International Telecommunication Union

ITU-T

TELECOMMUNICATION
STANDARDIZATION SECTOR
OF ITU

FG-DFC

(07/2019)

ITU-T Focus Group Digital Currency including Digital Fiat Currency

---

Reference Architecture and Use Cases Report

Focus Group Technical Report

ITU-T

International Telecommunication Union

FOREWORD

The International Telecommunication Union (ITU) is the United Nations specialized agency in the field of telecommunications, information and communication technologies (ICTs). The ITU Telecommunication Standardization Sector (ITU-T) is a permanent organ of ITU. ITU-T is responsible for studying technical, operating and tariff questions and issuing Recommendations on them with a view to standardizing telecommunications on a worldwide basis.

The procedures for establishment of focus groups are defined in Recommendation ITU-T A.7. TSAG set up the ITU-T Focus Group Digital Currency Including Digital Fiat Currency (FG DFC) at its meeting in May 2017. TSAG is the parent group of FG DFC.

Deliverables of focus groups can take the form of technical reports, specifications, etc., and aim to provide material for consideration by the parent group in its standardization activities. Deliverables of focus groups are not ITU-T Recommendations.

Reference Architecture and Use Cases Report

About this Report

This Technical report was prepared by the Reference Architecture Working Group of the ITU-T Focus Group on Digital Currency including Digital Fiat Currency, with contributions from:

- Isabelle Corbett, R3
- Sonja Davidovic, IMF
- John Kiff, IMF
- Thomas Kudrycki, eCurrency
- Klaus Löber, European Central Bank
- Dinesh Shah, Bank of Canada
- Srinivas Yanamandra, New Development Bank

The authors would like to thank Dan Conner (DisLedger) and Marla Dukharan (Bitt) for their inputs on the use cases and to all members of the Reference Architecture Working Group for their feedback on the report.

If you would like to provide any additional information, please contact Vijay Mauree, Programme Coordinator, ITU at tsbfgdfc@itu.int.

Disclaimer: The opinions and views expressed in this report are those of the authors and do not necessarily reflect the views of the author's organization, central banks referenced in the report, or the International Telecommunication Union or its membership.

Table of Contents

Executive Summary

Digitalization is reshaping economic activity across the world. In some advanced economies, it is shrinking the role of cash and spurring new digital forms of money. In developing countries, it may provide new financial inclusion options, and reduce operational costs and risks associated with the management of physical currency. Central banks have been pondering whether and how to respond to these new developments, especially considering the private sector's increasing prominence in digital payment systems.

One possibility for central banks is to explore wholesale Central Bank Digital Currency (CBDC) and privately-issued Digital Fiat Currency (DFC) that facilitate wholesale payment transactions between the national central bank and participating financial institutions. Another option is to issue a retail CBDC, which is a widely accessible digital form of fiat money that could be legal tender. In economies that are highly depended on cross-border transactions such as remittances, central banks would want to consider introducing a cross-border dimensionality to their retail or wholesale CBDCs.

The rationale for CBDC issuance will drive a central bank's choice of the operating model, architecture, and technology. There are universally applicable design features for all types of CBDC such as security, robustness, and flexibility of the architecture as well as the central bank mandate market environment, and legal and regulatory framework that provide the context a in which the CBDC. The relevance and prominence of other design features will vary by the specific type of CBDC. Although specific design features will be aligned with the CBDC type, it is important to consider all design features holistically to account for possible trade-offs and gaps within the architecture.

This report presents the architecture options for three types CBDCs -wholesale, retail, or cross-border CBDCs based on stylized examples. Without prescribing any specific design and technology choices for the CBDC architecture, it merely serves as a reference document for policymakers that can guide and inform their decision-making process. For standard-setting bodies such as the International Telecommunications Union (ITU), the report will provide key inputs for a possible standardization of CBDC issuance, distribution and payment transactions.

1 Introduction

This document will refer to digital fiat currency (DFC) as a tokenized, digital representation of a sovereign currency issued by an authorized public or private entity. When issued and distributed by a central bank or other monetary authority, it is a central bank digital currency (CBDC). If it is issued by a private entity, it may be e-money (e.g., AliPay and M-Pesa) or another form of digital commercial bank money/private digital tokens/stablecoins, even if backed by central bank money.[1] An important difference between the two is that CBDC is generally designated as legal tender.[2] This document will focus on three variations of CBDC:

- Wholesale CBDC limited to banks and other members of national payment systems, and made available for settlement purposes, updating, complementing or replacing central bank deposit technology.
- Retail CBDC that is a widely accessible digital representation of a sovereign currency that is issued by, and a liability of, a jurisdiction's central bank or monetary authority, and would likely be designated as legal tender as stipulated in pertinent legislative acts.
- CBDC for both retail and wholesale purposes a Cross-Borders, for example remittance flows.

To date no central bank has issued CBDC in production, but according to Barontini and Holden (2019) at least 44 are currently (or will soon be) engaged in CBDC work. Of those, 38 are focusing on widely accessible retail CBDC that could be legal tender, and 30 are focusing on wholesale CBDC. Table 1 lists over thirty jurisdictions where central banks are currently (or have been) engaged in retail CBDC work, based on publicly-available information. Table 2 lists jurisdictions conducting wholesale CBDC investigations, based on publicly available information.

A number of central and private banks are actively exploring wholesale CBDC and privately-issued DFC. Wholesale CBDC theoretically facilitate wholesale payment transactions between the national central bank and participant financial institutions. More generally, privately-issued wholesale DFCs (such as JP Morgan's JPM Coin) could facilitate additional functional possibilities for payment systems such as inter-operability of ledgers and capabilities for atomic transaction execution.[3] This could allow smart contracting choices to market players, opening further possibilities for programming the currency.

Recent central bank pilot studies indicate that distributed ledger technology (DLT) based systems provide for possibilities of tokenization of both cash and securities on a single shared ledger resulting in better asset interactions during delivery-versus-payment (DVP) settlement relative

[1] Stablecoins are crypto-assets designed to minimize price volatility, usually versus a fiat currency, although some are pegged to baskets of fiat currencies (e.g., IMF Special Drawing Rights). Most stablecoins are collateralized, or backed, by the assets they are pegged to. This is the case with the major USD-pegged coins such as Tether (USDT) and Circle (USDC). Some stablecoins are backed by other crypto-assets. For example, USD-pegged DAI is currently 150% overcollateralized with Ether (ETH) – every $100 million DAI outstanding is backed by $150 of ETH. According to one view, private stablecoins backed by central bank money could be considered indirect or "synthetic" CBDC (Kumhof and Noone, 2018; Adrian, 2019).

[2] Prevailing practice is that a state designates by legislation a currency of its issuance as legal tender within its territory. However, legal tender has been an elusive concept, and its meaning varies from country to country. Even today, countries sometimes prohibit contracts denominated and payable in non-local currencies within their territories, though such prohibition can be best described as foreign exchange control. There have also been cases where a state gave private bank currencies legal tender status. Also, some countries decide to adopt a dollarization policy and designate a foreign currency as legal tender either unilaterally or bilaterally and with or without parallel issuance of its own currency.

[3] Atomic transactions occur completely or not at all with no partial results such as withdrawal of money from an ATM and charges to a credit card.

to current settlement mechanisms. DLT refers to the processes and related technologies that enable nodes in a network (or arrangement) to securely propose, validate and record state changes (or updates) to a synchronized ledger that is distributed across the network's nodes (BIS, 2017). Transactions recorded using DLT-based DFC payment systems could be cheaper in aggregate than transactions recorded across multiple siloed accounts increasing the utility of the wholesale payments system.

At least two central banks (Ecuador and Uruguay) are known to have conducted limited-scale pilot retail CBDC issuance, and others are researching pilots (e.g., Bahamas, Eastern Caribbean Currency Union, Sweden, and Ukraine). Senegal and Tunisia have purportedly issued CBDCs, but these appear to be DFC not issued by the respective central banks.[4] Some central banks (e.g., Barbados and Philippines) are supporting private sector DFC in regulatory sandboxes.

Central banks have been exploring various technological solutions and operating models for their retail CBDCs. While some central banks have opted to centrally manage the entire infrastructure including wallets (e-Peso), others control the issuance while enabling financial institutions to carry out the distribution through API access (e-Krona). Central banks can choose between different technological architectures that are either DLT or non-DLT based. Traditional n-tier architecture offers compelling benefits especially for centrally managed operating models.[5]

Any DLT-based implementations of CBDC will likely be based on private permissioned networks because they fit best with the need to oversee transactions among network participants and regulate access to the network.[6] Some central banks are considering retail CBDC in the form of a card or a mobile wallet app on which prepaid values are stored locally rather than on a ledger providing offline capabilities to provide near the same 24/7 availability as cash. The Riksbank is considering this in addition to an account-based CBDC.

So far, DFC projects have focused on domestic-only applications, but central banks and others are starting to think about cross-border systems. Most domestic settlement systems are not based on a common platform hence a reference architecture will need to assume a variety of settlement systems. Common sets of standards and interfaces in these domestic settlement systems will facilitate easy integration. Currently, several real time gross settlement (RTGS) operators are looking at modernizing and renewing their payments infrastructure to facilitate change in payments and settlement.

Although the design principles will be specific to the CBDC type, there are several key design principles that are universally applicable to all types. First, the rational for CBDC issuance should drive the choice of the operating model, architecture, and technology choice. The CBDC architecture should be robust, secure, and aspire to mitigate cyber-security risks. Any specific design choice should consider the existing IT infrastructure capacity, the legal and regulatory framework, the central

[4] In the case of Senegal's eCFA e-currency, the only connection to the central bank seems to be that the e-currency complies with the e-money regulations of the Banque Centrale des Etats de l'Afrique de l'Ouest. In Tunisia, the post office has been operating an e-Dinar digital money wallet since 2000, and in 2016 it partnered with Monetas and DigitUs to offer a blockchain-based payments app, but there is no central bank involvement.

[5] N-tier architectures are a very mature and well-known architectural approach, thus representing lower risk than adopting the new technologies. They enable separation of concerns, e.g. the ability to scale up transaction processing at the back-end of the system while allowing the user experience to remain untouched. Many of the world's largest transactional systems, including payment system, are built on the n-tier approach, there are many design patterns and many vendors have technologies that work with n-tier.

6 DLT platforms can be "public" (accessible by anyone) or access could be restricted to a group of users ("consortium) or just one ("private"). Ledger integrity can be managed by a selected group of users ("permissioned") or by all users ("permissionless").

bank mandate and the market environment with a specific focus on the end-users and key private sector actors such as digital financial service providers. Finally, the design of the CBCD should be technology agnostic and the choice of technology should come at the very last stages of the design process.

The document opens with a discussion of the wholesale CBDC. The section provides a definition, the main benefits of a wholesale CBDC and design considerations specific to wholesale CBDCs. In the next section, the document will analyse retail CBDCs introducing the different operating models, technological solutions and retail CBDC-specific design considerations. The document will conclude with the cross-border dimensionality of retail and wholesale CBDC with a focus on requirements to accommodate payments across jurisdictions and currencies. The document illustrates the three CBDC types based on detailed use cases included in the annexes.

Table 1. Countries Where Retail CBDCs Are Being Explored	
Australia (on hold)	*Korea* (and *rejected*)
Bahamas	Lebanon
Bahrain	Lithuania
Canada	New Zealand (on hold)
China (and here)	Norway (ongoing)
Curaçao en Sint Maarten	*Pakistan*
Denmark (rejected)	*Palestine*
Eastern Caribbean	*Philippines*
Ecuador (pilot complete)	*Russia*
Egypt	South Africa
Euro Area (and rejected)	Sweden
Hong Kong	*Switzerland*
Iceland (rejected)	Trinidad and Tobago (rejected)
India	*Tunisia*
Indonesia	Ukraine
Iran	United Arab Emirates
Israel (rejected)	United Kingdom
Jamaica (rejected)	Uruguay (pilot)
Sources: Central banks and various news sources.	

Table 2. Countries Where Wholesale CBDCs Are Being Explored	
Cambodia	Japan
Canada	Singapore
European Central Bank	South Africa
Hong Kong	Thailand
Sources: Central banks and various news sources.	

2 Wholesale CBDC

Wholesale CBDC facilitate wholesale payment transactions between financial market participants and between the national central bank and participant financial institutions. For this purpose, wholesale CBDCs should demonstrate that their reference architecture meets the existing operational standards such as the Principles for Financial Market Infrastructures (BIS-IOSCO 2012) and their deployment enhances efficiencies in payment and settlement systems. This chapter therefore deals with reference architecture considerations for design and deployment of wholesale DFCs.

The reference architecture of wholesale CBDC could facilitate additional functionalities for payment systems. These functionalities include the handling securities settlement, liquidity savings mechanism. At the same time, consideration should be given to security, efficiency and wider market implications that such architecture could introduce into payment systems. In order to achieve these objectives, central banks should develop the reference architecture in collaboration with private sector participants right from inception in the context of the national eco-systems and legal frameworks.

2.1 Central Bank Oversight and Operation of Wholesale Payment Systems

The reference architecture constitutes an important consideration in ensuring the successful deployment of wholesale CBDCs. The wholesale CBDC architecture should foster the central bank mandate with respect to security and efficiency of the wholesale payment system as well as financial stability and integrity. Wholesale CBDCs should include an appropriate design that supports the central bank's oversight function (or any appropriate national authority entrusted with such oversight role) over the system itself, individual transactions and associated payment instructions (see below).

In traditional centralized RTGS payment systems, the central bank participates directly in all payment instructions. The central bank acts as an intermediary sitting in the middle of each transaction between two contracting financial institutions (either directly as first level validator or through a processor as second-level validator). The central bank's focal role in transaction between financial institutions settled on an RTGS helps enforce the accuracy, completeness and finality of settlement of transactions.

A decentralized wholesale CBDC design could inspire a new paradigm for the central bank's role in the validation of transactions. In a decentralized architecture, the central bank would merely receive a copy of the transaction information between financial institutions with no operational involvement in transaction processing. This will reduce the settlement time required for transaction processing, leaving the central bank to focus more on its oversight role. The central bank can engage

more in ongoing automated monitoring of transactions, and customised interventions in case of identified suspicious or invalid transactions with varying degrees of sensitivity. These interventions can be improved over time through data analytics and proactive strategies to further reduce risk in the payments system.

Decentralised architecture using technologies such as DLT has recently captured the attention of central banks. In the context of payment, clearing, and settlement, DLT enables entities using established procedures and protocols, to carry out transactions without necessarily relying on a central authority to maintain a single "golden copy" of the ledger. The existence of distributed ledgers across network participants removes the need for reconciliation of ledger entries and facilitates closing and reporting processes as ledger entries occur in real-time. A DLT-enabled wholesale CBDC may also improve the audit process, as internal and external auditors as nodes in the network could gain full access rights to the ledger thereby further alleviating the back-office function. This architecture can result in significant cost savings for all participants, reducing operational costs and promoting efficiencies in the system. DLT-based payment systems can also help to reduce fees and financial statement risks as well as optimization of interbank settlement processes (IBM 2018). However, governance of decentralized systems across institutions is far more complex as are operational process such as system updates and coordinating fault remedies etc. Notable recent DLT-based experiments include those conducted by the European Central Bank (ECB) and the Monetary Authority of Singapore (MAS). Box 1 summarizes the results of DLT-based wholesale CBDC pilots conducted by the MAS and Reserve Bank of South Africa (SARB), and research on the topic by the Central Bank of Brazil.)

Box 1: Select Central Bank DLT-Based Wholesale CBDC Case Studies and Research

a) ***Project Ubin (Monetary Authority of Singapore - MAS)***: The project concluded that multiple work-stream designs adopted for the pilot study have successfully demonstrated the feasibility of removing a central infrastructure operator in a DLT-based RTGS system. Given the system's feasibility, the project concluded that the role of MAS as an infrastructure operator in facilitating interbank payments needs to be re-evaluated (MAS 2017).

b) ***Central Bank of Brazil Staff Research Paper (Burgos et al, 2017):*** The paper analysed different DLT platforms in the context of local inter-bank payment and settlement systems (SALT). The project suggested installing a DLT-based system, without involving any DFC, as a backup to the "normal payments infrastructure". The project concluded that while DLT enabled payment systems could be inherently resilient, there are still certain unresolved issues relating to data transparency, privacy, settlement finality in certain DLT platforms.

c) ***Project Khokha by South African Reserve Bank (SARB)*** had shown that it is technically feasible to process wholesale payments between participants in a decentralized manner with full visibility to the central bank from an operational perspective (***SARB 2018***).

DLT arrangements for DFC can be designed in several ways and can support some, or all parts of a transaction flow. There are various technical and institutional design considerations in this context. Technical design typically involves concepts that specify the information to be kept on the ledger and how the ledger is to be updated. Choices in the context of ledger maintenance include maintaining either a history of all transactions or a set of account balances. Options for updating the

ledger depend upon the number of communication protocols between nodes that facilitate consensus in the network about the current state of the ledger as well as its historical record (BIS, 2017). Institutional design considerations typically involve governance decisions regarding the roles and responsibilities of actors in the operation of and access to the arrangement.

Alternative technology arrangements for DFCs, such as distributed concurrence ledgers, are also emerging in recent times, with different design considerations. These ledgers are designed in such a way that transaction processing is handled privately between only the actual counterparties to the transaction (instead of updating of ledger with involvement of all participating nodes as envisaged in a DLT arrangement (Disledger, 2017).

2.2 Efficiency of CBDC Wholesale Payment Systems

This subsection summarizes key aspects of wholesale CBDC reference architectures.

The reference architecture should follow the operational standards in existing wholesale payment systems: Wholesale payment systems ensure operational standards through their commitment to implement defined principles such as those encapsulated in the Principles for Financial Market Infrastructures (PFMIs) laid down in a joint work by the Committee on Payments and Market Infrastructure (CPMI) of the Bank for International Settlements (BIS) and International Organization of Securities Commissions (IOSCO) (CPMI-IOSCO 2012).

The reference architecture should enhance the operational efficiencies of existing wholesale payment systems. In most jurisdictions, existing domestic payments services are viewed as relatively efficient compared to cross-border services. This reflects consumers' trust in highly regulated national infrastructure providers and financial institutions, and the central monetary authority as the settlement institution in wholesale payment systems. Compared with the cross-border experience, consumers of domestic payments services are offered greater variety and lower-cost payment options; well-established rules, standards and procedures governing the use and acceptance of these various payment instruments; and reliable and/or timely funds availability (***BOC 2017***).

Participation in these wholesale payment systems is typically layered with participating financial institution representing not only their own interest, but also those of other institutions. Given the large volume of activity in these systems,[7] erroneous and duplicate entries can occur, possibly escalating into costly disputes between participating financial institutions. Such errors and disputes typically require manual or semi-automated reconciliation by the affected institutions. Currently, all participants of the domestic wholesale payment systems expend significant resources in back-office reconciliation efforts to verify and validate the information they receive from the payment system operator.

The CBDC reference architecture should enable scalable payment systems*:* Arguably, DLT is an ecosystem rather than application-level technology. Efficiencies identified above are more likely accrue only with increase in scope and scale of the ecosystem. Scalability depends on a number of factors, including confidentiality and consensus mechanisms adopted in the reference architecture, the node architecture[8] and latency as further impacted by system parameters in case of DLT

[7] There could be tens of thousands of payment messages and batch-file entries per day in a wholesale payment system.

[8] The number of nodes participating in the payment system, and the distance between these nodes.

employing block-chain architecture[9]. Central bank studies show that DLT-enabled wholesale systems are able to accommodate current volumes in the existing centralized infrastructure. However, these studies also indicated that the technology is still in its nascency and needs to evolve further to provide the desired speed for large-scale applications to operate in a live environment (Box 2).

The architecture should promote confidentiality of institutional transactional details*:* The wholesale payment systems for which this technology is now being considered for operates within a finite number of users whose identities are known to each other in a closed environment. Within such a closed system, there is a possibility that each participant will inevitably interact with all network participants. This might enable the participants to acquire a great deal of sensitive data and extract transaction graphs for a large part of the network. This capability could adversely affect the whole financial system by providing participants with confidential information about their peers and their transactions thereby introducing information asymmetry and compromising competition. The wholesale CBDC architecture should ensure that transaction details remain fully confidential, while allowing the central bank or other regulatory and supervisory bodies to have full access to the payment system. Anonymity with traceability components could enable an effective level of privacy and confidentiality relevant for permissioned decentralized networks.

Enhanced resilience of payment systems and their availability to market players should be available*:* Layered technology architecture prevalent in current wholesale payment systems operated by various central banks is susceptible to technical faults (including cyber-attacks). A DLT-enabled wholesale payment system architecture with a resilient design could address some of the technical issues by promoting "zero-incident" operations (scenario in which the multiple incidents of disruption at different nodes is minimized). A consensus mechanism that allows the independent validation of multiple-nodes could prevent contagion spreading from a cyber-hack of a single central point. Experiments by Singapore and South Africa provide insights into design considerations through presence of notary and supervisory nodes, coordinated end-to-end procedures and sufficient disaster recovery procedures. These design considerations contribute to achieving high availability redundancy and ensure business continuity.

Facilitate wider access to wholesale payment systems by non-financial institutions: Allowing access to non-bank participants has been tested in several projects such as the Hong Kong Monetary Authority (HKMA), Project Lion Rock through DLT-enabled corporate payments at the wholesale level, in addition to domestic inter-bank payments and the settlement of delivery-versus-payment of debt securities. However, this expanded access would require multiple policy changes such as the new licensing regime of Bank of England under which non-bank fintech firms are allowed to participate in central bank payment systems directly. Operational efficiency gains introduced by matured DLT systems, would allow the wholesale CBDC system to allow wider access to the networks without expanding the processing capacity of the payment system (***IBM 2018***).

Ensure acceptable trade-offs between various design considerations: Central banks should consider the individual design considerations holistically and not in isolation. The design considerations typically involve trade-offs in payment system requirements. Central bank experiments (such as Project Jasper Phase 2) point to resilience related challenges, while

[9] The number of transactions grouped together in a block (linked to the batch size), and the minimum interval needed to create a new block (timeout).

demonstrating robust privacy and acceptable transaction speed. Although the existing trade-offs are inevitable currently, technological development efforts will aspire to address these issues in the near future. For instance, settlement finality (identified as a potential design issue during early central bank experiments) has been resolved as a number of alternative consensus mechanisms have emerged[10].

Box 2: Trade-offs between Design Requirements

a) ***Project Jasper Phase 1& 2 (Bank of Canada):*** Project Jasper is a collaborative research initiative by Payments Canada, the Bank of Canada, R3 and a number of Canadian financial institutions. The project aims to understand how DLT could transform the future of payments in Canada through the exploration and comparison of two distinct DLT platforms, while also building some of the key functionalities of the existing wholesale interbank settlement system. The findings indicate that DLT platforms that employ a proof-of-work consensus protocol, as was built in Phase 1, did not deliver the necessary settlement finality and low operational risk required of core settlement systems. However, Phase 2 built a distributed ledger platform that employed an alternative consensus model using a "notary node", which delivered improvements in settlement finality scalability and privacy. However, the architecture did not adequately address operational risk requirements. Thus, the project concluded that further technological enhancements are required to satisfy the PFMIs required for any wholesale interbank payments settlement system.

b) ***Project Stella (Joint DLT Project of the ECB and the Bank of Japan):*** The project conducted in-depth experiments to determine whether certain functionalities of their respective payment systems could run on DLT. The project finds that a DLT-enabled solution could meet the performance needs of current large value payment systems. The project also confirmed the well-known trade-off between network size and node distance on one side and performance on the other side[11]. In terms of resilience and reliability, highlighted DLT's potential to withstand issues such as (i) validating node failures and (ii) incorrect data formats. As for the node failures, the test results confirmed that a validating node could recover in a relatively short period of time irrespective of downtime. The results also showed that transactions were rejected whenever the certificate authority was not available, which could possibly constitute a single point of failure (processing restarted without any other system intervention once the certificate authority became available again).

c) ***Project Khokha (South African Reserve Bank):*** The goal of the Project was to build a proof-of-concept wholesale payment system for interbank settlement using a tokenised South African rand on a DLT platform. The Project represented a central bank experiment which for the first time used the Istanbul Byzantine Fault Tolerance consensus mechanism and Pedersen commitments for confidentiality. Furthermore, the DLT nodes were operated under a variety of deployment models (on-premise, on-premise virtual machine, and cloud) and across distributed sites while processing the current South African real-time gross settlement system's high-value payments transaction volumes within a two-hour window.

[10] It is assumed that currently for CBDC a permissioned network with a consensus mechanism involving voting by participating nodes are being considered in central bank experiments.

[11] Increasing the number of validating nodes led to an increase in payment execution time. Moreover, the distance between validating nodes has an impact on performance: the time required to process transactions increased with the distance between sets of validating nodes.

The findings of the Project demonstrated an ability of the DLT system to process transactions within two seconds across a geographically distributed network of nodes using a range of cloud and internal implementations of the technology. The findings further indicated that while adopting DLT would bring about several benefits, the technology is not viable for some use cases unless adequate levels of privacy are achieved. Furthermore, the team concluded that, currently, such levels are not fully supported for the four explored deployment models with true decentralization, i.e., without relying on a trusted node or party.

2.3 Additional Functionalities for Wholesale Payment Systems

Initial pilot studies of central banks focused on building simple proofs-of-concept of wholesale payment systems using DLT, and gradually expanded their scope in subsequent phases to investigate the interconnected issues of scalability, resilience, confidentiality and finality. Emerging pilot studies of central banks are taking this experimentation further forward with central banks moving beyond the replication of existing systems and looking at how DLT can enable new models as outlined in the following paragraphs.

Based on the results of these emerging pilot studies, the reference architecture of wholesale DFC could facilitate additional functionalities of payment systems leveraging the new technology tools. In particular, payment systems deploying wholesale DFC architecture could facilitate additional functional possibilities of payment systems such as facilitating inter-operability of ledgers and promoting capabilities for atomic transaction execution. This could in turn allow smart contracting choices to market players.

Traditional settlement of transactions in financial markets involving wholesale payment systems operate under the concept of delivery v. payment (DvP) – where one asset changes hands only if the other asset changes hands (and both these ledgers for payment and asset flows are separate from each other). DvP Settlement mechanisms achieve this by linking the transfer of two assets in such a way as to ensure that the transfer of one asset occurs if and only if the transfer of the other asset also occurs. The outcome of such settlement is either both parties successfully exchanging those assets, or no transfer taking place. Such a condition is also often referred to as "atomicity" in computer science. (Note: The word, "atomic", comes from Greek meaning indivisibility or irreducibility. Atomic operations cannot be divided into smaller operations; either (i) all operations are fully performed or (ii) they are not performed at all).

Recent central bank pilot studies indicate that DLT based systems provide for possibilities of tokenization of both cash and equities on a single shared ledger resulting in better asset interactions during DVP settlement relative to current settlement mechanisms (Box 3). Transactions recorded on DLT using such DFC payment systems thus could be cheaper in aggregate than transactions recorded across multiple siloed accounts increasing the utility of the wholesale payments system. This technical feasibility (whereby any participant or function can directly interact with the assets on-ledger) and the possibilities of associated efficiency gains may offer opportunities to streamline the implementation of various DVP models beyond traditional technologies. These opportunities could be in the form of smart contracting choices between participant financial institutions, without necessarily requiring connections and institutional arrangements between them.

The design of reference architecture to unleash this opportunity could therefore merit further exploration. Reference architecture for DFC could involve considerations of interoperability,

providing central banks flexibility in determining forms in which the tokenisation of assets should take place, variables in the payment and settlement of smart contracts, and the logic / characteristics / behavioural features of smart contracts to render them immutable. DFC deployed on that architecture could be part of an atomic transaction, enabling the full and final settlement of money coupled with the movement of, or change to, the asset.

Another operational case in point for such smart contracts include DLT-based liquidity management facilities, which would enable bilateral transaction netting. It is theoretically argued that central operators cannot make entirely accurate assessments or set system parameters as they have no way of assessing the importance of payments beyond the coarse priority categorizations the systems currently allow. Neither can they assess an individual bank's cost of liquidity provision, which varies across banks and throughout the day. A decentralized approach is therefore argued to allow individual participants to make netting proposals that reflect, in real time, their own current conditions (Furgal et al 2018). However, the legality of such a mechanism is unclear.

Banks with existing unsettled payment obligations would announce these obligations to their respective obligees. System participants would collect information about netting opportunities through a recursive scanning algorithm, and competitive proposals from each bank would reflect market conditions. This structure would allow for continuous net settlement, allowing real-time netting of positions between counterparties. In essence, liquidity management can operate through a market solution facilitated through DLT, rather through the planner's solution.

The practical implementation of this, however, remains an open question considering the degree of complexity involved in determining netting solutions, quantum of information to process and proposing cost allocations. These complex situations sometimes result in a gridlock situation, whereby outgoing payments cannot be fulfilled unless an incoming payment is received or a gridlock resolution is triggered. Other practical considerations also include the manner in which as a decentralized liquidity saving mechanism might perform under extreme stress scenarios. Recent experiments of central banks are therefore exploring this operational case weighing down the necessary costs and benefits involved in using DLT for liquidity management.

DLT systems focusing on additional capabilities for payment systems should also be mindful of the safety, efficiency and wider market implications such architecture could expose the payment systems to. In this context, reference is drawn to the work of the Committee on Payments and Market Infrastructures of the BIS on the DLT in payment, clearing and settlement systems (BIS 2017).

Box 3: Select Central Bank DVP Settlement Case Studies

a) ***Project Stella (the ECB and BOJ):*** Phase 2 of Project Stella marked the beginning of extension of central bank pilot studies for considering how DLT can enable new DvP models of settlement mechanisms. DvP could be conceptually and technically designed in a DLT environment with cash and securities on the same ledger (single-ledger DvP) or on separate ones (cross-ledger DvP). Conceptual analysis and conducted experiments in Phase 2 have proven that cross-ledger DvP could function even without any connection between individual ledgers, a novelty which does not exist in current DvP settlement mechanisms. It was further observed that functionalities such as "cross-chain atomic swaps" have the potential to help ensure interoperability between ledgers (of either the same or different DLT platforms) without necessarily requiring connection and institutional arrangements between them. The key

elements to achieving cross-chain atomic swaps are the use of digital signatures and "Hashed Time Lock Contracts" (HTLC)[12] to support the atomicity in transferring two assets across two separate ledgers.

The findings however also indicated that the concrete design of DvP depends on the characteristics of the DLT platforms (e.g. range of information shared among participants, data structure and locking of delivered assets). In addition, depending on the use case, the design of DvP can be influenced by a number of factors including the interaction of the DvP arrangement with other post-trade infrastructures. The Phase 2 findings thus further indicated that depending on their concrete design, cross-ledger DvP arrangements on DLT may entail certain complexity and could give rise to additional challenges which would need to be addressed.

b) ***Project Jasper (Phase III), Bank of Canada:*** Jasper Phase III explored DLT-based interactions between the wholesale interbank payment infrastructure and the Canadian securities settlement infrastructure. Jasper Phase III enabled the parties to explore and correlate some of the specific opportunities and challenges in building out a DLT-based FMI platform. The main output was the creation of a shared ledger for token interactions with cash and equities over a single distributed network. It is observed during the pilot study that the DLT platform enables loose coupling of the components controlling cash, equities, and positions in the ecosystem. This simplifies integration with the different participants' existing systems and is expected to ease extension to additional asset and transaction types. This loose integration framework left the two authorities involved — the Bank of Canada for cash and CDS for equities — in full control of their respective instruments or tokens. The Project finally concluded with a recommendation of a more ambitious re-imagining of clearing and settlement in a decentralized form, guided by market pain points in the settlement life cycle, to arrive at a more informed premise for benefits assessment.

c) ***Project Ubin (Monetary Authority of Singapore):*** The DvP-on-DLT project is an extension of Project Ubin. This project sought to examine possible DvP settlement models and inter-ledger interoperability while achieving settlement finality on separate DLTs. Prototypes of different DLTs with varied capabilities and features were developed which allowed the transfer of tokenised assets such as SGS and CDRs on a trade-by-trade basis. It was observed that this setup provides the flexibility to compress settlement cycles, simplify post-trade settlement processes, and thereby reduces underlying risk exposures. The project findings encourage the possibility of DLT to potentially act as an enabler for smart contracting choices for DvP with consistent and coherent implementation of rights and obligations that will increase investor confidence and reduce compliance costs in the market.

Phase 2 of Project Ubin further explored the use of DLT for specific RTGS functionalities. Particularly, it focuses on the feasibility of decentralising Liquidity Saving Mechanisms, while maintaining privacy of banking transactions. The Project prototypes demonstrate that there are different methods to initiate gridlock resolution in a decentralised system (and also detect and avoid simultaneous gridlock resolution). In other words, there is flexibility to select how and which node initiates gridlock resolution, be it scheduled, user-triggered or based on a predefined state or event. However, the mechanism of initiating gridlock resolution may lead to unintended consequences and inequality among participants in the network. In addition,

[12] For further information about HTLC, refer to Joseph Poon and Thaddeus Dryja (January 2016)

LSM processing may take a longer time in a large network, which may result in delay to the settlement.

2.4 Market Environment and Eco-system Considerations

DLT platforms could make possible to create a unique shared view of a large variety of information fed and replicated across institutions. In order to achieve this possibility, the development of reference architecture of wholesale DFC should be undertaken by central banks with the participation of private sector participants right from inception, and with due considerations to national eco-systems for embracing new technologies.

DFC architecture should be developed in partnership with private sector (including technology providers). DFC should be designed in partnership with the private sector as it is necessary to engage stakeholders from the start, rather than impose new technology on participants. The design considerations with respect to message flows (either directly to central bank or via a processor, in a centralised architecture) and mechanisms for validation of transactions (pre-defined audit tools and ongoing monitoring criteria for defining invalid transactions in unambiguous terms, together with rights of parties in case of such invalidations later by central banks – all in case of a decentralised architecture) are better implemented with the involvement of private sector players right at the inception stage in developing the right DFC architecture.

Experiments by Central Bank of Brazil, for instance, indicated that the value of DLT platforms is intimately tied to the network effect. Partnerships with another government agencies and private enterprises are therefore considered very important for exploring the emerging new possibilities, when it comes to share information between agencies, with large foreseeable benefits to society.

At this juncture, it should be further noted that such experiments should also be mindful of the safety, efficiency and wider market implications such architecture could expose the payment systems to.

DFC using DLT architecture will be as much successful as the maturity of the ecosystem that is ready to embrace its fully potential. This maturity is attained only if the whole ecosystem involving market participants are convinced that the technology that runs this system is inviolable and absolutely correct under all circumstances. This would mean that the participants should collectively agree that there is no opportunity for any form of malicious behaviour to upset the logic of the system once set in place. This requires trust in the hardware, network, DLT and application layers – all facilitated through legal and institutional pre-requisites for addressing the unforeseen eventualities.

3 Retail CBDC

A retail CBDC as a widely accessible digital representation of a sovereign currency that is issued by, and a liability of, a jurisdiction's central bank or monetary authority, and generally be legal tender.

Motivations for exploring CBDC issuance vary from country to country. The dwindling use of cash in advanced economies such as Sweden catalyzed the potential role of retail CBDC as an

alternative, robust, and convenient payment method. The central banks of Ecuador and Uruguay are exploring retail CBDC to improve operational and cost efficiency. In countries with underdeveloped financial systems and many unbanked citizens, CBDCs may be seen as a means to improve financial inclusion. For some central banks in emerging market economies additional motivations relate to supporting digitalization, combatting financial crime, and expanding macro-prudential tools (Barontini and Holden, 2019). CBDC would also help facilitate monitoring illegal activities otherwise resulting from the use of (anonymous) physical cash.

Retail CBDC may also contribute to optimizing the payment function of fiat money, reducing reliance on payment services provided by the private sector, alleviating the regulatory burdens and pressure on the central bank, and strengthening the authority of fiat money. Moreover, CBDC may help to address the dilemmas of modern monetary policies, including inefficiencies in policy transmission, difficulties in countercyclical control, flow of currency away from the real economy toward the virtual economy, and inadequate management of policy expectations (Qian, 2018).[13]

Specific design features depend on CBDC policy objectives, while key design principles are foundational and independent. Key design principles such as security, user-centricity, and flexibility by design form the foundation for and CBDC and guide the design process from the onset of the implementation. Central banks can also leverage specific design principles to develop a business and technology architecture, which best suits their policy objective. These specific design principles are independent of a specific technology choice. Traditional back-end and front-end solutions, distributed ledger technology (DLT), hybrid versions or other technologies can be considered, but only at the final stages of implementation.

CBDCs can be designed in line with international AML/CFT standards, while allowing for a certain degree of anonymity and privacy. The Financial Action Task Force (FATF) [14] has issued a set of pertinent AML/CFT standards that intend to guide financial institutions and designated non-financial businesses in implementing customer due diligence and monitoring and reporting of suspicious transactions. A well-designed CBDC will strike the right balance between the need to comply with AML/CFT standards and provide some level of anonymity and privacy. A certain level of anonymity is important particularly if the CBDC is designed for use in countries, where large segments of the population lack identification and cash remains the prevalent means of payment.

On the flip-side, a greater level of anonymity introduces challenges to detecting fraud or for users to prove and claim ownership over lost or stolen CBDC. In this case, user identities could be linked to the mobile wallet or device that the CBDC is stored in. In the case of the e-Peso, digital banknotes were assigned a unique series ID that is linked to a specific user wallet. The ePiso required identification for amounts that exceed a certain threshold. Even if identity is determined at the device or wallet-level managed by third-party, sensitive user identity data needs to be protected from

[13] IMF (2018) concludes that the introduction of CBDC is unlikely to significantly affect the main channels of monetary policy transmission under plausible CBDC designs. Even in the scenario where private banks were no longer involved in intermediating payments, having lost the business to CBDC when demand for reserves would disappear, monetary policy has the means to remain effective through adjustments of the interest rate paid on CBDC (Woodford 2000). In fact, even an unremunerated CBDC could increase the efficiency of monetary policy transmission because the speed of transmission of monetary policy into market interest rates would likely increase (Duffie 2019).

[14] The FATF is an independent inter-governmental body that develops and promotes policies to protect the global financial system against money laundering, terrorist financing and the financing of proliferation of weapons of mass destruction.

unauthorized disclosure, misuse or breaches. Adequate regulation and legislation can ensure consumer and data protection, as could contractual agreements between the central bank and third-party wallet or telecommunication providers.

CBDC could have offline capabilities to provide the same 24/7 availability as cash. This would be useful when temporary electricity or infrastructure breakdowns occur, but no digital currency will be impervious to catastrophic events.[15] Such designs include recharge cards, quick response (QR) code based prepaid cards and smart chip enabled banknotes.[16] Sveriges Riksbank (2018) suggests that an account-based CBDC could offer offline functionality with a "regulatory framework that defines how the risks (in particular liquidity risks) are divided between different agents, how many payments can be made offline and in what amount."

A CBDC could be designed to pay interest to incentive its adoption. Also, an interest-bearing CBDC would eliminate the effective lower bound on interest-rate policy, but only with constraints on cash usage.[17] Paying interest would bring operational challenges to interest calculation and have an adverse impact on the anonymity due to tax reporting requirements. None of the central banks exploring CBDC issuance are considering making them interest-bearing. However, Sweden's eKrona, will have the built-in ability to pay interest if the central bank ever opted to introduce this feature.

Alternatively, transaction fees could be introduced to supplement financial control and prevent overload or misuse of the whole system. CBDC could potentially expand its usage to the internet of things (IoT) machine-to-machine transactions. A fee structure could mitigate the risk of IoT-enabled denial-of-service (DoS) attacks shut down the system. [18] Transaction fees could be fixed amounts, percentage or volume based and could vary depending on types of transactions or transaction volumes. For example, business-to-business transactions might draw higher fees than person-to-person ones.

3.1 Retail CBDC design principles and attributes

The table below summarizes the design principles and attributes collated from various publicly available sources.

Table 3: Summary of Retail CBDC design principles and attributes

[15] A recurrence of the 1859 Carrington Event could knock out communications and power for up to a year, and render any digital money useless.

[16] It is worth noting that combining blockchain with smart chip and near-field communication (NFC) technologies, a "smart banknote" could be used just like cash. The smart banknote has a tamper proof chip securing a private key, the balance can be verified by any NFC enabled smartphone, the settlement can be instantaneous, and the anonymity feature is preserved.

[17] Policy rates could reach deep into negative territory. In the interim, other measures have been proposed to do so, but with questionable feasibility and without necessarily requiring CBDC. Cash could be barred altogether as argued in [Rogoff (2014)], made costly to hold as suggested in [Bordo and Levin (2017)], or made to depreciate against CBDC which would become the sole legal tender as in [Agarwal and Kimball (2015)]. Note that if CBDC were not interest bearing, the effective lower bound could bind at even higher rates of interest, as CBDC could be stored more cheaply than cash. CBDC has also been touted as a means to implement helicopter drops by crediting CBDC accounts, or wallets holding CBDC tokens. However, doing so would not necessarily reach all citizens. Moreover, the issue of legitimacy remains: how does the central bank decide how much to transfer to each household given the notable and very explicit redistributional consequences? Finally, helicopter drops would continue to be viewed as a form of monetary financing, thus undermining central bank independence.

[18] Denial of Service attacks are designed to overload APIs with a massive number of requests until the service stops responding.

Policy	✓ Designed within the central bank's monetary policy and financial stability framework. ✓ Mitigates the risk of financial sector disintermediation, possible by including it in the ecosystem (see below). ✓ Could pay interest or be interest free with an option to include it at a later date. ✓ Mimics cash functionality; fast and efficient value transfer regardless of load, free or low cost to transact, ubiquitous, widely available 24/7 with or without connectivity, and can be used by users who do not have bank accounts. ✓ If there are multiple versions of the CBDC available, they should be interchangeable. ✓ Mechanisms for issuance, distribution and payments should be technology agnostic.
Security	✓ Highly secure, trusted modern cryptographic mechanisms; not easily counterfeited ✓ Generated and destroyed in a secure, supervised activity
Auditability and traceability	✓ Parameterized to balance between privacy and traceability of transactions and parties ✓ Traceable; auditable in terms of proof of issuance and ownership, and transactions for all ecosystem participants within privacy constraints. ✓ Recovery of funds in case of system failure, for example, in the event of wallet failure, loss or theft, or failure of a service provider.
Flexibility	✓ The platform is developed on a foundation that can be built on later in stages. ✓ Configurable in design to keep pace with market and technology developments and can keep up with growing demand. ✓ Interoperability at all levels throughout the payment system

The above principles and attributes are expected to evolve as the central banks and international organizations continue their research into the topic and as the pilot projects and commercial implementations continue to contribute to the body of knowledge.

3.2 Possible DFC Architectures

Retail CBDC implementations can follow many architectural principles and mix various technological approaches to solve the various challenges and accommodate the above,

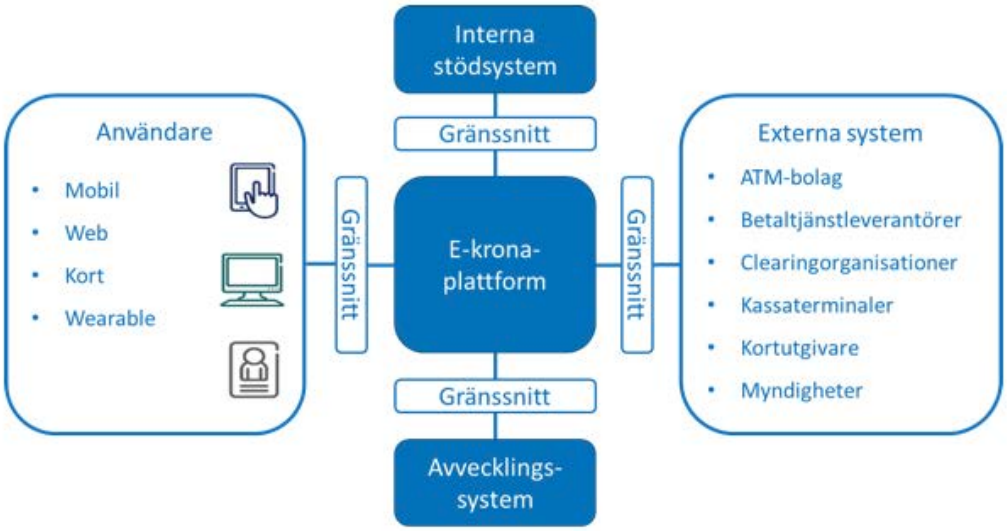
sometimes conflicting, principles and features. A few possible architectures emerged recently and fall into three broad categories; centralized system, widely accessible and centralized "DFC as a service" systems, and hierarchical, distributed networks with centralized control of supply.

3.2.1 Centralized system

In centralized implementations, the central bank controls the technical infrastructure through which and end-to-end DFC solution is delivered to the public. The system delivers all necessary components and features, including the electronic wallets available to the public, the DFC itself, security, and transactional ability to effect the payments, including interfaces to other financial systems. This approach appears to have been taken by the now defunct dinero elecrónico project in Ecuador.

3.2.2 Accessible DFC as-a-service

In a DFC as-a-service architecture the central authority controls the components necessary to deliver DFC capabilities through APIs available to banks and other financial institutions including e-money operators. The transactional ability is centralized but the wallets are managed by the financial institutions who can continue to compete and provide value-added services. This approach appears to be taken by the Sveriges Riksbank e-Krona project. The following diagram is taken from the e-Krona project documentation.



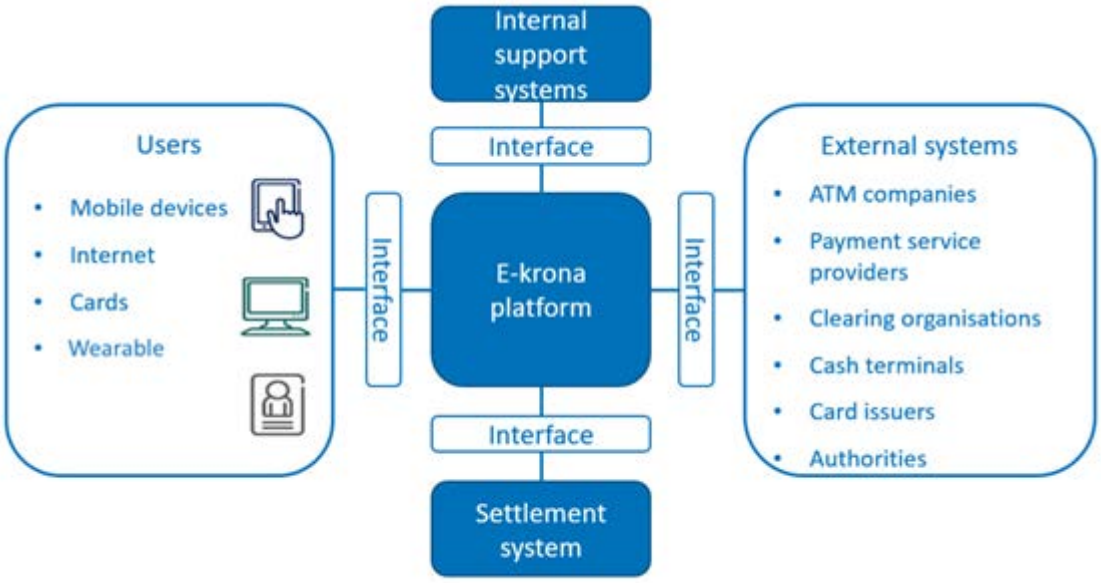


Figure 1: Riksbank e-Krona Architecture

3.2.3 Hierarchical, distributed network

In a hierarchical, distributed network approach, the central bank controls the source of DFC including its security and amount to be created and distributed, but the distribution and transaction chain closely matches that of physical cash. The DFC value is distributed along the existing channels of commercial banks and e-money operators and ends up in the hands of the public. This is the approach being discussed by the People's Bank of China (PBOC)[19] and apparently taken recently by the South African Reserve Bank (SARB). The following diagram is taken from the solicitation of the Expression of Interest to "…investigate the feasibility, desirability and appropriateness…" of the retail CBDC[20].

[19] https://www.itu.int/en/ITU-T/Workshops-and-Seminars/20180718/Documents/Yao%20Qian.pdf https://www.itu.int/en/ITU-T/Workshops-and-Seminars/20180718/Documents/Yao%20Qian.pdf

[20] https://www.resbank.co.za/AboutUs/Departments/FinancialServices/ProcNew/Lists/News%20and%20Publications/Attachments/40/EOI%20MR01-2019-0.pdf https://www.resbank.co.za/AboutUs/Departments/FinancialServices/ProcNew/Lists/News%20and%20Publications/Attachments/40/EOI%20MR01-2019-0.pdf

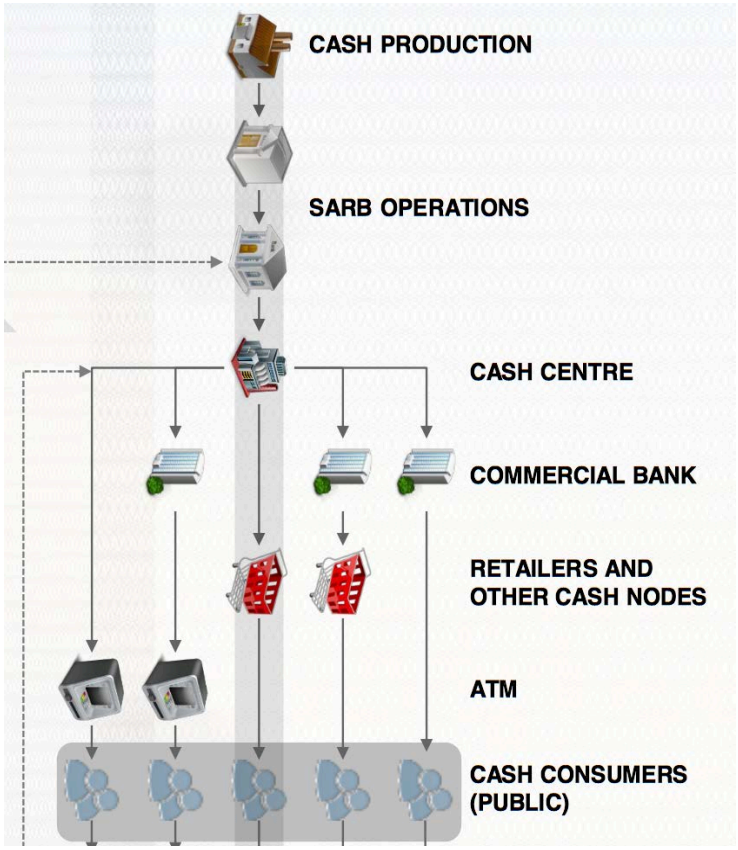


Figure 2: SARB Retail CBDC Architecture

4 Cross-Border CBDC

So far, DFC projects have focused on domestic-only applications, but central banks and others are starting to think about cross-border systems. Many concerns related to domestic large value payment systems will be of relevance to cross-border payment systems for wholesale and retail purposes. However, there are specific concerns related to cross-border payments which we run through below.

4.1 Heterogeneity of Domestic Systems

Cross-border systems will typically require updates to multiple systems but at a minimum of two settlement systems in different jurisdictions. Most domestic settlement systems are not based on a common platform hence a reference architecture will need to assume a variety of settlement systems.

Common set of standards and interfaces in these domestic settlement systems will facilitate easy integration. Currently, several RTGS operators are looking at modernizing and renewing their payments infrastructure to facilitate change in payments and settlement. For example, many of these projects are moving towards implementing ISO 20022 messaging standards.[21] These initiatives can help to harmonise standards and help to improve integration between systems.

[21] ISO 20022 is a global standard for exchanging electronic messages between financial institutions.

4.2 Sovereignty, Oversight and Governance

A cross-border transaction spans two or more jurisdictions and there may be a lack of common payment standards and regulator requirements across jurisdiction. A reference architecture will need to demonstrate functional support for the laws and regulations for multiple jurisdictions and be able to manage any variations across jurisdictions. Appropriate governance structure can introduce and maintain common regulatory standards and regulations across multiple jurisdictions to reduce duplication of activities (e.g., sanctions screening, payment purpose codes). One approach may be for the reference architecture to reflect some *common* set of functions supporting oversight and governance in a manner that is extensible for additional requirements by jurisdiction.

4.3 Compliance

Today an international regulatory framework exists alongside domestic regulation to combat money laundering and the financing of terrorism and other cross-jurisdiction economic crimes. Many jurisdictions have additional domestic regulatory requirements, which add more complexity. Banks across the payment value chain must comply with multiple regulatory requirements (e.g., FATF AML/CFT standards) and assessment of collateral requirements. The divergence in regulatory standards across jurisdictions adds to overall cost, delay in processing etc. The reference architecture will need to support mechanisms to facilitate regulatory compliance as the transaction travels through different jurisdictions.

4.4 Business Models

Cross-border payments involve multiple jurisdictions with different designs. Domestic forces in each jurisdiction will shape the CBDC designs which can be quite different from other jurisdictions. For example, one central bank may decide to operate the CBDC itself while another may decide to outsource the operations to regulated third-party entities. These differences in CBDC design should be accommodated by the reference architecture while not impacting seamless interoperability, which is important for cross-border payments.

4.5 Trust Model

Cross-border payments today rely on correspondent banking that is subject to counter party risk, inefficient liquidity management and cumbersome reconciliation. CBDC reference architecture should aim to make cross-border payments less risky and more efficient. In BoC et al., 2019, Bank of Canada and MAS linked up Project Jasper and Project Ubin, their respective experimental domestic payment networks built on two different DLT platforms (Corda for Jasper and Quorum for Ubin). The project used Hash and Time-Locked Contracts (HTLC) to connect the two networks and allow a cross-border payment without the need for a trusted third-party intermediary.

4.6 Settlement Instrument

Central bank money is a risk-free instrument, consequently it is the preferred instrument for settlement (defined as the point where the obligation of a payer is extinguished, and the transaction is irreversible). Except for payment between two accounts at the same institution (and 'on us' transaction) payments ultimately are settled in central bank money (they may be aggregated in retail systems and settled in central bank large value systems). Any reference architecture will have to encompass the idea that cross-border payment will end in settlement on the books of the central bank.

In systems such as the Jasper experiments, where a *proxy* for central bank money resides on a distributed ledger (rather than a ledger at the central bank), the reference architecture will need to distinguish between two possibilities: where there is legal underpinning such that exchange of the proxy (often referred to as a token) is considered settlement; where there is no such legal underpinning and the exchange of the proxy is only part of clearing, and final settlement still takes place on the large value payment system.

In the case of a universal currency (U-CBDC) the situation is similar to that of a domestic system. A U-CBDC is a wholesale CBDC backed by a basket of currencies and accepted by all participating jurisdictions. In this case, the liability of the issued instrument is with the issuing institution(s), i.e. any institution could use the U-CBDC unit of account, but settlement would have to be on the books of the issuing central bank(s) (or possibly a pan-national institution with similar risk characteristics to a central bank).

Cross-border payments often involve foreign exchange (FX) since the sender holds local currency, while the receiver would like to receive funds in its own local currency which is the foreign currency from the sender point of view. In this scenario, a cross-border payment transaction can be considered as two separate logical steps that can be carried out in either order: Step 1 is FX trade of local currency to foreign currency, and Step 2 is a transfer of foreign currency to the receiver.

4.7 Confidentiality

The degree of confidentiality vis-à-vis the central bank needs to be balanced among other things with concerns relating to compliance with, for example, anti-money laundering, anti-terrorist financing etc. As per the note of oversight above, the reference architecture will need to address the differing privacy regimes across jurisdictions.

4.8 Transparency

There is a lack of transparency in the current cross-border system in terms of fees charged by the correspondent banks in the payment process, the time it takes for the payment to settle, and where in the process a transaction currently sits. The reference architecture will need to describe mechanisms to balance privacy, transparency and compliance in a manner flexible enough across the needs of different jurisdictions.

4.9 Access

CBDC reference architecture should ensure broad access to the wide range of domestic and foreign entities to enable effective cross-border payments. However, today, the range of eligible institutions with access to central bank money and access to RTGS settlements accounts varies somewhat across jurisdictions, but eligibility is limited and the bar to access is high. In addition, there are regulatory requirements for all payment system participants to comply with counter terrorism financing, prevention of money laundering and international sanctions regimes. Often these regulatory standards differ across jurisdictions or may be supplemented by additional requirements such as currency controls.

Combining technical requirements with different regulatory standards across jurisdictions further complicates a particular institution having access to settlement accounts in different countries simultaneously. Consequently, few banks are willing to maintain a global network of settlement accounts in multiple jurisdictions.

4.10 Speed

The reference architecture should aim for real-time or near real-time settlement of the cross-border payment transaction. In that regard, the CBDC objective is to ensure cross-border payment velocity and, therefore, that funds can be credited to the beneficiary quickly.

4.11 Cost

CBDC reference architecture should aim to enable cross-border payment process optimization to reduce the overall cost to the consumer. Today, cross-border payments are typically perceived as expensive (compared to domestic payments) and lacking in transparency in terms of costs. This is primarily due to complexity of cross-border payment and settlement processes involving multiple entities in execution and settlement, differences in regulatory policies and standards across jurisdictions, and the use of legacy systems and infrastructure.

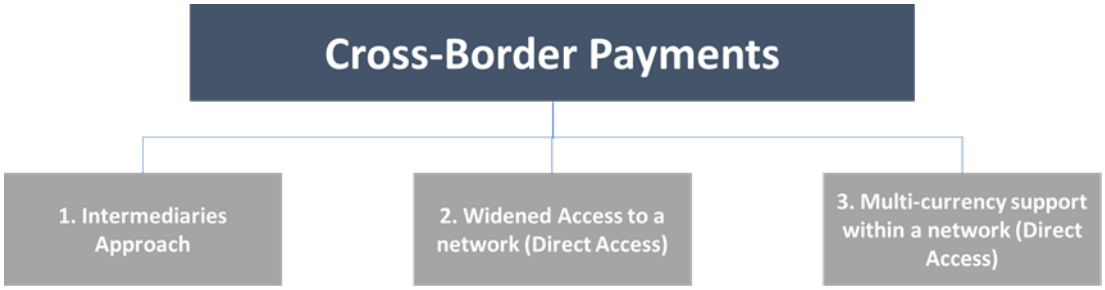
5 Cross-Border CBDC Architecture Options

The two main high-level architecture options for Cross-Border are interoperable domestic CBDCs and a universal CBDC.

5.1 Interoperable Domestic CBDCs

There are many architecture options available for a domestic CBDC: centralized solutions, DLT-based decentralized solutions and hybrid solutions consisting of some central components in a DLT-based solution. These domestic CBDC solutions must be efficiently interoperable to best support cross-border payment transactions.

BoC et al., 2018 proposed three broad conceptual design options for cross-border payments. The first option involves intermediaries and the second and third involve granting transacting parties access to the central bank's liabilities.



Intermediaries approach	**Direct** **widened access**	**Direct** **multiple-currencies**
• also known as **asset swap via intermediary** • needs intermediary for foreign exchange and transfer	• also known as direct access • does not involve intermediary	• also known as **asset transfer** • allows for multiple currencies within the same network • still need intermediary (which could be the central banks) for transfer

Figure 3: Cross-Border Payment Options (Source: BoC et al., 2018)

5.2 Universal CBDC

Several participating jurisdictions, through either their respective central banks or a global multilateral institution, agree to create a U-CBDC. The U-CBDC will be backed by a basket of currencies issued by the participating central banks. The U-CBDC would be issued via an exchange specifically created to allow for issuance and redemption of such U-CBDCs.

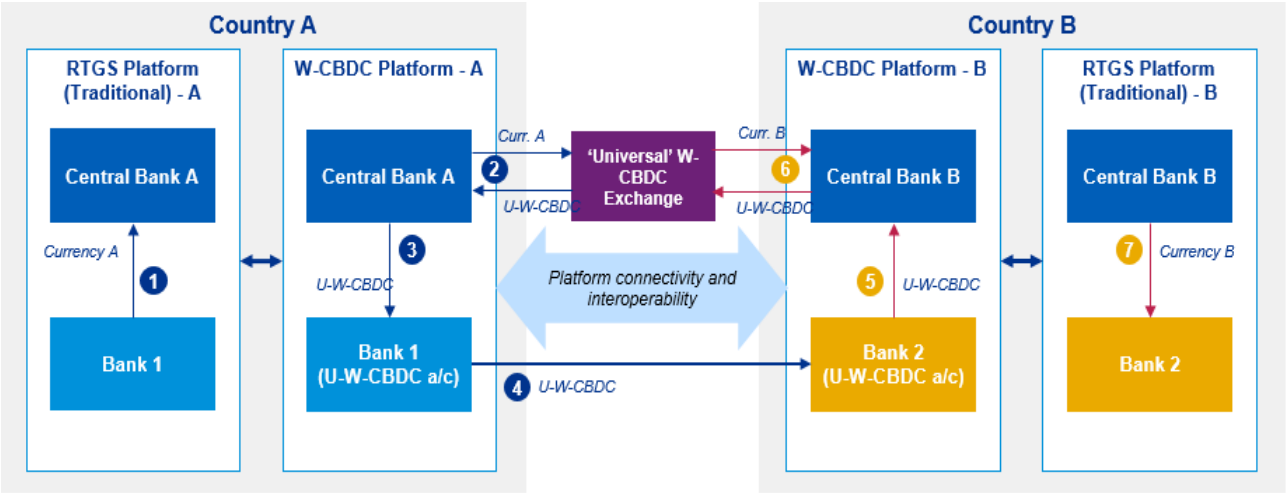


Figure 4: Universal CBDC (Source: BoC et al., 2018)

6 Cross-Border Wholesale CBDC Case Studies

This section summarizes some of the research projects that have recently been undertaken by the industry in the cross-border payment area.

6.1 Cross-Border Interbank Payments and Settlements

This project is a collaboration between the Bank of Canada (BoC), the Bank of England (BoE) and the Monetary Authority of Singapore (MAS) in consultation with a group of commercial banks. It examines the existing challenges and frictions in the cross-border payments and proposes new and more efficient models for processing cross-border transactions.

As part of this project, the following challenges were explored from end-users, commercial banks and central banks prospective:

- Lack of transparency regarding payment status, visibility and certainty of outcome
- Limited availability of cross-border payment services
- Time taken for payment processing
- High costs associated with the correspondent banking model
- Challenges associated with legacy payments infrastructure across networks, central banks and commercial banks

The project proposed a potential future state with the list of capabilities that must be delivered by any future model for cross-model payments and settlement. It also proposes three hypothetical models that might deliver some of the future-state capabilities and benefits:

- Model 1: is the collection of current and planned industry initiates.
- Model 2: is based on the expanded role for the industry RTGS operators that acts as "super-correspondents" for settling cross-border payments instead of relying on intermediary banks as corresponding banks.

- Model 3a, 3b and 3c are variations based on the settlement of cross-border payments between banks using W-CBDCs. These are a tokenized, limited-access form of central bank liabilities used for wholesale interbank payment and settlement transactions.

Model 3a is based on currency-specific W-CBDCs where these W-CBDCs can be transmitted and exchanged only ***within their home jurisdictions*** and cannot be transmitted outside their home jurisdictions. In this model, each central bank provides wallets for W-CBDC only in their own currency. This would require commercial banks to open wallets with multiple central banks if they wish to hold multiple currencies.

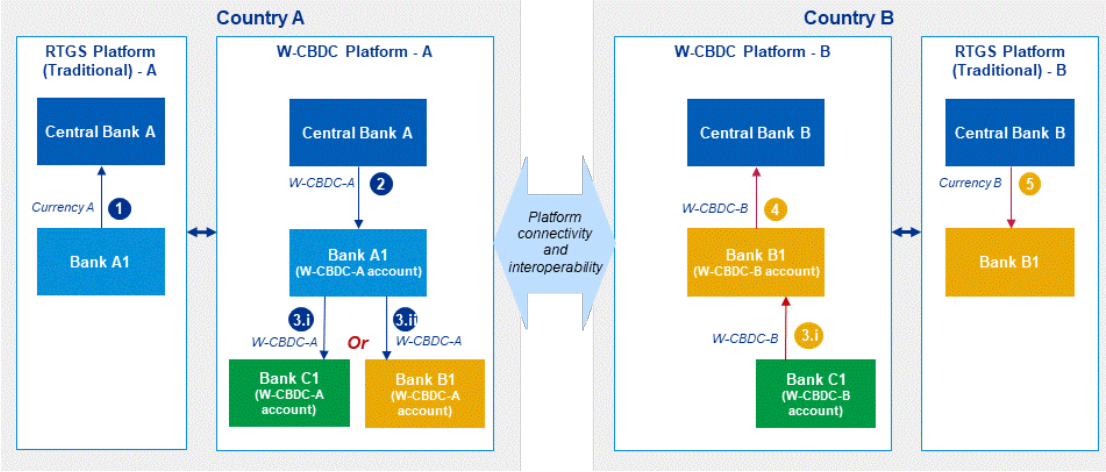


Figure 5: Model 3a Cross-Border Wholesale CBDC (Source: BoC et al., 2018)

Model 3b is similar to Model 3a but based on currency-specific W-CBDCs that can be transmitted and exchanged ***beyond their home jurisdictions.*** In this model, commercial banks can hold multiple W-CBDC wallets with their home central bank (e.g., a bank based in Canada could hold W-CBDC in Canadian dollars, pounds sterling and Singapore dollars in a wallet with the Bank of Canada). This would require each central bank to support multiple W-CBDC tokens.

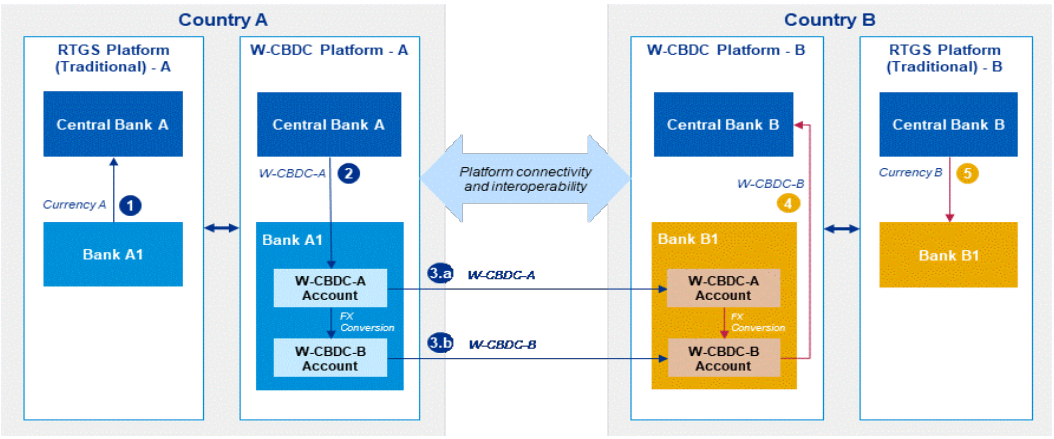


Figure 6: Model 3b Cross-Border Wholesale CBDC (Source: BoC et al., 2018)

Model 3c is based on a universal W-CBDC that is backed by a basket of currencies and accepted by all participating jurisdictions. In other words, this model does not involve the use of multiple currency-specific W-CBDCs like Model 3a and Model 3b do; rather, it involves a single universal W-CBDC.

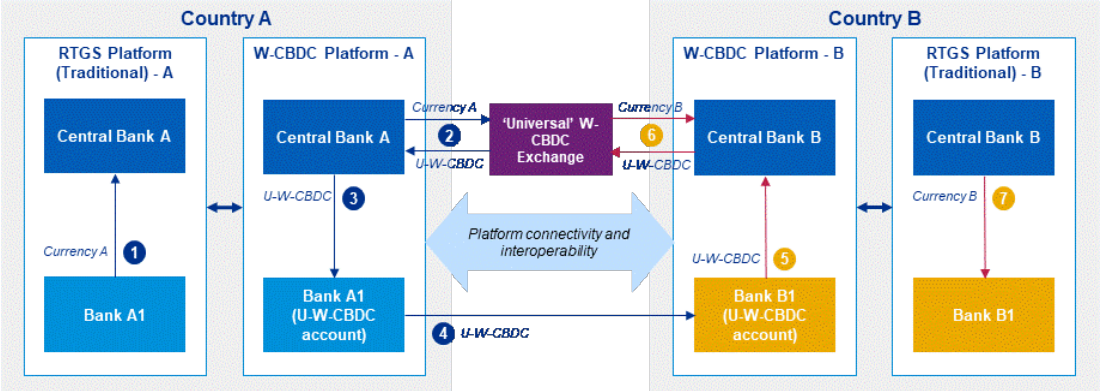


Figure 7: Model 3c Cross-Border Wholesale CBDC (Source: BoC et al., 2018)

The project report emphasizes that it provides a starting point for further analysis of these potential future models. Further consideration should be given to the following topics:

- The legal and regulatory requirements and risks associated with each model
- The necessary cross-jurisdictional governance framework required to ensure harmonized standards—both in definition and in implementation
- The impact on monetary policy and the degree to which the central bank will continue to exercise control over it
- Legislative changes required to recognize W-CBDCs as legal tender for interbank payments and settlements
- Eligibility criteria for banks to become direct participants in these models, including coordination between central banks to align eligibility criteria
- Industry adoption of the selected model via incentives and regulatory changes

BoC and MAS further collaborated to explore the technical architecture for two of the models (Model 3a and 3b) by building a proof of concept to understand the technical challenges in implementing these models.

6.2 Enabling Cross-Border High Value Transfer Using Distributed Ledger Technologies

This project (Jasper-Ubin) is a collaboration between the Bank of Canada (BoC) and the Monetary Authority of Singapore (MAS). This project assumes that DLT-based domestic gross settlement (RTGS) systems sit on different platforms in each country – in this case, on R3's Corda platform in Canada and JP Morgan's Quorum platform in Singapore. A tokenized form of a wholesale CBDC (W-CBDC) is issued on these DLT networks by each respective central bank for use by commercial banks. As part of this project, the BoC and MAS, together with Accenture and JP Morgan designed and build proof of concept solutions to realize an atomic transaction for a Canadian Dollar (CAD) – Singapore Dollar (SGD) payment across two DLT platforms, based on HTLCs, without a trusted third party.

The project proposes three broad conceptual design options for cross-border payments where a sender and a receiver are transacting on different ledgers with different currencies. The first option involves using intermediaries, and the second and third involve granting transacting parties access to the central bank's liabilities.

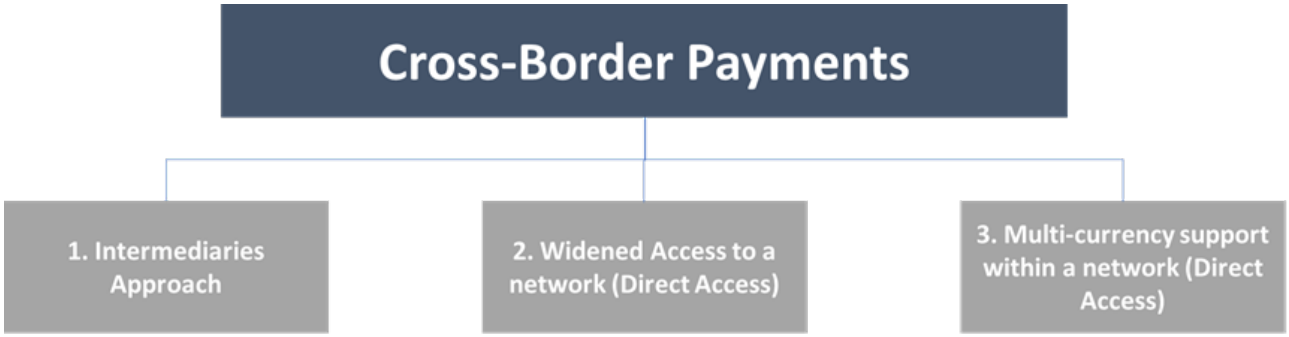


Figure 8: Cross-Border Transaction Approches (Source: BoC et al., 2019)

The following table summarizes the characteristics of these three design options.

Table 4: Cross-Border Payments Summary (Source: BoC et al., 2019)

Intermediaries approach	Direct widened access	Direct multiple-currencies
• also known as asset swap via intermediary • needs intermediary for foreign exchange and transfer	• also known as direct access • does not involve intermediary	• also known as **asset transfer** • allows for multiple currencies within the same network • still need intermediary (which could be the central banks) for transfer

As part of the project, HTLC sequence flows are designed for these design options and are documented in the report. To verify the design, a proof of concept was successfully developed to prove the technical feasibility of transacting atomically across two dissimilar blockchain networks using HTLC. In the Singapore network, local Bank A and Intermediary A in Singapore will use two different Quorum nodes. In the Canada blockchain, Intermediary A and local Bank B in Canada will use two different Corda nodes. Intermediary A has a presence in both networks and acts as an intermediary. (See Figure 7 for the proof of concept set-up)

The project successfully implemented and demonstrated the ability to perform atomic transactions between a Quorum-based network in Singapore and a Corda-based network in Canada using HTLC. Following are the key findings, challenges and limitations of these solutions:

- The DLT platform must support the specific features (locking, secret disclosure and timeout) to successfully build the HTLC functionality
- Further study and experiments are required to prove the feasibility of HTLC across more than two networks.
- More study and experiments are required to prove the scalability of the design in real-world scenario where there are hundreds to thousands of participants on each network.
- The HTLC protocol requires off-chain transfer of secret in a timely manner which introduces some failure scenarios that needs to be handled.

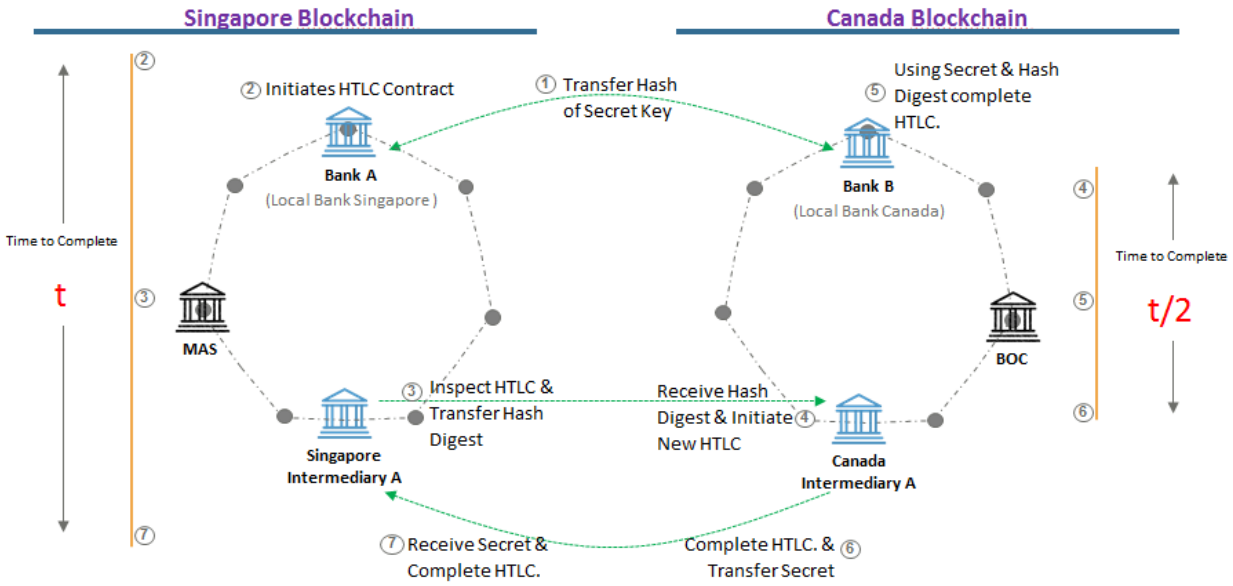


Figure 9: Cross-Border Payment Proof of Concept Setup (Source: BoC et al., 2019)

6.3 Utility Settlement Coin

The Utility Settlement Coin (USC) project involves several of the world's largest financial institutions (FIs) to provide a tokenized payment instrument on a DLT/blockchain platform.[22] The value proposition is based on the hypothesis that the wholesale asset markets are tokenizing and that without an equivalent tokenized pay leg, this asset tokenisation is unlikely to completely achieve the desired efficiencies that their business cases promise. USC is intended to provide the payment leg to those tokenized assets. The settlement coin will be a digital currency, backed by the cash assets at a central bank (but is not issued by, and therefore not a liability of, the central bank), with the objective of easy ownership transfer with reduced process complexity and settlement time.

USC uses the DLT framework (Autonity) provided by Clearmatics and is based on an Ethereum Fork. Autonity supports deterministic finality, and the ability to permission validators and network access. Autonity works in harmony with Ion, a general interoperability framework, to support interoperability between Ethereum chains, and even Ethereum and non-Ethereum platforms.

Unlike Bitcoin, USC will not be a cryptocurrency. It will be a digital cash equivalent of each of the major currencies backed by central bank money, such as a dollar or euro. Each USC would represent fiat currency on a one-to-one basis and would thus be 100% backed by collateral at the domestic central bank. It will act as a convertible stand-in for major currencies.

The USC consortium is taking a phased approach for designing and implementing USC from concept (Phase 1) to legal and regulatory compliance (Phase II) to test (Phase III) and finally to live implementation (phase IV). In June 2019 the USC consortium closed a £50 million Series A equity funding round of and is pursuing regulatory clearance.[23]

6.4 Cross Border Settlement with Central Bank Money

[22] These are the 11 FIs that were originally made public in 2018: Barclays, CIBC, Credit Suisse, HSBC, MUFG, State Street, UBS, BNY Mellon, Deutsche Bank, Santander and Nex (CME).

[23] https://blog.fnality.org/news-views/usc-continues-to-evolve

R3 conducted a study, "Cross-Border Settlement Systems: Blockchain Models Involving Central Bank Money," intended to invite further development of new, different approaches for improving wholesale cross-border settlement using distributed ledger technology (DLT). While the first group of proposed models would heavily involve central banks, the second group would involve a trusted third party and a more passive role for central banks.

The models were evaluated based on monetary supply implications, impact on liquidity management for commercial banks, settlement risk, credit risk, and complexity for central banks. For each option, the components of the method, the actions undertaken, and conceptual evaluations of the method are presented.

Intermediate Cryptocurrency

The paper proposes an intermediate cryptocurrency, which would circulate only within the interbank market, accessible solely to financial institutions. Such an approach has several fundamental requirements:

1. **Wide adoption**: An intermediate cryptocurrency should be honored as a valid settlement asset across multiple currency jurisdictions at least. Some examples would be universally accessible.
2. **Stable market value**: An intermediate cryptocurrency should have stable market value to fulfill the function of value storage and facilitate value transfer across currency zones. Therefore, an intermediate cryptocurrency issued by a central bank should be pegged and convertible with the fiat currency issued by the central bank at par. The value of the cryptocurrency would be solidly supported by the value of the corresponding domestic fiat currency. The cryptocurrency also inherits the popularity from domestic money and would fit better with existing market infrastructures.
3. **Deep liquidity**: As both the volume and value of transactions are large through the cross-border wholesale payment system, there should be large and fluctuating demand for converting between the intermediate cryptocurrency and desired local currencies, which requires the existence of market makers to provide sufficient liquidity.

Central Bank Issuer

Three models proposed assume active involvement of central banks. The first model involves central banks issuing their own cryptocurrencies. The second model involves central banks coordinating to issue a dual-registered cryptocurrency for a specific currency pair. The third model involves credit lines. The first two models were determined to be particularly useful to continue to develop. Conversely, the third significantly departs from the traditional role of the central bank, and has the potential to dramatically expand the central bank's balance sheet and influence the money supply.

Trusted Third Party (TTP) Issuer Models

In contrast to the central bank focus of the previous models, the second set of four models use a trusted third party that is not a central bank. They are differentiated based on how the issuer of the DR is involved in the process of clearing and settlement and who bears what kinds of risk. The paper evaluated a private sector-issued intermediate cryptocurrency, a pre-funded escrow account approach, a CLS-like model, and a deficit-funded account model.

For this approach, there would be value in having regulators play a role as coordinators. This would bring market participants together to develop best practices and standards for TTPs. The regulator could monitor transaction activity on the ledger and see how market structure may change with the introduction of DLT. Regulators (and also central banks) would need to at least have a passive role in the development of any of these solutions.

Annex 1: Potential configurations of DLT arrangements (Source: BIS 2017)

<table>
<tr><td>Description of arrangement</td><td>One entity maintains and updates the ledger
(for example, a typical FMI)</td><td>Only approved entities can use the service; entities can be assigned distinct restricted roles</td><td>Only approved entities can use the service; entities can play any role</td><td>Any entity can use the service and play any role</td></tr>
<tr><td>Operation of the arrangement</td><td>Single entity</td><td colspan="3">Multiple entities</td></tr>
<tr><td>Access to the arrangement</td><td colspan="3">Restricted</td><td>Unrestricted</td></tr>
<tr><td>Technical roles of nodes</td><td colspan="2">Differentiated</td><td colspan="2">Not differentiated</td></tr>
<tr><td>Validation and consensus</td><td>Within a single entity</td><td>Within a single entity or across multiple entities</td><td colspan="2">Across multiple entities</td></tr>
</table>

Annex 2: Retail CBDC Use Cases

A. E-Piso Use Cases

The following set of DFC use cases are based on a commercial implementation of a system in which a commercial bank, utilizing its banking license which allows it to create different forms of money, creates some of that money in a form of digital objects possessing all the characteristics of DFC. The use cases are complementary and should be reviewed as a set, which in its whole, reproduces the attributes and behaviours of cash issued in digital form.

The commercial bank operating this system under a permission of the Bangko Sentral ng Pilipinas (BSP) is the Rizal Commercial Banking Corporation in Manila. E-Piso is used as the digital cash brand name.

E-Piso Use Case: Issuing DFC

Use Case Summary			
Use Case ID:		**Use Case Type:**	
Submission Date:	13 June, 2019	**Is Use Case supporting SDGs**	
Use Case Title:	Secure DFC issuance	**Domain:**	Public, private, central bank, e-money
Status of Case	Commercially implemented	**Sub-Domain**	
Contact information of person submitting/ managing the use-case	Full Name: Thomas Kudrycki (eCurrency) Job Title: Chief Technology Officer E-mail address: tom.k@ecurrency.net Web site: https://www.ecurrency.net		
Proposing Organization	eCurrency, USA		
Short Description	Secure creation of a fixed DFC supply amount in accordance with central bank monetary policies. The issuance is akin to printing physical banknotes. It creates a supply of DFC to be subsequently distributed through payment channels.		
Long description	One of the main characteristics required of DFC by the central banks is similarity to the existing physical cash processes. See for example see the Swedish Riksbank eKrona landing page (https://www.riksbank.se/en-gb/payments--cash/e-krona/) and the South African Reserve Bank CBDC expressions of interest documents (SARB, 2019). The key element of this similarity is the initial issuance process by which a supply of the DFC is created by the issuing entity. The main considerations for the issuance process are: - Security of the process - Security of the created supply		

	- Controls on the process, such as presence of multiple participants, storage and handling of the tool used - Controls on the created supply such as means of delivery of the supply into storage and further delivery into circulation - Chain of custody on all inputs and resulting artefacts - Auditability and traceability of the process - Permanence and storage of the audit trail		
Value Transfer:	DFC, just like cash, is created by an edict of a sovereign entity, therefore value is not transferred in this use case. It is created. More precisely, only a potential value is created at this time. The output of this process does not have any actual value until it is injected into circulation and thus increases the money supply. This is exactly analogous to printing physical paper banknotes and storing them in a secure vault at the central bank as a form of "inventory", until it is injected into circulation and must at that point be accounted for. The creating entity must account for the value, but the value is a seed at the root of the hierarchy and thus accounting for it is done in external systems, outside of the DFC realm. This may be considered a boundary condition, or "event zero".		
Transfer Frequency	Weekly to yearly	**Number of Actors:**	10 to 30
Stakeholders:	High-level central bank personnel, ministry of finance officials, offices of the president or prime minister		
Inputs:	Issuance being the initial seeding process, the inputs exist outside of the strict DFC environment. Inputs may include: - Estimate of the required supply based on demand for this form of cash - A formal agreement between the central bank and the ministry of finance		
Actors:	High-level central bank personnel, ministry of finance officials, security personnel, external auditors and similar. In some cases, international organizations may supervise or participate in the process.		
Tools	The following elements are assembled: Cryptographic computer ("printing device") used to create the DFC value 1. Associated infrastructure and equipment to operate the printing device, such as UI, power etc 2. Recording devices to monitor the process 3. Cryptographic computer to accept the DFC supply and store it for distribution ("the supply storage")		

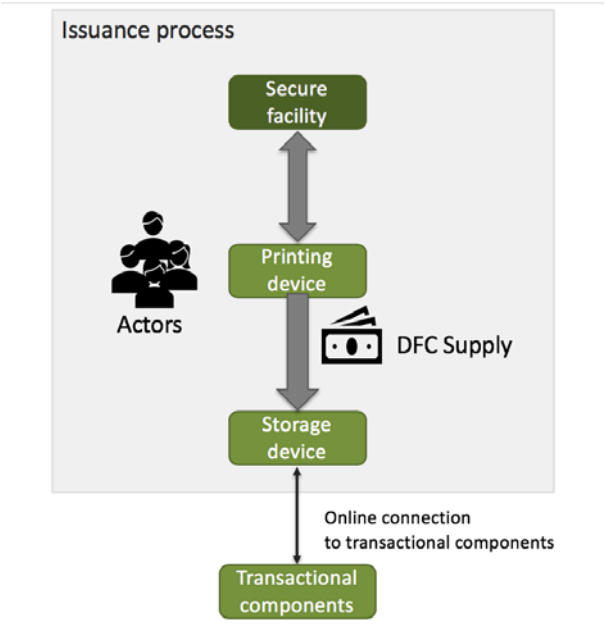
Outputs:	The following artefacts are generated by the process: - DFC supply: a cryptographic token representing the created value - An electronic record of the process, including the full identity and selected biometrics of the participants, time, location and similar

Overview of the Process

The process proceeds as follows:

1. The actors described above gather at a secure facility of the issuing authority, such as a secured conference room at a central bank
2. Actors' identities are verified
3. Tools are recovered from secure storage as per policy and best practices, for example the tools are delivered by armed security guards
4. The actors verify that the tools have not been tampered with and that the inputs are proper
5. The actors perform the DFC creation process as defined in the policies of the issuing authority
6. The resulting DFC supply is securely injected into the supply storage vault
7. The tools are returned to secure storage as required by the policy of the issuing authority
8. The audit record is verified to be correct and is signed and sealed
9. The audit record is published to an appropriate audience as per the policy

Process schematic



Implementation dependencies

A variety of technologies can be used to implement this use case. Discussion of possible implementation techniques is beyond the scope of this use case definition.

In the commercial implementation of this use case, the role of the central bank is played by RCBC.

E-Piso Use Case: Distributing DFC

Use Case Summary			
Use Case ID:		**Use Case Type:**	
Submission Date:	13 June, 2019	**Is Use Case supporting SDGs**	
Use Case Title:	DFC distribution	**Domain:**	Public, private, central bank, e-money
Status of Case	Commercially implemented	**Sub-Domain**	
Contact information of person submitting/ managing the use-case	Full Name: Thomas Kudrycki (eCurrency) Job Title: Chief Technology Officer E-mail address: tom.k@ecurrency.net Telephone number: +1 415.235.5986 Social media: https://www.linkedin.com/in/tkudrycki/ Web site: https://www.ecurrency.net		
Proposing Organization	eCurrency, USA		
Short Description	Distribution of DFC supply through banking and e-money payment systems. The distribution of DFC happens through channels analogous to the ones used in the distribution of physical currency i.e. commercial banks and existing and future payment systems.		
Long description	In order to be widely adopted, the retail DFC should augment and evolve, rather than disrupt the existing payment rails. This is one of the characteristics required of DFC by some central banks. See for example the Swedish Riksbank eKrona landing page (https://www.riksbank.se/en-gb/payments--cash/e-krona/) and South African Reserve Bank CBDC expressions of interest documents (SARB, 2019). This allows the central banks to introduce DFC gradually and not disintermediate critical commercial players such as banks and mobile money operators. The main considerations for the distribution process are: - Security of the process - Conservation of the amount of the money supply - Controls on the process, such as presence of multiple participants, access to the tools used - Auditability and traceability of the process - Permanence and storage of the audit trail		
Value Transfer:	DFC distribution in the implemented scenario is hierarchical, but with possible multiple interconnections, it is not a straightforward tree.		

	The initial distribution is from the stock created in "Use Case 1 – Issuance" to the first level of the distribution channel, typically a tier 1 commercial bank. This initial transfer is done in exchange for some other assets the target institution deposits with the central banks as per standard processes applied to acquisition of any other form of the central bank money. This initial distribution event in the implemented RCBC scenario is executed by the central bank personnel through a set of checks and approvals organized as a workflow. In other scenarios it can be initiated by an external system through an API into the DFC implementation. Subsequent distributions to other layers of the financial system hierarchy follow the process outlined above. Some central banks express a need to follow the existing cash distribution paths through various levels of commercial banks down to individual DFC e-wallet providers. Some others are taking an approach of distributing DFC directly to the e-money wallet providers.		
Transfer Frequency	Daily to hourly	**Number of Actors:**	100s to 1,000s
Stakeholders:	The central bank, commercial banks, payment system operators.		
Inputs:	- Cash orders - Proofs of pledges of other assets acceptable to the central bank, such as physical cash, government bonds etc - If integrated with RTGS or core banking systems, authenticated API calls from such systems to effect the distribution		
Actors:	Cash management departments at the central banks, commercial bank cash management and back office management teams, financial and accounting teams at payment system operators. In the subsequent description the organization requiring DFC from a distributor is called a *requestor*, and the DFC source (distributor) is called a *grantor*.		
Tools	The following elements participate in this use case: 1. DFC API (see submission of the API by eCurrency to this standards organization) for use by the Actors' computer systems 2. DFC management user interface for use by the Actors 3. eCurrency cryptographic appliances for storage of, and transacting with, the DFC value tokens 4. Telecommunication networks with VPN protocols and secured by mutual authentication of endpoints for sending and receiving the distributed DFC		
Outputs:	The following artefacts are generated by the process: - Modified DFC objects representing the new values owned by the institutions represented by the Actors		

	- An immutable electronic record of the transactions signed by the parties for non-repudiation.

Overview of the Process

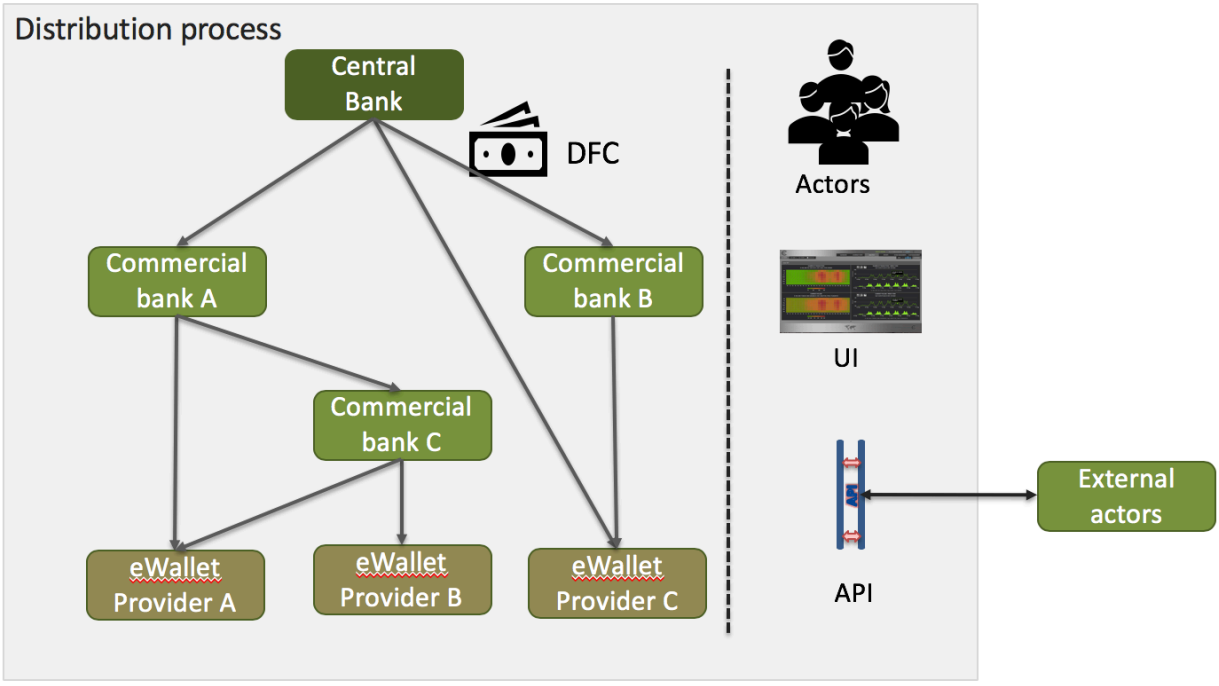
In the UI driven case (human intervention within he DFC system), the process proceeds as follows:

10. The actors representing DFC requestor initiate the DFC request through the DFC UI
11. The request enters the requestor's workflow and is approved. The request may contain attachments to document its validity. It is electronically signed by the workflow participants.
12. The approved request is automatically submitted to the identified grantor through the secure network
13. The request enters grantor's workflow
14. The grantor verifies the validity of the pledged assets used to purchase DFC and grants the request
15. DFC transaction effecting the transfer of DFC from the grantor to the requestor is performed using the DFC cryptographic appliances
16. An electronic record of the transaction signed by all the participating parties is created and stored. The record is made available to the transacting parties per their policy.

In the API driven case the process is largely the same except some steps are assumed to be executed outside of the DFC system. Different mixes of UI and API initiated events are possible. For example:

1. Points (1) and (2) above are executed outside of the DFC system
2. Point (3) is initiated by the DFC API call
3. Various aspects of (4) and (5) are executed outside of the DFC system, for example by a core banking system.
4. Point (6) can be initiated by the DFC API call from grantor's other computer systems

Process schematic



Implementation dependencies
A variety of technologies can be used to implement this use case. Discussion of possible implementation techniques is beyond the scope of this use case definition. In the commercial implementation of this use case, the role of the central bank is played by RCBC.

E-Piso Use Case: Transacting in DFC

Use Case Summary			
Use Case ID:		**Use Case Type:**	
Submission Date:	13 June, 2019	**Is Use Case supporting SDGs**	
Use Case Title:	DFC transactions	**Domain:**	Public, private, all payments P2P, P2B, G2P, G2B. B2B, G2G
Status of Case	Commercially implemented	**Sub-Domain**	
Contact information of person submitting/ managing the use-case	Full Name: Thomas Kudrycki (eCurrency) Job Title: Chief Technology Officer E-mail address: tom.k@ecurrency.net Telephone number: +1 415.235.5986 Social media: https://www.linkedin.com/in/tkudrycki/ Web site: https://www.ecurrency.net		
Proposing Organization	eCurrency, USA		
Short Description	Transacting using DFC throughout banking and e-money payment systems. The transactions happen through the existing e-money and banking systems. Transactions can be routed through existing and future e-money switches such as National Payment Switches.		
Long description	In order to be widely adopted, the retail DFC should augment and evolve, rather than disrupt the existing payment rails. This is one of the characteristics required of DFC by some central banks. See for example the Swedish Riksbank eKrona landing page (https://www.riksbank.se/en-gb/payments--cash/e-krona/) and South African Reserve Bank expressions of interest documents (SARB, 2019). This allows the central banks to introduce DFC gradually and not disintermediate critical commercial players such as banks and mobile money operators. The main considerations for transacting in DFC are: - Security of the process - Conservation of the amount of the money supply - Auditability and traceability of the process - Permanence and storage of the audit trail		

	- A balance between privacy of transactions versus the need to control the process, such as AML requirements - Rules governing the transactions, such as the maximum per transaction or daily amounts, need to be readily supported by the implementation - Instantaneous settlement in the base, central bank money - Reliability and scalability to support large economies		
Value Transfer:	DFC transactions in the implemented use case scenario happen at the minimum necessary level of the hierarchical money system: - P2P transactions can happen off-line - Transactions can involve e-wallets of the same e-money operator and in that case should be executed within the single e-money system - Transactions involving multiple e-money or payment system operators should be routed through existing or any future national payment switches - Transactions can cross between e-money and bank money, for example for the purpose of topping-off an e-wallet from one's bank account - DFC transactions should be executable using any appropriately secure physical medium, such as prepaid cards, e-wallets etc This use case does not distinguish among many possible variants of the transactions, such as P2P, B2B, G2P etc. In all cases the transactions transfer value between two or among several actors and settle it instantaneously. The instantaneous settlement is accomplished by directly transferring the actual DFC, value-bearing objects among the transacting parties.		
Transfer Frequency	Multiple transactions per minute or per second among all users simultaneously	N**umber of Actors:**	100,000 to many hundreds of millions
Stakeholders:	Commercial banks, payment system operators, merchants, e-money agents, government entities accepting or making payments, general public with or without bank accounts.		
Inputs:	- Transaction requests from authenticated sources issued through the DFC API		
Actors:	Any individual or entity legally capable of possessing cash and transacting with it.		
Tools	The following elements participate in this use case: 1. DFC API (see submission of the API by eCurrency to this standards organization) for use by the Actors' computer systems 2. eCurrency cryptographic appliances for storage of, and transacting with, the DFC value tokens		

	3. Telecommunication networks with VPN protocols and secured by mutual authentication of endpoints for sending and receiving the DFC units across the entire ecosystem 4. Payment switches to route transactions among multiple payment systems 5. User devices, such as prepaid secure cards, mobile phones, browser UIs, ATMs, Point of Sale terminals etc. 6. If offline transactions are needed, sufficiently secure user devices containing HSMs are required
Outputs:	The following artefacts are generated by the process: - Modified DFC objects representing the new values owned by the Actors - An immutable electronic record of the transactions signed by the parties for non-repudiation.

Overview of the Process

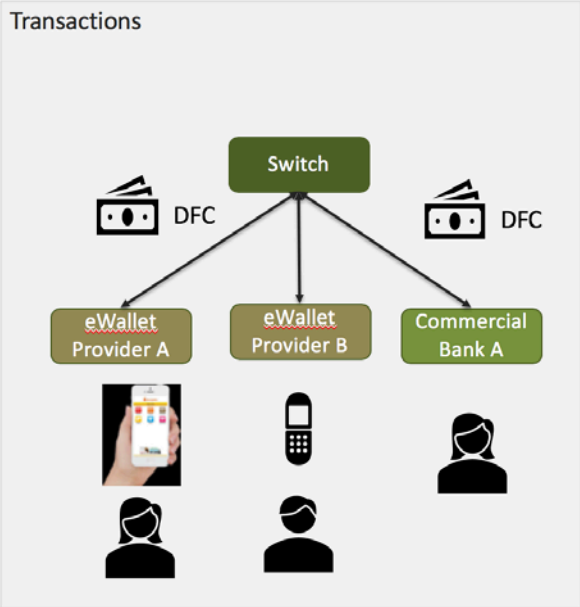
The process execution can take many paths and involve many actors belonging to many actor types. All cases involve a sender and at least one recipient, and in all cases can be bolied down to the following steps:

1. The sender accesses a payment system through a UI which can take many forms such smart phones, feature phones, browser UIs, prepaid cards etc.
2. The sender authenticates and initiates the DFC transfer request
3. The request is delivered to the DFC system through an API (contributed by eCurrency to this standards body) and contains the DFC object representing the DFC value held by the sender prior to the transaction
4. The request is routed to the recipient
5. Sender's and recipient's DFC objects transact inside the cryptographic appliances to exchange the required value
6. Modified sender and recipient objects are returned to them and now represent the value post-transaction
7. An electronic record of the transaction signed by all the participating parties is created and stored. The record can be made available to the transacting parties, e-money operators or the government as allowed by the corresponding laws, in many scenarios requiring a legal discovery process.

In point (5) above, the cryptographic DFC appliance can take many forms:

1. It can be a powerful computing environment allowing many thousands of transactions per second
2. It can be a small environment represented by a (logically) single appliance
3. It can be a hand-held device containing a secure element and interacting with another similar device via short-distance communication (NFC, Bluetooth etc.)

Process schematic



Implementation dependencies
A variety of technologies can be used to implement this use case. Discussion of possible implementation techniques is beyond the scope of this use case definition. In the commercial implementation of this use case, multiple payment systems interface to the DFC environment and transact directly or indirectly (through a switch) with the DFC cryptographic appliances using the contributed API. In the commercial implementation of this use case, the role of the central bank is played by RCBC.

B. E-Peso Use Case for Financial Inclusion in Uruguay

Use Case Summary			
Use Case ID:		**Use Case Type:**	
Submission Date:	10-May 2019	**Is Use Case supporting SDGs**	Yes
Use Case Title:	Public sector lending transparency	**Domain:**	Government and public sector
Status of Case	PoC	**Sub-Domain**	Government and non-profit transparency
Contact information of person submitting/ managing the use-case	Full Name: John William Kiff (IMF) Job Title: Senior Financial Sector Expert E-mail address: jkiff@imf.org Telephone number: +1-202-623-4052 Social media: https://www.linkedin.com/in/kiffmeister/ Web site: https://www.imf.org/external/index.htm		
Proposing Organization	IMF, Washington D.C.		
Short Description	This retail CBDC use case refers to the digital version of the Uruguayan Peso called e-Peso. The Banco Central del Uruguay (BCU) completed a six-month pilot project in April 2018 to test out technical and operational aspects related to the e-Peso such as currency production and circulation. The pilot project offered the BCU a controlled environment, in which the stakeholder could learn about CBDCs without assuming excessive risks.		
Long description	The e-Peso was designed as an electronic platform for the Uruguayan Peso with legal tender status. The BCU worked closely with a telecom provider and IT and payment solutions providers. The BCU issued 20 million e-Pesos with 10,000 participating mobile phone users selected on a first-come-first-serve basis. The e-Pesos were created at the BCU and transferred from the e-vault to the participants' digital wallets. The users could use the e-Pesos in their mobile phone wallets to pay for goods and services in registered stores and businesses as well as for peer-to-peer transfers among registered users. The BCU built incentive structures that ensured users converted cash into e-Pesos at the onset of the project and continued using the currency through the duration of the project. The system provided for mobile-enabled instantaneous settlement, not requiring any bank account. The digital wallets and encrypted vault included system-designed anonymity while still allowing for traceability. Given that the e-Peso never leaves the circulation platform and just changes ownership between participants, the actual notes were secure even in cases when users lost their phones or passwords for their digital wallets. Each e-Peso had a unique serial number that could be traced to a user rendering the bills traceable and pre-empting double-spending and forgery.		

	The initial pilot assessment revealed that most transactions were peer-to-peer. The pilot project did not encounter any technical incidents and the number of participating retails stores increased over time with banks expressing interest in joining the pilot.		
SDG in Focus (when applicable)	1. Promote sustained, inclusive and sustainable economic growth, full and productive employment and decent work for all 2. Build resilient infrastructure, promote inclusive and sustainable industrialization and foster innovation.		
Value Transfer:	Digital fiat currency	Number of Users:	10,000
Types of Users:	General population, small retail business (retail stores)		
Stakeholders	Government, Central Bank, telecommunications company, IT and wallet providers, citizens, private retail businesses, banks.		
Data:	Data available from the pilot: - Number of participating users and retail businesses - Volume and size of transactions - Number of notes in circulation - Serial numbers of notes in circulation - Mobile phone numbers - Any user identity data linked to the participating mobile phone - Amount of e-Peso per wallet		
Identification:	The users are anonymous. User identity is linked to their mobile phone and associated mobile phone number.		
Predicted Outcomes:	- Lower cost of financial transactions - Efficiency gains - Expanded financial inclusion - Prevention of fraud and tax evasion - Improved consumer protection		

Overview of the Business Problem or Opportunity
In Uruguay, there are opportunities to reduce transaction costs in payments systems. The main costs for using physical cash are related to the costs of production of notes and coins for the CBU, transportation and security-related costs for banks and retailers, and fees and opportunity costs for the consumers (e.g. time commitment and fees associated with cash withdrawal from ATMs, risk of holding cash etc). Estimates show that the cost of using cash in Uruguay is approximately 0.58 percent of GDP with most of the cost borne by the private sector. If paper money and checks were fully replaced by digital means of payment, including retail CBDCs, the transaction costs would be reduced by about 0.60 percent of GDP.
Why Retail CBDC?
- The introduction of efficiency gains in payment systems would lower the cost of producing, transporting, and using cash. Lowering the cost of cash would contribute to private sector development.

- The proactive contribution to financial digitalization through the e-Peso project would allow the BCU to develop financial markets and infrastructures. The introduction of the e-Peso might spur the development of related innovative financial products and entice the growth of a start-up community.
- The digitalization of payments for goods and services would pre-empt tax evasion with a positive contribution to the government's fiscal position.
- The traceability of the e-Peso would allow supervisors and law enforcement officers to improve the monitoring and reporting of suspicious transactions.

Current Process

Current Solutions
The central bank produces and distributes physical cash (coins and bank notes) and when they become too worn they destroy and replace them.

Existing Flow (as-is)		
Step	**User Actions**	**System Actions**
1.	The BCU produces the coins and bank notes	The BCU contracts with and pays third-party firms outside of Uruguay to print finished banknotes.
2.	The BCU distributes the physical cash.	The BCU distributes the cash to commercial banks, who pay for them with a debit to their reserve account at the BCU. The banks then distribute the cash to the general public.
3.	The BCU destroys coins and notes that have become too worn out to be useful.	The commercial banks presumably ship the cash to the BCU, the BCU credits their accounts accordingly, and the BCU destroys the cash.

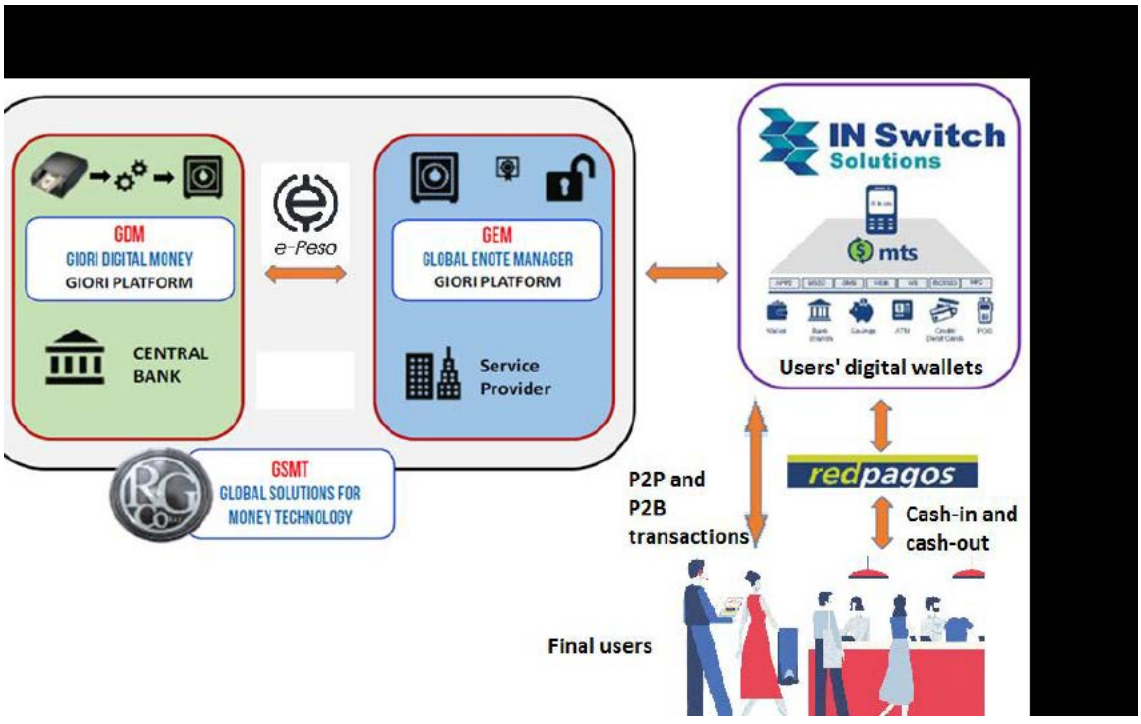
Data and information (as-is)		
Data	**Type**	**Description**
1	Fiat money transactions	The way value is transferred between: (a) the BCU (b) the commercial banks and (c) the general public.

Participants and their roles (as-is)		
Actor	**Type/Role**	**Description**
1	BCU	Central Bank
2	Commercial bank	Financial institution to distribute the cash to the public.
3	General Public	Entity who uses the cash to pay for goods and services.

Pilot project process

Pilot project flow		
Step	**User Actions**	**System Actions**
1.	The BCU produces the Giori Digital Money (GDM) using software provided by the Roberto Giori Company Limited (RGC).	The BCU manages the GDM production, given that the Banco Central del Uruguay has the exclusive right of issuing legal tender money in Uruguay.
2.	The e-Pesos that are produced by the BCU are transferred to the RGC Global E-Note Manager (GEM) that serves as virtual vault and digital wallet.	This component provides the storage, security, verification and certification of all transactions. The GEM was managed by IBM during the pilot, but it could be managed by the BCU if it goes live.
3.	IN Switch Solutions provides the mobile payment application for the user.	Users' digital wallets in the Giori GEM platform are linked to their mobile phone numbers in the IN Switch application.
4.	RedPagos manages the store front operation.	Users cash in and out of GDM at RedPagos branches.
5.	IBM provides cloud storage facilities and runs the call center.	

Process scheme (to-be)



Data and information (to-be)		
Data	**Type**	**Description**
1	Digital money transactions	The way value is transferred between: (a) the BCU and (c) the general public.

Participants and their roles		
Actor	**Type/Role**	**Description**
1	BCU	Central bank
2	Roberto Giori Company Limited	CBDC Solution Provider
3	IBM	Cloud service and call centre provider
4	Antel	Telcom company
5	IN Switch	Mobile Payment Application provider
6	RedPagos	Money transfer operator

Security and privacy
1. Must meet financial integrity standards 2. Transactions must anonymous but traceable 3. Wallet contents must be recoverable in the event of loss or theft

Main Success Scenario
1. Widespread adoption by public and merchants 2. Running cost is less than that of physical cash

Performance needs
1. Can be used as seamlessly as physical cash 2. Provides instantaneous settlement 3. 24/7/365 availability

Legal considerations
The current legal framework was sufficient for issuing electronic bills as a complement of paper ones. More precisely, article 7 A. of the Central Bank Charter says that “the Bank will: A. Have under its exclusive responsibility the issuing of currency notes, minting coins, and withdrawal of currency notes and coins in all of the Republic.” Since the law does not determine (neither forbid) a specific form for currency notes, it allows that physical and digital notes may be issued as long as both of them maintain similar security standards. In addition to that, the Central Banks does not need to require further authorization to issuing currency notes.

Risks
1. Cyber risk; 2. Central bank reputation risk; 3. Poor uptake; 4. Telcom failure;

Special Requirements
N/A
External References and Miscellaneous
Bergara, Mario and Jorge Ponce, 2018, "Central Bank Digital Currency: The Uruguayan E-Peso Case," in Gnan, Ernest and Donato Masciandaro (ed.), Do We Need Central Bank Digital Currency? Economics, Technology and Institutions, SUERF/BAFFI CAREFIN Centre Conference. https://www.suerf.org/docx/s_cf0d02ec99e61a64137b8a2c3b03e030_7025_suerf.pdf

C. CBDC-Based Digital Financial Ecosystem in Carribean Region

Use Case Summary			
Use Case ID:		**Use Case Type:**	Vertical
Submission Date:	28-may 2018	**Is Use Case supporting SDGs**	Yes
Use Case Title:	Blockchain / DLT - based Central Bank Digital Currencies	**Domain:**	Financial Technology Sector
Status of Case		**Sub-Domain**	
Contact information of person submitting/ managing the use-case	Full Name: Marla Dukharan Job Title: Chief Economist E-mail address: marla@bitt.com Telephone number: (246)-231-2115 Social media: Web site: www.bitt.com		
Proposing Organization	Bitt Inc, Barbados		
Short Description	Our mission at Bitt Inc is to create simpler, safer, and more cost effective payment systems for individuals, merchants, commercial banks, Central Banks, and Governments, which promote financial inclusion and socio-economic progress.		
Long description	Bitt provides a full-stack service for creating a digital financial ecosystem. This is achieved from three main products: 1. Blockchain-based Central Bank Issued Digital Currency (CBDC) to enable the issuance, distribution, redemption and destruction of digital legal tender in the economy, and to conduct cross-border payments. 2. Provide state of the art AML Compliance services to commercial banks 3. Provide a suite of software applications that enable transactions to be executed and managed at each level in the economy, including retail and merchant wallets, licensed financial institution (LFIs), and Central Banks.		
SDG in Focus (when applicable)			
Value Transfer:		Number of Users:	
Types of Users:	*Central Banks, Commercial Banks, Government Institutions, Wallet Service Providers, Merchants, Consumers and Individuals*		

Stakeholders	*Same as above.*
Data:	Bitt envisions a blockchain-based CBDC network that enables the following actions, resulting in multiple data storage and transfer configurations: 1. Central Banks issue digital legal tender into a blockchain network. All currency on the network is cryptographically verified to ensure only Central Bank issued currency is transacted as legal tender. All balances are stored on the ledger, and appear as amounts of digital currency assigned to public keys. Central Banks are able to pull transaction data to analyze trends and gain economic insight, but are not able to identify counterparties to the transaction. 2. Licensed Financial Institutions (LFI) enable the exchange of deposits for CBDCs, transaction data is stored on the network which includes public keys and balances. LFIs can view transactions in which their clients are counterparties; LFI client data is stored on separate databases. 3. Wallet Service Providers (WSP) enable retail users to transact in CBDC. Transaction Data is stored on the ledger. WSPs can view transactions in which their clients are counterparties; while WSP client data is stored on separate databases. 4. Merchants and Retail wallet users perform transactions on the network using various applications. Said users are able to see their own transaction data, but not transactions on the ledger.
Identification:	Name, address, date of birth, ID, and proof of address is required. This data is not stored on the ledger, but on secure encrypted databases held with the LFIs and WSPs.
Predicted Outcomes:	- Increase security while decreasing cost of issuing legal tender by facilitating digital issuance - incorporate MSMEs into the digital payment space and allow all merchants to accept affordable digital payments - Provide users financial services that are unavailable to the currently unbanked and underbanked portions of the population including: digital payments, money tracking, peer-to-peer transfers, which in turn has been proven to increase economic participation standard of living.

Overview of the Business Problem or Opportunity
Central Banks ● Central Bank currently face costly services when issuing, transporting and disseminating newly created banknotes and coins. Converting the process from issuing physical notes and coins to a digital version would save institutions time, money and improve security. ● Traditional forms of trade settlement require costly cross-border transactions consist of sending payments via correspondent banks in the US and/or Canada. These transactions

include lengthy settlement times that sometimes take weeks and high costs. Sending payments digitally would instead save time and money because settlement times could be reduced to minutes and costs reduced to a fraction of the current costs.

Commercial Banks

- Commercial banks can benefit from new and improved KYC such as facial recognition to match scanned copies of IDs
- They can provide their customers with advanced digital wallets to improve their banking experience

Retail/ General Public

- MSMEs are limited and prevented from accepting digital payments because of the high operating costs of credit/debit card machines
- There are high portions of the population that are prohibited from accessing financial services such as opening basic bank accounts.
- Peer-to-Peer transactions currently consist of bank transfer which can take days to settle, with a digital wallet, users can send money to their friends and family directly from their phone in a matter of seconds.
- Paying monthly utility bills is regularly an onerous task resulting in large segments of the workforce waiting many hours of productive time every month.
- Many persons obtain foreign exchange from street dealers in order to travel within the region increasing the risk of financial loss.

Government

- The drive to improve efficiency in the public sector is especially important in the Caribbean, where the size of Governments on a per capita basis, and the 'government intensity' of GDP, is higher than most countries. E-government platforms and digtization of public services more broadly, are gaining adoption therefore. A CBDC is complementary to this effort and could bolster the level of transparency and auditability of the flow of funds into and out of Government agencies.
- In countries where there is a substantial unbanked population, an e-government platform could serve to further marginalize and exclude them. But this could be counteracted if a CBDC is used on a mobile payments platform that is integrated with the e-government platform, as a payment option, alongside the traditional payment mechanisms such as credit cards, debit cards, bank transfers, etc.

Why Distributed Ledger Technology?

Distributed ledger technology has a number of features that enable secure, efficient, transparent, and robust transaction of CBDCs.

1. Elimination of single point of failure risk; multiple nodes operated by various stakeholders constantly verify ledger state and process transactions.
2. Elimination of counterfeit currency; real time node validation ensures only authentic currency issued by the Central Bank is transacted on the network.
3. Enforcement of 100% AML Compliance; only entities approved by the Central Bank (LFIs and WSPs) can access the CBDC network for the purpose of building payment applications, enabling clients to transact on the network.
4. Provision of low cost payments; DLT lowers the cost electronic payments, facilitating financial inclusion and economic participation.

Current process

Current Solutions
Notes and coins comprise the only Central Bank money that is available to retail level users. Deposits are represented electronically, but aren't guaranteed by the Central Bank, however they are guaranteed by the Licensed Financial Institutions (LFI) on whose balance sheet they lie.

Existing Flow (as-is)		
Step	**User Actions**	**System Actions**
1	Establish currency requirements and engage supplier with denominations and quantity	<-
2	Arrange delivery of currency stock	Enter currency denominations into inventory system
3	Issue currency to requesting licensed financial institutions	Enter currency into circulation.
4	Redeem currency from financial institutions	<-
5	Sort currency, add fit notes / coins into stock	Enter currency denominations into inventory system

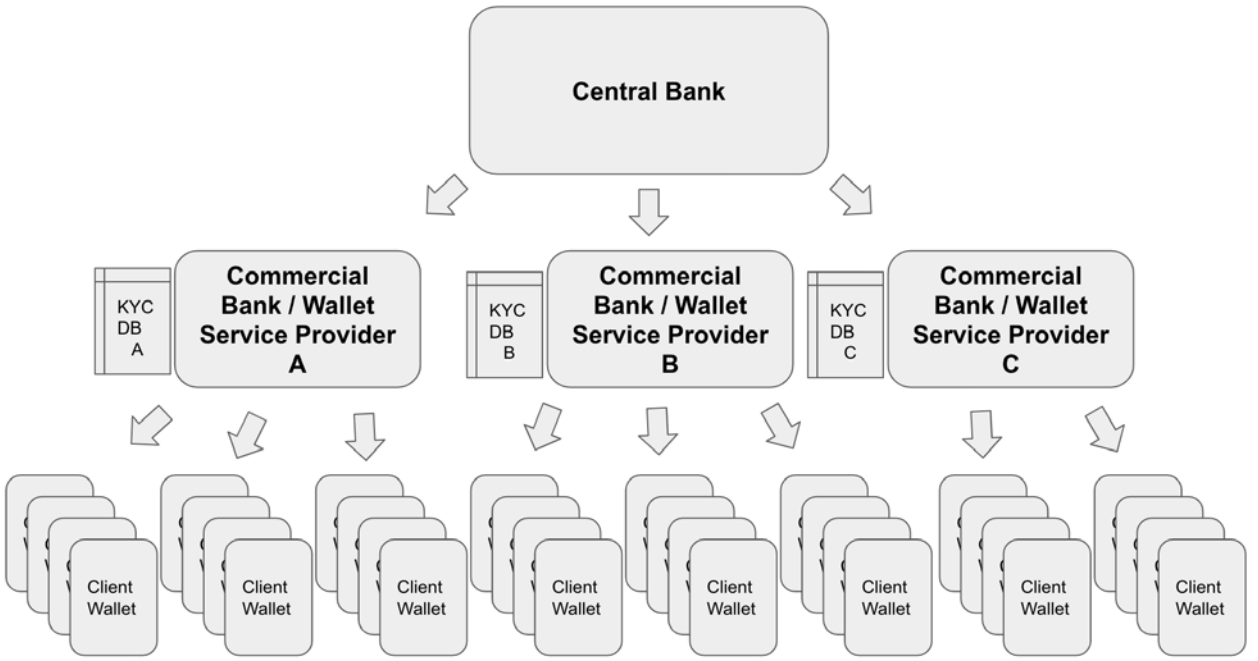
Data and information (as-is)		
Data	**Type**	**Description**
1	Total Notes In Circulation	<-
2	Total Coins in Circulation	<-
3.	Lifespan of notes and coins	<-
4	Notes and Coins circulated by specific LFI	<-
5	Historical data on the demand for new notes and coins	<-
6	Foreign reserve balances that contribute to the currency backing ratio	<-

Participants and their roles (as-is)		
Actor	**Type/Role**	**Description**

1	Central Bank	Financial institution responsible for issuance of legal tender, maintaining economic and financial stability
2	Commercial bank	Financial institution to provide transfer/payment between parts
3	Retail Merchants	Provide goods and services to the public in exchange for payment
4	Users	Partake in the economy through the purchase of goods and services and by sending money to friends and family

Expected process

Expected Flow (to-be)		
Step	**User Actions**	**System Actions**
1.	Central Bank issues digital legal tender in CBDC blockchain network.	New CBDC units created on network, creation by Central Bank verified cryptographically via network.
2.	LFI / WSP requests CBDC from Central Bank.	Request message sent through secure platform, and received by Central Bank via Central Bank Management Panel.
3.	Central Bank approves request and sends specific amount of CBDC to LFI / WSP per contractual terms.	CBDC sent from Central Bank wallet to LFI / WSP wallet; balances are managed via web-based panels (Central Bank panel and LFI Panel).
Trigger event	LFI / WSP provides CBDC to their clients in exchange for deposits.	Transfer of CBDC between LFI / WSP accounts and clients' accounts.
	Wallet users transact in CBDCs P2P and P2B.	Wallet users send CBDCs to friends and family via mobile wallets; wallet users pay for goods and services via mobile wallet.
	Enterprise users transact in CBDCs B2P and B2B.	Enterprise users accept CBDCs in exchange for goods and services, and user CBDCs to purchase goods or services from other businesses. Enterprise users can also transfer CBDC to retail users eg. to pay an employee salary direct to their mobile wallet.

Process scheme (to-be)


Transition Vision

A blockchain-based CBDC network requires segregated testing prior to integration into the traditional financial system. Network security and operational uptime are amongst the most crucial elements to test and confirm prior to a live deployment. Application functionality for the end user also needs to be rigorously tested and confirmed prior to live deployment.

Once the network and associated applications have been sufficiently tested with functionalities confirmed, and shortcomings addressed, API bridges can be built to the traditional payment networks to facilitate payment and exchange integration. Such APIs will also need to be rigorously tested in a sandboxed environment prior to enabling the general public to use them.

Future and Transition Vision

Participants and their roles		
Actor	**Type/Role**	**Description**
1	Central Bank	Financial institution responsible for issuance of digital legal tender, maintaining economic and financial stability.
2	Commercial bank	Financial institution to provide transfer/payment between parts, provide credit to end users, and connect Wallet Service Providers to the traditional financial system.
3	Retail Merchants	Provide goods and services to the public in exchange for payment, accepted via Point-of-Sale wallet application.

4	Users	Participate in the economy through the purchase of goods and services, and by sending money to friends and family via mobile wallet.
1	Central Bank	Financial institution responsible for issuance of digital legal tender, maintaining economic and financial stability.

Data and information		
Data	**Type**	**Description**
1	Transaction Data including: Public Keys & CBDC Balances	The Central Bank is able to view the entire distributed ledger, however they are only able to see public keys and corresponding CBDC balances. This allows them to analyze anonymous transaction data to derive economic insight.
2	Transaction Data including: LFI public keys & balances Client public keys & balances Client KYC information	LFIs and WSPs are able to view transaction data for their own transactions, and all of their clients transactions for the purpose of transaction monitoring and reporting requirements. LFIs and WSPs must keep KYC information to ensure AML Compliance best practices are maintained.
3	Transaction Data	Wallet users are able to view all transactions they have executed via the mobile wallet or online wallet interface.

Security and privacy
1.Security is if the utmost importance when dealing with legal tender, for this reason the technology used by the central banks will meet the CBDC standard, and will be informed by the specific requirements and operating policies and procedures of the Central Bank. 2. The central bank would have access to the transactional data for the customers, all of which would have submitted the relevant KYC documents to verify their identity 3. DLT system should be able to provide mechanisms of DLT data integrity control; 4. DLT data and related services (System Actions) should be available in 24/7/365 mode; 5. The entity identity solution should prevent identity fraud. 6. The products and services type identification solution should prevent fraud. (Future Vision only)

Main Success Scenario
1. The Central Bank securely issues CBDC; 2. LFIs and WSPs provide low cost payment services using CBDC, including P2P, B2P, B2B, P2B, and remittance transactions;

Conditions (pre- or post-)
1. The Central Bank would issue CBDC as legal tender 2. Commercial Banks and Wallet Providers would have the necessary set ups to provide digital payment services to their customers 3. General public will have access to a digital wallet and have signed up as users with the necessary compliance procedures 4. Merchants to be set up to accept CBDCs as a form of payment

Performance needs
1. Transactions processing near real time; 2. 24/7/365 availability;

Legal considerations
Regulations need to be amended to better suit the utilization of central bank issued digital currencies

Risks
1.Security risks: hacks, bad actors, etc. 2. Network reliance risk: should the internet go down, the CBDC network will not be able to operate. Offline transaction mechanisms are being tested yet are not operational yet.

Special Requirements
N/A

External References and Miscellaneous
1. Current Pilot Project with the Eastern Caribbean Central Bank to issue a legal, digital EC Dollar: https://www.eccb-centralbank.org/news/view/eccb-to-issue-worldas-first-blockchain-based-digital-currency

Bibliography

1. Adam Furgal, Rodney Garratt, Zhiling Guo, Dave Hudson (2018). "***A Proposal for a Decentralized Liquidity Savings Mechanism with Side Payments"***. R3 Report. June 11.
2. Adrian, Tobias (2019), ***"Stablecoins, Central Bank Digital Currencies, and Cross-Border Payments: A New Look at the International Monetary System,"*** Remarks at the IMF-Swiss National Bank Conference, Zurich, May 14.
3. Agarwal, R., and M. Kimball (2015). "***Breaking through the Zero Lower Bound***." IMF Working Paper 15/224, International Monetary Fund, Washington, DC.
4. Bank of Canada et al (2017). "***Project Jasper: A Canadian Experiment with Distributed Ledger Technology for Domestic Interbank Payments Settlement***". Report prepared jointly by Bank of Canada, Payments Canada and R3. September.
5. Bank of Canada et al (2018). "***Jasper Phase III: Securities Settlement Using Distributed Ledger Technology***". Report prepared jointly by Bank of Canada, TMX Group, Payments Canada, Accenture and R3. October.
6. Bank of Canada (BoC) and Monetary Authority of Singapore (MAS) (2019). "***Enabling Cross-Border High Value Transfer Using Distributed Ledger Technology***," May.
7. Bank of Canada (BoC), Bank of England (BoE) and Monetary Authority of Singapore (MAS) (2018). "***Cross-Border Interbank Payments and Settlements***," November.
8. BIS – Bank for International Settlements
   - (2003) "***The role of central bank money in payment systems***". CPMI papers. No. 55. August 12.
   - (2012) "***Principles for Financial market infrastructures***". CPSS, BIS and Technical Committee of IOSCO Paper. April.
   - (2017). "***Distributed ledger technology in payment, clearing and settlement***". CPMI. No. 157. February.
   - (2018). "***Central bank digital currencies***". Report submitted by Working Groups chaired by Klaus Löber (European Central Bank) and Aerdt Houben (Netherlands Bank). Committee on Payments and Market Infrastructures & Markets Committee. March.
9. Bordo, M., and A. Levin (2018). "***Central Bank Digital Currency and the Future of Monetary Policy***". Monetary Policy and Payments 3:143–78.
10. Burgos et al (2017). "***Distributed Ledger Technical Research in Central Bank of Brazil: Positioning Report***". August.
11. Duffie, D. (2019). "***Digital Currencies and Fast Payment Systems: Disruption is Coming***". Presentation to the Asian Monetary Policy Forum, May.
12. European Central Bank & Bank of Japan (2017). "***Stella: Payment Systems: Liquidity Saving Mechanisms in a Distributed Ledger Environment***". September.
13. European Central Bank & Bank of Japan (2018). "***Stella: Securities Settlement Systems: Delivery versus Payment in a Distributed Ledger Environment***". September.

14. IBM (2018). "***Central bank digital currencies***". Report prepared by the Official Monetary and Financial Institutions Forum in collaboration with IBM Blockchain World Wire. September.

15. IMF (2018). "***Casting light on Central Bank Digital Currency***". IMF Staff Discussion Note. SDN/18/08. November.

16. Joseph Poon and Thaddeus Dryja (2016), "***The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments***". January

17. Kumhof, Michael and Clare Noone (2018), ***"Central Bank Digital Currencies — Design Principles and Balance Sheet Implications,"*** Bank of England Staff Working Paper No. 725, May.

18. Monetary Authority of Singapore & Deloitte (2017). "***The future is here - Project Ubin: SGD on Distributed Ledger***". A report developed with the contributions of Bank of America Merrill Lynch, BCS Information Systems, Credit Suisse, DBS Bank, HSBC, J.P. Morgan, Mitsubishi UFJ Financial Group, OCBC Bank, R3, Singapore Exchange and UOB Bank

19. Monetary Authority of Singapore, Association of Banks in Singapore & Accenture (2017). "***Project Ubin Phase 2: Re-imagining Interbank Real-Time Gross Settlement System Using Distributed Ledger Technologies***". November.

20. Monetary Authority of Singapore, Singapore Exchange and Deloitte (2018). "***Delivery versus Payment on Distributed Ledger Technologies: Project Ubin***". A report developed with the contributions of MAS, SGX, Anquan Capital, Deloitte and Nasdaq.

21. Payments Canada, Bank of Canada and R3 (2017). "***Project Jasper: A Canadian Experiment with Distributed Ledger Technology for Domestic Interbank Payments Settlement".***

22. Rogoff, K. (2014). "***Costs and Benefits to Phasing Out Paper Currency***". NBER Working Paper 20126, National Bureau of Economic Research, Cambridge, MA.

23. Qian, Y. (2019). "***Central Bank Digital Currency: Optimization of the Currency System and Its Issuance Design***". China Economic Journal, Volume 12, Issue 1.

24. South African Reserve Bank (SARB) (2018). "***Project Khokha: Exploring the use of distributed ledger technology in interbank payments settlement in South Africa***". June.

25. South African Reserve Bank (SARB) (2019). ***Procurement Division Expressions of Interest***. May.

26. Samman and Masanto (2019). "***The State of Stablecoins 2019 – Hype vs. Reality in the Race for Stable, Global, Digital Money***". February.

27. Woodford, M. (2000). "***Monetary Policy in a World without Money***." NBER Working Paper 7853, National Bureau of Economic Research, Cambridge, MA.