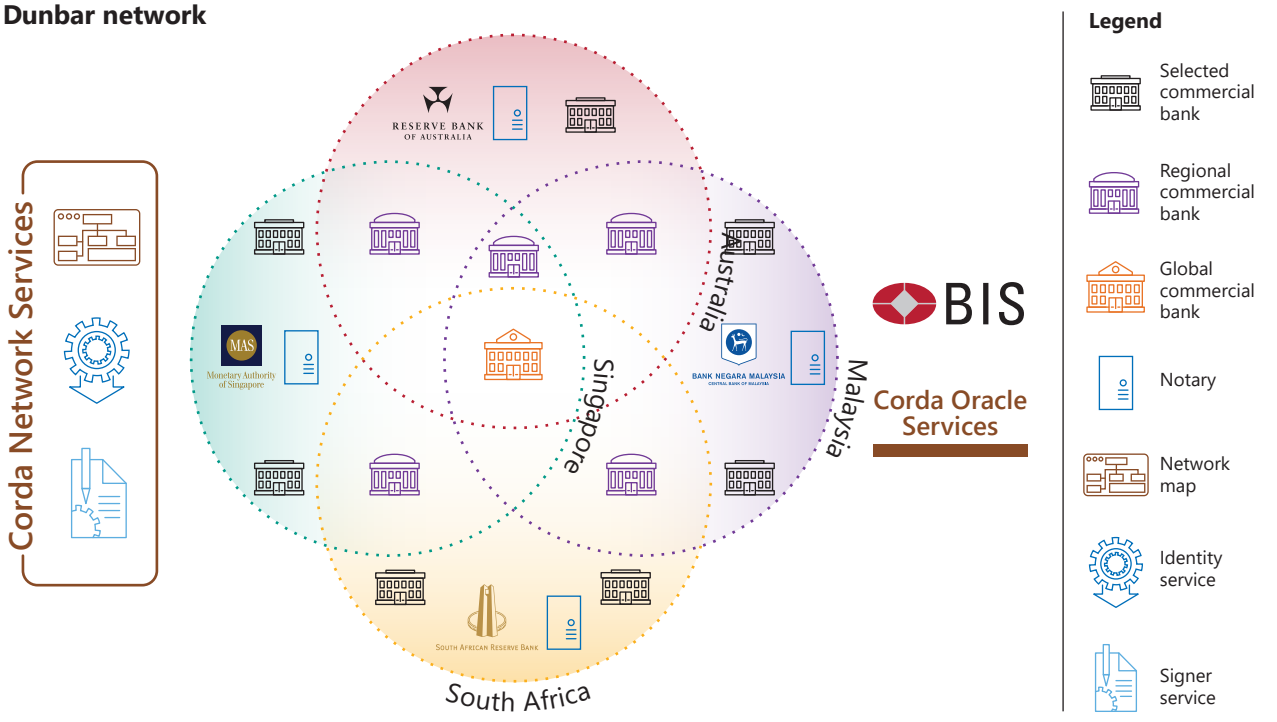
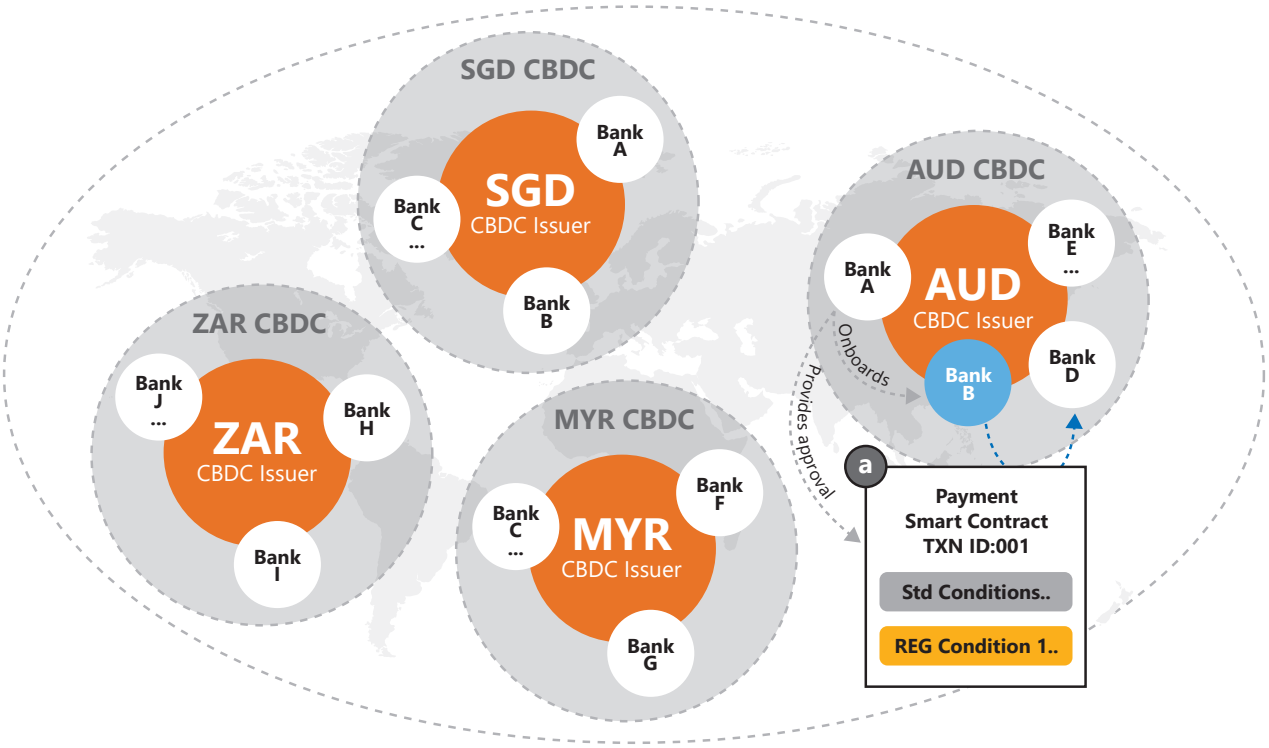


Figure 19: Domestic transfer



8.2 Applications

Applications contain the logic for processes performed on the platforms and are developed as CorDapps using Java or Kotlin programming languages on Corda, and as dApps using the Solidity programming language on Quorum.

As the applications were developed based on the specifications from the design workstream, they are similar on both platforms. Some additional functionalities, such as for issuance, transfer and redemption of CBDCs – as well as balance enquiry were available OOTB, and were used for testing purposes. Approval steps for the transactions were simulated as manual approvals for the purposes of testing and demos. These steps could potentially be automated if integrated into existing systems.

One of the specific requirements for the project was on membership types, and this was developed based on the participants and stakeholders defined in the design workstream, with different privileges defined for different roles. Controls were built to apply rules and ensure that only parties with the appropriate privileges can perform certain roles.

For example, issuance of CBDCs can only be performed by the appropriate central bank.

Such rules can also be applied at the currency and jurisdiction levels. Central banks can apply their customised rules by developing and deploying smart contracts that are used by participating banks for transactions. An example of such currency-level rules includes the approval routing rules for sponsoring banks, where a transaction initiated by a non-resident bank will be routed to its appointed sponsoring banks for approval.

Summary and next steps

09

9.1 Summary

Project Dunbar is one of the first technical experiments in the nascent space of multi-CBDCs. As an exploratory project, the focus was to shine a light into the unknown and show that there is a viable path forward. The project focused on developing design approaches to address three critical challenges to the development of a shared multi-CBDC platform:

Access – enabling non-resident banks' access to CBDCs. Prototypes were developed to flexibly support both "hybrid" as well as "direct" CBDC access models. In jurisdictions where the regulatory frameworks allow direct access to CBDC by non-resident banks, approval routing to "sponsoring" banks could be disabled to move from a "hybrid" to "direct" CBDC access model.

Jurisdictional boundaries – differentiating settlement and non-settlement processes. Differentiating between settlement and non-settlement processes in cross-border payments allows non-settlement processes to be processed off platform and in country, subject to local regulations. This separation would enable the clear delineation of jurisdictional boundaries, adherence to regulatory policies of different jurisdictions and streamlining of settlement processes.

Governance – optimising universality and autonomy. A shared platform implies a level of universality. Certain features and capabilities of the platform are universal and available to all participants. Rules and policies are applied universally and fairly across participants. To enable this universality, governance structures and decision-making powers must be designed to ensure that a diverse group of stakeholders are able to be represented, and collective decisions are able to be made fairly and equitably. Central banks are also granted autonomy within the boundaries and parameters of a universal platform-level framework, such as in the application of jurisdiction- and currency-level rules.

The design approaches to solving the three challenges were validated through the development of technical prototypes that demonstrated practicable solutions. In that regard, this initial phase of Project Dunbar has successfully achieved its aim of proving that the concept of multi-CBDCs was technically viable. This is an important step, but still just a first step into the space.

While prototypes have been successfully developed and tested in the project, they were built based on a preliminary design, with the best possible set of assumptions known to the team while doing the project. As the project progresses, new information and better understanding resulted in continuous refinement of the assumptions. Previously *unknown unknowns* were uncovered, enabling a clearer understanding of the challenges that need to be solved. Some unknowns also became knowns, as challenges were better understood and subsequently solved. However, even at the completion of this first phase, there are still more unknowns than knowns. Assumptions will continue to be challenged as new information arises, and designs and prototypes will continue to improve.

9.2 Areas for further exploration

As an exploratory project with a limited timeline, Project Dunbar ended with more questions than answers, and more questions than before it started. This is to be expected of an exploratory project, which focuses as much on identifying problems as it does on solving them.

The areas for further exploration can be broadly categorised into three themes: policy, business and technology. While the themes are useful for grouping together related areas, many of the problems or questions cut across multiple themes. For example, access for non-resident banks may be considered primarily a policy question, while the perspective of the sponsoring arrangements between banks would take on a business and commercial lens. Also, solutions

could be devised from a different perspective to the problem – for example, a policy challenge could be solved via business or technological means. Very often, advances in technological capabilities create new policy options, allowing for policy concerns to be better addressed, or break traditional trade-offs and achieve a superior solution that fulfils previously conflicting needs.

Policy

Trade-offs in access models – one recurring debate relates to the comparison of access models, with the "direct" CBDC access model viewed as difficult to implement due to the need for harmonisation of and changes in regulations, and for mutual reliance on other central banks or regulators, and the "hybrid" CBDC access model was viewed as inefficient. More thorough analysis, including potential refinements to the access models, should be conducted to validate this view. For example, while regulations are often different across jurisdictions, further study is required to understand the specific differences and their consequences, and the actual regulatory changes that might be required to implement a "direct" access model. Also, there are likely to be differences in regulatory approaches across regions, and thus analysis could be done at a regional level or within a logical grouping of central banks. The inefficiencies of needing intermediaries for control processes in a "hybrid" access model should be analysed in the context that it may be possible for some of these processes to be performed in an automated and straight through manner.

Enabling common shared control processes on-platform – one potential benefit of a shared platform is in enabling shared processes to be performed on the platform. For example, sanctions screening could be conducted just once in the cross-border payments process, instead of at each bank. Such consolidation of processes may bring about system-level efficiency gains but may be difficult to implement due to the need for mutual reliance and shared liability amongst participants. Improved visibility and traceability through technology may help to mitigate these risks.

Extending access beyond banks – while the project focused on commercial banks as participants of the network, it would also be possible for non-bank financial institutions (NBFIs) such as payment services providers and exchanges to transact directly on the platform. The policy question of whether to extend access beyond banks should be considered. Within the participating central banks, some already allow NBFIs to access their real-time gross settlement systems. Widening access to NBFIs may improve competition, resulting in lower fees for consumers but may pose risks. There is also a technical consideration of scalability and performance in widening the number of participants directly connecting to the network; this is discussed below under Technology.

Impact of AML/CFT regulation – while the project took into consideration the need to comply with local AML/CFT regulations, an in-depth investigation into how AML/CFT regulations relate to CBDC, and cross-border transactions using CBDC more specifically, was not within scope, and is an area that would require further exploration.

Regulatory changes – implementing a new multi-CBDC solution may require regulatory changes. This needs to be analysed in greater detail, while also considering the potential use of technological solutions to address differences in policies – for example, a rules engine could ensure compliance with the different regulatory requirements thereby negating the need for complete harmonisation across the jurisdictions.

Business

Commercial models for "sponsoring" bank arrangements – a "hybrid" CBDC access model would require commercial banks to take on "sponsoring" roles and perform certain control processes on the sponsored banks. Banks typically perform such roles as part of the correspondent banking relationship, accruing benefits through holding foreign currency deposits and charging fees for the transactions. As they would no longer benefit from holding the funds of transacting banks in a multi-CBDC platform, new commercial models will need to be explored. Various possibilities have been

identified, such as reciprocal arrangements where banks take on a sponsoring role for each other for different CBDCs, obligations imposed as conditions of access where banks are required to sponsor a specified number of participants and fees where sponsored banks are charged on a commercial basis. These will need to be further evaluated with industry participants to determine the commercial viability.

Commercial use cases and applications – another commercial perspective relates to the use cases of the multi-CBDC platform. Aside from cross-border payments, there may be interest in other types of services that could be provided by the platform. Examples include issuance and transacting of other digital assets, conditional payments, and integration with other platforms and applications to support use cases such as trade finance.

Quantitative study on efficiency gains and cost-savings – while the project highlighted the potential benefits of a multi-CBDC platform, these were focused on qualitative aspects and were at a fairly high level. Detailed analysis and quantification of the benefits would be important in performing a cost-benefit analysis and building a business case for future implementation.

Liquidity challenges of real-time settlement – real-time settlement requires transacting parties to possess, at the point of the transaction, the required funds to fulfil their obligations. The high liquidity requirements are costly for commercial banks and may lead to slow adoption. Seamless on-/off-ramping of funds may alleviate part of the problem by allowing banks to easily manage their liquidity positions. Liquidity-saving mechanisms, such as netting, could also reduce liquidity needs. Further exploration is required to understand how banks will likely use and transact on a multi-CBDC platform, the resulting challenges in liquidity requirements, and how they can be alleviated.

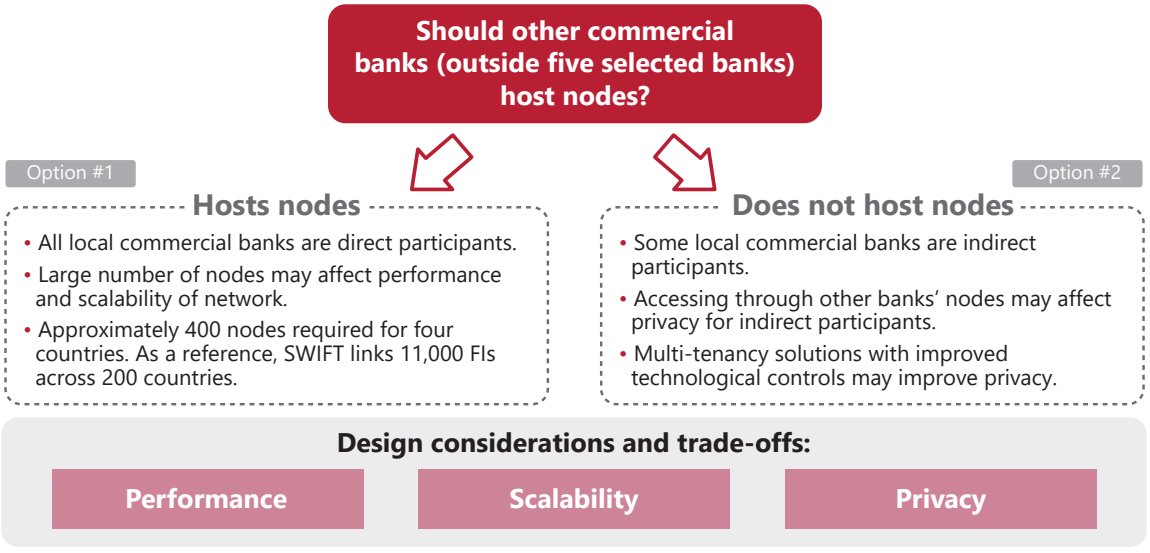
Technology

Integration with peripheral services and features – the current phase of the project focused on transactions within a multi-CBDC platform. However, the platform would be only one part of the end-to-end payment flow; it will likely also need to connect with central banks' systems for the pledging of assets backing the issuance of CBDCs, and with commercial banks' systems for customer transactions. Furthermore, a payment is often only one part of a bigger transaction. For example, it could be a payment in exchange for securities, or payment for goods in an international trade. Such use cases could benefit from connecting directly to the multi-CBDC platform for automation of the end-to-end transaction, allowing the automated release of funds when goods are received. Further development and testing of technical connectivity and integration with external systems will be important and could be explored, together with the business perspective of supporting other commercial use cases and applications.

Standards and interoperability – a multi-CBDC platform will need to connect with other external systems. Furthermore, to enable global payments across all jurisdictions and currencies, a regional multi-CBDC platform will need to connect with other national or regional multi-CBDC platforms. Interoperability, or the ability for these systems to communicate with each other easily and seamlessly, will be crucial for global connectivity. Standards, or a common language and set of expectations, will be key to enabling interoperability between these systems.

Technical challenges and trade-offs – in designing a system, there are often technical trade-offs that need to be considered. Such trade-offs may not be obvious in an experiment due to the limited scope. For example, the project simulated only five commercial banks per jurisdiction for technical testing. Increasing this number could result in uncovering potential technical challenges of scalability. Tiering of system access is a possible option for resolving that. While some potential challenges were reviewed in the design phase, a thorough review can only be performed through more comprehensive technical testing.

Design considerations: performance, scalability and privacy



One design consideration was about banks that are allowed to host nodes and connect directly to the network, as discussed in Section 8. The number of banks ranges from hundreds to thousands across jurisdictions. Besides the business consideration of infrastructure costs, there is also a technical consideration of the optimum number of nodes that can be supported on the network. Scalability and performance may be affected if all local commercial banks host nodes as direct participants.

One potential solution to this scalability problem is to allow only central banks and selected commercial banks to host nodes, with other local commercial banks connecting as indirect participants through these node hosts. However, this may affect privacy for indirect participants as there is a possibility that a node host could view transactions passing through the node despite the security measures implemented. Such technical considerations will need to be further evaluated, including through scalability testing and security assessments.

9.3 Next steps

The vision and broader objective of Project Dunbar is enabling a global network of connected CBDC platforms and interoperable CBDCs. An ideal state and the epitome of efficient cross-border payments would be a single global settlement platform that connects all central banks and commercial banks. Given the complexity of having multiple central banks sharing critical financial infrastructures and the unique requirements of each jurisdiction, a common multi-CBDC platform may be more likely to be implemented as a series of regional platforms rather than as a single global platform. This naturally leads to considerations around how it may be possible to connect these individual regional platforms to realise synergies such that participants transact directly across jurisdictions, including via the lower-volume corridors.

In the roadmap to achieving the vision of Project Dunbar, the next major step is developing and testing a regional multi-CBDC platform to a high level of production fidelity. While still an experiment, this could be viewed as production-*ready*. This would entail the development of a detailed platform rulebook, and reviewing legal and regulatory frameworks across participating jurisdictions. It would also require the formation of governance committees for the project and these could potentially transit into governance committees for a future live regional platform. Finally, technical development and testing at a large-scale industry level would be required. Such experiments could be conducted at a regional level within existing and established regional groupings.

Once such multi-CBDC projects have been established on a regional level, the next step would be to develop mechanisms to ensure connectivity between these multi-CBDC projects and experiments. Other than technical connectivity, there will also be questions around governance and policies that will need to be addressed.

Acknowledgements

Project Steering Committee

Organisation	Representative
BIS Innovation Hub	Andrew McCormack
Reserve Bank of Australia	Chris Thompson
Bank Negara Malaysia	Tay Gim Soon
Monetary Authority of Singapore	Sopnendu Mohanty
South African Reserve Bank	Herco Steyn

Project Management Team

Name	Organisation
Toh Wee Kee	BIS Innovation Hub (Project Lead)
Benjamin Lee	BIS Innovation Hub
Cameron Dark	Reserve Bank of Australia
Yip Kah Kit	Bank Negara Malaysia
Alan Lim	Monetary Authority of Singapore
Gerhard van Deventer	South African Reserve Bank

Central banks

Name	Organisation
John Kenyon	Reserve Bank of Australia
James MacNaughton	Reserve Bank of Australia
Riaan Louw	Reserve Bank of Australia
Adam Gorajek	Reserve Bank of Australia
Norasyikin binti Mohamad Razali	Bank Negara Malaysia
Chai Yi Wei	Bank Negara Malaysia
Sharmaine Nadirah binti Roslan	Bank Negara Malaysia
Zahilah binti Ismail	Bank Negara Malaysia
Charmaine Tew Shu Yi	Bank Negara Malaysia
Ng Yin Shia	Bank Negara Malaysia
Dr. Normasita binti Sidek	Bank Negara Malaysia
Chew Ming Heong	Bank Negara Malaysia
Pham Khai Uy	Banque de France
Anne-Catherine Bohnert	Banque de France
Alvinder Singh	Monetary Authority of Singapore
Jonathan Chan	Monetary Authority of Singapore
Vincent Pek	Monetary Authority of Singapore
Margaret Olivier	South African Reserve Bank
Annah Masoga	South African Reserve Bank
Patrick Johnson	South African Reserve Bank
Hein Timoti	South African Reserve Bank
Pearl Malumane	South African Reserve Bank
Larry Cooke	South African Reserve Bank
Jan Mohotsi	South African Reserve Bank
Darren Chamberlain	South African Reserve Bank
Lyle Horsley	South African Reserve Bank
Anikó Szombati	Magyar Nemzeti Bank
Péter Fáykiss	Magyar Nemzeti Bank

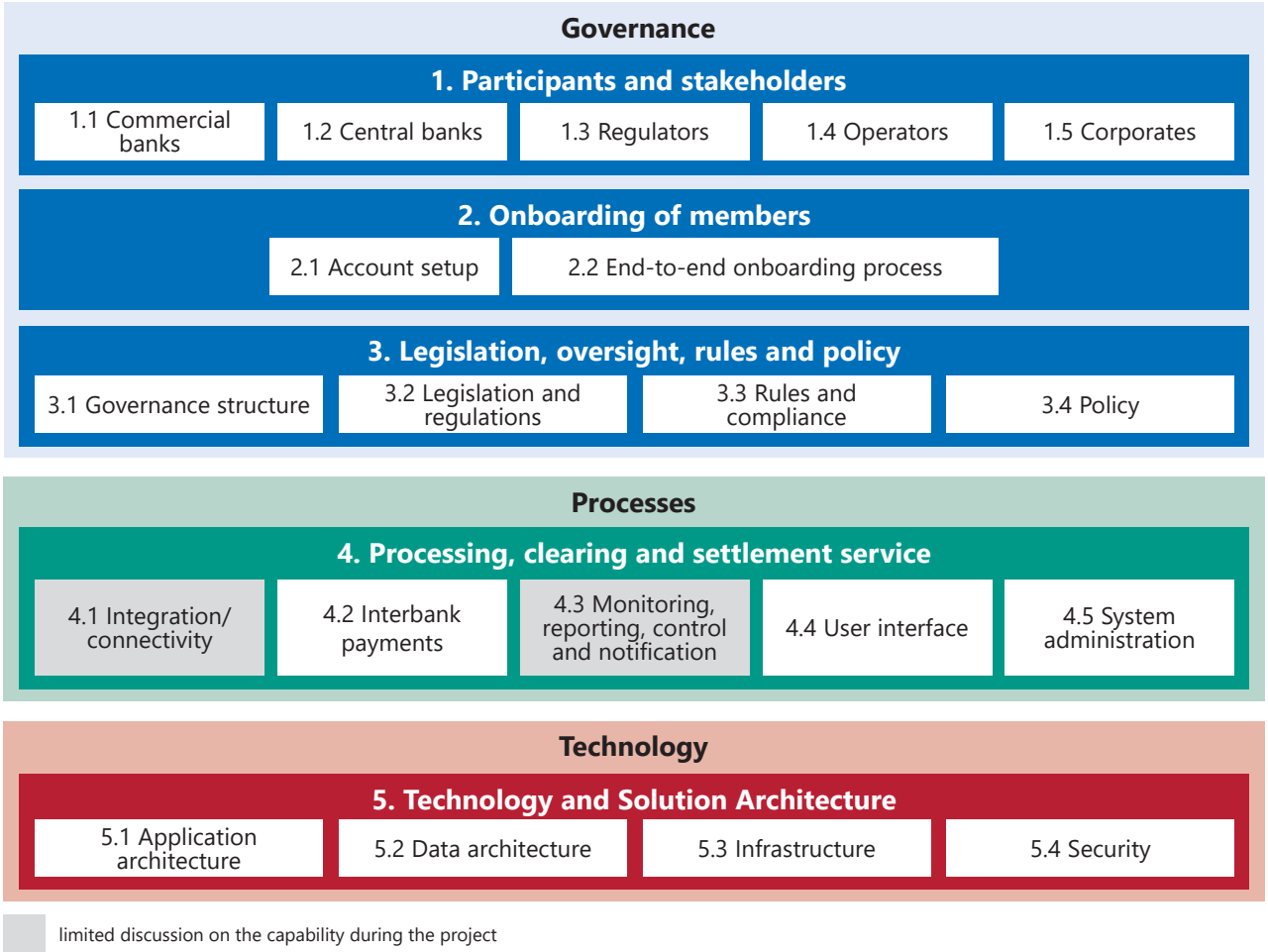
Technology and design partners

Name	Organisation
James Gan	Accenture
William Lim	Accenture
Desiree Teh	Accenture
Chan Chian Lyn	Accenture
Willy Lim	R3
Pallavi Thakur	R3
Shobana Kandaswamy	R3
Indra Suppiah	R3
Stefano Franz	R3
Arnab Chatterjee	R3
Jason Thompson	Partior
Dmitry Avramenko	Partior
Ng Peng Khim	DBS Bank
Zhenqian Tay	DBS Bank
Yeoh Han Long	DBS Bank
Lee Muh Hwa	J.P. Morgan
Sai Valiveti	J.P. Morgan
Claire Ng	J.P. Morgan
Pradyumna Agrawal	Temasek
Laura Loh	Temasek

We acknowledge and appreciate the support of the following organisations for participating in project workshops: Absa, AMBank, ANZ, Bank of New Zealand, CIMB, Citi, Commonwealth Bank of Australia, FirstRand, Goldman Sachs, Hong Leong Bank, HSBC, Investec, Macquarie, Maybank, National Australia Bank, Standard Bank, Standard Chartered Bank, United Overseas Bank, and Westpac.

Appendix

1.1 Dunbar capabilities and considerations



1. Participants and stakeholders

1.1	**Commercial banks**	Commercial banks are entities which offer financial services to their clients, including facilitating cross-border transactions. A local commercial bank must be licensed to operate within the local jurisdiction.
1.2	**Central banks**	Central banks are parties that manage and execute their monetary policy and objectives. They may be operators of their own payments systems (see Section 2.4). Central banks oversee the issuance, destruction and management of their own central bank digital currency (CBDC).
1.3	**Regulators**	Regulators are the regulatory authority for all financial institutions within their local jurisdiction, and activities include supervisory and regulatory policy development. There may be multiple different regulators within a jurisdiction – ie for prudential oversight and AML.
1.4	**Operators**	An operator is the central party that maintains the system and that coordinates changes or upgrades from a technical standpoint.
1.5	**Corporates**	Corporates are the customers of banks. In wholesale inter-bank settlement, they transact only through the banks and not directly on the system.

1.1 Commercial banks

1.1.1	**Selected commercial banks**	These are a limited number of large commercial banks of good standing that have been identified to be key participants of the scheme. These participants would be provided with additional privileges and may be required to comply with more stringent requirements.
1.1.2	**Other commercial banks**	This refers to commercial banks that operate via a selected commercial bank. They may have a limited number of privileges on the system, and are typically subject to less stringent requirements.
1.1.3	**Non-resident banks**	This refers to banks in other jurisdictions, and not in the local jurisdiction.

2. Onboarding of members

2.1	**Account setup**	Set up participant accounts in the system in adherence with system's principles of account structure.
2.2	**End-to-end onboarding process**	Onboarding steps required for new members to participate in the scheme.

2.2. End-to-end onboarding process

2.2.1	**Customer configuration**	Support changes to a participant's settings or parameters with respect to the system, and based on each participant's regulatory or specialised operating requirements.
2.2.2	**Technical integration with system**	Integrate a new participant into the system or remove a participant from the system based on defined guidelines and a checklist. This includes industry testing and certification processes. Eg a new participant must meet minimum standards to join the network, and must meet local jurisdiction requirements to operate in the jurisdiction. Eg a participant being offboarded needs to redeem all CBDCs in its wallet.

3. Legislation, oversight, rules and policy

3.1	**Legislation and regulations**	Ensure that the payments FMI complies with its obligations arising from legislation and any other regulatory obligations.
3.2	**Rules and compliance**	Ensure the payments FMI has defined rules aligned with legislation, regulatory requirements and the payments FMI's policies, and that both the payments FMI and participants comply with all required legislation, regulations and rules.
3.3	**Policy**	Define principles, guidelines and courses of action for the payments FMI to achieve its statutory objectives. Policy may be crafted into rules for implementation.

4. Processing, clearing and settlement services

4.1	**Integration/ connectivity**	Standards and patterns for integration and connectivity of the Dunbar platform with other systems. This may include payments systems for on- and off-ramping of CBDCs.
4.2	**Interbank payments**	Core system functionalities that facilitate the transfer of funds between members in various currencies.
4.3	**Monitoring, reporting, control and notification**	Tools to allow participants to monitor their systems performance and payments activity, and enable alerting, reporting and management of user notifications.
4.4	**User interface**	Front-end(s) for users to interact with the application. This includes the ability to view and access payments data (position, history, search, collaterals), print, perform reporting, login/logoff, manage permissions and block users, etc.
4.5	**System administration**	Tools that allow the operators to change system configurations, enable rules and procedures for creating and managing user access, and enforce security management.

4.2 Interbank payments

4.2.1	**Position management**	Calculate and manage holdings in currencies that are supported by the system.
4.2.2	**Issuance/redemption**	Issuance refers to the process of participants exchanging or pledging assets for central bank digital currencies (CBDCs). Redemption is the process of participants exchanging CBDCs with the issuing central bank to redeem the assets backing the CBDC.
4.2.3	**Default management**	Calculate and manage key metrics for default management (eg collateral pool and participants' contributions, survivor's contribution to cover any default shortfall). *FUTURE PHASES: while the current phase takes the assumption of gross settlement, a future iteration could consider handling defaults under a net settlement model.*
4.2.4	**Risk management**	Operationalise the system's risk model through processes and tools (eg maximum values on limits, checks against pre-defined thresholds, access control) to support a risk framework covering credit/counterparty risk, settlement risk, AML/CFT, as well as system risk.
4.2.5	**Liquidity management**	Processes and tools to: (i) allow participants to use liquidity pools to settle all payment priority, (ii) allocate liquidity for specific payment priority, (iii) reserve liquidity for specific payments, (iv) and monitor liquidity.
4.2.6	**Payments processing**	Core processes of payments including queues, message types and formats, message-routing, viewing and tracking.
4.2.7	**Settlement**	Manages selected systems processes, including the timing and cycles of settlements and the debit and credit of participants' CBDC wallets.

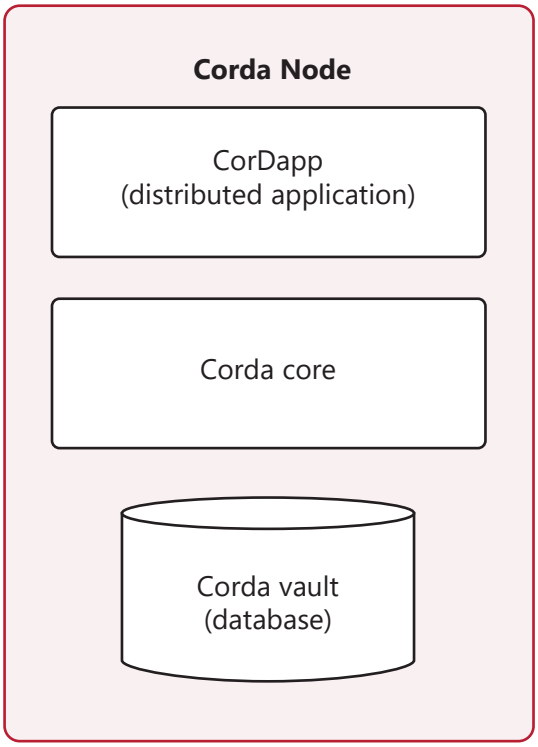
1.2 Prototype developed by R3 on Corda platform

1.2.1 R3 Technical Architecture

Built for the needs of highly regulated institutions, Corda is an evolved distributed ledger technology (DLT) platform that delivers privacy, scalability and security, making it widely used within financial services and beyond. R3's Corda is a scalable, permissioned peer-to-peer (P2P) DLT platform, which differs from others that operate based on the concept of global-broadcast. This enables Corda applications to foster and deliver digital trust between parties in regulated markets.

At the heart of the platform is a Corda Node. It uses Java Virtual Machine (JVM) run-time with a unique network identity that runs the Corda software components as follows:

Figure 20: Corda node anatomy



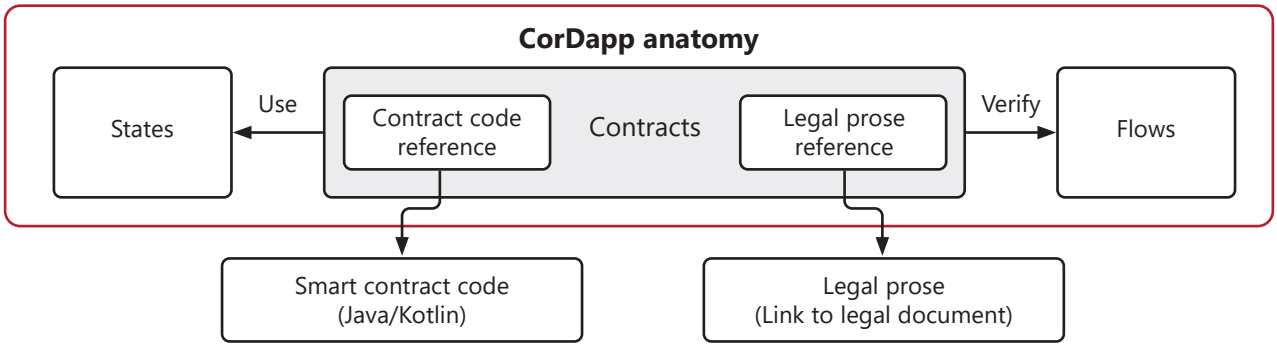
CorDapps (Corda distributed applications) – CorDapps are distributed applications that run on the Corda platform. The goal of a CorDapp is to allow nodes to reach agreement on updates to the ledger. They achieve this goal by defining flows that Corda node-owners can invoke over a remote procedure call (RPC). An RPC is the event that takes place when a computer programme causes a procedure (or a subroutine) to execute in a different address space (commonly on another computer on a shared network), which is coded as if it were a normal (or local) procedure call, without the programmer explicitly coding the details for the remote interaction.[9]

Corda vault – A Corda vault is the component that stores on-ledger shared facts for a node. Each node on the network maintains a vault, which is a database where it tracks all of the current and historic states about which it is aware, and which it considers to be relevant to itself.

1.2.1.1 CorDapp anatomy

The CorDapp is made of several components as depicted in the diagram below.

Figure 21: CorDapp anatomy



States – These define the facts over which agreement is reached. States represent on-ledger facts, and are evolved by marking the current state as historic and creating an updated state. Each node has a vault where it stores any relevant states to itself. A state is an immutable object representing a fact known by one or more Corda nodes at a specific point in time. States can contain arbitrary data, allowing them to represent facts of any kind (eg stocks, bonds, loans, KYC data and identity information).

Contracts – These define what constitutes a valid ledger update. In Corda, contracts are the mechanism used to impose constraints on how states can evolve. Contracts in Corda are quite different to the smart contracts of other distributed ledger platforms. They are not stateful objects representing the current state of the world. Instead, like a real-world contract, they simply impose rules on what kinds of transactions are allowed. Contracts are written in Java or Kotlin. Contract execution is deterministic, and transaction acceptance is based on the transaction's contents alone.

Legal prose – Each contract also refers to a legal prose document that states the rules governing the evolution of the state over time in a way that is compatible with traditional legal systems. This document can be relied upon in the case of legal disputes.

Flows – Corda's "flow framework" is a unique feature that enables moving of data around the network just-in-time, on-demand and on a point-to-point basis. These flows define a routine for the node to run, usually to update the ledger. They automate the process of agreeing ledger updates. Communication between nodes only occurs in the context of these flows, and is point-to-point. Built-in flows are provided to automate common tasks.

[9] See www.corda.net/blog/corda-rpc-reconnecting-client/#

1.2.1.2 Corda networks

A Corda network is made up of nodes, each of which runs an instance of Corda and one or more CorDapps. Communication between nodes is point-to-point and does not rely on global broadcasts.

Each node has a certificate that maps its network identity to a real-world legal identity.

The network is permissioned, with access requiring a certificate from the network operator.

1.2.1.3 Basic Corda network architecture components

A Corda network is a peer-to-peer network of nodes. Each node represents a legal entity, and each runs the Corda software (an instance of Corda and one or more Corda applications, known as **CorDapps**). All communication between nodes is point-to-point and encrypted using transport layer security (TLS). This means that data is shared only on a need-to-know basis. There are **no global broadcasts.** All of the nodes in the network have the potential to communicate with other nodes. Why do we say "potential" to communicate? Because the connections on the graph do not have to be persistent. On the networking level, Corda uses persistent queues, but, as with email, if your recipient is offline, your messages will wait in an outbound queue until the recipient comes online.

Corda nodes

A node uses JVM run-time with a unique network identity running the Corda software. Nodes communicate with each other using Advanced Message Queueing Protocol (AMQP 1.0) over TLS.

Network services

Each node has a single well-known identity. The node's identity is used to represent the node in transactions; for example, if the node were involved in a transaction to purchase an asset.

The **network map service** maps each well-known node identity to an IP address. These IP addresses are used for messaging between nodes.

Corda nodes discover each other via a network map service. You can think of this service as a phone book, which publishes a list of peer nodes that includes metadata about who they are and what services they can offer.

The **identity manager service** acts as the gatekeeper to the network. It is formed of two components:

- **Issuance:** Responsible for issuing certificates to new nodes wanting to join the network.
- **Revocation:** (Optional) Responsible for handling certificate revocation requests as well as hosting the certificate revocation list (CRL) endpoints that are used by participants to check a certificate's revocation status.

The **signing service** acts as a bridge between the main network map and identity manager services, and the public key infrastructure (PKI) and hardware security module (HSM) infrastructure. This enables a network operator to verify and sign incoming requests and changes to the network. Large and important changes to the network should go through a series of checks before being approved and signed, ideally with a network operator manually verifying and signing new certificate signing requests (CSRs), CRLs, and network parameter changes. The signing service provides this behaviour, with HSM integration enabling the signing of any particular data to require authentication from multiple users.

Notary service

Notary clusters prevent "double-spends". Corda employs notaries as an alternative to proof-of-work. A notary cluster is a network service that provides **uniqueness consensus** by attesting that, for a given transaction, it has not already signed other transactions that consume any of the proposed transaction's input states.

Upon being asked to notarise a transaction, a notary cluster will either:

- Sign the transaction if it has not already signed other transactions consuming any of the proposed transaction's input states.

- Reject the transaction and flag that a double-spend attempt has occurred.

In doing so, the notary cluster provides the point of finality in the system. Until the notary cluster's signature is obtained, parties cannot be sure that an equally valid but conflicting transaction will not be regarded as the "valid" attempt to spend a given input state. However, after the notary cluster's signature is obtained, we can be sure that the proposed transaction's input states have not already been consumed by a prior transaction. Hence, notarisation is the point of finality in the system.

Every state has an appointed notary cluster, and a notary cluster will only notarise a transaction if it is the appointed notary cluster of all the transaction's input states.

Oracle service

Oracles in Corda are Corda nodes running Corda services which link the Corda network to the outside world. They are not generally participants in a business transaction but provide network services. A node in need of any data served by the oracle service would request the oracle node to provide signed external data, which the transacting node could then use in a business transaction.

In many cases, a transaction's contractual validity depends on some external piece of data, such as the current exchange rate. However, if we were to let each participant evaluate the transaction's validity based on their own view of the current exchange rate, the contract's execution would be non-deterministic: some signers would consider the transaction valid, while others would consider it invalid. As a result, disagreements would arise over the true state of the ledger.

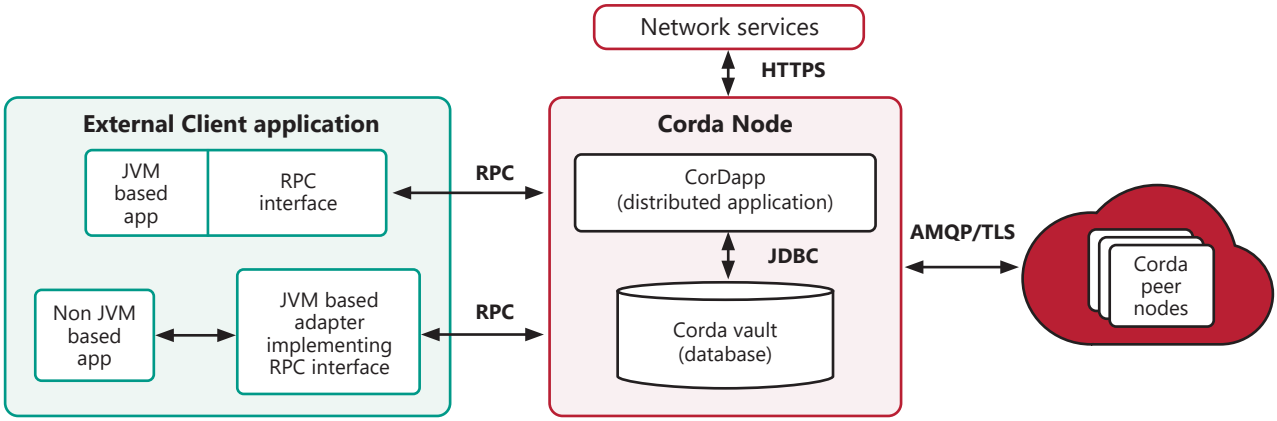
Corda addresses this issue using oracles. Oracles are network services that, upon request, provide commands that encapsulate a specific fact (eg the exchange rate at time x) and list the oracle as a required signer.

If a node wishes to use a given fact in a transaction, it requests a command asserting this fact from the oracle. If the oracle considers the fact to be true, it sends back the required command. The node then includes the command in its transaction, and the oracle will sign the transaction to assert that the fact is true.

For privacy purposes, the oracle does not need to have access to every part of the transaction, and the only information it needs to see is the embedded – related to this oracle – command(s). We should also provide guarantees that all of the commands requiring a signature from this oracle should be visible to the oracle entity, but not to the rest. To achieve this, we use filtered transactions in which the transaction proposer(s) uses a nested Merkle tree approach to "tear off" the unrelated parts of the transaction.

1.2.1.4 Integration points

Figure 22: Corda node integration points



Corda nodes communicate with each other using the asynchronous AMQP/TLS 1.2 protocols. HTTP communication is used only for the initial registration of Corda nodes and for sharing the Corda node address locations by way of the network map. Client applications communicate with Corda nodes using RPC calls. A node's vault is a database that relies on a Java Database Connectivity (JDBC) connection from the Corda node.

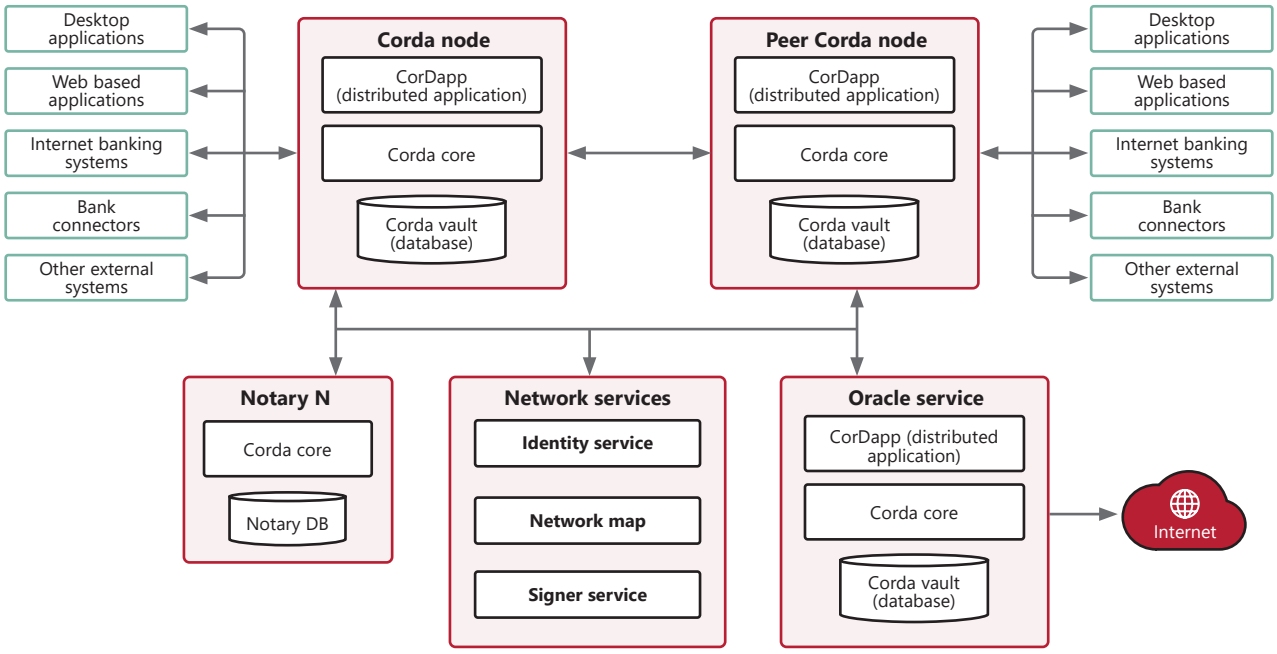
CorDapps are the functional aspect of Corda that define the operations of a business network for a given use case.

Corda nodes store states in a database (the vault) using JDBC.

Integration with external systems

Corda can integrate well with external world systems such as desktop applications, web-based applications, legacy systems and others. Each CorDapp can be accessed by invocating flows. To invocate a flow to your node, you should be able to connect the RPC endpoint of the node to your external system.

Figure 23: Corda network architecture



1.2.1.5 Project Dunbar Corda network

Keeping in mind the objectives of Project Dunbar, R3 has designed the Dunbar network on the BIS model 3. (For more on the model 3 approach, please refer to the definition in Section 2.2 above.) It is a private permissioned regional Dunbar network with four central banks, each of which has control over its sovereign domestic network through the notary node implantation. In other words, the Dunbar network is made up of four logically separated sovereign networks.

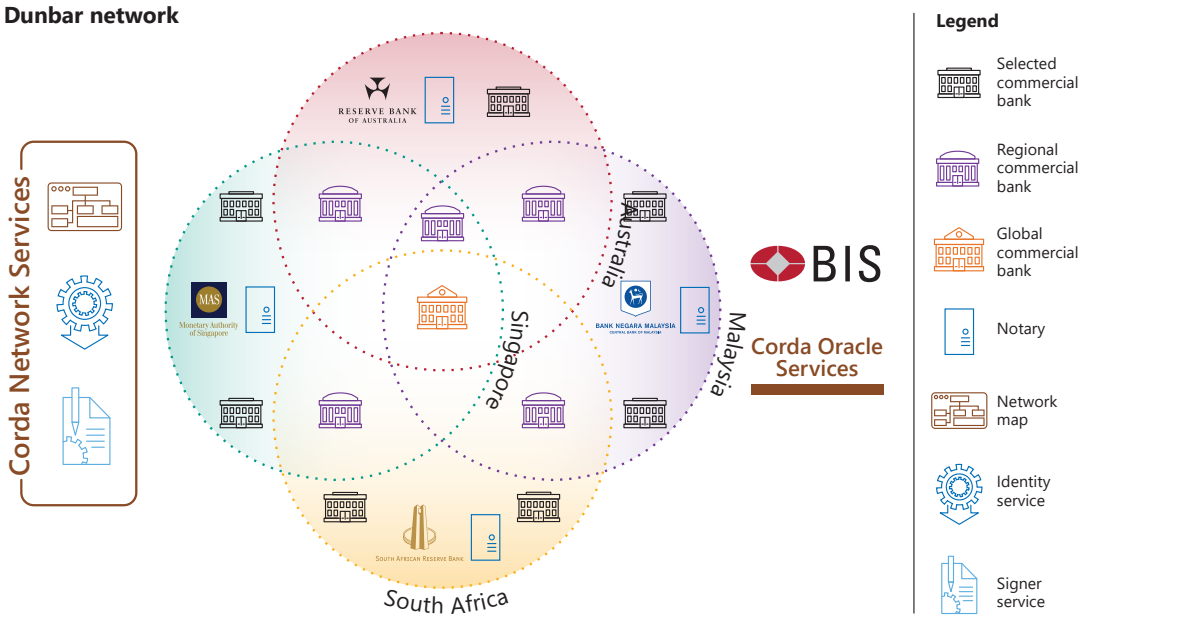
This enables each domestic sovereign network to be in complete control of its:

- Monetary sovereignty.
- Design and implementation of its own network membership criteria.
- Governance, policies, regulations and compliance.

A regional platform like this would require a network operator to perform activities such as:

- Day-to-day management of the network – tactical or operational role.
- Managing technical policies around the overall upgrade schedule of the application, its infrastructure and maintenance.
- Network services that control admission of participants to the Dunbar network.

Figure 24: Dunbar network in Corda



In the network design diagram above, the regional Dunbar network is a single Corda private network (marked by the square box). The domestic sovereign networks are represented as four logical country networks in Corda (indicated by the four circles, each of which represents a country). In this representation, each country network is a combination of selected commercial banks, regional commercial banks, global commercial banks and the central bank that represents the current real-world scenario.

In R3's proposed model, each of the selected commercial banks, regional commercial banks, global commercial banks and the central bank hosts a Corda node. It is important to highlight that in our model it is sufficient that each bank in the entire Dunbar network hosts one node. The following example will explain what this means.

Selected commercial banks – These are local banks within their country networks and do not have a presence in any of the other three countries in the Dunbar network. The Corda node hosted will give capabilities to operate only in the logical network of the specific country on Dunbar.

Regional commercial banks – These are banks which have presence in two or more countries in the Dunbar network. The single Corda node hosted will give it the capability to operate in those countries.

Global commercial banks – These are banks which have presence in all four countries in the Dunbar network. The single Corda node hosted will give them the capability to operate in Singapore, Malaysia, Australia and South Africa.

Central banks – MAS, BNM, RBA and SARB each hosts a Corda node in their respective country networks. Because the central banks are the governing authorities managing the currency and monetary policies of each country, our model makes the central bank the notary of each of the logical country networks. The notary in Corda provides complete control of the CBDC created for each country network.

Network operator – This provides Corda network services such as the network map, identity service and signer service. In our model, we recommend that the BIS be the network operator working closely with the four central banks for governance. Please note that the network operator functionalities can also be performed by a technology provider on behalf of Dunbar's governing body.

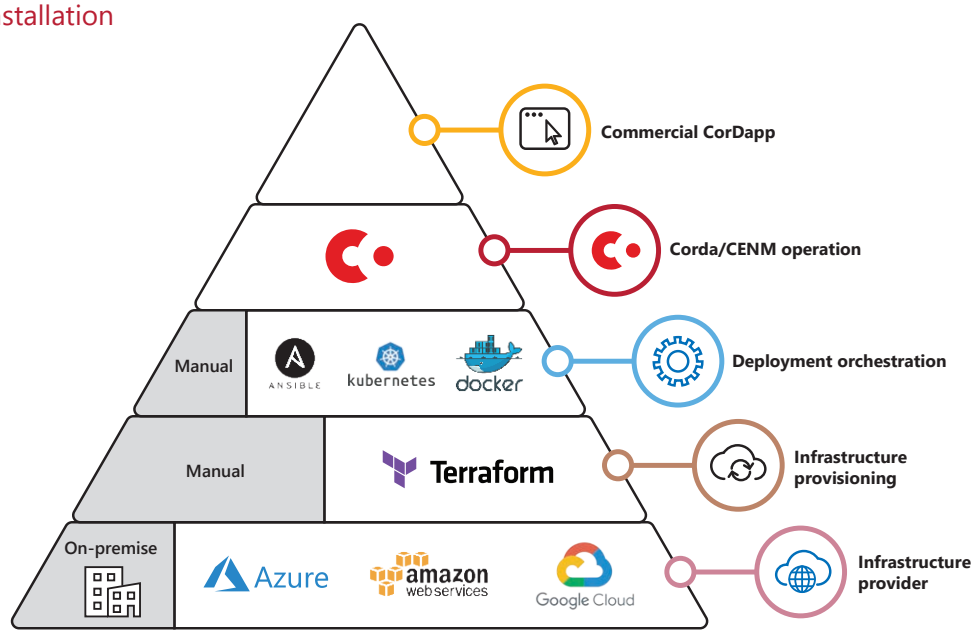
Corda oracle services – These provide external (off-ledger) data such as FX rates for validation to the different bank nodes in the Corda network.

1.2.1.6 Installation and infrastructure of Project Dunbar network on Corda

Each bank node and oracle service node is a Corda node running the Corda core software with CorDapps deployed on top of it that provide these nodes with business capabilities. These nodes can be hosted on the premises or in a cloud Infrastructure. These are the various deployment options available for Corda nodes.

During Project Dunbar, R3 used CBDC Accelerator which is a CorDapp that lets central banks, commercial banks, payment providers and more collaborate with one another in a "ready-made payments ecosystem" to evaluate CBDC use cases, learn, transact and test roll-out strategies and designs. The CBDC sandbox CorDapp is hosted in Microsoft Azure cloud services. It is currently hosted in R3's Azure cloud subscription but can be easily moved to another Azure cloud subscription.

Figure 25: Installation



1.2.1.7 Privacy model for access to information in Corda network

Corda's design is heavily influenced by the requirements of the financial industry to share data only with those with a legitimate need to know – thereby emphasising the significance of privacy. Corda's unique approach on this concept contrasts with other public blockchains where all transactions data on the ledger must be broadcast to other participants on the network and all of them must agree on all facts. In Corda, a transaction is agreed upon with consensus achieved only when all parties of that transaction provide their signatures. All transactions in Corda are governed by one or more smart contracts, which define what operations are allowed and who can perform them.

Corda is built on a data-centric design sometimes known as a UTXO model rather than a compute-centric design. By making data (contracts and agreements) primary, Corda brings the essence of data distribution to the heart of the programming model. It is designed to answer questions such as "Who should have this data and when?" "Under which circumstances?" "Who should verify or sign off on changes to this data?" "What evidence must be furnished to determine whether a proposed update is valid?"

Advanced Privacy Techniques:

Corda uses several techniques to maximise privacy on the network:

Transaction tear-offs: Transactions are structured in a way that allows them to be digitally signed without disclosing the transaction's contents. This is achieved using a data structure called a Merkle tree. You can read more about this technique in R3's document titled Defining transaction tear-offs.

Key randomisation: The parties to a transaction are identified only by their public keys, and fresh key pairs are generated for each transaction. As a result, an onlooker cannot identify which parties were involved in a given transaction.

States Reissuance: When a new transaction is created in Corda, input states are included in the proposed transaction by reference. These input state references link transactions together over time, forming a transaction backchain. Long transaction backchains are undesirable as resolution along the chain slows down performance. As well as all backchain transactions are shared with the new owner.

Prior to Corda 4.7, an approach to resolve the problem with long transaction backchains was for a trusted issuing party to simply reissue the state. This meant that the state could simply be exited from the ledger and then reissued. As there would be no links remaining between the exit transaction and the reissuance transactions, the transaction backchain would be pruned. Starting with Corda 4.7, there is a new State Reissuance algorithm that eliminates the risk of being left without a usable state if the issuing party fails to reissue the state for some reason (for example, if they are not online at the required time). This is achieved through the reissuing of an encumbered state before the original state is deleted. This allows the requesting party to unlock the reissued state immediately after the original state is deleted. State encumbrance refers to a state pointing to another state that must also appear as an input to any transaction consuming this state.

Hardware based Confidential Computing: Conclave is a confidential computing platform from R3 that enables the development of collaborative analytics solutions that aggregate and process multi-party data—without revealing the data to anyone. Confidential Computing describes a set of hardware techniques that fix this problem. It makes it possible to know what algorithm will process your information before you send it to a third party, and to be assured that the third party cannot subvert the integrity of the algorithm or observe it while it works. Conclave makes it easy to write applications that utilise these capabilities. Conclave makes it possible to isolate a small piece of code from the rest of the computer on which it runs (an enclave). Remote users can be shown what code

is running in the isolated world and then upload their secret data to it, where it can be processed without the owner of the computer in question getting access. Enclaves can be used to protect private data from the cloud, do multi-party computations on shared datasets and make networks more secure.

Intel SGX is an implementation of enclave-oriented computing. Conclave builds on SGX by making it easier to develop enclaves in high level languages like Java, Kotlin or JavaScript.

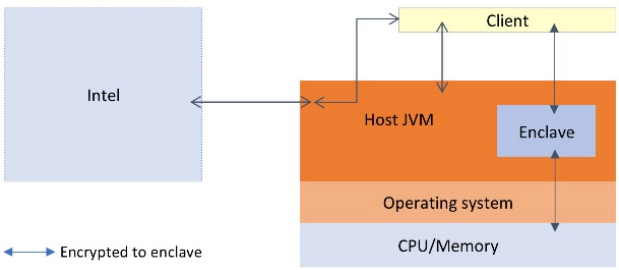
There are three entities in an application that uses Conclave:

Clients - send and receive encrypted messages to/from enclaves by interacting with the host over the network.

Host programs - load enclaves. From a security perspective they are fully untrusted and assumed to be malicious at all times. Hosts are relied on to provide the enclave with resources but beyond that work only with encrypted data.

Enclaves - are classes that are loaded into a dedicated sub-JVM with a protected memory space, running inside the same operating system process as the host JVM. Code running in an enclave cannot be tampered with by the host system or its owner, nor can the host system or its owner see the data that the enclave is processing. Enclaves communicate with clients via the host program.

Figure 26: Enclave communication



Software based Zero Knowledge Proof: Zero-knowledge proof (ZKP) is a cryptographic method whereby one party (the prover) can prove the truth of specific information to another party (the verifier) without disclosing any additional information. ZKP has been widely used to enhance the privacy of blockchain functionality and can be extended to solve inherent privacy issues of any distributed systems architecture. The Dutch bank ING's blockchain team has been working on ZKP solutions for quite some time. Their notable work has been the ZKP solution for enhancing privacy on Corda blockchain for validating transactions so that their contents can be kept private without compromising on safety.

1.2.2 R3's CBDC Accelerator

R3's CBDC Accelerator is the deliverable in collaboration with the CBDC Working Group, which started in September 2020 in partnership with 140+ public and private sector organisations. CBDC CorDapp is built on Corda Enterprise, hosted and offered by R3. R3's aim with the CBDC Accelerator is to demonstrate possible CBDC use cases on Corda.

Accelerator design is token-based, two-tier, hybrid CBDC, where CBDC tokens can be restricted to be issued by a central bank, as its liability, and distributed and transacted with a vast set of intermediaries like commercial banks, payment- or wallet service-providers catering for wholesale, retail and cross-border CBDCs in R3's CBDC Accelerator. R3's cross-notary and cross-network interoperability have helped implement features like delivery versus payment and payment versus payment. The CBDC Accelerator has been extended to support a UTXO-based decentralised exchange enabling innovative solutions for dynamic liquidity management and trade.

R3's CBDC Accelerator is designed as a ready-made digital ecosystem which brings to life the idea of a regulated DeFi or Open Finance solution, with CBDC as legal tender, at the core of the ecosystem.

R3's CBDC Accelerator has the below features prebuilt in:

- Token lifecycle management – Allows central banks to track the lifecycle of a token created ie pledge/ issue/ transact/ redeem/destroy and ensuring clear distinctions of roles and responsibilities.

- Member access – Allows central banks to control access to tokens and ensure KYC compliance.

- Re-issuance – Allows central banks to withdraw and re-issue tokens, an existing operational feature mirroring how central banks manage fiat currencies in the current state.

- Central banks will have visibility of transactions at the point of re-issuance. Technically, it will limit the backchain from growing too big and ensure good performance of the system.

- Delivery versus payment – Allows users (commercial banks/PSPs) to exchange a real-world asset (delivery) for digital currency (payment). In R3's CBDC Accelerator, bonds are exchanged with CBDC.

- Payment versus payment – Allows users (commercial banks/PSPs) or central banks to exchange a currency (payment) for another digital currency (payment). In R3's CBDC Accelerator, one CBDC is exchanged with another CBDC, which can be extended to be overlaid with workflow business rules.

- Programmable money – Allows central banks and users (commercial banks/PSPs) to define rules around assets so that they can behave or be used in a certain way. R3's CBDC Accelerator facilitates the ecosystem to explore innovative use cases such as real-time direct government-to-citizen payments for citizens' services such as tax refunds, healthcare support, childcare funding and stimulus payments.

- Dynamic liquidity management – Liquidity simply means "real time availability of liquid assets or cash". In CBDC parlance, it is the availability of CBDC tokens in a single- or multi-CBDC network. It allows users (commercial banks/PSPs) to offer spare liquidity to other users in the network at a certain rate (including the fees).

- Distributed exchange – A DEX is an extended version of the dynamic liquidity management feature where users or a group of users can be designated as market-maker. Rates can be set bilaterally (off-ledger) or using a bid-ask process (off-ledger). Liquidity offers are controlled broadcast giving flexibility to banks to choose their liquidity borrowers.

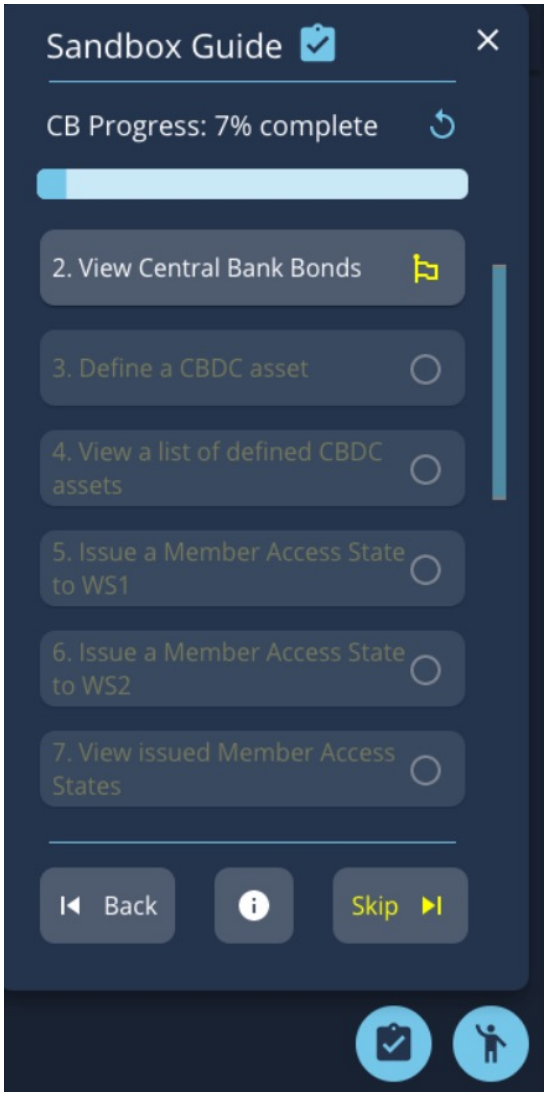
- Token analytics/money supply – Allows central banks to track assets within the ecosystem, and ensure they comply to regulatory and monetary compliance requirements governing the money supply. It helps central banks and regulators by providing real-time, 360-degree visibility of their assets in the ecosystem.

- Distributed interest – Allows central banks to implement positive/negative interest rates on their digital currency. Allows wholesale banks to loan spare liquidity for a fee (ie it is an incentive mechanism).

- Retail CBDC models – R3's CBDC Accelerator extends end-to-end support for a general purpose CBDC on a DLT framework. Features supported include token issuance by the central bank, and distribution by users (commercial banks/PSPs) that own and maintain retail accounts of end-customers. Retail account holders can initiate payments using the web app or mobile app using dynamic QR code to pay at point of sale or for peer-to-peer payments. R3's CBDC Accelerator has other retail features built in such as payee management, transaction-logging, and business rules' programmability.

R3's CBDC accelerator has how-to guides for the central bank and wholesale banks to learn how to perform tasks on the user interface. The guide is accessed by clicking the clipboard icon in the bottom right corner and provides step-by-step instructions for completing tasks.

Figure 27: CBDC Accelerator guide



CBDC Accelerator Network – Central Bank

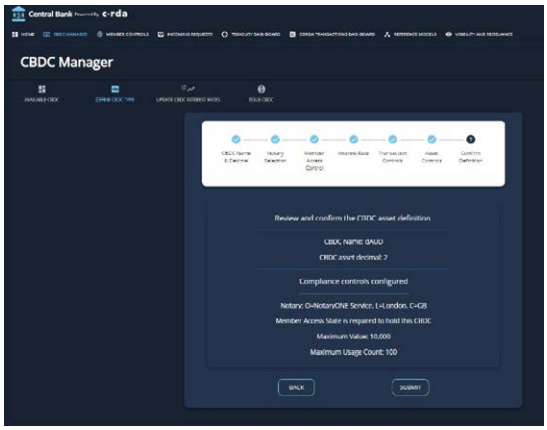
Figure 28: CBDC Accelerator Network – Central Bank

CBDC Manager: As a central bank, digital currency will be defined using the CBDC Manager panel.

It allows you to name the digital currency and optionally assign decimal places and/or make it access restricted and/or add interest rates and/or define controls around transaction usage.

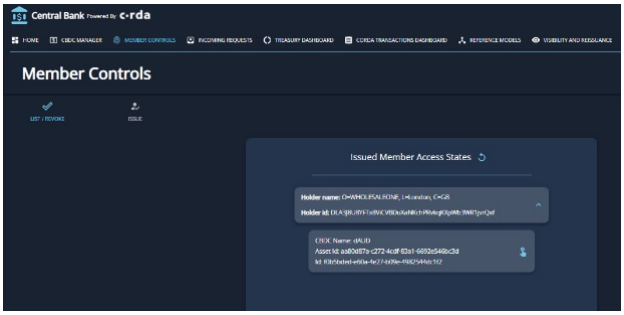
For example, dAUD is created with 2 decimal places, non-interest bearing and with access required to hold this currency. Additional transaction controls are configured where by any transaction above 10,000 dAUD or after 100 transactions should be reported to the issuers.

Figure 29: CBDC manager



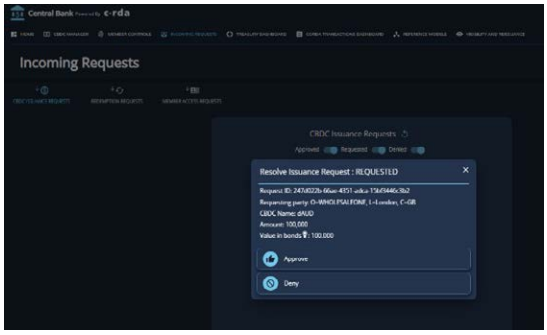
Member Controls: As a Central bank, you can control access to digital currency using member access panel, where access can be issued or revoked.

Figure 30: Member controls



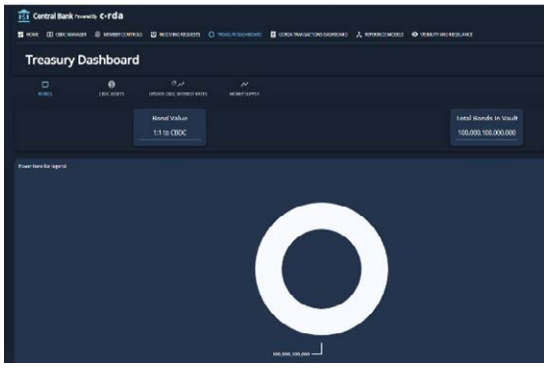
Request: An authorised user of a Central Bank, can approve or deny three different types of requests ie request to issue CBDCs, request to redeem CBDCs and request to provide access to hold CBDCs.

Figure 31: Request



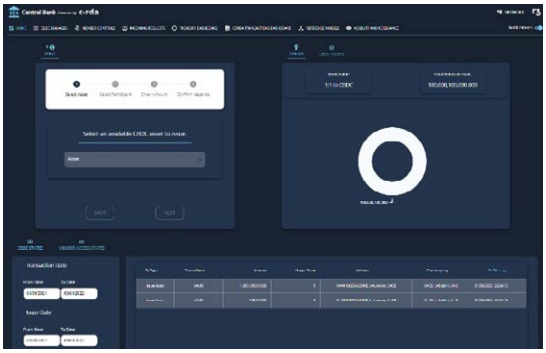
Treasury Dashboard: Authorised users of Central Bank, can monitor the issued CBDC, the total money in circulation, bonds that under held, using treasury dashboard panel.

Figure 32: Treasury dashboard



Transaction Log: Authorized user of a Central Bank can view transactions (issue, redeem, access) on a dashboard with the right timestamp and the counterparty, on the transaction dashboard panel.

Figure 33: Transaction log

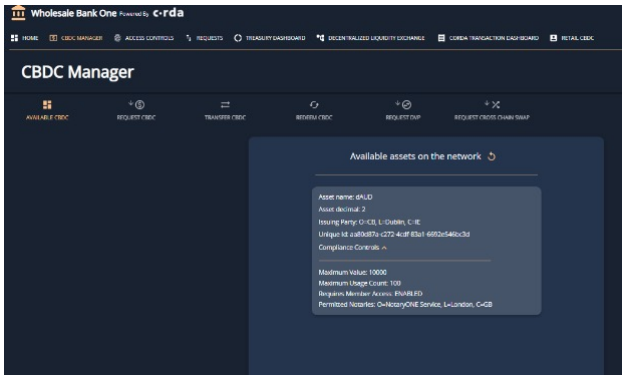


CBDC Accelerator Network – Wholesale Bank

Figure 34: CBDC Accelerator Network – Wholesale Bank

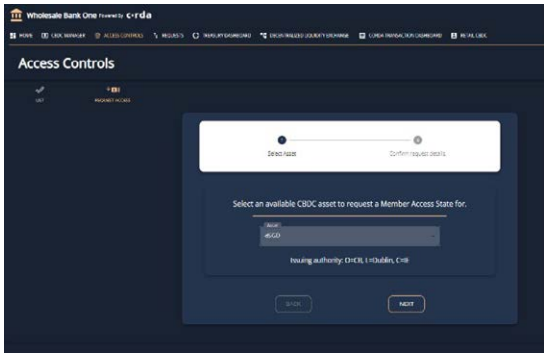
CBDC Manager: Authorized wholesale bank users uses this panel to check available CBDCs in the networks where it has been granted access. Depending on the user access, the panel extends to key operational workflow with the central bank issuer and counterparties.

Figure 35: CBDC manager



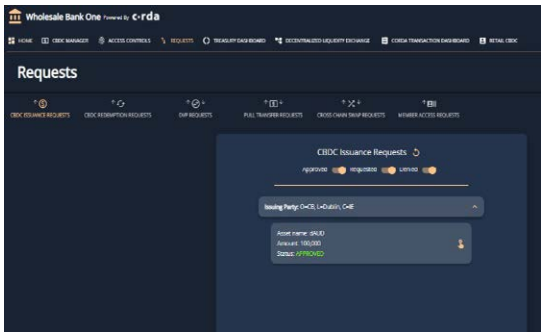
Member Controls: Wholesale bank authorised, users can request access to a CBDC on the network by requesting the issuers of that CBDC, using the access control panel.

Figure 36: Member controls



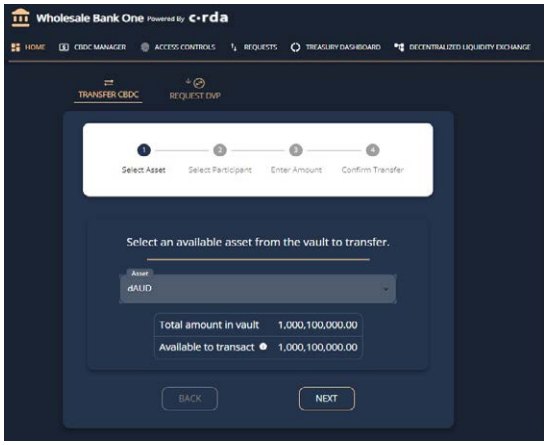
Requests: Depending on the user access granted, wholesale bank user can initiate different types of requests like request to issue CBDCs, request to redeem CBDCs, DvP requests, access request to hold CBDCs, using the request panel.

Figure 37: Requests



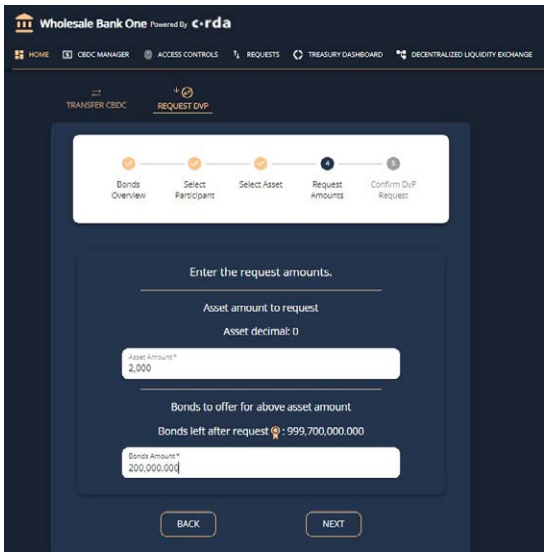
Transfer: Authorized wholesale bank users, use this panel to manage transfer of CBDCs to other banks or PSPs on the network,

Figure 38: Transfer



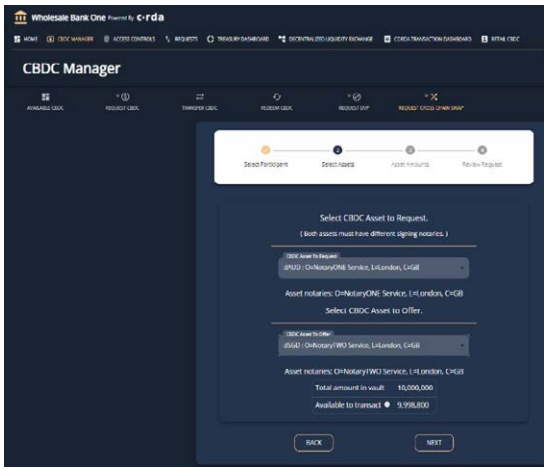
Authorized users of wholesale bank can initiate delivery vs payment requests by offering bonds (pre-configured asset) for CBDCs.

Figure 39: Request DvP



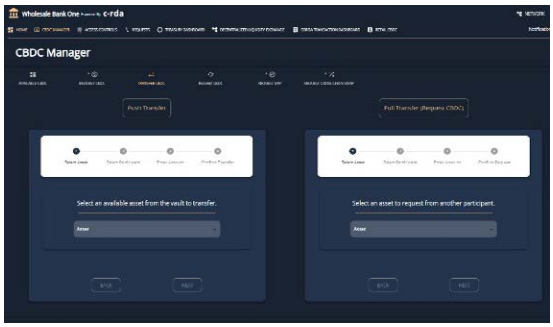
Authorized users of wholesale bank you initiate payment vs payment requests by offering one CBDC for another, using the cross chain atomic swap functionality in the request panel.

Figure 40: Request cross chain swap



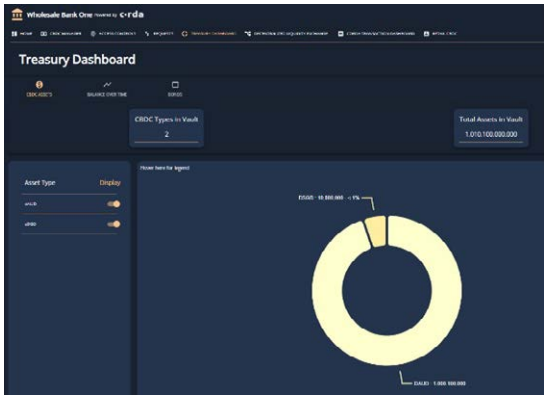
Authorized users of wholesale bank can initiate either a pull request (example: scheduled payments) or a push request (example: regular payments) for CBDCs, using the transfer panel.

Figure 41: Transfer CBDC



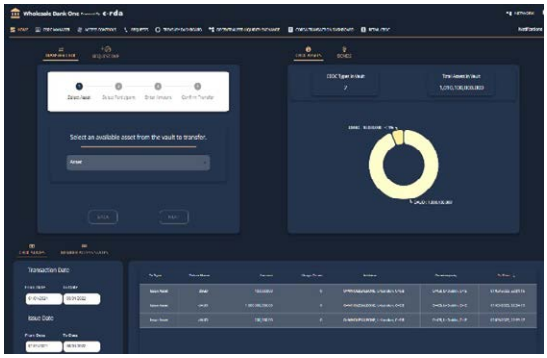
Treasury Dashboard: Authorized users of wholesale bank can monitor the different CBDCs that held, total amount of bonds in the vault and balance over time, using the treasury dashboard panel.

Figure 42: Treasury dashboard



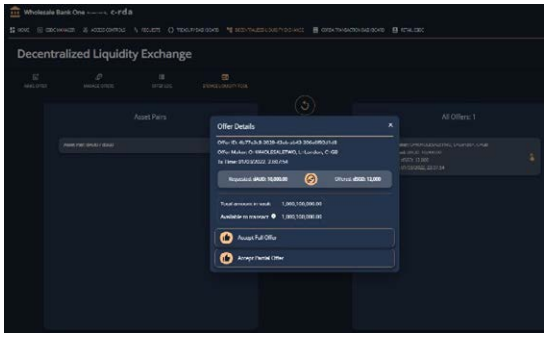
Transaction Log: Authorized users of wholesale bank can view all your transactions (issue, redeem, access request, transfer) on a dashboard with the right timestamp and the counterparty, on the transaction dashboard panel.

Figure 43: Treasury dashboard



Decentralised Liquidity Exchange: Authorized users of wholesale bank can make an offer for a currency pair, broadcast it to the network for an off-ledger exchange or spot exchange. Users can view the offer pool to look at offers from other wholesale bank and if in short of liquidity, can partially or in full, accept an offer.

Figure 44: Decentralised liquidity exchange



In cross border payments today, a wholesale bank has to manage it's liquidity positions for different currencies by inefficient and inaccurate payment forecasting. In most cases this has resulted in situations when there isn't enough liquidity to settle a cross border payment obligation, which leads to settlement delays. With decentralised exchange, the aim is to offer tools for buying real time liquidity from other wholesale banks to settle a cross border payment obligation. This tool can be further extended to provide automated market making capabilities in a multiple CBDC network for a basket of CBDCs. This is currently not built in the accelerator.

Retail CBDC: As a wholesale bank, you can be the distributor of CBDCs to end consumers and businesses.

All retail customers will have an account to hold and transact CBDCs. All retail customers are onboarded using customer onboarding process for a bank, adhering to KYC/AML requirements. Retail customers can be managed, using manage customer and accounts functionality.

Figure 45: Retail CBDC

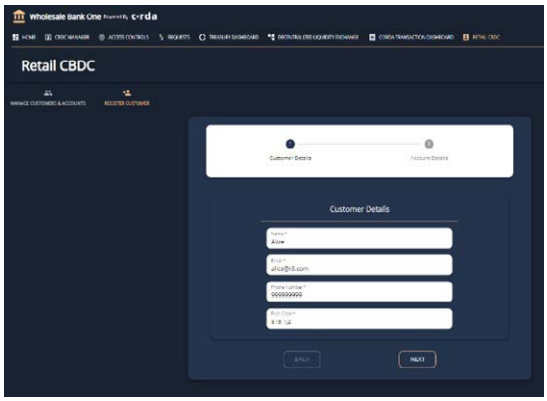
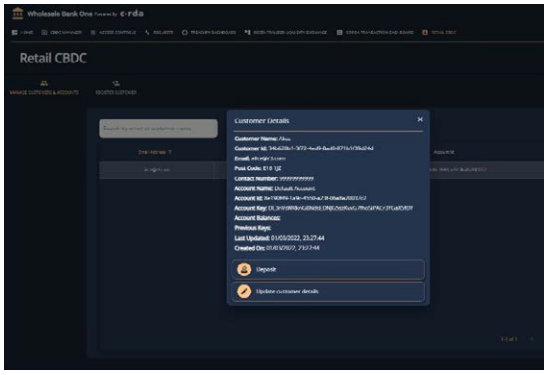


Figure 46: Customer details



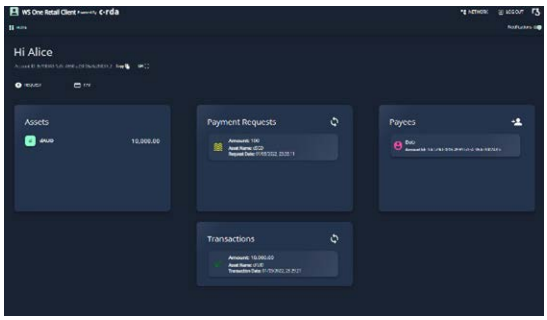
Customers of wholesale bank can credit account with CBDCs, by using deposit functionality.

Retail customer, can access their respective CBDC account by logging into web portal or scanning a QR code.

Figure 47: Retail login

Retail customers can send or receive payments, similar to a regular internet banking app.

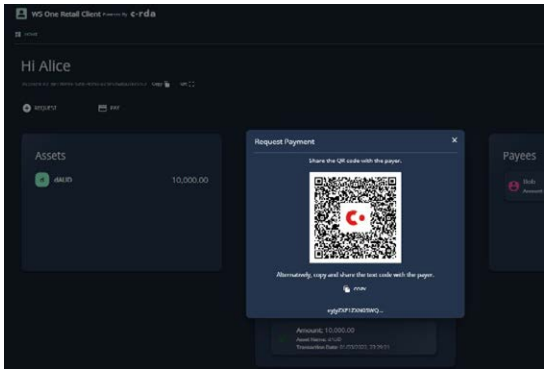
Figure 48: Retail user functionalities



Retail users can add payees, sent payments, monitor your total CBDC balance and view transaction history.

CBDC accelerator is embedded with dynamic QR code-based payments, where using the mobile app, retail users can tap and pay for goods and services.

Figure 49: Dynamic QR code-based payments



CBDC Accelerator Notary selection

In the CBDC accelerator, each central bank has an associated notary or a selection of notaries, responsible for issuance of CBDCs. These notaries ensure there are no duplicate issuance, or any double spend of CBDCs in the network. In Corda, as the notary node provides the required consensus, each CBDC is issued solely by the central bank without any dependency on the network.

1.2.3 R3 Security Controls

Designed primarily for financial institutions, the Corda platform offers security at multiple layers.

Corda uses industry-standard protocols to communicate different software components in the network. Corda nodes communicate securely between each other using **Advanced Message Queueing Protocol (AMQP**). This is a wire-level, application-layer protocol for message-oriented middleware and is a widely implemented binary messaging standard. AMQP messages are encrypted using **Transport Layer Security (TLS)** which ensures integrity and privacy of messages in transit. Nodes use **Hypertext Transfer Protocol Secure (HTTPS)** for their initial registration in a Corda network and for sharing node address locations through the network map.

A core component of the Corda Enterprise version is the **Corda firewall** component that enables a true Demilitarised Zone (DMZ). The Corda firewall, known as bridge/float component, is designed for enterprise deployments and acts as an application-level firewall and protocol break on all internet-facing endpoints. The Corda firewall encapsulates the peer network functionality of the basic Corda Enterprise node, so that it can be operated separately from the security-sensitive Java Virtual Machine (JVM) run-time of the node. The firewall can also serve two or more nodes, thus reducing the deployment complexity of multiple nodes in the same network. Corda is designed to prevent man-in-the-middle attacks by requiring that TLS connections are directly terminated between Corda firewalls.

Considering that cryptographic key lifecycle management plays a crucial role in the Corda platform, the Enterprise version supports integration with a variety of **Hardware Security Modules (HSM).** An HSM is well-trusted and performs a variety of cryptographic operations such as encryption and key management. An HSM ensures that the hardware used is well tested and has a security-focused operating system with very limited access to the external world. In the Corda ecosystem, operations involving private keys, such as signature generation, will be delegated by the Corda node to the HSMs, while operations involving public keys, such as signature verification, will be performed by the Corda node. Corda Enterprise supports a variety of HSMs such as Utimaco SecurityServer, Gemalto Luna as well as Azure Key Vault and AWS CloudHSM from the leading cloud providers.

1.2.3.1 Security controls at CBDC Accelerator CorDapp layer

Controls available on the CBDC Accelerator include:

Asset control – Asset controls are programmable on the sandbox giving issuers (central banks) authority over how and when their assets are used.

Transaction control – Issuers can programme transaction controls to give them authority over how the assets they have defined are transacted.

Notary selection – Notary selection lets issuers (central banks) choose a notary (or notaries) to use in transactions. The central bank designates a list of notaries that can validate a transaction when defining an asset. The sandbox automatically selects a notary from the list during the first transaction with a particular asset, based on availability. It uses the selected notary for all transactions involving the CBDC tokens associated with the initial transaction. Every transaction requires at least one notary.

By providing security at protocol and application levels, the Corda platform safely stores and secures end-users' sensitive personal identifiable information (PII). Built for financial institutions, the Corda platform understands the criticality of such user information involved in transactions on a CBDC ecosystem.

1.3 Prototype developed by Partior on Quorum platform

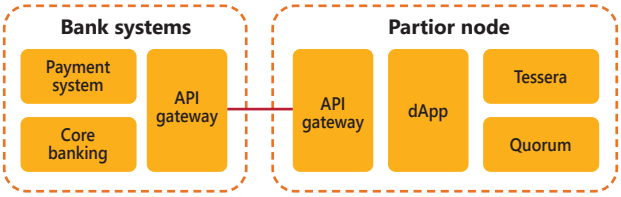
1.3.1 Partior Technical Architecture

1.3.1.1 Technical architecture

Partior is based on an Ethereum-based distributed ledger (Quorum) that is built with key considerations such as ease of integration and data privacy. It is a fork of Go Ethereum client (geth), the official GoLang implementation of the Ethereum protocol, designed as a private network with a permissioned group of known participants. Within the platform, the minimum necessary rule is core-to-transaction-processing, which means information is retrieved on a "need-to-know" basis. A network consists of multiple nodes, through which users connect to the platform.

Each node comprises several components including an API gateway, dApp, Tessera and the Quorum platform.

Figure 50: A node on Quorum



Partior node – It is a Quorem node, which is a minimal fork of Go Ethereum, providing privacy, new consensus mechanisms, network-permissioning and higher throughput.

dApp – A dApp acts as a middle layer between conventional systems to the DLT, serving as a translator to convert the user's API into the required smart contract format.

Tessera – A stateless Java application responsible for the encryption/decryption of private transaction data and off-chain private messaging.

There are two types of nodes:

Participant nodes communicate within the network to share transaction details for processing. Every node in a decentralised system has a copy of the blockchain.

Validator nodes are responsible for verifying transactions on a blockchain. Once verified, transactions are added to the distributed ledger. The central banks' nodes are configured to be the validator nodes in this setup.

In Quorum, validator nodes are to be connected with each other point-to-point.

Non-validating nodes are not required to be interconnected to all nodes in the network.

There are two ways for users to connect to the platform:

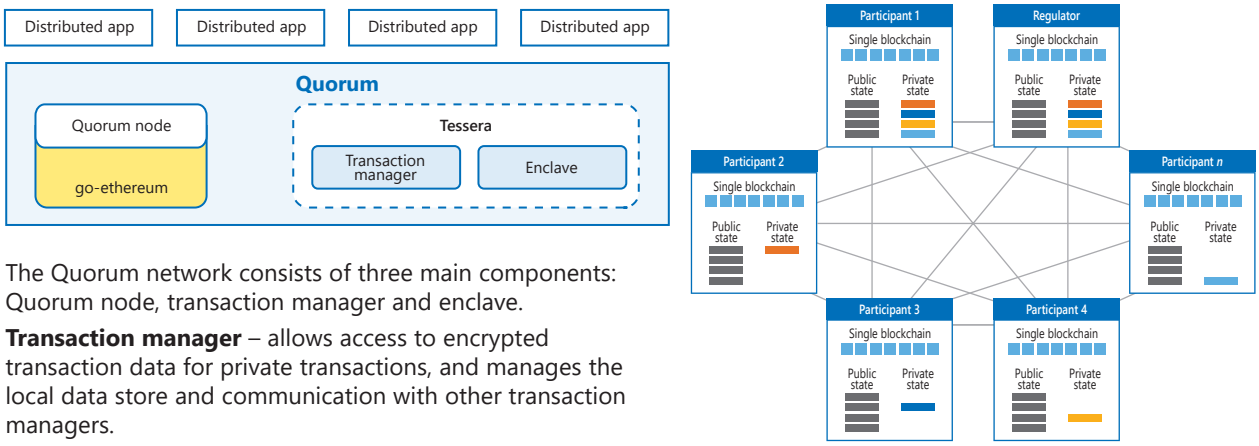
1. Self-hosted node by participants.

2. Third-party hosted node (PaaS): An independent operator is set and provides node-hosting services while at the same time maintaining the integrity of the network.

In establishing a connection with the platform, users are required to leverage a component known as a Distribution Application (dApp).

1.3.1.2 Network architecture

Figure 51: Quorum network architecture



The Quorum network consists of three main components: Quorum node, transaction manager and enclave.

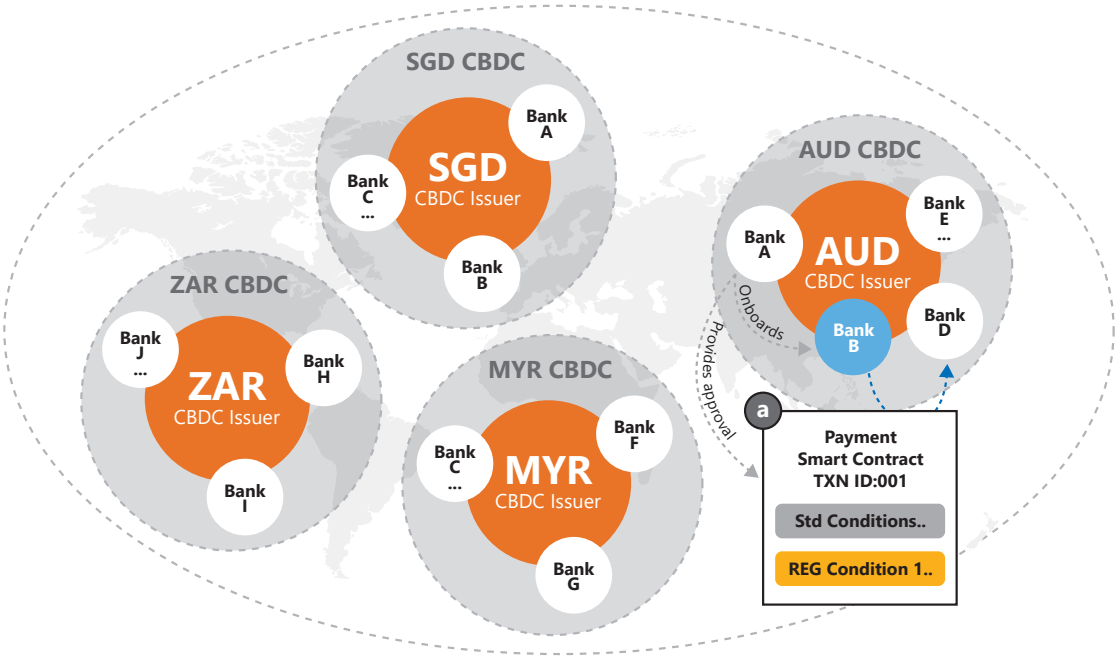
Transaction manager – allows access to encrypted transaction data for private transactions, and manages the local data store and communication with other transaction managers.

Enclave – responsible for private key management and for the encryption and decryption of private transaction data.

1.3.1.3 Project Dunbar Partior network

On the Project Dunbar Partior network, each host is in control of its own "mini" network, which is depicted by the individual circles in the diagram below. A domestic bank that is not a host may engage in transactions on the Dunbar platform by initiating a transaction with its sponsor bank, after which the transaction flows on to the multi-CBDC platform. The following examples illustrate (1) a domestic transfer and (2) cross-border FX settlement.

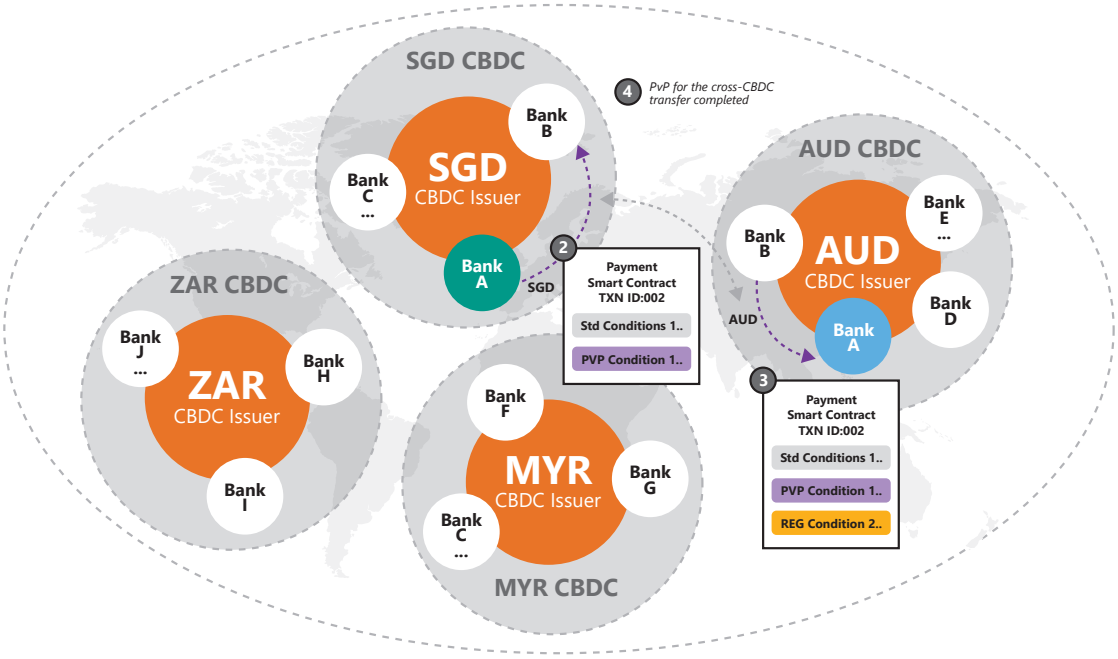
Figure 52: Scenario 1 – Domestic transfer



1. Bank A, a licensed bank in AU, is appointed by Bank B as its sponsoring bank in the AUD CBDC.
2. As Bank B performs the domestic AUD CBDC transfer to Bank D, Bank A, which is the sponsor bank for Bank B in the AUD CBDC network, will be required to provide its approval for the transaction.

Next, we consider a scenario of FX settlement from SGD to AUD.

Figure 53: Scenario 2 – FX settlement



1. Bank A has arranged for Bank B to perform the cross-CBDC PvP settlement (payment-versus-payment).
2. Bank A will transfer SGD CBDC to Bank B SG. The transfer will be effected once all pre-validation conditions are fulfilled.
3. Bank B AU will transfer AUD CBDC to Bank A's AUD wallet with the same transaction reference. The transfer will be effected once all pre-validation conditions are fulfilled.
4. Once both SGD and AUD CBDCs transfers are completed, PvP is effected and the cross-CBDC transfer is completed.

1.3.1.4 Installation and infrastructure of Project Dunbar network on Quorum

Each Partior node is an instance that can be hosted on the premises or with a cloud service provider (CSP). During Project Dunbar, the prototype was hosted with Amazon Web Services (AWS). AWS enabled efficient resource provisioning (ramping up and down) as necessary, complementing the agile delivery methodology adopted by the project.

Considerations for deciding the number of nodes and who should host them for a live platform include performance, efficiency and cost of investment. As the number of nodes increases, the resiliency of the platform against fraud or illegal activities increases by strengthening the ledger.

Generally, it is acknowledged that, from a feasibility perspective, central banks and selected commercial banks would be in the most appropriate position to be hosting nodes.

1.3.1.5 Access to information

Critical transaction data is processed on the platform through the nodes. A natural question that follows for indirect participants of the network is: Who has access to which parts of their data?

To illustrate the information that is available to each entity within a transaction, we consider the following network scenario:

1. Network of four nodes – Network operator, settlement bank, ABC bank (participant bank), XYZ bank (participant bank) node.
2. ABC bank and XYZ bank have a digital balance account with the settlement bank (AC2 and AC3 respectively).
3. Settlement bank has its own digital balance account AC1 on the network.

Scenario 1: Network instantiation

- All contracts are deployed, and accounts created with "privateFor"[10] for all nodes.
- All nodes have the visibility of the account numbers, and balances of all accounts are zero.

Figure 54: Network instantiation

Node	AC1	AC2	AC3
Settlement bank	0	0	0
ABC	0	0	0
XYZ	0	0	0
Network operator	0	0	0

Scenario 2: Deposit

- Each bank initiates a balance deposit.
- Transaction is marked "privateFor" for initiating bank and settlement bank (eg (settlement bank, ABC).

Figure 55: Deposit

Node	AC1	AC2	AC3
Settlement bank	0	2000	3000
ABC	0	2000	0
XYZ	0	0	3000
Network operator	0	0	0

Note:

- ABC balances are visible to settlement bank node and ABC node but not to XYZ node.
- Similarly, XYZ balances are visible to settlement bank node and XYZ nodes only.

Scenario 3: Transfer

- ABC initiates coin balance transfer to XYZ bank via settlement bank.
- The transaction is marked "privateFor" for all three nodes.

Figure 56: Transfer

Node	AC1	AC2	AC3
Settlement bank	0	1800	3200
ABC	0	1800	200
XYZ	0	-200	3200
Network operator	0	0	0

Note:

- Settlement bank is able to see the true balance of both ABC and XYZ.
- ABC and XYZ can see the true self balance.
- ABC and XYZ can only see their relative position with respect to each other and cannot see the true balance of each other.

Scenario 4: Withdraw

- XYZ bank initiates withdrawal.
- The transaction is marked "privateFor" for all settlement bank and XYZ nodes only.

Figure 57: Withdraw

Node	AC1	AC2	AC3
Settlement bank	0	1800	2700
ABC	0	1800	200
XYZ	0	-200	2700
Network operator	0	0	0

Note:

- Balance updates reflected only in settlement bank and XYZ bank node.
- ABC node will not have any information of this transaction.

[10] "privateFor" is a feature which allows for making a transaction decryptable only to a selected few parties (private transactions). https://consensys.net/docs/goquorum/en/stable/concepts/privacy/private-and-public/#private-transactions

A smart contract is a programme written in a high-level programming language that runs on a DLT.

There are three categories of smart contracts on a Quorum platform:

- A payment contract is used to facilitate funds transfer. Its capabilities include payment conditions management, payment lifecycle orchestration and status maintenance, as well as payment enquiry.
- A common contract is used for maintaining information. Its capabilities include access management, bank list and availability, and common codes, etc.
- Lastly, a settlement contract is used to manage a user's wallet. Its capabilities include transaction posting and balance enquiry.

1.3.2 Partior Applications

1.3.2.1 Types of transactions available on Partior sandbox

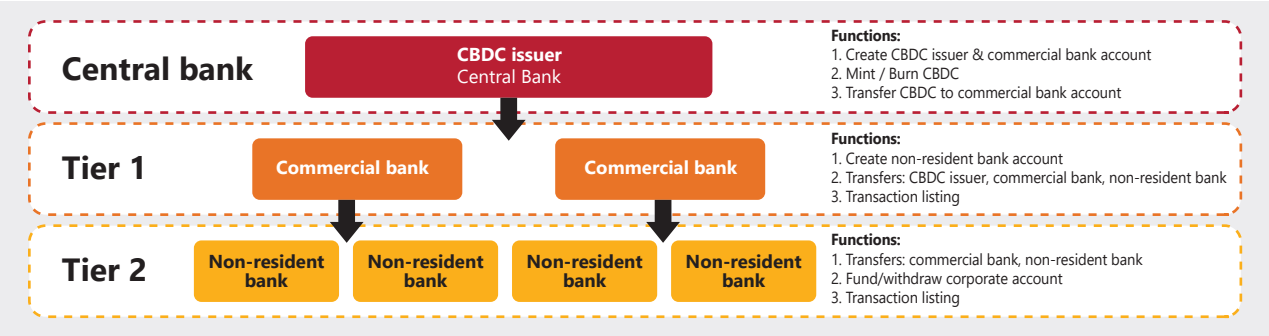
Partior's CBDC sandbox model allows central banks to leverage the existing banking infrastructure and relationships between corporate or retail accounts and commercial banks.

CBDCs that are minted from the central bank are transferred into the CBDC-designated CBDC "issuer" account. The corresponding CBDCs, which are central bank money, can be redeemed back to fiat currency where required.

Participants will be able to utilise the Dunbar platform on Quorum to conduct cross-issuer or cross-currency payments while at the same time reducing current frictions and latency, and minimising post-transaction exceptions-handling and reconciliation activities.

1.3.2.2 Partior membership types and their privileges

Figure 58: Partior CBDC Sandbox



CBDC issuer – Central bank: Ability to create CBDC issuer and commercial bank account, mint/burn CBDC, and transfer CBDC to commercial bank account.

Tier 1 – Commercial bank: Ability to create non-resident bank account, transaction listing, and make transfers to CBDC issuer, commercial bank and non-resident bank.

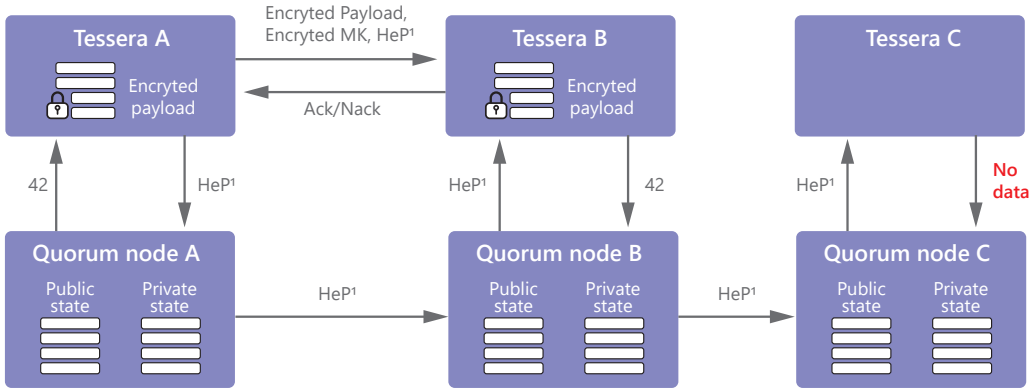
Tier 2 – Non-resident bank: Ability to fund/withdraw corporate account, transaction listing, and make transfers to commercial bank and non-resident bank.

1.3.3 Partior Security Controls

1.3.3.1 Multi-network CBDC governance model on the Dunbar platform in Quorum

Membership admission criteria are common and can be applied universally across the platform. All participants (nodes or banks) will be subject to a universal set of security policies.

Figure 59: Tessera encryption



[1]HeP = SHA3-512 hash (encrypted payload)

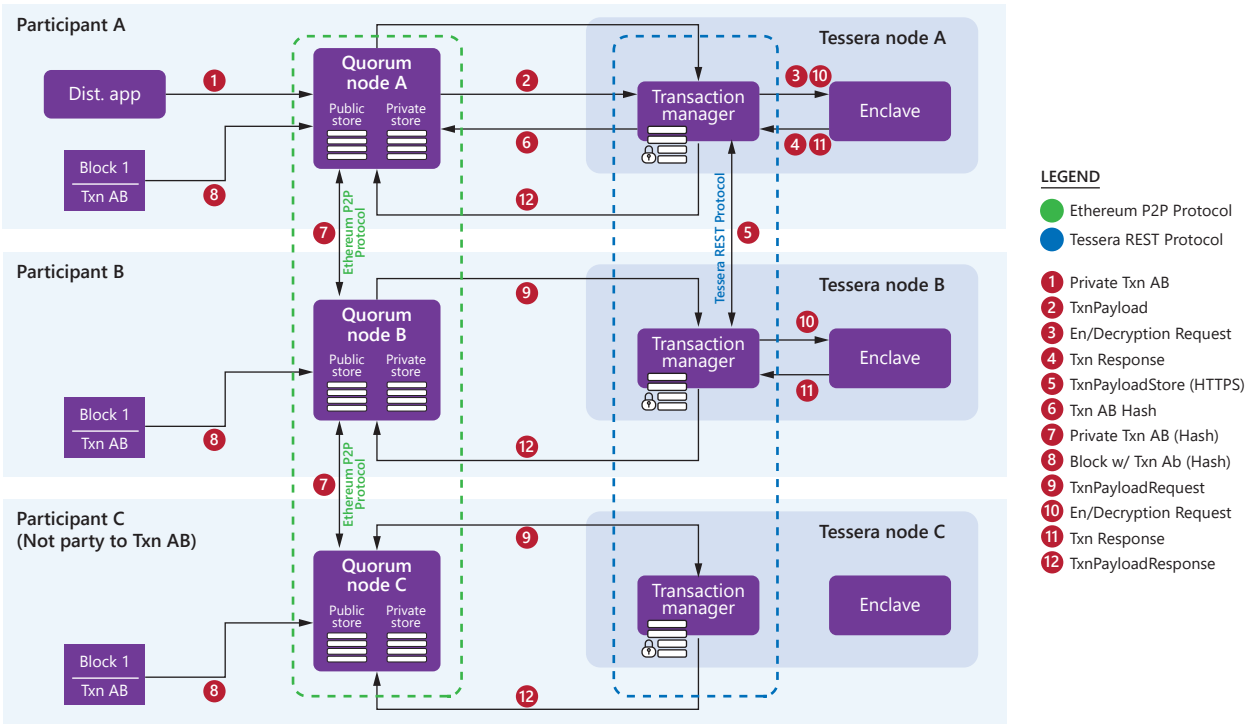
Quorum's decentralised architecture provides unique privacy advantages.

Partior's implemented sandbox did not place reliance on a central node or service, and as such there is no centralised datastore. This ensures decentralised privacy. A single-chain architecture with a chain that contains both public and private transactions would guarantee privacy while ensuring better security. It is designed to meet regulatory requirements around in-country data and is compatible with next-generation crypto primitives such as ZKP.

Privacy is achieved on Quorum through Ethereum modifications and Tessera.

Ethereum modifications – State trie is split into public state trie and private state trie; "v" value of private transactions is set to 37 or 38; privateFor is added to transaction parameters in order to specify an array of recipients that will receive the transaction's details; and the Ethereum virtual machine (EVM) is prevented from executing private-to-public writes.

Figure 60: Simple privacy diagram



1.3.3.2 Tessera cryptography and key management

Tessera uses the NACL crypto library, which includes payload encryption and authentication, public key encryption/authentication and hashing. Tessera generates key pairs and holds private keys, that are password-protected, locally.

Sending a private transaction

1. Participant A sends a transaction to their Quorum node.
2. A's Quorum node passes the transaction on to its paired TxMgr.
3. A's TxMgr makes a call to its associated enclave to validate the sender and encrypt the payload.
4. A's enclave checks the private key for A and, once validated, performs the transaction conversion:
   a. Generating a symmetric key and a random nonce.
   b. Encrypting the payload and nonce with the symmetric key from a.
   c. Calculating the SHA3-512 hash of the encrypted payload from b.
   d. Iterating through the list of transaction recipients, in this case A and B, and encrypting the symmetric key from a. with the recipient's public key (PGP).
   e. Returning the encrypted payload from step b., the hash from step c. and the encrypted keys (for each recipient) from step d. to the transaction manager.
5. A's TxMgr stores the encrypted payload then securely transfers (via HTTPS) data to B's TxMgr.
6. A's TxMgr returns the hash to the Quorum node which then replaces the transaction's original payload with that hash.
7. The transaction is then propagated to the rest of the network using the standard Ethereum P2P protocol.
8. The leader Quorum node (in this case A) creates a block containing Transaction AB and distributes to each party node on the network.
9. All parties attempt to process the transaction.
10. Since C does not hold the transaction, it will receive a NotARecipient message and will skip the transaction – it will not update its Private StateDB.
11. Enclave for A and B validates the signature and then decrypts the symmetric key using the party's private key that is held in the enclave, decrypts the transaction payload using the now-revealed symmetric key and returns the decrypted payload to the transaction manager.

The transaction managers for parties A and B then send the decrypted payload to the EVM for contract code execution.

To lessen the likelihood of fraudulent transactions, Quorum currently implements two consensus mechanisms – Istanbul BFT and Raft (the older QuorumChain is now deprecated). Enabling one or the other is done via flags passed at start-up time to the node client.

Raft – Based on the etcd's raft implementation, and enabled via the --raft flag upon geth start-up. It features high throughput with low latency. Blocks are communicated using the raft transport layer, not Ethereum's DEVp2p, and it is fork-preventing which ensures transaction finality.

Istanbul BFT – The Istanbul BFT (IBFT) features a three-phase consensus commit that is BFT-hardened. Validators are defined at the network start and must have direct connections. IBFT is enabled via the custom genesis block with Istanbul configuration option and validator list via etraData,[11] documented in detail via EIP 650.[12]

[11] https://github.com/ConsenSys/quorum-examples/blob/master/examples/7nodes/istanbul-genesis.json
[12] https://github.com/ethereum/EIPs/issues/650

Permissioning

This functionality on the Quorum platform controls which nodes may connect to other nodes. Permissions and public key whitelists are currently managed at the node level.

Smart contract-based permissioning archetypes (eg a single entity responsible for onboarding and rules-setting) , where a centralised governance authority does not need to replace distributed blockmaking/validation, will be supported.

Geth modifications

The "proof of work" consensus algorithm has been replaced, and the P2P layer has been modified to allow only connections to/from permissioned nodes. The block generation/ validation logic has been modified to replace the "global public state root" check. The State Patricia trie has been split into two: a public state trie and a private state trie.

Block validation logic has been modified to handle private transactions. Transaction creation has been modified to allow for transaction data to be replaced by encrypted hashes in order to preserve private data where required, preventing EVM from executing private-to-public writes. The price of gas has been set to 0 – gas itself remains.

1.4 Glossary of Terms

AML	Anti-Money Laundering
BISIH	Bank for International Settlements Innovation Hub
BNM	Bank Negara Malaysia
CBDCs	Central Bank Digital Currencies
CFT	Countering Financing of Terrorism
CPMI	Committee on Payments and Market Infrastructures
DLT	Distributed Ledger Technology
DvP	Delivery versus payment
EDD	Enhanced Due Diligence
FSB	Financial Stability Board
FX	Foreign Exchange
HTLC	Hash Time-Locked Contracts
IPS	Instant Payment System
KYC	Know-Your-Customer
MAS	Monetary Authority of Singapore
Multi-CBDCs	Multiple Central Bank Digital Currencies
PvP	Payment versus payment
RBA	Reserve Bank of Australia
SARB	South African Reserve Bank

Bank for International Settlements (BIS)

ISBN 978-92-9259-543-2 (online)