Project Atom

Exploring a Wholesale CBDC for Syndicated Lending

December 2021

RESERVE BANK OF AUSTRALIA

Commonwealth Bank of Australia

nab

Perpetual

CONSENSYS

KING&WOOD MALLESONS

Contents

Executive Summary

Research into the use of distributed ledger technology (DLT) and digital financial assets is advancing rapidly. The use of DLT and smart contracts has the potential to deliver benefits in the form of greater efficiency, transparency, liquidity and accessibility in asset markets, as well as enable the issuance of new forms of money, such as central bank digital currency (CBDC). Project Atom was a collaborative research project undertaken in 2020–21 between the Reserve Bank of Australia (RBA), Commonwealth Bank of Australia (CBA), National Australia Bank (NAB), Perpetual and ConsenSys, with additional input from King & Wood Mallesons (KWM). The project involved the development of a proof-of-concept (POC) for the issuance of a tokenised form of CBDC – a digital form of money that is a direct claim on the central bank – that could be used by wholesale market participants for the funding, settlement and repayment of a tokenised syndicated loan on an Ethereum-based DLT platform.

The project examined the potential use and implications of a wholesale form of CBDC, with a focus on:

- how access to a tokenised CBDC could be extended to a wider range of wholesale market participants than just commercial banks
- the potential benefits of integrating tokenised CBDC with a digital asset in the form of a tokenised syndicated loan on interoperable DLT platforms
- how an enterprise-grade version of the Ethereum blockchain platform could address some of the technical limitations in the public version of Ethereum, with a view to understanding whether DLT could be a viable technology for this type of system.

The POC explored a two-tier model for the issuance and distribution of the wholesale CBDC whereby the RBA would issue CBDC to commercial banks, and then banks could make the CBDC available to eligible wholesale market participants that they sponsor onto the platform. This model preserves several important aspects of the current role of commercial banks in the financial system, including customer onboarding and other customer-facing activities. There are a range of potential benefits in providing non-bank wholesale market participants with access to CBDC for settling transactions and as a store of value. However, broader access also raises a number of policy and legal issues that would need to be considered, including: who would be eligible to access CBDC; how CBDC could be used; the nature of the relationship between commercial banks and their sponsored participants; and the potential implications of commercial bank deposits migrating to CBDC for financial intermediation and financial stability.

The POC demonstrated that the digitisation of syndicated loans on a DLT platform could provide significant efficiency gains and reduce operational risk by replacing highly manual and paper-based processes related to the origination and servicing of these facilities. Moreover, integrating a tokenised CBDC on the same blockchain platform enabled instantaneous delivery-versus-payment (DvP) settlement of the loan drawdown, novation and repayment, and the smart contract functionality of DLT could potentially also be used to 'program' the automatic execution and settlement of more complex multi-stage and multi-party transactions involving conditions and interdependencies. While many of these potential benefits of using CBDC for the settlement of tokenised asset transactions could be achieved through the use of existing ('off-chain') payment systems, doing so could introduce additional risks and complexities that would need to be explored.

As regards the technology, the POC demonstrated that an enterprise-grade DLT platform with appropriate controls on access and security could address many of the possible requirements on a wholesale CBDC and tokenised assets platform, including in relation to certainty over transaction finality, efficiency, security and privacy. That said, the scope of the POC was necessarily limited and did not focus on non-functional requirements (for example, the scalability of the system, or how it would address cyber risk). Further exploration and testing of the technology would therefore be required to assess its suitability for a production system.

Overall, this project demonstrated many of the potential benefits and implications of issuing a wholesale CBDC to settle transactions in tokenised assets on DLT platforms. However, as is to be expected in a research project such as this, the project has also highlighted a range of additional questions and issues that need to be explored to help address the question of whether there is a case for a wholesale CBDC and how one could be developed. This project also demonstrated the benefits of collaboration in advancing the participants' knowledge and understanding of the role that CBDCs and asset tokenisation could play in shaping the future of finance.

1. Introduction

In recent years, technological innovation in relation to blockchain and DLT has stimulated considerable research and experimentation related to tokenised assets. The tokenisation of assets is the process of creating digital tokens that represent ownership rights to real-world assets, which can be traded, stored and transferred on DLT platforms. The use of DLT and smart contracts in asset tokenisation has the potential to deliver a number of benefits, including improving the efficiency, transparency, liquidity and accessibility of asset markets. While much of the focus has been on tokenising traditional financial assets, such as loans and equities, it could potentially be applied to a wide range of assets, both tangible and intangible. Interest in asset tokenisation has also stimulated discussion about the role of CBDCs and what role they might play in facilitating activity in tokenised asset markets.

Many central banks are currently researching the potential benefits and other implications of issuing CBDC as a complement to existing forms of money. In most economies, including Australia, the bulk of money already exists in digital form as deposits with commercial banks, which are used by households and businesses to make payments using a variety of electronic payment services. Central banks also provide digital money in the form of balances held in accounts that commercial banks and a few other types of financial institutions can hold at the central bank to settle payment obligations between each other. The only form of central bank-issued money that is universally accessible is physical money in the form of banknotes (i.e. cash). A CBDC would be a new digital form of money issued by, and therefore a direct liability of, a central bank. It could be designed for retail (or general purpose) use, which would be like a digital version of cash that is essentially universally accessible, or for wholesale use, where it is accessible only to a more limited range of wholesale market participants (such as financial institutions and large corporates, for example) for use in wholesale payment and settlement systems (Figure 1).[1]

1 This figure draws on Bjerg O (2017), 'Designing New Money: The Policy Trilemma of Central Bank Digital Currency', Copenhagen Business School, CBS, MPP Working Paper.

Figure 1: Different Forms of Money

The RBA has been researching CBDC for a number of years, looking at both retail and wholesale use cases. In 2020, the RBA published an article that outlined some of the possible design considerations, and the case for and potential implications of issuing a retail CBDC.[2] The article noted that while there was not a strong public policy case for issuing a retail CBDC in Australia at present, the RBA would continue to consider the case for a retail CBDC, including how it might be designed, the various policy implications and potential use cases.

Separate to its work on retail CBDC, the RBA has also been exploring a wholesale form of CBDC. In a speech in 2017, the RBA Governor noted that the RBA was open to exploring whether there was a case to issue a CBDC in the form of digital tokens that could be exchanged between wholesale market participants in specialised payment and settlement systems based on DLT.[3] Such a system could function as an alternative to the RBA's existing real-time gross settlement (RTGS) system, RITS, which commercial banks already use to settle payment obligations between themselves using the balances in the Exchange Settlement Accounts (ESAs) they hold with the RBA.

This type of CBDC could offer benefits in terms of allowing payment and settlement processes to be more closely linked with other business processes on a DLT platform (for example, the trading of other tokenised assets), which may generate efficiencies or risk reductions for businesses. CBDC tokens might also be able to be programmed using the smart contract functionality of DLT platforms, enabling multi-stage transactions with potentially complex dependencies to take place securely and automatically.

2 See: Richards T, C Thompson and C Dark (2020), 'Retail Central Bank Digital Currency: Design Considerations, Rationales and Implications', RBA Bulletin, September.

3 Lowe P (2017), 'An eAUD?', Address to the 2017 Australian Payment Summit, Sydney, 13 December.

The RBA commenced technical experimentation on wholesale CBDC in 2018–19 with the development of a POC of a tokenised form of CBDC issued on a private, permissioned Ethereum network. The POC simulated the issuance of central bank-backed tokens to commercial banks in exchange for ESA balances, the exchange of these tokens among the commercial banks, and their eventual redemption back to the central bank. The project was useful in exploring the technical features of DLT and its potential use in implementing a CBDC. While DLT may offer some benefits in terms of resilience, the project highlighted a number of other features associated with the decentralised nature of the technology that could limit its suitability for implementing a CBDC, including in relation to transaction privacy, finality, throughput and efficiency. The limited scope of the POC – involving only the central bank and commercial banks – also highlighted that there were few functionality benefits compared with the RBA's existing RTGS system that banks can already use to settle their payment obligations. These findings highlighted the need for further research to explore the potential use cases for a wholesale CBDC and how one might be implemented.

Aside from the RBA's research, the Australian market has also seen the development of some other significant DLT initiatives with participation from multiple stakeholders across financial institutions, corporates and technology companies:

- CBA has developed DLT projects spanning fixed income, agricultural commodities, small business loans and retail payments. CBA's most notable project was 'Bond-i', one of the first digital bonds to be issued and managed on a blockchain platform globally. Bond-i is a A$110 million digital bond issued by the World Bank with eight institutional investors (including QBE, Northern Trust and TD Securities among others) on an Ethereum-based platform built by CBA's Innovation Lab.
- ANZ, CBA and Westpac have formed a new venture, Lygon, in partnership with IBM and Scentre Group. Launched in 2019, Lygon's blockchain solution (built on Hyperledger Fabric) enables the digitisation and automation of bank guarantees for retail property leasing.
- ASX Ltd started in 2017 an ambitious project to replace CHESS, its core equities clearing and settlement infrastructure, with a new DLT-based solution developed in partnership with Digital Asset, a New York-based technology company. While the initiative is currently focused on the upgrade of equities post-trade infrastructure, ASX has stated that this marks the first step of its digital asset strategy, which the exchange intends to extend to other asset classes and services in the coming years.

Box: CBDC developments

In recent years, central banks have been increasingly interested in CBDC, with more than 85 per cent of central banks 'engaged in' some form of work on CBDC according to an October 2020 survey.[4] Motivations for carrying out work on retail and wholesale projects differ, however, as do the motivations in emerging and advanced economies.

Emerging economies' motivations for retail CBDC projects tend to be related to improving financial inclusion through greater access to payment services to unbanked residents and enhancing their domestic payments systems more generally. Notable examples include China's retail CBDC project, the eCNY, which has progressed to a series of city-wide pilots, and the launch of the Bahama's 'Sand Dollar' in October 2020. In contrast, advanced economies' motivations for retail CBDC projects tend to relate to enhancing payments system efficiency, safety and robustness.

Both advanced and emerging economies consider improving the efficiency of cross-border payments as a key motivation for wholesale CBDC. This is reflected in a range of international work programs, such as the Financial Stability Board's Roadmap to Enhance Cross-Border Payments, which is endorsed by the G20 and includes work to explore the role of new payment arrangements, including CBDC. In addition, enhancing settlement processes for digital assets remains a key motivation for central banks' exploration of wholesale CBDC. This is reflected in a number of wholesale CBDC projects, such as:

- Project Helvetia, a joint POC by the Bank for International Settlements Innovation Hub Swiss Centre, SIX Group AG and the Swiss National Bank, which explored the integration of tokenised assets and central bank money on a distributed ledger as well as the linking of DLT to existing payment systems.
- Project Ubin Phase 3, a collaborative project between the Monetary Authority of Singapore and Singapore Exchange, which developed a tokenised form of the Singapore dollar on a DLT platform with capabilities for the DvP settlement of tokenised assets.

Project Atom contributes to the breadth of CBDC research by exploring the implications of extending access to wholesale CBDC to non-bank wholesale market participants and the implications of atomic DvP settlement on a DLT platform.

4 Boar, C and A Wehrli (2021) 'Ready, steady, go? – Results of the third BIS survey on central bank digital currency', Bank for International Settlements Papers No. 114, January.

2. Overview of Project Atom

In late 2020, the RBA, CBA, NAB, Perpetual, and ConsenSys agreed to collaborate on a project, known as Project Atom, to explore the potential use and implications of a wholesale form of CBDC, building on the research the RBA conducted in 2018–19. The objective of the project was to develop a functional POC to demonstrate how a wholesale CBDC could be issued and used for the settlement of a tokenised asset on a DLT platform. The project extended the RBA's initial in-house project in three main ways:

- It explored how access to a tokenised CBDC could be extended to a wider range of wholesale market participants, including those that would not ordinarily have access to ESAs at the RBA.
- It integrated another digital asset in the form of a tokenised syndicated loan that allowed for exploration of the implications of 'atomic' DvP settlement as well as other potential benefits of combining CBDC and tokenised assets on interoperable DLT platforms.[5]
- It explored how an enterprise-grade version of the Ethereum blockchain platform could deal with some of the technical limitations of the public version used in the RBA's initial project.

The POC incorporated a two-tier distribution model for the issuance and distribution of the CBDC. In this model, the central bank is responsible for issuing CBDC to commercial banks who hold ESAs (**ESA holders**), who are in turn responsible for making the CBDC available to eligible wholesale market participants (**sponsored participants**). The ESA holder acts as a sponsor for these participants and is responsible for ensuring that only eligible parties can access the CBDC. This contrasts with a model of universal access (i.e. a retail CBDC), which would raise a number of very different challenges and considerations and was beyond the scope of this project. The advantage of a two-tier distribution model, rather than one in which the central bank makes CBDC available to wholesale market participants directly, is that the sponsor commercial bank retains responsibility for a wide range of customer-facing activities that a central bank is unlikely to have a comparative advantage or risk appetite to engage in, such as customer support, know your customer (KYC) and probity checks, transaction monitoring for compliance with anti-money laundering (AML) and counter-terrorism financing (CTF) obligations and general account-keeping services.

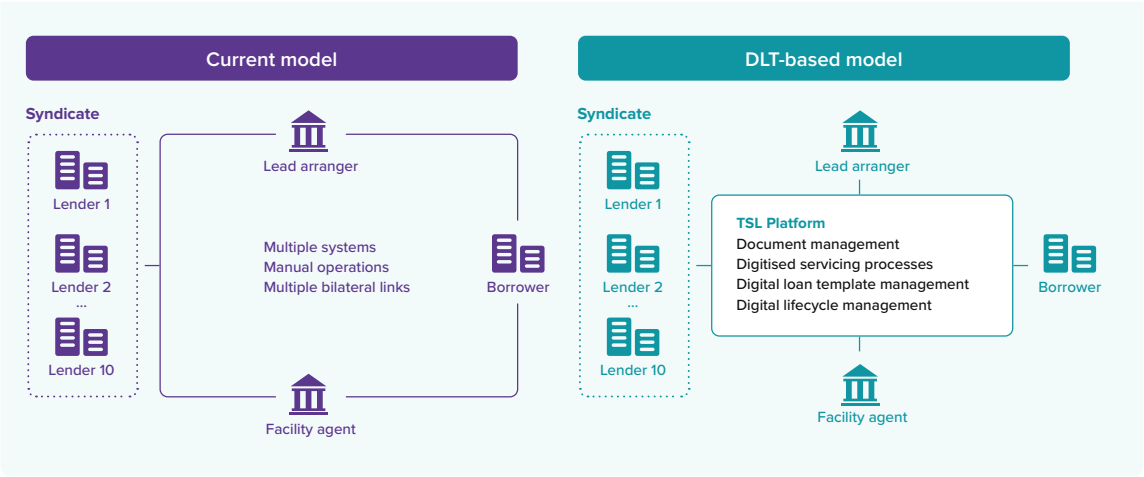
5 Atomic DvP refers to a settlement process by which a transaction is executed and settled in an integrated and instantaneous fashion such that the delivery of the asset and the associated payment occur simultaneously and in a way that ensures that one leg cannot occur unless the other does. Traditionally, these legs occur in separate systems and although they may be designed to occur simultaneously, they may well have delays or occur at different times due to separation between each system.

2.1 Syndicated lending

This project explored the use of wholesale CBDC for the funding and repayment of a tokenised syndicated loan. A syndicated loan is a loan between a syndicate of lenders (usually banks) and a borrower entered into through a syndicated facility agreement (SFA) and usually used to fund large projects or borrowers. In the Australian market, SFAs are typically bespoke, high-value, and low-volume corporate financing instruments.

An SFA is usually established through a **lead arranger**, which is responsible for structuring the facility and marketing it to other **lenders**, who form part of the syndicate, on behalf of a **borrower** (Figure 2). The lead arranger may also underwrite the facility for an additional fee, lending funds to the borrower prior to or during the establishment of the syndicate. The SFA is administered by a **facility agent** (which could be one of the syndicate lenders or some other third party), which acts as the primary point of communication between the parties. The facility agent also manages the initial flow of funds to the borrower and the repayment of the loan by the borrower. Settlement and repayment of syndicated loans occurs through existing payment rails provided by the banks.

Figure 2: Syndicated Lending
Stylised models

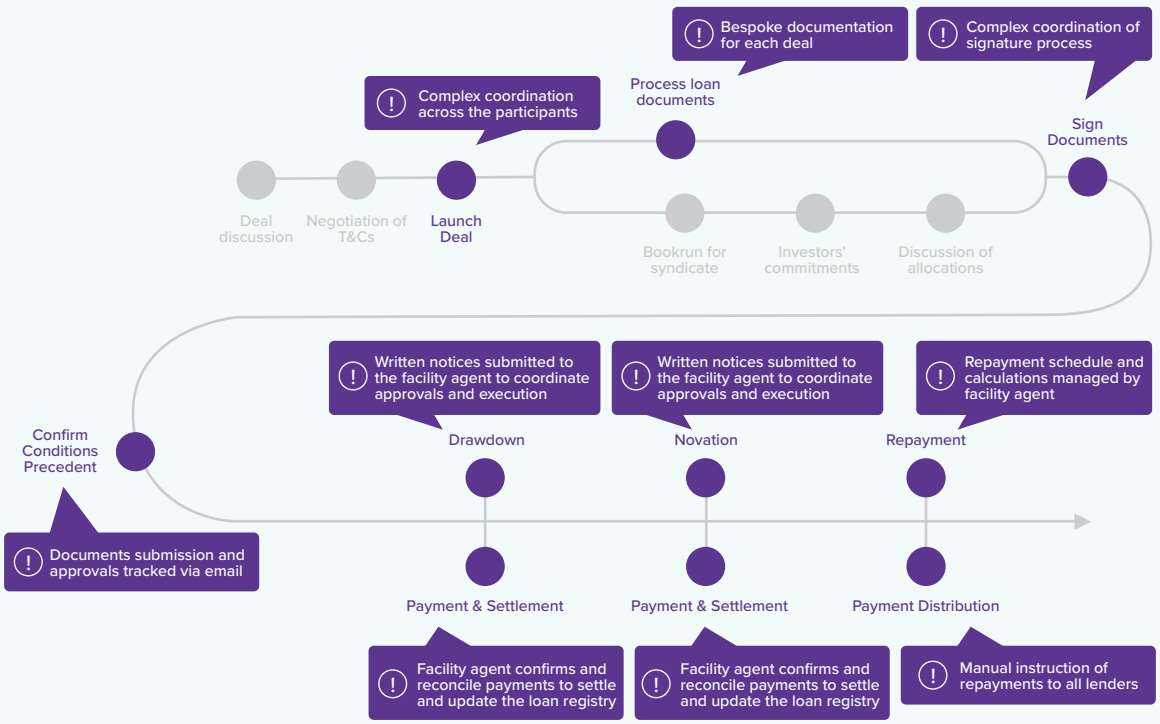


Syndicated loans were chosen as the use case for this project for a number of reasons:

- They involve multiple participants who have overlapping roles, including intermediaries who administer the facility and lenders.
- All participants, including the borrower, are wholesale market participants.
- At settlement, all parties are required to have agreed to the same terms and a large amount of funds must be transferred in a manner where time and certainty of settlement is important.

The distributed nature of the syndicated lending market also makes it an interesting use case in which to experiment with DLT. Indeed, independent of any CBDC aspects, the use of DLT could provide benefits by providing a single, technologically immutable record of the SFA that all parties can access without relying on a central intermediary. In addition, DLT could provide benefits through digitisation and automation of the manual and paper-based processes that are still common in the syndicated lending market (Figure 3).

Figure 3: Current Syndicated Loan Process



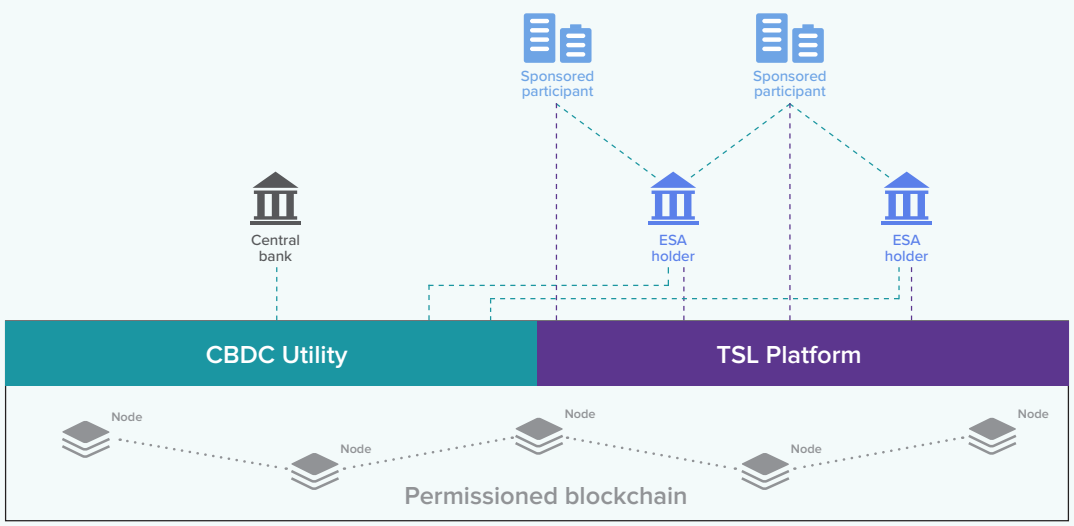
2.2 Design of the proof-of-concept system

The POC involved the development of two interlinked components:

1. A **CBDC Utility**, which manages the issuance, transfer and redemption of a wholesale CBDC.
2. A Tokenised Syndicated Loan Platform (**TSL Platform**), which manages the issuance, drawdown, novation and repayment of a tokenised syndicated loan.

Both components share a private and permissioned blockchain network built on Hyperledger Besu, an enterprise-grade Ethereum client (Figure 4).[6,7] In the POC system, the RBA, CBA, NAB and Perpetual were each assigned a node on the network that holds a copy of the ledger (i.e. a record of all transactions in each of the CBDC Utility and the TSL Platform).[8] Each time a transaction is processed, all nodes are synchronised using a process to share and verify updates.

Figure 4: Proof-of-concept System



6 In addition to Hyperledger Besu, the DLT platform consists of several other ConsenSys and third-party components that provide additional functionality, such as management of the blockchain network and transaction privacy. Refer to Appendix A for the technical architecture.

7 As a private network, access to both view transactions on the platform and operate the platform is limited. In a permissioned network, existing participants who operate the platform must authorise any new participant to connect to the network. Permissionless networks, which are common in public DLT platforms such as Bitcoin, allow any person to operate a node.

8 There was also a fifth node managed by ConsenSys for monitoring purposes. See Appendix A for more detail on the technical design.

Although each node holds a record of all transactions on the ledger, various privacy restrictions were implemented so that only certain transactions are able to be viewed or accessed by each participant. For example, each ESA holder can only view transactions it is a party to in the TSL Platform, and in the CBDC Utility, an ESA holder can only view its own transactions or transactions that relate to its own sponsored participants. Further, a sponsored participant is only able to view the records in the ledger that relate to its own accounts or transactions to which it is a party. Access to this information would be made available by their sponsoring ESA holder.

A key feature of the POC is that the CBDC Utility and the TSL Platform are interoperable. This enables atomic DvP settlement of transactions in the tokenised syndicated loan, with the change in ownership/status of the loan (delivery) occurring simultaneously with the transfer of the CBDC (payment). The following sections outline the key functional aspects of the design for the CBDC Utility and the TSL Platform, and how their interoperation enables atomic DvP settlement.

2.3 CBDC Utility

In the POC, the CBDC Utility is administered by the RBA, as the central bank. Access to the CBDC Utility is restricted to ESA holders and sponsored participants. This arrangement reflects the two-tier model for issuing CBDC, in which CBDC is issued by the RBA and made available either directly to ESA holders or indirectly to sponsored participants. ESA holders would be responsible for onboarding and making CBDC available to their sponsored participants and for all other customer-facing activities.

CBDC is issued ('minted') by the RBA in response to a request via the CBDC Utility from an ESA holder (either as a direct request or indirectly following a request from one of its sponsored participants). While the POC did not build any connection with RITS, a database and APIs were used to mimic the link between off-chain ESAs and the on-chain ledger. The design envisaged that on receipt of a request for CBDC, the RBA would:

- debit the ESA balance of the ESA holder (or the sponsoring ESA holder) by the amount of CBDC requested
- credit that amount to an 'omnibus' account in RITS[9]
- issue ('mint') CBDC tokens on the CBDC Utility into the 'wallet' of the ESA holder (or its sponsored participant).[10]

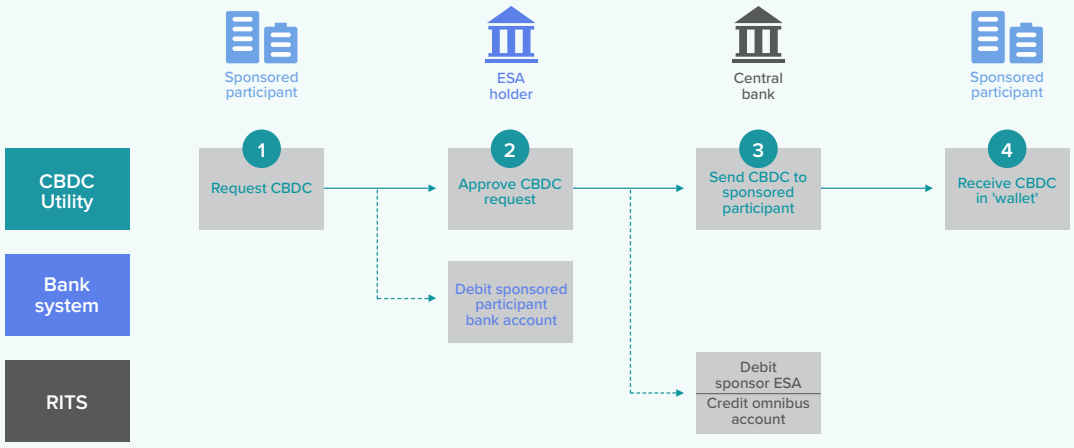
9 An omnibus account would be a new type of account in RITS that co-mingles the funds of different ESA holders and backs all of the CBDC tokens on issue. The advantage of this structure is that transactions in CBDC tokens that have already been issued can occur without the ESA balances of the relevant participants having to be continually updated.

10 A wallet corresponds to a unique address on the Ethereum network for each participant that holds CBDC either directly or through a sponsoring ESA holder. A sponsored participant may have more than one unique address if they have more than one sponsoring ESA holder.

The redemption process to convert CBDC back into another form of money would work in reverse: CBDC tokens on the CBDC Utility are destroyed ('burned'), the omnibus account in RITS is debited and the relevant ESA holder's ESA balance is credited. Issuance and redemption of CBDC for sponsored participants follows the same process, but the request must also be approved by the participant's sponsor ESA holder. The sponsor ESA holder would also debit/credit the account that the sponsored participant has with the ESA holder as payment for the CBDC (Figure 5).[11]

In addition to requesting issuance and redemption of CBDC, participants can also use the CBDC Utility to transfer CBDC from one wallet to another.[12]

Figure 5: CBDC Transaction Flow
Acquisition of CBDC by a sponsored participant*



* The POC used databases to simulate the activity in RITS and commercial bank systems.

At any point in time, the balance in the omnibus account in RITS would represent the total amount of CBDC on issue. CBDC would be a claim on the assets in the omnibus account, being a liability of the RBA. Because of the use of the omnibus account, the RBA would not need to keep a live record in RITS of who holds the CBDC on issue at each point in time. This overcomes the challenges of real-time reconciliation between RITS and the CBDC Utility and also has the advantage that CBDC can continue to be transferred between participants using the CBDC Utility even if the connection to RITS was down (although further issuance and redemption would not be possible in this case).

11 Processes undertaken by an ESA holder outside the CBDC Utility and the TSL Platform (such as maintaining a record of CBDC held by a sponsored participant) were not considered as part of the POC.

12 The minimum denomination of CBDC tokens was initially set at A$1 but had to be increased to A$1,000 (i.e. 1 CBDC token = A$1,000) to deal with performance issues associated with the privacy-related encryption process implemented in the POC – see Appendix A4 for more details.

The tiered distribution model for CBDC is reflected in the structure of CBDC wallets held on the DLT platform (and accessed via the CBDC Utility). ESA holders have their own wallets, but they also host wallets for their sponsored participants, with the relationship maintained via a digital registry.[13] The model also allows sponsored participants to have a CBDC wallet with more than one ESA holder (similar to operating multiple commercial bank accounts). The POC was configured so that the RBA could monitor use of CBDC by all participants onboarded to the CBDC Utility, regardless of whether they are ESA holders or sponsored participants. ESA holders, meanwhile, facilitate and monitor use of the CBDC Utility for the participants they sponsor.

Once onboarded to the CBDC Utility, both ESA holders and sponsored participants can use a web-based interface to acquire, transfer and redeem CBDC. These instructions are facilitated by a set of automated rules and conditions governed by the RBA. In particular:

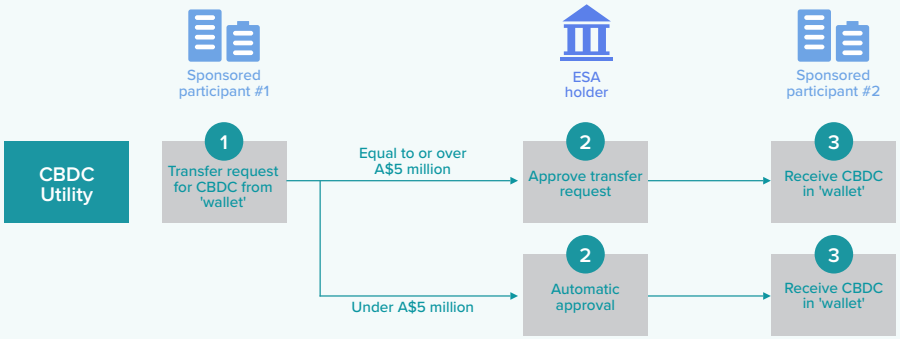
- Instructions from ESA holders are automatically processed by the CBDC Utility without requiring approval by the RBA.
- When an instruction is received from a sponsored participant, the CBDC Utility requires the instruction to be approved by the participant's sponsor ESA holder. This is because issuance/redemption of CBDC ultimately impacts the sponsor's ESA. Before CBDC can be acquired or redeemed by a sponsored participant, its sponsor ESA holder needs to review the instruction and approve it (otherwise it expires within a certain timeframe). Upon approval to issue/redeem, the ESA holder would debit/credit the deposit account that the participant holds with the sponsor and funds are automatically transferred between the ESA holder's ESA and the omnibus account as required.[14] The CBDC Utility then issues/redeems CBDC in the sponsored participant's wallet.

Transfers of CBDC between participants of the CBDC Utility are also governed by a set of programmable conditions that could be defined by the RBA. For example, the transfer amount is validated in the account of the ESA holder or the sponsored participant before the instruction for the transaction can be submitted. If the amount transferred is greater than A$5 million, the CBDC Utility was configured to require the approval of the recipient before processing, as a way to reduce errors and assist in reconciliation (Figure 6). There are a range of other programmable conditions that could have been implemented using smart contracts to improve the functionality and efficiency of the system. For example, it would be possible to validate that a recipient was authorised to use the platform and control the use of CBDC tokens in particular types of transactions.

13 A digital registry, implemented through a smart contract, captures and maintains the relationship between sponsor ESA holders and their respective sponsored participants.

14 Any debit/credit to the sponsored participant's bank account would be handled through the bank's own internal ledger system.

Figure 6: CBDC Transaction Flow
Transfer of CBDC between two sponsored participants, with optional sponsor approval



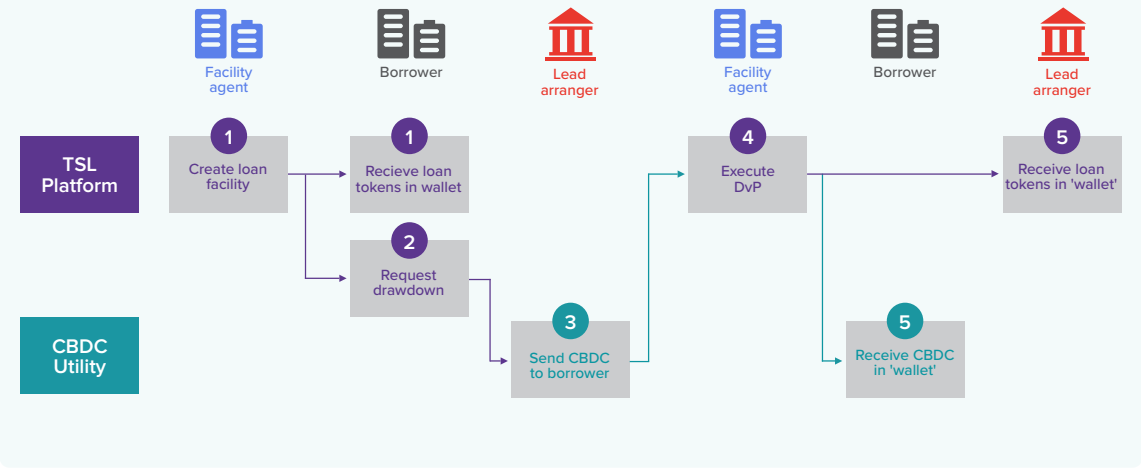
2.4 TSL Platform

The TSL Platform manages the issuance, drawdown, novation and repayment of an underwritten syndicated loan facility. The platform is administered by the facility agent and enables the automation of business processes and data sharing between the lead arranger, facility agent, lenders and the borrower. It is important to note that the project only focused on the digitisation of back-office functions related to the origination and servicing of a syndicated loan facility. It did not cover business processes that precede the establishment of a facility, including negotiations between the lead arranger and borrower regarding the structure and terms of the facility or documenting and marketing the facility to lenders. Nor did it consider the necessary legal requirements, as this was beyond the scope of the POC.

The facility agent is responsible for configuring the syndicated loan on the TSL Platform, which creates a smart contract with portions of the loan represented by digital tokens that can be transferred between participants.[15] Each loan token contains the key information about the syndicated loan (e.g. amount and interest rate) and represents A$1 of debt that has been made available to the borrower (i.e. the tokens represent a claim on the borrower). When the loan agreement is approved on the TSL Platform, the loan tokens are initially issued to the borrower in an 'undrawn' state and are only allocated to lenders in a 'drawn' state once drawdown of the loan occurs (Figure 7).

15 Smart contracts are self-executing computer code running on a DLT platform which automatically perform various functions. They allow parties to enter into agreements knowing that they will be enforced without the need to trust each other.

Figure 7: Tokenised Syndicated Loan
Facility creation and drawdown

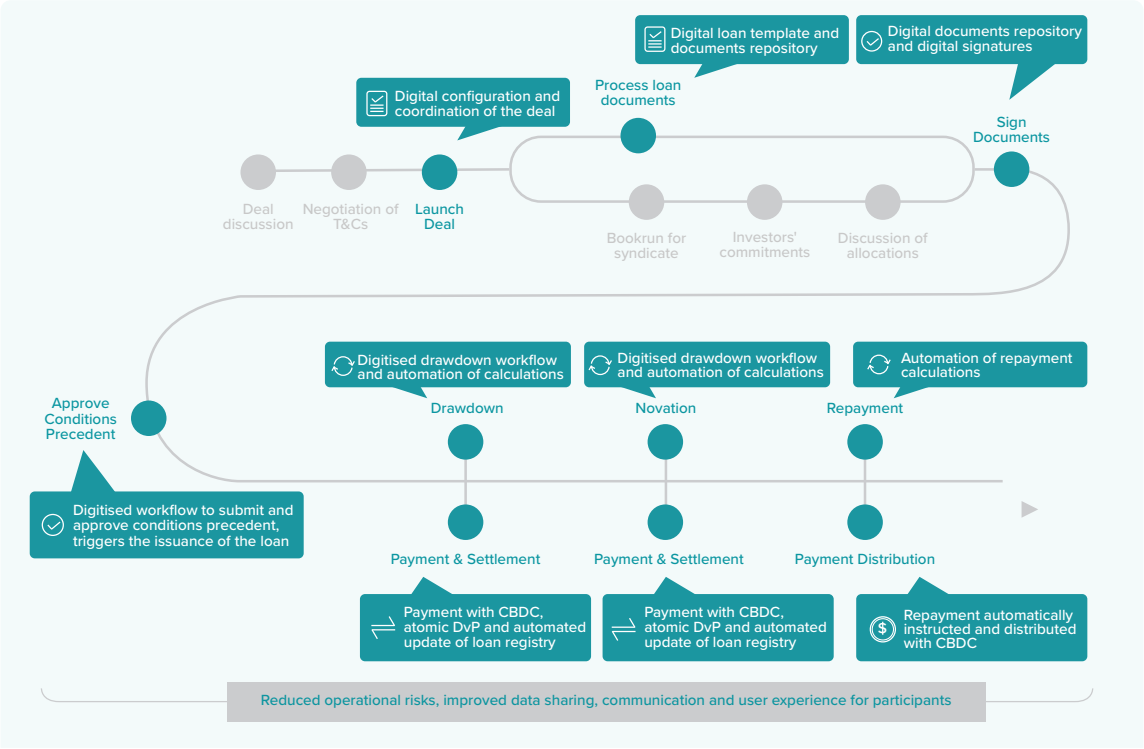


The loan tokens allow the TSL Platform to maintain an accurate record of the positions of each participant in the syndicate, as well as manage the drawdown, novation and repayment of the loan. For example, the novation of a syndicated loan would involve the transfer of 'drawn' loan tokens from the wallet of one lender to another. The TSL Platform also ensures that data related to a syndicated loan are only accessible to participants of that facility. This is important in a system where financial institutions may participate together in one facility, but not in others.

The TSL Platform uses digital workflows, smart contracts and digital signatures to streamline a number of steps in the syndicated loan lifecycle (Figure 8). These steps demonstrate how an SFA may be entered into, but the project did not consider the legal requirements of executing an SFA. Examples of the TSL Platform tasks include:

- The creation of a loan facility, which embeds information such as the facility limit, the parties involved, the interest rate, the facility start/end date and any applicable fees (e.g. commitment fees) into a smart contract. Digital documents are also uploaded and stored in the platform, including term sheets and other loan documentation.
- Drawdown approval, which involves the use of digital signatures to sign loan agreements and confirm that the conditions precedent have been met.
- Automatic calculation of fees related to the drawdown, novation and repayment of the loan facility.

Figure 8: Lifecycle of a Tokenised Syndicated Loan
Streamlined process



2.5 Platform interoperability and DvP settlement

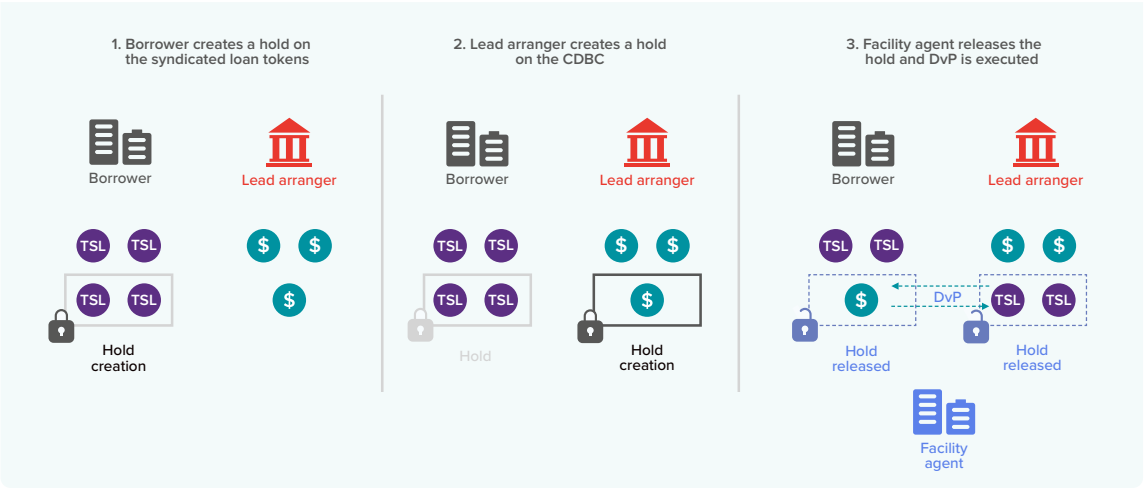
A key objective of this project was to examine how CBDC could be used during the lifecycle of a tokenised syndicated loan. The CBDC Utility and TSL Platform were designed to facilitate the use of CBDC at the following points in the lifecycle of a tokenised syndicated loan:

- **Initial drawdown of the loan.** The lead arranger uses CBDC to fund the initial drawdown of the loan. Settlement occurs when ownership of the loan tokens transfers from the borrower to the lead arranger, the status of the loan tokens is updated from 'undrawn' to 'drawn' and the required amount of CBDC tokens is transferred from the lead arranger to the borrower.
- **Novation to incoming syndicate lender.** An incoming syndicate lender uses CBDC to purchase a share of the loan from the lead arranger (or another syndicate lender). Settlement occurs when ownership of the loan tokens transfers from the lead arranger (or existing syndicate lender) to the incoming lender and the required amount of CBDC tokens is transferred from the incoming lender to the lead arranger (or other syndicate lender).
- **Repayment of the loan.** The borrower uses CBDC to repay the loan. Settlement occurs when CBDC tokens are transferred from the borrower to the lender(s) and the equivalent amount of loan tokens is destroyed.[16]

16 The POC was designed for a term loan facility where loan tokens are destroyed when the loan is repaid. However, it would also be possible to accommodate a revolving credit facility whereby repaid loan tokens are returned to the borrower in an 'undrawn' state, where they can be re-used for further borrowing.

In each case, the issuance, transfer, or destruction of the loan tokens (delivery) occurs simultaneously with the transfer of the CBDC tokens (payment). The POC system facilitates this through the use of a 'lock-up' mechanism, which prevents the transfer of the CBDC and loan tokens before performing the atomic (or simultaneous) DvP settlement (Figure 9).

Figure 9: DvP Settlement
Initial loan drawdown



The lock-up mechanism is implemented through a smart contract on the CBDC Utility. The smart contract allows participants to place a time-bound hold on the CBDC and loan tokens for use in a specific transaction. This prevents CBDC or loan tokens from being transferred until the 'hold' is removed, a specified period of time has elapsed, or the corresponding action occurs, 'atomically' settling the transaction and delivering the asset. The use of this form of smart contract has several benefits. It eliminates the risk of double spending of CBDC or loan tokens, which could lead to a settlement failure, and it allows participants to control their tokens until the transaction is completed. A participant can remove the hold on their CBDC or loan tokens at any time, but the smart contract will delay settlement until both of the holds have been established. The smart contract removes the need for an intermediary (typically the facility agent) to have custody of the CBDC or loan tokens during settlement.[17]

Besides coordinating and executing the DvP settlement process, smart contracts also automate a number of other aspects of loan transactions, including fee calculations (i.e. calculating the net proceeds to be paid to the borrower at loan drawdown after fees) and tracking changes in ownership of the loan tokens (i.e. tracking changes in outstanding obligations to each lender). While not implemented in the POC, it would also be possible to incorporate external data sources into smart contract calculations.[18] For example, a smart contract could use a benchmark rate to determine repayment amounts, or draw on external data to automatically monitor compliance with loan covenants.

17 Note that this smart contract is not intended to change the legal rights to the tokens, it is merely a technological feature designed to facilitate DvP settlement.

18 An oracle is a third-party service that provides information from external data sources to enable smart contracts to take actions based on data that is not stored on the DLT platform.

3. Non-functional requirements

This section discusses some of the non-functional requirements of a wholesale CBDC and tokenised syndicated loan platform and how they have been addressed in the POC.

3.1 Efficiency and transaction finality

The decentralised nodes in a DLT platform reach agreement on the current state of the ledger and remain synchronised by participating in a process known as 'consensus'. The consensus mechanism typically used in public, open-access ('permissionless') platforms such as Bitcoin or Ethereum is designed to allow verification of the ledger between parties that do not necessarily know or trust each other; this form of consensus, known as 'proof of work', is inefficient and generally characterised by high energy use and low throughput. It is also a probabilistic form of consensus, meaning that true settlement finality can take some time as it relies on there being sufficient confidence that a transaction is properly incorporated in the ledger. For example, Bitcoin transactions are not considered final until around an hour has passed from the transaction being added to the ledger, while Ethereum transactions are only considered final after about a minute.[19] This type of consensus mechanism would be inappropriate for a wholesale payment system, where settlement must be immediate, final and irrevocable.

To address this issue, the POC used a different consensus protocol known as 'proof of authority' that is more appropriate for a private, permissioned network where participants know and trust each other. This approach assigns a number of nodes as 'validator nodes' that take turns (rather than compete) to verify and add transactions to the ledger in a round-robin arrangement. Once added to the ledger, transactions are considered final and irrevocable. This more efficient consensus process allows a significantly higher number of transactions per second to be processed than the public version of Ethereum. However, the actual rate of transaction throughput can vary depending on a range of factors, such as the number of nodes in the network, network speeds and the complexity of transactions.

The POC was not developed with high throughput and scalability as key requirements and so this aspect has not been a focus of the testing. However, demonstrations suggest that the system processes most transactions in about 10–15 seconds. This may be adequate for a low-volume use case like syndicated loans, but may not be adequate for higher-volume use cases like retail payments, trading shares or other financial products. Further research would be necessary to test the efficiency and scalability of different DLT platforms for particular CBDC use cases and to also compare this with other technologies.

19 These times can vary depending on the throughput on the network.

3.2 Confidentiality and privacy

Ethereum, like most other public blockchain platforms, does not provide for transactions to remain confidential. This is because the record of all transactions on the ledger is broadcast to all nodes, which is a key requirement for validating transactions and maintaining the integrity of a decentralised network. Moreover, while the parties to a transaction are only identified by their blockchain address, which is a random alphanumeric string that contains no personal information, this is a pseudonymous form of identity, as it is possible to identify a user from knowledge of the entities with whom you have previously transacted. Addressing these privacy shortcomings was a key focus for the POC.

3.2.1 CBDC Utility

The POC implemented a privacy protocol for Ethereum called Aztec that encrypts transaction information so that only parties to the transaction can see the details of the transaction. Aztec uses a technique known as 'zero-knowledge proofs', which allows the necessary logical checks to be performed by a validator node to verify transactions without the need for the underlying transaction information to be revealed (see Appendix A for further details). CBDC transaction information is encrypted, which allows participants that are not a party to a transaction to see that a transaction occurred, but not the information about the transaction, such as the payer, payee or amount. For the POC, the privacy solution was configured so that ESA holders have visibility of the CBDC transactions of their sponsored participants, and the RBA has visibility of all CBDC transactions given its role as administrator of the CBDC Utility.

The Aztec privacy protocol addressed many of the privacy concerns associated with Ethereum. However, its application in the POC did give rise to unforeseen performance issues. In particular, it was found that the computational demands of implementing the encryption process increase sharply when a large number of tokens have been minted. When the minimum denomination of CBDC tokens was initially set at A$1, it resulted in unreasonably slow transaction times. A work-around was to increase the minimum denomination of CBDC tokens (from A$1 to A$1,000) to reduce the number of CBDC tokens on issue at any given time. While this alleviated the performance issues, it meant CBDC holdings and transactions must be in multiples of A$1,000, reducing the flexibility of the CBDC as an alternative to digital account-based payment systems. Ideally, the minimum value of a CBDC token would equal one cent so that tokens and amounts in ESAs are fully fungible and convertible one-for-one.

There is research underway in the DLT community to address this issue. The forthcoming version of the Aztec privacy protocol is expected to be significantly more efficient from a computational perspective.

3.2.2 TSL Platform

A different approach was used to ensure loan transaction privacy in the TSL Platform. An 'allow list' in the smart contract registry ensures that only participants that are a party to a loan facility are able to view information related to the facility. This information includes the identities of other participants, distribution of loan shares and financial information relating to the facility and borrower. For the purpose of this project, the POC was configured such that the RBA did not have access to the TSL Platform, nor did it have visibility of information related to individual facilities. However, the platform could easily be configured to provide the RBA or any other relevant authority with access to some or all of the information on a particular tokenised loan facility.

3.3 Security and resilience

Because the POC was only intended to demonstrate how DLT could be used to implement interoperable CBDC and a tokenised syndicated loan facility, security and resilience were not core requirements driving the POC design. It would therefore be inappropriate to draw conclusions on how secure or resilient this kind of system would be if it was developed. Nonetheless, the POC incorporated a number of features common to DLT platforms that indicate how security could be managed in a distributed system:

- Access to the private and permissioned blockchain network was restricted to authorised nodes. In practice, it is likely these nodes would be operated by, in respect of the CBDC Utility, the RBA and some or all of the ESA holders, which would be authorised by the RBA, and in respect of the TSL Platform, the lead arranger, facility agent and lenders.
- Cryptographic techniques using public/private keys are used to access accounts and to sign and submit transactions on the DLT platform.[20] ESA holders would be responsible for managing their own private keys and the private keys of their sponsored participants.
- Access to the CBDC Utility is restricted to authorised users that have been nominated by the RBA or sponsored by an ESA holder. Similarly, access to the TSL Platform is restricted to authorised users that have been sponsored by an ESA holder. In the POC, participants accessed the CBDC Utility and/or TSL Platform using a username and password. More advanced access controls, such as two-factor authentication, could also have been implemented.

20 Public/private key cryptography is a form of encryption that uses two different keys: a private key (that a user keeps secret) and a public key that can be shared with others. When a user signs a transaction, their private key is used to generate a random string of characters or 'hash' that is attached to the transaction. Other participants can then apply the user's public key to the hash to verify that the transaction was submitted by the authorised user and that the contents of the transaction are correct and have not been altered.

The POC highlights a number of potential resilience benefits for the settlement of syndicated loan transactions compared to using RITS, which is typically how drawdowns of these loans would be settled. Because it is based on a completely different technology to RITS, a DLT-based CBDC system may be less susceptible to an outage or cyber-attack that affects RITS. In addition, because it is distributed rather than centralised, the system can continue to operate even if one or more of the participant nodes (including the RBA) are offline. However, there are two cases where the functionality of the POC system would be limited due to an outage to RBA systems or one or more of the nodes:

- The RBA holds a unique role in the POC system as the issuer of CBDC tokens and operator of RITS. In the event of an outage to RBA systems (e.g. RITS), requests by participants to issue or redeem CBDC tokens would be unable to be processed. Participants could, however, transfer CBDC issued prior to the outage to RBA systems. This risk would be mitigated through the RBA's usual business continuity and back-up arrangements.
- As noted earlier, the POC uses a form of consensus known as 'proof of authority', which relies on a small number of trusted validator nodes to verify transactions. This approach requires a minimum of four validator nodes for the network to function correctly and reach consensus; if there are fewer than four validator nodes the network will stop verifying transactions.[21] The risk of there not being enough operational validator notes could be reduced by running more nodes (e.g. by a greater number of ESA holders) or the running of multiple nodes by the RBA and/or ESA holders (as part of normal operations or business continuity arrangements). Consideration would also need to be given to operating nodes in dispersed geographic locations to reduce the risk of outages related to natural disasters, for example.

21 See Appendix A3 for more information on the consensus mechanism.

4. Policy, legal and other considerations

This section highlights a number of policy, legal and other considerations associated with a wholesale CBDC and tokenised syndicated loan platform that were discussed during the development of the POC. The project did not attempt to resolve or take a position on these issues, rather the purpose here is to highlight some of the issues that would need to be considered in further research.

4.1 Implications for monetary policy

4.1.1 Would interest be paid on CBDC balances and, if so, how?

The POC allowed for the possibility that interest could be paid on CBDC balances. This would be an important policy decision for the RBA, with potentially significant implications for how CBDC was used. One possibility would be to not remunerate CBDC balances; depending on the level of interest rates in the economy, this could create incentives to minimise overnight CBDC holdings.[22] Such an approach might be appropriate where the CBDC is mainly designed to facilitate payments rather than be a store of value. Alternatively, the RBA could pay interest on CBDC balances, possibly at the same rate as on ESA balances. A further decision is whether interest would be paid directly to the CBDC holder (whether an ESA holder or a sponsored participant) or just to the ESA holder (in respect of all CBDC held by it and its sponsored participant). In the latter model, it would be a commercial decision of the ESA holders as to whether and how they pay interest to their sponsored participants for their CBDC holdings.

4.1.2 Are there implications for the implementation of monetary policy?

The POC envisages that CBDC would be issued to ESA holders and their sponsored participants in exchange for ESA balances. The level of ESA balances is important for the RBA's monetary policy settings, including because it influences the cash rate (i.e. the interest rate on unsecured overnight loans of ESA balances between banks), which is targeted by the Reserve Bank Board and is the key short-term (near) risk-free benchmark rate in Australia. Accordingly, policy decisions around how this form of CBDC would be operationalised could have implications for how the RBA implements monetary policy. For example, if CBDC was primarily used to facilitate payments and earned no (or relatively little) interest, demand for CBDC may be fairly low, stable and predictable, and so the effect on ESA balances would likely be more manageable, at least in normal circumstances. On the other hand, if there was stronger demand to hold CBDC as a store of value (e.g. because it earned an attractive rate of interest and/or was seen as a safe asset, particularly by entities that ordinarily do not have access to ESAs), then this higher level of holdings could be associated with greater volatility of flows and therefore greater volatility in ESA balances (and potentially the cash rate).

22 A similar outcome could be achieved with a negative interest rate on CBDC balances.

The implications of a CBDC for control over ESA balances could also vary depending on liquidity conditions in domestic money markets. Where ESA balances are abundant, as they are at present, even sizeable demand for CBDC should have little impact on the cash rate. In contrast, where ESA balances are scarcer, as they have been historically, the RBA would need to be more responsive in offsetting changes in demand for CBDC to achieve the target cash rate.

4.2 Non-bank access to wholesale CBDC

As discussed previously, a key feature of the POC is that it extended access to central bank money (in the form of the CBDC) to non-bank wholesale market participants that are not otherwise eligible to hold an ESA. This was achieved using a two-tier model for issuing CBDC, in which CBDC is issued by the RBA to ESA holders, who in turn can facilitate the acquisition of CBDC by their sponsored wholesale customers.[23] This is a key point of difference from other wholesale CBDC projects (including the RBA's 2018–19 project), which have focused on the use of wholesale CBDC by commercial banks (which already have access to digital central bank money via their ESAs). Broadening access to CBDC does, however, raise a number of policy and legal issues, some of which are briefly discussed in this section.

In exploring how to provide wider access to CBDC, the presumption is that there would be a range of potential benefits of providing eligible non-bank wholesale market participants with access to CBDC for settling transactions and to hold as a store of value. For example, in the syndicated loans use case explored in this project, there could be efficiency and risk management benefits to the facility agent given its role in administering syndicated lending facilities, which involves coordinating payments between syndicate members. Non-bank wholesale participants would also benefit from having another option for where they could hold their liquid assets, and one that would also not carry any credit risk as it would be a claim on the central bank.

Under the model considered in this project, issuing CBDC transforms a liability on the RBA held by a commercial bank with whom the RBA has a relationship, into a liability on the RBA that can be held by a wider range of sponsored wholesale market participants with whom the RBA does not have a direct relationship. While issuing CBDC to sponsored participants is not intended to create a relationship between sponsored participants and the RBA, holding CBDC could be seen as holding a claim on a portion of the balance of the omnibus account. A detailed assessment of the implications of using an omnibus account structure in the issuance of CBDC was beyond the scope of the project and further work would be required to clarify the nature of the legal claim associated with holding a CBDC, especially where an entity does not otherwise have a relationship with the central bank.

23 Legally, the sponsored participant would hold a claim on the RBA. However, the nature of the arrangements between sponsored participants and their sponsor commercial banks was not considered as part of this project.

4.2.1 Implications for financial intermediation

The two-tier issuance model preserves several important aspects of the current role of commercial banks in the financial system, including their role in onboarding and providing services to their customers. Expanding access to CBDC to eligible wholesale customers of ESA holders would provide those entities with access to a digital form of central bank money that they otherwise would not have access to. Depending on a range of factors, including the interest rate applying to CBDC and the convenience that CBDC offers for payments, there could be significant demand to hold CBDC as an alternative to commercial bank deposits. Any large-scale displacement of commercial bank deposits by CBDC could have implications for credit conditions and the provision of credit in the economy. The impact this has on credit conditions will partly depend on the competitive response of the non-bank financial sector. It is beyond the scope of this report to examine these potential impacts in detail, but a key point to highlight is that widening access to a CBDC has the potential to influence the role of banks in financial intermediation and the provision of credit in the economy, which would need to be carefully considered in the design of any CBDC.

4.2.2 Controlling access to and use of the CBDC

In the POC, sponsored participant access to CBDC was controlled by ESA holders. In theory, the RBA could place restrictions on who could access CBDC and how it could be used. These restrictions could take several forms, some of which would be more complex to implement than others. It is likely that access to a wholesale CBDC would be restricted to wholesale market participants that require the use of a CBDC for settlement. However, further consideration would need to be given to:

- who is considered a 'wholesale market participant', what determines their eligibility to be a sponsored participant, and how the participation restrictions would be imposed
- whether sponsored participants should be further restricted in how they can use CBDC (e.g. in this example, whether it can be used for payments to other participants that are unrelated to syndicated loans).

Another consideration is how any restrictions on access to and use of wholesale CBDC would be enforced on sponsored participants, with whom the RBA does not have a direct relationship. Restrictions could be implemented a number of ways using DLT, including via the use of 'allow/deny' lists and programming access and usage rules into the smart contracts that govern the use of the CBDC tokens. In addition, as CBDC is only accessible by an ESA holder or a sponsored participant through its sponsoring ESA holder, further consideration would need to be given to questions related to the operation of the CBDC. For example, whether a sponsored participant would be able to hold CBDC in multiple wallets or with multiple ESA holders, or how CBDC holdings should be managed when a relationship between an ESA holder and a sponsored participant ends.

4.3 Requirements for operating a node

An important consideration in the design of a decentralised system is which entities are authorised to operate a node. In the POC, nodes were assigned to the RBA, two ESA holders and one sponsored participant; these nodes are responsible for validating transactions on the CBDC Utility and TSL Platform. This differs from centralised systems, where a system operator is typically responsible for validating transactions and maintaining the system. Were this to proceed further, it will be necessary to consider, amongst other things:

- What entities (if any), other than the RBA, would be authorised to operate a node?
- Should entities other than the RBA be permitted to validate CBDC transactions, and should the RBA be involved in validating syndicated loan transactions?
- What operational requirements would they be required to maintain?
- What access should a node operator be granted to the information held on the node?
- Should there be different node holders or different nodes for the CBDC Utility and the TSL Platform?

These questions have both technological and legal elements. While the POC highlighted a number of potential resilience benefits resulting from the decentralised nature of the system, there remains potential for systemic risk. This relates to the underlying technology and entities that play a role in operating and managing that technology. While the use of DLT enables the validation and recording of transactions to be decentralised, some components of the system are not decentralised and there would continue to be a role for a system operator in maintaining the system. This would present a similar set of risks to those in centralised systems, augmented with a different set of risks stemming from the decentralised operation of the blockchain components of the system. Legal and/or regulatory measures may be required to protect against these risks. This may include, for example, ongoing commercial arrangements between the RBA, the operator of the CBDC Utility, as well as any node operator, or regulatory oversight if the system was assessed to be systemically important.

4.4 Impact on ESA holders' liquidity management

The issuance of a wholesale CBDC could impact how ESA holders manage their liquidity. ESA holders that request CBDC from the RBA in exchange for ESA balances are effectively splitting their liquidity into two pools. The degree to which banks' liquidity management could be affected by the issuance of a CBDC would depend on the ease and speed with which ESA holders could move between ESA balances and CBDC. Accordingly, the RBA would need to consider the design of appropriate mechanisms that assist ESA holders in managing their liquidity. The Fast Settlement Service (FSS) used to settle New Payments Platform (NPP) transactions provides an example of how these mechanisms could be designed, as well as how the liquidity implications of a 24/7 payment system can be managed in the context of the more limited operating hours of RITS.[24] Nonetheless, the issuance of a wholesale CBDC would introduce additional risk and complexity in how banks and other financial institutions manage their ESAs.

4.5 Implications of wholesale CBDC and tokenised syndicated loans

4.5.1 Digitisation of syndicated lending processes

In implementing the tokenised syndicated loan on the TSL Platform, the project focused on the digitisation of back-office functions related to the origination and servicing of those facilities. In this regard, the POC demonstrated potential efficiency gains and risk reduction from replacing highly manual and paper-based processes. Because the design of the POC retained the roles and functions performed by existing participants in the syndicated lending market, additional gains through the use of DLT by reducing or removing the involvement of some participants and processes were not explored. For example, the approval and settlement functions performed by a facility agent, which typically acts as an intermediary between the syndicate lenders and the borrower, could have been further automated through the TSL Platform and indeed one of the key advantages of DLT is removing the need for intermediaries. One possibility is that the facility agent's role could evolve to become the operator or administrator of the TSL Platform, for example. Aside from the potential automation, efficiency and risk benefits of digitising syndicated loans on a DLT platform, other potential benefits discussed during the project included the possibility of standardising loans and slicing them into much smaller tranches. This could open them up to a much broader investor base and support a more active secondary market.

24 For example, RITS provides ESA holders with tools (during RITS hours) to manage the level of ESA balances allocated to the FSS, including the ability to set trigger points for the automatic top up or withdrawal of balances.

4.5.2 Legal considerations

The TSL Platform was designed to test the technological (as opposed to the legal) process for entering into the agreement. As it is currently designed, the platform includes a digital copy (in PDF form) of the SFA executed outside the platform. The terms entered on the platform (some of which are implemented as smart contracts) reflect some of these agreed terms but are not the agreement itself. Another important consideration is whether an SFA could be legally entered into and managed through the TSL Platform. Were the TSL Platform to be developed further, it will be necessary to ensure that an SFA entered into through the platform meets all requirements of the parties and is legally enforceable. This would require an in-depth review of the SFA's terms to determine which are required to be entered into and customisable on the TSL Platform, which are to be held on any blockchain part of the platform and which are to remain outside the platform. Further standardisation of the SFA's terms, which are typically quite bespoke, would also be necessary to fully realise the efficiency gains from the TSL Platform's digital workflows. Further, for this to be legally enforceable, reliance on electronic signatures should be considered.

It will also be necessary to ensure appropriate rules around operation of the platform are in place. These rules would give effect to the purpose for which the TSL Platform is created, and manage access to the TSL Platform by users. These rules are likely to be set out in additional documents, which form the legal architecture for the TSL Platform and manage the relationships and interactions of all parties who will access the TSL Platform. Once established, the legal architecture should enable the platform to operate in the digital environment with the ability to, where necessary, step into an analogue environment and back into the digital environment as necessary.

4.6 Benefits and disadvantages of CBDC compared to other settlement options

A key objective of the project was to examine how CBDC could be used to facilitate transactions during the lifecycle of a tokenised financial asset. To help evaluate the potential benefits of using CBDC, the project considered the implications of using other, non-DLT payment systems for the settlement of tokenised syndicated loans (though these alternative settlement models were not part of the POC).

In the absence of a CBDC, the TSL Platform could be configured to initiate a payment by sending a secure message (e.g. via an API) to a non-DLT payment system. The payment system, which could, for example, be RITS or the NPP, would verify the payment request, execute the payment and send a confirmation message back to the TSL Platform.

The lock-up functionality in the CBDC Utility required for DvP settlement could be replaced with a third-party escrow agent or functionality that could reserve or hold funds (e.g. the reservation function in RITS or a new NPP overlay service).[25] It is not clear that the use of a non-DLT payment system would increase settlement risk associated with a syndicated loan facility, which is already quite low due to the structure of these facilities. RITS is already used in the drawdown, novation and repayment of syndicated loan facilities, so it is likely that many of the potential benefits from tokenising syndicated loans on a DLT platform could still be realised without a CBDC.

However, the use of existing payment systems to settle transactions on a DLT platform could introduce additional risks and complexities related to the need for frequent on/off-chain interactions and creating additional potential points of failure in the settlement process. Without having carried out a technical design or POC considering how a DLT-based system might interact with RITS or NPP, it is difficult to assess how significant these issues are.

A further consideration is that while a DLT-based CBDC may not offer many apparent benefits when used solely for syndicated loans, the benefits could be significantly greater if there were a much larger range of assets and/or business processes on DLT that could also utilise a CBDC. Indeed, it is possible that the availability of a CBDC on a DLT platform could act as a catalyst for innovation in the use of DLT for digitising assets and business processes, with significant implications for efficiency and risk in a range of wholesale markets.

Finally, it is worth noting that instead of (or in addition to) a CBDC, it is possible that privately-issued digital assets such as stablecoins could also function as a settlement asset in DLT-based systems such as that explored in this project.[26] However, for a stablecoin to offer comparable benefits to a CBDC in this context, it would likely need to be denominated in a fiat currency and be fully backed by safe and liquid assets, such as government securities or other highly rated securities, have well-designed governance arrangements and be appropriately regulated. It is unlikely that cryptocurrencies such as Bitcoin, which are not denominated in fiat currency, backed by any assets or have any issuer standing behind them, would be a suitable settlement asset in DLT-based asset markets.

25 The reservation function in RITS enables near real-time settlement of interbank obligations relating to property transactions by linking lodgement of the property title transfer with the financial settlement process. See: De Freitas G and E Fitzgerald (2021), 'Property Settlement in RITS', RBA Bulletin, March.

26 A stablecoin is a type of privately issued digital asset (or crypto-asset) that is specifically designed to maintain a stable value relative to a national currency or other reference asset, with the intention of making them more attractive as a means of payment or store of value. One way they seek to maintain a stable value is by holding assets that back the coins on issue, which is supposed to ensure redeemability at par. See: Richards T (2021), 'The Future of Payments: Cryptocurrencies, Stablecoins or Central Bank Digital Currencies?', Address to Australian Corporate Treasury Association, Sydney, 18 November.

5. Conclusion

Project Atom involved the successful development of a POC for the issuance of a tokenised form of CBDC that can be used by wholesale market participants for the funding, settlement and repayment of a tokenised syndicated loan on an Ethereum-based DLT platform. The project examined the potential use and implications of a wholesale form of CBDC, focusing on:

- how access to a tokenised CBDC could be extended to a wider range of wholesale market participants, including those that would not ordinarily have access to ESAs at the RBA
- integration of a digital asset in the form of a tokenised syndicated loan to explore the implications of atomic DvP settlement as well as other potential benefits of combining CBDC and tokenised assets on interoperable DLT platforms
- whether an enterprise-grade version of the Ethereum blockchain platform could address some of the technical limitations of the public version in implementing a CBDC.

The project used a two-tier model for issuing CBDC, in which CBDC is issued by the RBA to ESA holders, which in turn can facilitate the acquisition of CBDC by their sponsored wholesale market participants. This model preserves several important aspects of the current role of commercial banks in the financial system, including their role in onboarding and providing services to their customers. This is a key point of difference from other wholesale CBDC projects, which have tended to focus on the use of wholesale CBDC by commercial banks. There are a range of potential benefits of providing non-bank wholesale market participants with access to CBDC for settling transactions and as a store of value. However, further consideration is needed on who would be eligible to be a sponsored participant and the appropriate level of controls that would be imposed on their use of CBDC.

Tokenisation of the SFA focused on the digitisation of back-office functions related to the origination and servicing of those facilities. In this regard, the POC demonstrated significant efficiency gains and risk reduction from replacing the highly manual and paper-based processes still used in these markets. Aside from the potential automation, efficiency and risk benefits of digitising syndicated loans on a DLT platform, other potential benefits from tokenisation include the possibility of fractionalising these loans to make them available to a broader investor base, thereby enhancing liquidity in these markets.

The project also considered the possibility of using non-DLT payment systems to settle transactions on a DLT platform. While many of the potential benefits from tokenising syndicated loans on a DLT platform could still be realised without a CBDC, the use of existing payment systems to settle transactions on a DLT platform could introduce additional risks and complexities. There could also be a role for appropriately regulated and asset-backed stablecoins to function as a settlement asset, which could achieve comparable benefits to a wholesale CBDC in settling tokenised asset transactions.

More generally, the availability of a tokenised form of money on a DLT platform could also act as a catalyst for innovation in the use of DLT for digitising assets and business processes. Careful consideration of the legal architecture to give effect to a wholesale CBDC and the issuance and management of a tokenised SFA on a DLT platform would be required before undertaking further work in this area. This would include analysis of contractual arrangements as well as an assessment of relevant regulatory and legislative requirements.

Overall, the project has advanced our knowledge on the technical feasibility and implications of using DLT for a wholesale CBDC and tokenised assets. In particular, the POC demonstrated that an enterprise-grade DLT platform with appropriate controls on access and security could address many of the requirements for a wholesale CBDC system, including in relation to transaction finality, efficiency, security and privacy. The exploration of the tiered distribution model has highlighted a range of issues that would need to be considered in opening up access to a CBDC more broadly. More generally, the project has suggested a number of areas where further research and experimentation will be required to address the question of whether there is a case for a wholesale CBDC and how one could be developed.

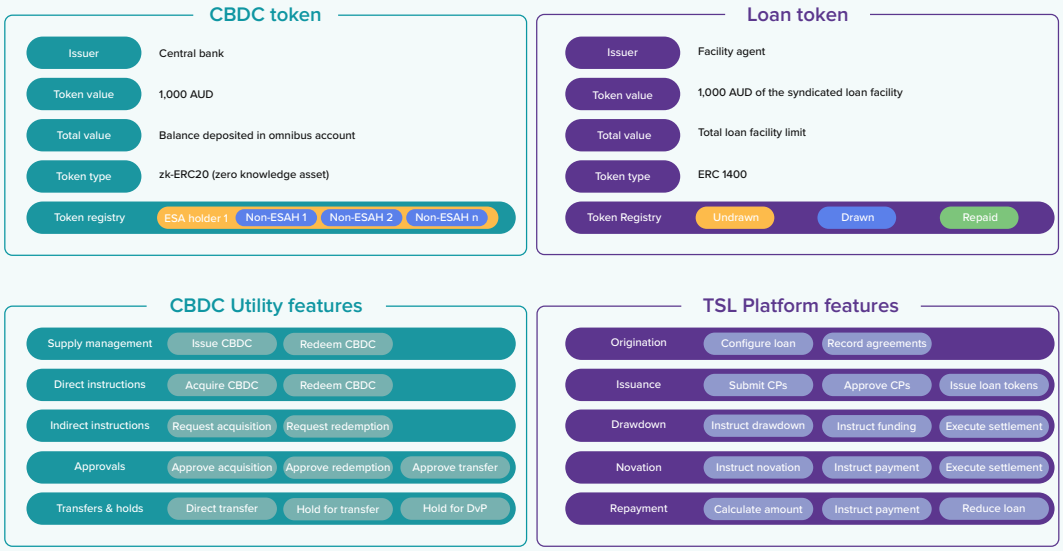
Appendix A: Technical solution

A1. System overview

Two interlinked platforms were implemented in the POC:

1. A **CBDC Utility**, which manages the issuance, transfer and redemption of a tokenised CBDC (**CBDC tokens**).
2. A Tokenised Syndicated Loan Platform (**TSL Platform**), which manages the issuance, drawdown, novation and repayment of a tokenised syndicated loan (**loan tokens**). The two platforms are interoperable, which allows the CBDC Utility to execute payments to settle transactions (e.g. loan drawdown, novation, and repayment) initiated on the TSL Platform. Figure 10 provides a summary of the features of the two types of tokens and the corresponding applications.

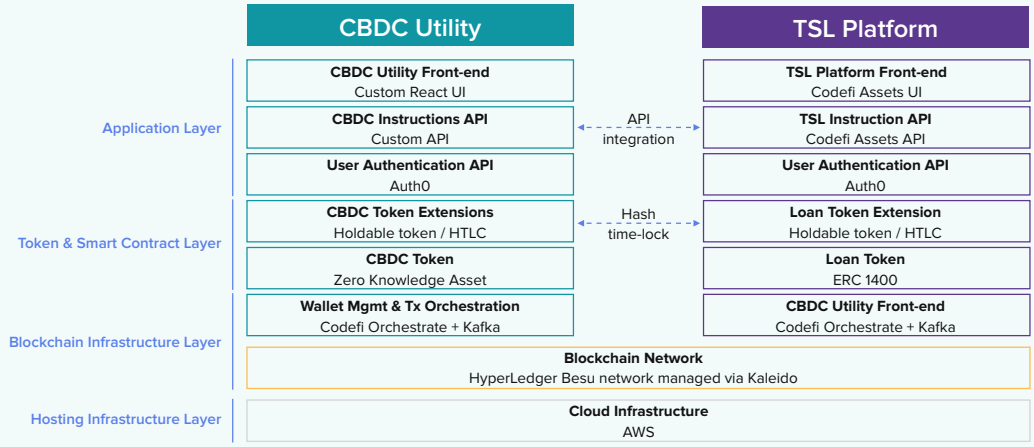
Figure 10: Summary of POC Features



A2. Technical architecture

The CBDC Utility and the TSL Platform share a private and permissioned blockchain network built on Hyperledger Besu, an enterprise-grade Ethereum client; the two components are interoperable through smart contracts and API integrations. Figure 11 outlines the technical architecture of the two applications.

Figure 11: Technical Architecture



The infrastructure at the bottom of the stack stores all the data and core logic of the two applications. It comprises two sub-layers:

- The **Hosting Infrastructure Layer** leverages Amazon Web Services cloud infrastructure to host off-chain application data and services. For example, the databases used to simulate the balances of ESAs and commercial bank accounts are hosted in this layer.
- The **Blockchain Infrastructure Layer** validates and records all the data and transactions that are processed on the private blockchain network. It maintains a distributed, synchronised record of the balances of CBDC and loan tokens held in participants' wallets. More details on the blockchain network configuration and the wallet management solution are provided in the following sections.

The **Tokens and Smart Contract Layer** encodes the rules for the issuance of the tokens and the execution of the transactions on the blockchain network. Together with the APIs and user interfaces in the **Application Layer**, these components implement the business logic and user workflows for both the CBDC Utility and the TSL Platform.

The CBDC Utility is comprised of the following components:

- CBDC token configured as a zero-knowledge asset leveraging the Aztec protocol, which supports private issuance, transfer and redemption of CBDC (see details below).
- Holdable token and hashed time-locked contract (HTLC) smart contract extension that enables conditional transfers of CBDC and atomic settlement against loan tokens.

Dedicated instance of the Auth0 API to authenticate the users accessing the application.

- Custom-built CBDC Instructions API that enables the following instructions:
  - Direct acquisition and redemption of CBDC by an ESA holder.
  - Indirect acquisition and redemption of CBDC for a sponsored participant with the approval of their sponsor ESA holder.
  - Direct transfer of CBDC.
  - Conditional transfer of CBDC with approval of the recipient for amounts greater than A$5 million.
  - Conditional transfer of CBDC with approval of the facility agent for atomic DvP settlement of tokenised syndicated loan transactions.
- A dedicated user interface built in React that enables users to submit instructions and view their balances and transaction records.

The TSL Platform is comprised of the following components:

- Loan token configured as an ERC 1400 token, which is an Ethereum token standard commonly used for tokens which are financial instruments (see details below).
- Holdable token and HTLC smart contract extension that enables conditional transfers of loan tokens and atomic settlement against CBDC tokens.
- Dedicated instance of the Auth0 API to authenticate the users accessing the application.
- Dedicated instance of the Codefi Assets API with additional custom-built workflows that manage the following events in the syndicated loan lifecycle:
  - Signing of a digital document by all the parties (leveraging an e-signature solution).
  - Confirmation of conditions precedent prior to loan drawdown, which initiates the issuance of undrawn loan tokens to the borrower.

  - Drawdown and novation, which holds the loan tokens for atomic settlement against CBDC tokens with approval of the facility agent.
  - Repayment, which instructs the repayment of a loan in CBDC and the 'burning' of loan tokens.
- Customised version of the Codefi Assets UI specifically designed to enable users to manage the lifecycle of a syndicated loan and view information about facilities to which they are a party.

A3. Blockchain infrastructure

The blockchain network is comprised of five blockchain nodes that continuously execute a consensus algorithm to record and maintain a distributed, synchronised record of CBDC and loan token transactions and balances held in participants' wallets. The network was configured as an Enterprise Ethereum network based on the Hyperledger Besu client, hosted and managed by ConsenSys through Kaleido. There are four validator nodes assigned to CBA, NAB, the RBA and Perpetual, plus one monitoring node assigned to ConsenSys.

Hyperledger Besu leverages the IBFT 2 (Istanbul Byzantine Fault Tolerance 2) consensus mechanism, which is a voting-based proof-of-authority algorithm. This consensus algorithm allows approved nodes, known as validators, to validate transactions and blocks. Validators take turns to create new blocks, which must be signed by a super-majority (greater than 66 per cent) of validators before the block is added to the blockchain. IBFT 2 is an enterprise-grade consensus algorithm designed for high transaction throughput and immediate finality. It can achieve immediate finality because there is a single version of the blockchain and a single block proposed at any given block height. Because block creation rotates between validators, a faulty node cannot exert long-term influence over the chain.

Further development of the solution beyond a POC would require the implementation of a more robust blockchain network with an increased number of validator nodes more broadly distributed across the participating entities. Future implementations of the blockchain network could also consider segregating on-chain data between the CBDC Utility and the TSL Platform. This could be achieved by either:

- maintaining a single blockchain network for both applications and leveraging Hyperledger Besu's privacy groups to establish sub-groups of nodes that validate and store application-specific transactions and data (private state) (Figure 12)
- establishing a separate blockchain network for each of the two applications, each maintained by the relevant entities. Interoperability solutions, such as HTLCs and cross-chain bridges, could be implemented to integrate the two networks (Figure 13).

Figure 12: Single Blockchain Network with Privacy Groups

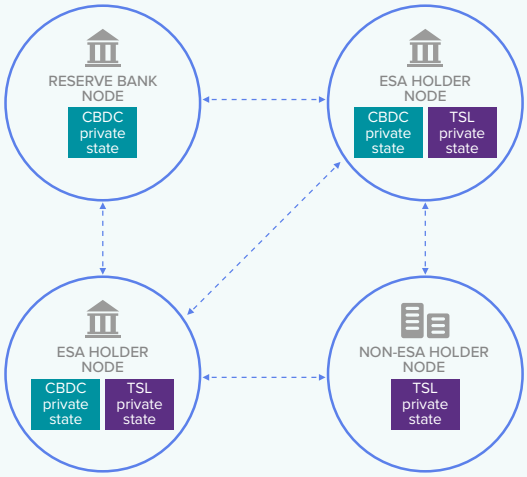
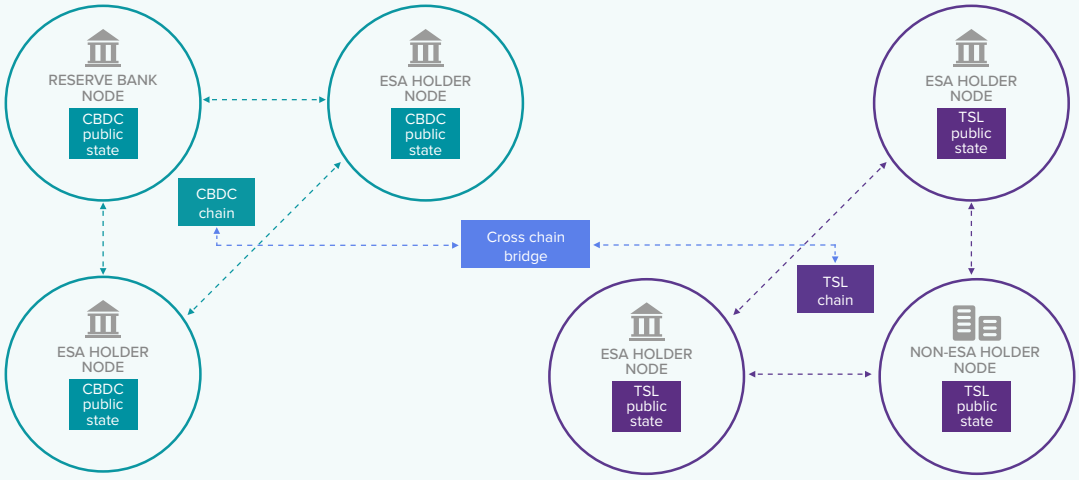


Figure 13: Interoperable Blockchain Networks



The solution implemented for Project Atom also leverages Codefi Orchestrate, a 'blockchain middleware' API developed by ConsenSys that acts as the link between applications and the underlying blockchain network. Codefi Orchestrate enables a range of functionality in the CBDC Utility and the TSL Platform, which significantly simplifies user interactions with the blockchain layer, including:

- End-to-end transaction management, including gas and nonce management, signing, sending, listening, event streaming, and receipt decoding.
- Account management and identification to link the users' on-chain and off-chain interactions.

- Secure private key management with enterprise-grade vaults for key storage and operation.
- Encrypted network messaging across private bilateral or multilateral channels for secure data sharing.

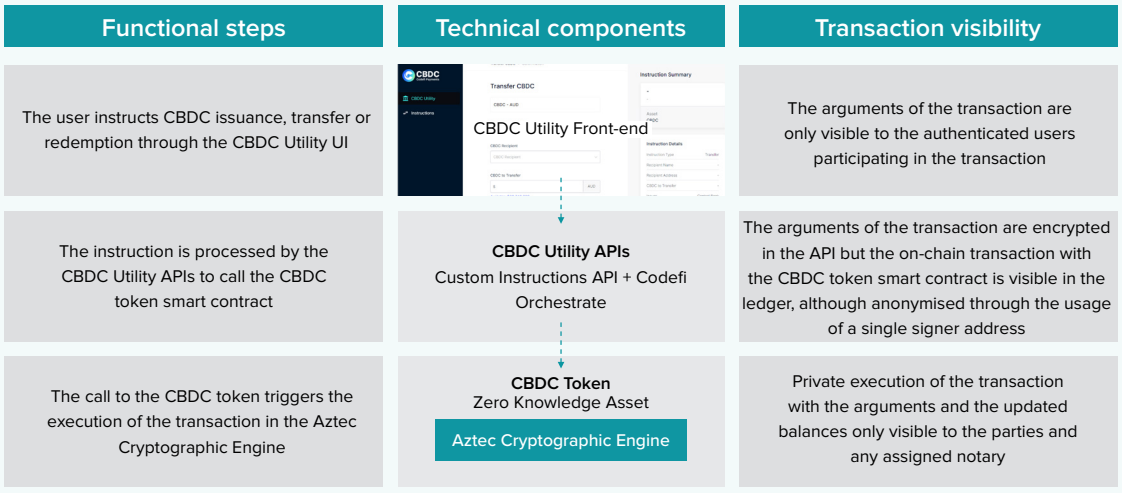
A4. Implementation of privacy in the CBDC token

Zero-knowledge proofs (ZKPs) enable mathematical verification of encrypted information without the need to know the content of the encrypted information. The Aztec protocol, which was used to implement privacy in the CBDC token, is one implementation of ZKPs in a blockchain context.

The Aztec protocol implements privacy through the Aztec cryptographic engine, which uses a system of 'notes' to privately record CBDC token balances. The RBA is configured as a notary in the Aztec cryptographic engine and has viewing rights on the private token balances and transfers. When a participant instructs the issuance, transfer or redemption of CBDC, a smart contract calls the Aztec cryptographic engine to update the ownership and/or value of one or more notes. Each of the nodes in the blockchain network can verify the integrity of a transaction without knowing the parties to a transaction, their balances or the transaction value.

Figure 14 outlines the technical steps involved in the private transfer of CBDC tokens.

Figure 14: Private Transfer of CBDC Tokens



Throughout the POC we observed performance issues related to the use of ZKPs. The time to complete a zero knowledge transaction increases significantly as the number of notes in circulation increases (Table 1). This reflects an increase in the complexity of the proofs that are calculated by the Aztec cryptographic engine and the time to complete a typical transaction increases from around 3 seconds to more than 10 seconds. In addition, the computation effort to complete each transaction (measured in 'gas') increases significantly (Table 2).[27]

27 Computation effort on an Ethereum network is measured in gas, which refers to the cost necessary to process a transaction; in the POC, this cost was set to zero, therefore the use of ZKPs did not have any implications for the cost of processing transactions.

To address this issue, the unit of each CBDC token was increased from A$1 to A$1,000, which reduced the number of notes in the Aztec cryptographic engine, which in turn reduced the complexity of the proofs. There is research underway in the DLT community to address this issue. The forthcoming version of the Aztec privacy protocol is expected to be significantly more efficient from a computational perspective.

Table 1: ZKP Performance Estimates
Average time to complete transaction (seconds)

Input notes	Output notes						
	1	2	4	8	16	32	64
1	0.5	0.6	0.7	0.9	1.5	2.6	5.4
2	0.6	0.6	0.8	1.2	2.0	2.8	5.3
4	0.6	0.7	0.9	1.1	1.7	2.7	5.5
8	0.8	1.0	1.3	1.4	2.0	3.3	6.1
16	1.5	1.7	1.8	2.5	2.5	3.6	6.3
32	2.5	2.5	2.7	3.0	3.5	4.8	7.6
64	5.0	4.8	5.0	5.5	6.2	7.3	10.5

Table 2: ZKP Performance Estimates
Average computational effort

Input notes	Output notes						
	1	2	4	8	16	32	64
1	314	399	570	911	1,594	2,961	5,703
2	373	458	629	970	1,653	3,020	5,763
4	490	576	746	1,088	1,771	3,138	5,881
8	725	811	981	1,323	2,006	3,374	6,118
16	1,196	1,282	1,452	1,794	2,478	3,846	6,592
32	2,139	2,224	2,395	2,737	3,421	4,792	7,543
64	4,031	4,117	4,288	4,631	5,317	6,690	9,449

A5. Implementation of the ERC 1400 token standard in the loan token

ERC 1400 is a token standard introduced in late 2018 to facilitate the tokenisation of securities and other financial instruments on the Ethereum blockchain. It provides a set of standardised properties and control mechanisms that can be used to restrict the usage and transfer of the token to meet regulatory requirements.

The ERC 1400 token standard extends on the ERC 20 token standard by enabling:

- injection of signed data 'certificates' into issuance, transfer and redemption transactions to add conditions and check the validity of transactions
- creation of token partitions (i.e. partially fungible token classes and states) through the attachment of metadata to the partial balance of a token holder
- setup of an entity (e.g. an issuer, an agent or a regulator) as a controller that has the ability to approve transactions and force the transfer of tokens.

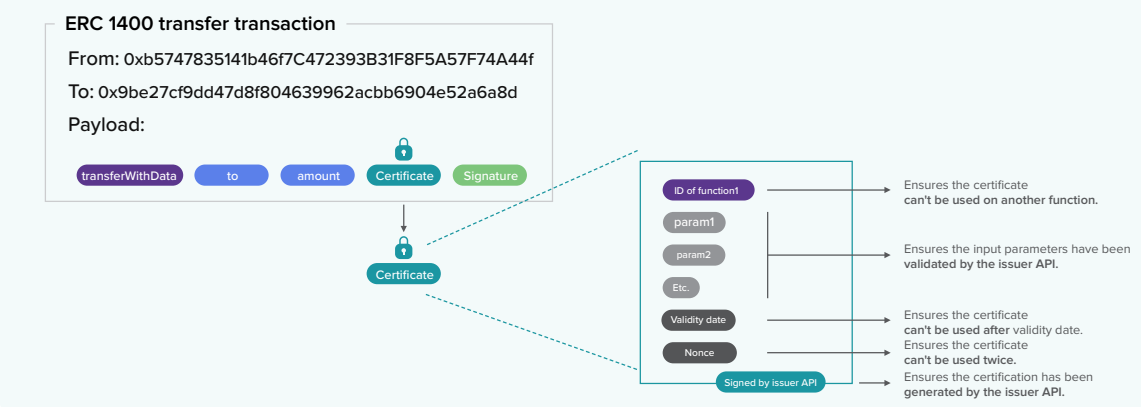
In Project Atom, the ERC 1400 token standard was used to implement the loan token.

Key features include:

- Execution of transactions (e.g. issuance of loan tokens upon confirmation of condition precedents and transfer of loan tokens following drawdown, novation and repayment) is validated through data certificates signed by the parties to the transaction.
- The participants to the syndicated loan are captured in an allow list, which is used to validate their interaction with the syndicated loan smart contract.
- Partitions are used to manage the state of the token as it moves through the lifecycle of the syndicated loan (e.g. undrawn to drawn).

The facility agent is configured as the token controller and is able to approve transactions, enforce settlement and even force the transfer of loan tokens, which could be used to resolve issues that require it to unilaterally update the loan registry.

Figure 15: ERC 1400 Transfer Transaction with Data Certificate



The TSL Platform also leveraged Codefi Assets, a ConsenSys product that enables the issuance and management of tokenised securities and other financial instruments. Codefi Assets' APIs and user interfaces were modified and extended to implement the core workflows of the tokenised syndicated loan and enable the instruction and execution of the underlying token transactions.

A6. Settlement with token holds and hashed time-locked contracts

In centralised payment systems, DvP settlement usually requires a trusted intermediary (e.g. an agent or exchange) to operate accounts that can temporarily maintain ownership of both the cash and asset, and simultaneously execute both legs of the transaction. In contrast, DLT platforms can enable DvP settlement of tokenised assets and tokenised cash to occur simultaneously without relying on a trusted intermediary or escrow accounts. This is known as atomic DvP settlement.

The solution implemented in Project Atom achieves atomic DvP settlement by using 'token holds' and HTLCs. Token holds allow a third party to transfer tokens on behalf of the token holder, while imposing transaction-specific conditionality on the tokens, which prevent the token holder from using the tokens in a different transaction unless the hold is cancelled. The tokens are essentially locked or reserved through a sort of self-escrow mechanism, but remain in the account of the token holder. In addition to enabling DvP settlement, token holds are also used to implement conditional transfers of CBDC tokens. For example, in transfers greater than A$5 million, the sender has the option to require the recipient approve the incoming transfer.

HTLCs enable a smart contract to implement a time-based escrow that requires the recipient to acknowledge a transfer within a certain period of time. The combination of token holds and HTLCs is particularly suitable for enabling DvP settlement in more complex scenarios, such as:

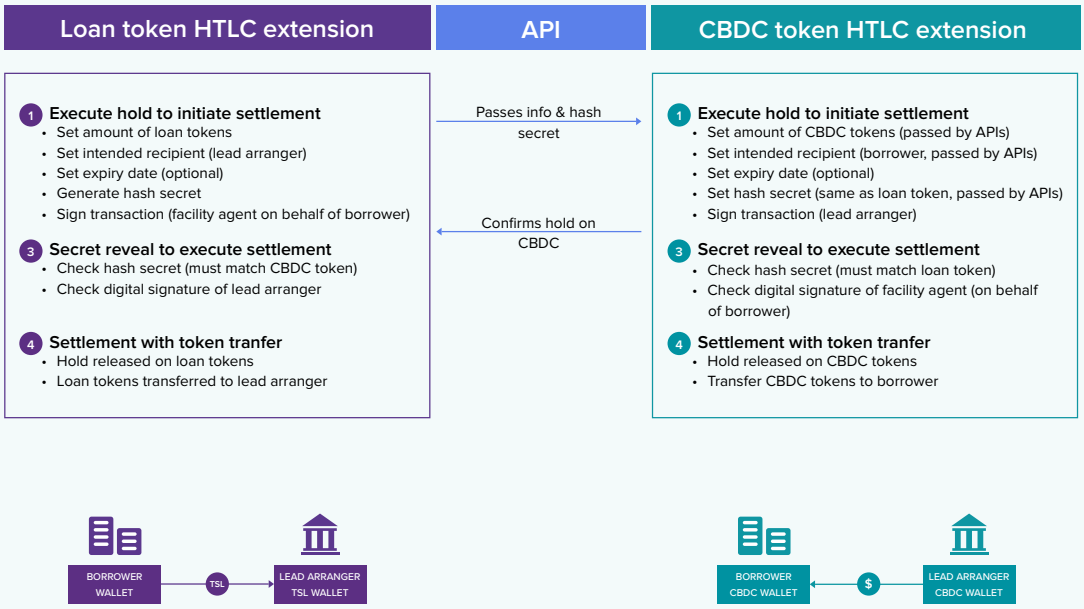
- cross-chain swaps, where the tokens to swap are hosted on two different blockchain networks
- swaps involving private assets, such as when one or both of the assets are represented by private tokens (e.g. the CBDC token).

In these scenarios, HTLCs enable atomic DvP settlement through a two-stage process. An initial 'commit' phase, in which each party puts their asset on hold, is followed by a 'reveal' phase. Once the first leg of the transaction is claimed, the second leg is automatically released to the counterparty. In Project Atom, the CBDC token is implemented as a zero-knowledge asset. For this reason, the POC leverages both the token hold and HTLCs mechanisms to enable DvP settlement through dedicated and interoperable smart contract extensions applied to both the CBDC token and the loan token:

1. The first party initiates the DvP process by creating a hold on the loan token with a random secret (hash) generated by HTLC extension.
2. The secret is shared with the counterparty through an API integration. The counterparty uses the secret to create a hold on the CDBC token. At this point both assets are on hold and can only be swapped by using the same secret.
3. The first party uses the secret to release the hold on the CBDC token and claim it. This simultaneously triggers the release of the loan token to the counterparty.

Figure 16 describes the process for a loan drawdown transaction. Communication between participants is implemented via APIs.

Figure 16: Settlement of Drawdown Transaction with HTLC Mechanism



Appendix B: Acknowledgements

Steering Committee			
RBA	Chris Thompson		
CBA	Sophie Gilder		
NAB	Charlotte Cadness		
Perpetual	Matthew Neece		
ConsenSys	Claudio Lisco		
Project Group			
RBA	Cameron Dark	Alexandra Spicer	
CBA	Erika Carnogoy		
NAB	Lisa Wade		
Perpetual	Sarah Mattson		
ConsenSys	Matthieu Bouchaud	Olga Kravtsova	Arafet Ben Makhlouf
	Gauthier Petetin	Fernando Garcia Ruiz	Salah-Eddine Saakoun
KWM	Hannah Glass		
Subject Matter Experts			
RBA	David Emery	Michael Shen	Susan Slocum
	Jaan Smith	Dmitry Titkov	
CBA	Julita Hardjono	Luke Jericho	Nico Lassing
	Michael Tran		
NAB	Mark Bower		
Perpetual	Mimi Bui	Shirley Ong	Johnny Rashidi
	Mehul Shaha		
ConsenSys	Didier Le Floch	Matthieu Saint Olive	
KWM	Scott Farrell	Urszula McCormack	

ISBN 978-0-6489163-5-2 (Online)