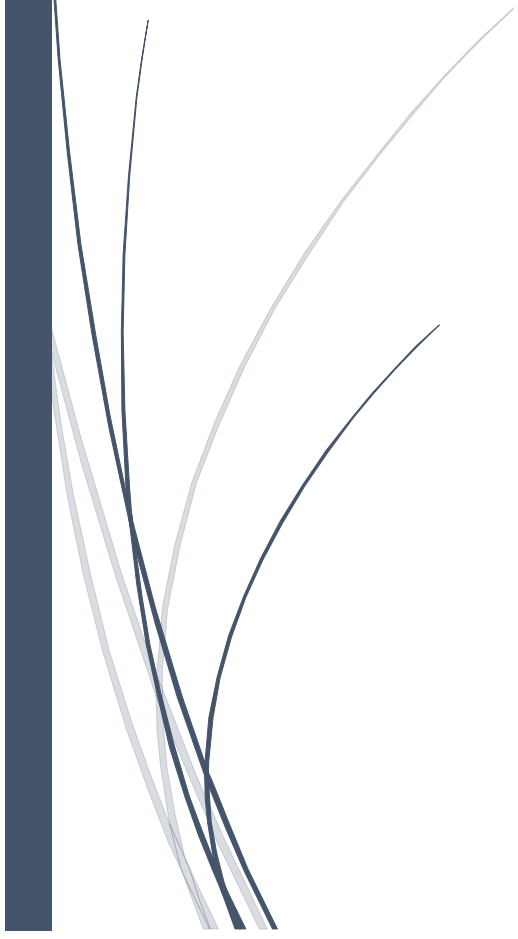
Request for Comments

e-HKD: A technical perspective



In Collaboration with BISIH Hong Kong Centre

Executive Summary

1. The HKMA's CBDC journey in a nutshell

The HKMA began researching CBDC under **Project LionRock** in 2017, and has since then actively collaborated with other central banks in broadening our knowledge of **wholesale CBDC**.

In 2019, the HKMA and the Bank of Thailand (BOT) jointly initiated **Project Inthanon-LionRock** to study the **potential of wholesale CBDC for cross-border payments**. The project entered the second phase in 2020 and was subsequently renamed to **Multiple CBDC Bridge** (mBridge) in February 2021, when it was joined by the Central Bank of the United Arab Emirates and the Digital Currency Institute of the People's Bank of China (PBoC), and strongly supported by the Bank for International Settlements (BIS) Innovation Hub Centre in Hong Kong.

Building on the knowledge and experience in wholesale CBDC, in June 2021, the HKMA commenced **Project e-HKD**, which is a **retail or general-purpose CBDC (rCBDC) project** that aims to study the feasibility of e-HKD. It comprises two components: a **technology experimentation study** and a **comprehensive study of other issues**, including legal and policy considerations.

2. Aim of this technical whitepaper

This whitepaper is part of the technology experimentation study under Project e-HKD. It explores **potential architectures and design options** that could be applied to the construction of the **infrastructure for distributing e-HKD**, and reports the **initial thoughts and findings**.

Specifically, it aims to explore technology solutions that address the problems of **cross-ledger synchronisation, over-issuance prevention, privacy-preserving transaction traceability**[1], and **flexible instantiations of different two-tier distributions models**.

3. Proposed architecture

The architecture proposed in this whitepaper is most notable for its ability to **flexibly and efficiently instantiate different two-tier distribution models of rCBDC while achieving breakthroughs in privacy-preserving transaction traceability and cross-ledger synchronisation of decoupled ledgers**.

In gist, the proposed architecture consists of **two layers**: a **wholesale system** for the central bank to issue and redeem CBDC, and a **retail system** for commercial banks to distribute and circulate either rCBDC or CBDC-backed e-money. The design of the proposed architecture was guided by **three key principles**, namely: safety, efficiency, and openness to change, innovation, and competition.

4. The HKMA's stance

[1] This whitepaper is aware of the existence of different notions of privacy with more a precise meaning in the academic literature (e.g. privacy, confidentiality, anonymity and pseudonymity, unlinkability, l-diversity, t-closeness). For the purpose of this whitepaper, the term privacy is loosely used as a broad concept to refer to the general protection of personally identifiable information in transactions.

It should be noted that the proposed architecture is **not a blueprint for e-HKD**, nor does it approach a decision on the CBDC distribution models chosen for implementing e-HKD. Rather, it should be seen as the **outcome of initial research** as well as a **basis for initiating dialogues** with central banks, the academia, and the wider fintech community to collaboratively explore solutions for rCBDC.

5. Solicitation of input

Based on an initial, preliminary analysis of the proposed architecture, the HKMA has identified a number of areas for further discussion, which are summarised as **seven problem statements** (Table 1). We would like to **invite the academia and industry to comment on our proposed architecture** by making reference to the seven problem statements; as well as **solicit new ideas and project proposals** from them**.**

In particular, **security modelling and analysis** for the proposed design, as well as ideas for **novel use cases and capability** that can be uniquely enabled by rCBDC are sought. Feedback on the proposed architectural design and suggestions for improvement to the design can be submitted to fintech@hkma.gov.hk by 31 December 2021.

Problem Statements:		
1	 **Privacy**	• To study different privacy models (e.g. anonymity, pseudonymity, metadata obfuscation, and transaction confidentiality) and their applicability to the context of rCBDC and CBDC-backed e-money • To propose new designs which maintain user privacy while assuring integrity of systems (i.e. free from unauthorised manipulation) and transactions (i.e. correct recording of transactions and prevention of frauds)
2	 **Interoperability**	• To research the interoperability between conventional Financial Market Infrastructures (FMIs) and emerging Distributed Ledger Technology (DLT)-based systems based on different underlying technologies (e.g. Corda, Hyperledger Fabric, and Ethereum) • To explore emerging interoperable platforms
3	 **Performance and scalability**	• To study the trade-offs between performance and other metrics (security, privacy, etc.) • To enhance the scalability of DLT and other distributed systems with respect to increasing number of users, number of validation parties and transaction volume
4	 **Cybersecurity**	• To enumerate the attack vectors of rCBDC systems • To propose efficient solutions to withstand high-risk attacks in order to maintain reasonable cyber-resilience, service availability and transaction security

5	 **Compliance**	• To explore computing methods to achieve regulatory compliance goals such as AML/CFT
6	 **Operational robustness and resilience**	• To study rCBDC system designs which could operate correctly across a wide range of known operational conditions (e.g. flash transaction demand) • To study rCBDC system designs which could adapt to and recover from unforeseeable adverse conditions (e.g. offline-to-offline payments in case of connectivity outage)
7	 **Technology-enabled functional capabilities**	• To investigate how rCBDC solutions can improve existing business applications in terms of e.g. efficiency, security, and resilience and/or bring in new functionalities, features and applications which cannot be achieved by existing means of payments

Table 1. Research problems on CBDC

Table of Contents

1. Introduction 7
   1.1. The HKMA's CBDC journey 7
      1.1.1. Project LionRock 7
      1.1.2. Project Inthanon-LionRock 7
      1.1.3. Multiple CBDC Bridge 8
      1.1.4. Project e-HKD and Project Aurum 8
   1.2. Purpose of this technical whitepaper 8
   1.3. Structure of this technical whitepaper 9
   1.4. The HKMA's stance 9
2. Background 10
   2.1 The two elements of an rCBDC 10
   2.2 Different architectural designs 10
      2.2.1 Direct (or one-tier) rCBDC model 10
      2.2.2 Two-tier rCBDC models 10
   2.3 Four types of distribution models 11
      2.3.1 Variant of direct CBDC model 11
      2.3.2 Hybrid model 11
      2.3.3 Intermediated model 11
      2.3.4 CBDC-backed e-money 12
   2.4 Trade-offs between different models 14
3. Key design considerations and questions of a two-tier distribution model 14
   3.1 Elements that make a good design 14
      3.1.1 Decoupling of wholesale and retail layers 14
      3.1.2 Cross-ledger synchronisation 15
      3.1.3 Privacy-preserving transaction traceability 15
      3.1.4 Flexible and reconfigurable 16
   3.2 Key design questions 17
4. Principles guiding solution ideation 18
   4.1 Safety 18
   4.2 Efficiency 19
   4.3 Openness to change, innovation and competition 19
5. Architecture of one possible design 20
   5.1 Tier 1 – wholesale system 21

5.1.1 Technology employed 21
5.1.2 Cybersecurity considerations 21
5.2 Tier 2 – retail distribution and circulation system 22
5.2.1 Method of distribution from wholesale to retail layer 23
5.2.2 Synchronisation and validation of the decoupled ledgers 24
5.2.3 Redemption mechanism 25
5.3 Alternative tier 2 distribution and circulation system with a UTXO-based tier 1 wholesale system 26
5.4 rCBDC based on UTXOs with account balances 27
5.4.1 Benefits 29
5.4.2 Different coinbase transaction definitions under UTXO 30
5.4.3 Trade-offs of speeding up UTXO tracing 31
5.5 Validator infrastructure designed as a UTXO database 31
5.5.1 Purpose 31
5.5.2 One implementation of the validator infrastructure 32
5.5.3 Other design considerations 32
5.5.4 Two-tier architectures based on different validator infrastructures 35
5.6 Pseudonym system with evolving public keys 35
5.6.1 Improved privacy with dynamic public keys 35
5.7 Support for cross-border interoperability 37
6. Preliminary analysis 38
6.1 Over-issuance prevention 38
6.2 Asset and transaction traceability 39
6.3 Flexibility 39
6.4 Safety 40
6.5 Efficiency 41
6.6 Openness to innovation 42
7. Future work 43
8. Acknowledgement 44
9. Bibliography 45

Table of Figures

Figure 1. The CBDC journey of the HKMA 7
Figure 2. Division of work between central bank and the private sector in different two-tier rCBDC architectures. 13
Figure 3. Trade-offs between different models 14
Figure 4. A two-tier distribution model for rCBDC 15
Figure 5. Design principles for the two-tier distribution infrastructure for rCBDC 18
Figure 6. Distribution Model of rCBDC 23
Figure 7. Transaction flow for distribution from wholesale to retail system 24
Figure 8. Redemption transaction flow 25
Figure 9. Transaction flow for distribution from intermediary to user 26
Figure 10. Transaction flow for retail payment transaction between users 26
Figure 11. Cross-ledger synchronisation with UTXO-based DLT Platform (Corda) for the Wholesale System 27
Figure 12. A sample UTXO transaction 28
Figure 13. Account balance/UTXO Hybrid Model 29
Figure 14. Validator's UTXO database stores unspent transaction outputs in a relational database and signed transactions in a NoSQL database 32
Figure 15. The two cases how the transaction chain of a coinbase is stored 34
Figure 16. Pseudonym system for transactions with mapping between real identities and pseudonyms (or public keys) kept at intermediaries only 36
Figure 17. Normal payment process versus payment process with pseudonym system requiring public key registration 37
Figure 18. Extensions of the architecture with a server gateway to support overseas users 38
Figure 19. UTXO transaction structure and the related token/account implementation as the key anchor layer for applications built on it and the underlying infrastructure arrangement. 43

Tables

Table 1. Research problems on CBDC 2
Table 2. Key design questions for two-tier distribution infrastructure for rCBDC 17
Table 3. Comparison of accounts, tokens and UTXOs for solving the design issues of two-tier distribution infrastructure for rCBDC 30
Table 4. Comparison of different hosting configurations of the validator infrastructure and their fraud prevention capability 35

Technology for eHKD: Potential Architecture, Design Options, and Challenges Ahead

1. Introduction

1.1. The HKMA's CBDC journey

1.1.1. Project LionRock

The HKMA began researching CBDC under Project LionRock in 2017. In collaboration with the three note-issuing banks, the Hong Kong Interbank Clearing Limited, and the R3 consortium, the HKMA commenced a study on CBDC in 2017 with a view to better understanding its feasibility, implications, and possible benefits through exploring its use in domestic inter-bank payments, corporate payments, and delivery-versus-payment debt securities settlement. In view of the potential benefits of the use of CBDC at the wholesale level highlighted by the study, the HKMA continued to explore the potential use and cross-border use of CBDC at the wholesale level.

1.1.2. Project Inthanon-LionRock

Against this backdrop, the HKMA has been actively collaborating with other central banks in research and proof-of-concept (PoC) studies to broaden our knowledge of CBDC. The HKMA and the Bank of Thailand (BOT) initiated Project Inthanon-LionRock in 2019 to study the application of CBDC to cross-border payments. The project was completed in December 2019 and a Distributed Ledger Technology (DLT)-based PoC prototype was developed together with 10 participating banks from Hong Kong and Thailand. The prototype allows banks to conduct funds transfers and foreign exchange (FX) transactions across the two jurisdictions on a payment-versus-payment basis through a cross-border CBDC Corridor Network. The HKMA and the BOT jointly published a report in January 2020 to present the key findings. It was then concurred that further joint research work in relevant areas will be carried out, including exploring business cases and connections to other platforms, involving participation of banks and other relevant parties in cross-border funds transfer trials. Together with Thailand, Hong Kong was ranked first in the category of interbank CBDC development of the PwC CBDC Global Index 2021.

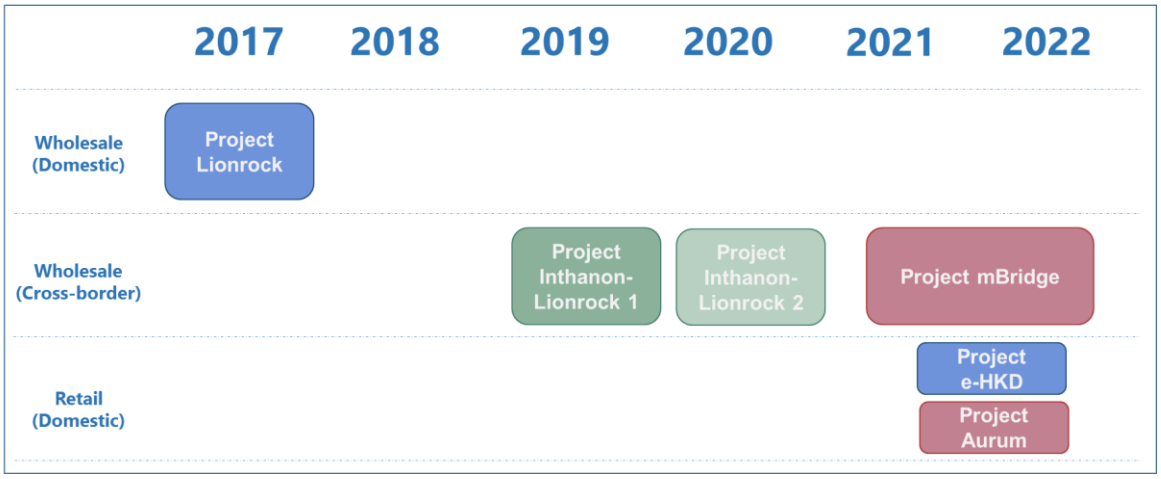


Figure 1. The CBDC journey of the HKMA

1.1.3. Multiple CBDC Bridge

Upon completion of Project Inthanon-LionRock, the research project has entered its second phase and was renamed as Multiple CBDC Bridge (mBridge) in 2021. Following the joining of the Central Bank of the United Arab Emirates and the Digital Currency Institute of the People's Bank of China (PBoC), Project mBridge is now a collaboration of four central banks and is strongly supported by the Bank for International Settlements (BIS) Innovation Hub Centre in Hong Kong. The project aims to improve cross-border settlement efficiency, liquidity management efficiency, and compliance with any local regulations on FX control while fostering a collaborative environment for central banks and financial institutions to study the potentials of DLT in enhancing the financial infrastructure for cross-border payments. An interim report was published in September 2021.

1.1.4. Project e-HKD and Project Aurum

With the knowledge and experience built up in wholesale CBDC studies, and in the light of the increasing public appetite for digital payments, in June 2021, the HKMA commenced Project e-HKD, a feasibility study on rCBDC and digitisation of Hong Kong Dollar (named e-HKD) to explore the potential benefits and risks of issuance of e-HKD. This move is in line with the global trend of CBDC research and the HKMA would like to contribute to the central bank discussions on rCBDC.[2] Notwithstanding, **the HKMA has not yet made a decision on whether to introduce e-HKD, but will remain open-minded to consider related questions carefully**.

Project e-HKD consists of two parts: a technology experimentation study on rCBDC and a comprehensive study of other issues pertaining to the feasibility of issuing e-HKD. The former is purely a technological investigation of the infrastructure needed for issuing and distributing rCBDC, specifically, on how the recognised issues of rCBDC can be addressed or mitigated through suitable architectures and designs. The latter covers use cases, benefits, related risks (such as data privacy, AML, and cybersecurity), and considerations (such as legal and monetary policy).

The HKMA has also been partnering with the BIS Innovation Hub in a PoC study named **Project Aurum** to explore the technical feasibility and trade-offs of two of the architectures, namely intermediated CBDC and CBDC-backed e-money. The PoC study also aims to develop a basic prototype to implement selected elements of the architecture presented in this whitepaper.

1.2. Purpose of this technical whitepaper

This technical whitepaper, as part of the technology experimentation study under Project e-HKD, reports the initial thoughts and findings of the exploration of the potential architectures and design options that could be applied to the construction of the distribution infrastructure of e-HKD. Based on a reasonably rigorous evaluation of different distribution models for rCBDC, as informed by past studies carried out by other central banks and the private sector, this whitepaper outlines an illustrative technology architecture of rCBDC designed to enable households and businesses to hold and make payments with CBDC while alleviating some of the major risks and drawbacks of rCBDC. The purpose of this whitepaper is to begin a dialogue on the

[2] A BIS study (Auer et al., 2021) indicates that, as of July, 2021, 69 projects on rCBDC and 31 projects on wholesale CBDC have been reportedly carried out by central banks.

appropriate design of e-HKD and an evaluation of whether the benefits of e-HKD, and rCBDC in general, outweigh its risks.

Based on an initial, preliminary analysis of the proposed architecture, the HKMA has identified a number of areas for further discussion, which are summarised as **seven problem statements** (Table 1). We would like to **invite the academia and industry to comment on our proposed architecture** by making reference to the seven problem statements; as well as **solicit new ideas and project proposals** from them**.**

1.3. Structure of this technical whitepaper

The organisation of this whitepaper is structured with reference to the design thinking process, and inputs and suggestions for subsequent iterations of the whitepaper are invited. Chapter 2 presents the background of CBDC research, empathizing with known concerns on rCBDC and setting the backdrop for problem formulation. Chapter 3 defines the problem and design issues to be explored in this technology study. Chapter 4 sets out the design principles for technology solution ideation and Chapter 5 suggests the possible architectural designs. Chapter 6 presents a preliminary evaluation and direction for further testing. Chapter 7 outlines the areas for further research.

1.4. The HKMA's stance

This technical whitepaper mainly pertains to the technology for the infrastructure of rCBDC. It will not address whether or why a central bank should issue an rCBDC. Instead, it focuses on how a central bank can issue an rCBDC practically if it considers that such issuance is desirable in the local context. Specifically, it covers some feasible technological architectures and design options of the rCBDC infrastructure that could address some of the known operational concerns.

The architecture proposed in this whitepaper is not a blueprint for the infrastructure of e-HKD, nor does it approach a decision on the CBDC distribution model chosen for implementing e-HKD. Rather, it should be seen as the outcome of initial research as well as a basis for initiating dialogues with central banks, the academia, and the wider fintech community to collaboratively explore practical and robust solutions for rCBDC.

2. Background

2.1 The two elements of an rCBDC

There are two elements in any rCBDC, namely, the CBDC itself (i.e. the asset and payment instrument per se) and the underlying infrastructure that allows CBDC to be transferred and used for payments. The former pertains to the economic design, concerning aspects such as access, remuneration, quantitative limits, and convertibility. The latter concerns how a CBDC is provisioned, its functional design, the technology to be used, and the operational processes and rules to be implemented. The provision arrangement delineates between a central bank and the private sector their responsibilities and functions involved in providing a CBDC. The functional design concerns how users and different stakeholders would interact with a CBDC and the types of payments that can be made with the CBDC. It would have impact on user-friendliness, level of privacy of the system, and the technological choices for implementing the infrastructure.

2.2 Different architectural designs

2.2.1 Direct (or one-tier) rCBDC model

If an rCBDC is provisioned through a one-tier system fully operated by a central bank, which is called the direct CBDC model, such an arrangement would face various operational and policy challenges. A direct CBDC model would imply a large shift of operational tasks and costs associated with customer-facing activities from the private sector to the central bank (Auer & Böhme, 2021; Bank for International Settlements, 2021). These include account opening, account maintenance, enforcement of AML/CFT rules, user authentication, and other day-to-day customer services. Such a shift would detract the central bank from its role as a relatively lean and focused public institution at the helm of economic policy (Bank for International Settlements, 2021). In addition, an rCBDC could become a new target for cyber threats (Quarles, 2021; Waller, 2021). Maintaining cybersecurity and availability of the infrastructure at a scale commensurate with the user base of an rCBDC is challenging and unprecedented for central banks. In particular, unlike a wholesale system, a retail system is relatively open, meaning that not all the participants are fully trustworthy.

There are also privacy concerns and impact on long-term innovation associated with the direct CBDC model. User privacy is often seen as the most valued property and a key success factor that determines whether an rCBDC would be generally accepted and used by the general public (European Central Bank, 2021). Under this model, the central bank, which processes retail transactions, could become a repository for economy-wide transaction-level data. The responsibilities of the central bank for protecting privacy and user data, including from other arms of the government, could be onerous (Auer & Böhme, 2021; Group of Thirty, 2020). On the other hand, a payment system in which the central bank has a large footprint would imply that it could quickly find itself assuming a financial intermediation function that private sector intermediaries are better suited to perform. This has long-term impact on financial innovation as banks and PSPs are in a better position than the central bank to lead innovative initiatives and integrate payment services with consumer platforms and other financial products (Bank for International Settlements, 2021).

2.2.2 Two-tier rCBDC models

An rCBDC is therefore best designed as part of a two-tier system, with an appropriate division of labour between the central bank and private sector intermediaries for the distribution and circulation of CBDC. A typical two-tier distribution model of rCBDC consists of

two separate, connected layers, namely, the wholesale interbank system and the retail user wallet system. The central bank and private sector intermediaries (including banks and PSPs) could continue to work together in a complementary way, with each doing what they do best (Auer & Böhme, 2020; Bank for International Settlements, 2021). The central bank can focus on providing the core, foundational infrastructure of a CBDC, guaranteeing the stability of its value and overseeing the system's security, so as to promote a level playing field for the private sector (Bank for International Settlements, 2021; Group of Thirty, 2020). In turn, the majority of the operational tasks and consumer-facing activities can be delegated to private sector intermediaries, which could use their creativity and ingenuity to provide retail services to customers on a competitive basis, and leverage their network effects to innovate in business and service models.

2.3 Four types of distribution models

2.3.1 Variant of direct CBDC model

Depending on the division of labour between the central bank and the private sector, and how the ledger of retail account balances is administered, different two-tier distribution models can be designed, with different trade-offs. These models are named based on Auer & Böhme (2021) and depicted in Figure 2. In the simplest form, with only customer-facing and authentication tasks delegated to the private sector intermediaries, the central bank still maintains the retail balances and processes retail payment transactions. This is seen as a variant of the direct CBDC model (Bank for International Settlements, 2021; Auer & Böhme, 2021).

2.3.2 Hybrid model

In the hybrid CBDC model, in addition to the common customer-facing tasks and user authentication, the private sector intermediaries also process all retail payment transactions in real time. But the central bank, though not processing retail transactions, would still record all retail balances, as communicated from the intermediaries. Depending on the design, an intermediary could keep a whole copy or part of the retail ledger, and synchronises its copy with the central bank record, and possibly with the copies held by other intermediaries, in real time or periodically, with or without using DLT. This hybrid CBDC model allows the central bank to act as a backstop to the payment system. Should an intermediary fail, the central bank still has the necessary information to allow it to substitute for the intermediary and guarantee a working payment system (Auer & Böhme, 2021; Bank for International Settlements, 2021). The downside is that the central bank's responsibility to safeguard user data would be greater.

2.3.3 Intermediated model

In an alternative model called the intermediated CBDC model, the central bank does not record any retail balance. It only keeps the wholesale balances of individual intermediaries. The detailed records of retail transactions and balances are maintained by the respective intermediaries (Auer & Böhme, 2021; Bank for International Settlements, 2021). The infrastructure and operation would be roughly similar to that of the fast retail payment systems. The operational burden on the part of the central bank is minimum, and better cyber resilience may be achieved through a higher degree of decoupling between the wholesale and the retail ledger. Since the central bank does not need to record retail balances or user transactions, its responsibility to safeguard user data is also lower. This is also in line with the observation that people tend to trust traditional financial institutions more to safeguard their data (Bank for International Settlements, 2021). However, the downside is that additional safeguards or oversight (and prudential standards) would

be necessary, as the intermediaries would need to be supervised to ensure at all times that the wholesale holdings they communicate to the central bank accurately reflect the retail holdings of their clients (Bank for International Settlements, 2021).

2.3.4 CBDC-backed e-money

The same infrastructure used in the two-tier distribution models of CBDC may also be used for intermediaries' issuance of e-money, which is fully backed by CBDC. This CBDC-backed e-money is compatible with the note-issuing bank system of Hong Kong. Unlike an rCBDC, which is a direct liability of the central bank, CBDC-backed e-money is private money (i.e. a liability of the issuing intermediary) despite that such arrangements are often termed indirect or synthetic CBDC (Adrian & Mancini-Griffoli, 2019; Kumhof & Noone, 2018). While an rCBDC would strike a new balance between central bank money and private money (Bank for International Settlements, 2021), CBDC-backed e-money tends to preserve the existing two-tier monetary system. Insufficient transparency in the management of the backing assets and inadequate consumer protection are usually cited as the main issues of typical stablecoin arrangements (Bullmann et al., 2019). The benefits of CBDC-backed e-money are improved safety and customer protection.[3] Since the central bank is not the issuer of the CBDC-backed e-money, the central bank would not have to maintain retail balances, and its responsibility to safeguard user data is also lowered. Its oversight responsibility is to ensure that an intermediary would not over-issue e-money without adequate backing of CBDC. However, the central bank may lack information to honour claims on the backing assets under its custody when an issuing intermediary becomes insolvent

[3] Compared to the arrangement that private payment service providers hold customer balances as bank deposits, full backing by CBDC could reduce the systematic risks and runs on money market funds, which are identified by Group of Thirty (2020), that may be introduced in face of concerted redemptions by customers.

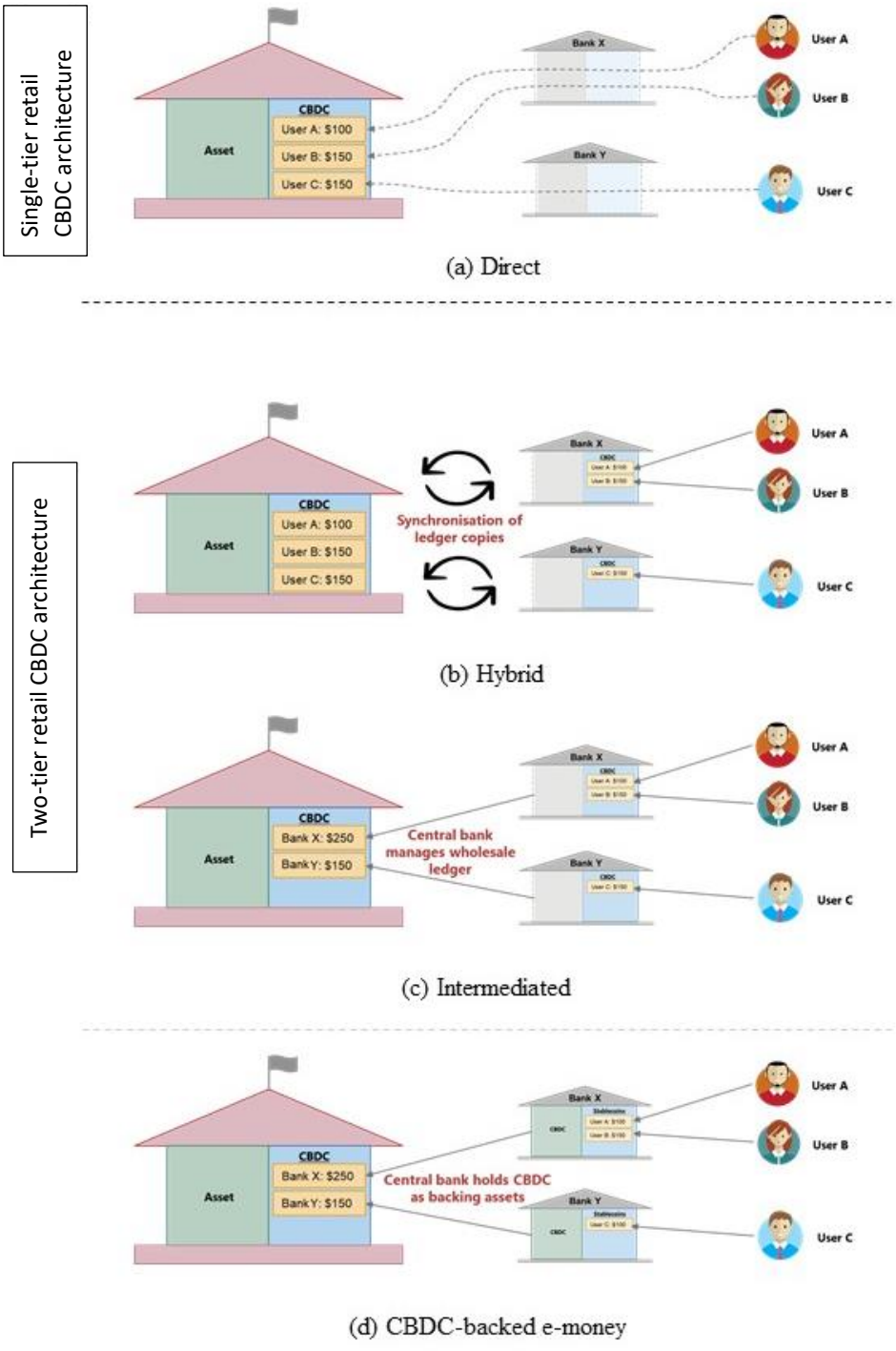


Figure 2. Division of work between central bank and the private sector in different two-tier rCBDC architectures. Source: Adapted from Auer and Böhme (2021)

2.4 Trade-offs between different models

Different trade-offs can be observed in these two-tier distribution models, namely, the central bank's operational burdens, the level of decoupling between the wholesale and retail ledger, the central bank's responsibility to safeguard user data, and the required level of trust on the intermediaries (or correspondingly the central bank's supervisory burden). The level of decoupling between the two ledgers has implications on cyber resilience, based on the principle of privilege separation or network segmentation (Provos et al., 2003; Australian Cyber Security Centre, 2019). The intermediated model and CBDC-backed e-money have a higher level of decoupling, and hence better cyber resilience, than the hybrid model. The central bank's operational burden and responsibility to safeguard user data are also lower in these two models. However, as a trade-off, these two models require a higher level of trust on the intermediaries, or stronger safeguards or oversight on their activities, which translates into higher supervisory burden on the central bank. Auer and Böhme (2021) nicely summarises the dynamics regarding the choice between the hybrid and intermediated model: the central bank has to operate either a complex technical infrastructure or a complex supervisory regime.

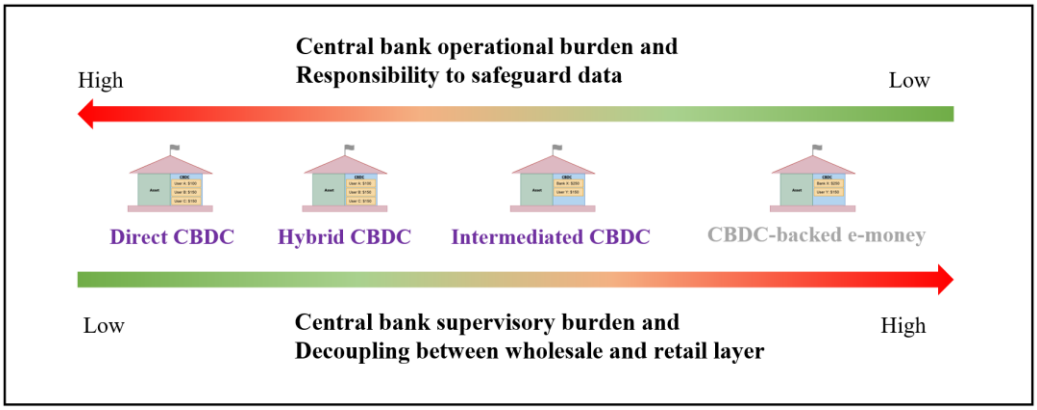


Figure 3. Trade-offs between different models

3. Key design considerations and questions of a two-tier distribution model

3.1 Elements that make a good design

3.1.1 Decoupling of wholesale and retail layers

A typical two-tier distribution model of rCBDC consists of two separate, connected layers, namely, the wholesale interbank system and the retail user wallet system. Only intermediaries (banks and PSPs) — which are relatively more trustworthy — can participate in the wholesale layer, whereas, the retail layer is an open system accessible to the general public. In other words, adversaries may exist in the retail layer to launch cyber attacks, aiming to undermine the operation of the CBDC system. Ideally, a good design should decouple the two layers as much as possible in order to ensure that cyber attacks from the retail user system will not be cascaded into the wholesale interbank network, which may possibly undermine the CBDC issuance process. The intermediaries with presence in both layers would be the only channel for cross-layer communications. In addition,

in two-tier distribution models like the intermediated CBDC model and CBDC-backed e-money, for user privacy considerations, the system is designed such that the central bank does not record retail balances, resulting in minimum interactions between the two layers when payments are made in the retail layer. The intermediaries would be responsible for maintaining the correctness of the retail balances.

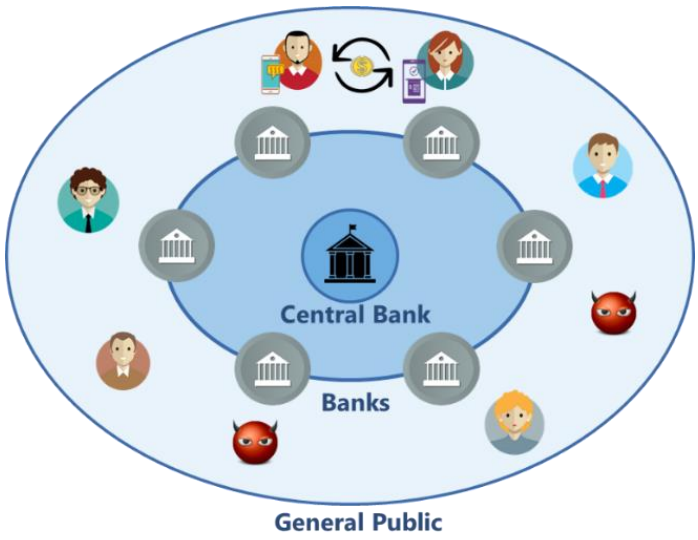


Figure 4. A two-tier distribution model for rCBDC

3.1.2 Cross-ledger synchronisation

While desirable for cyber resilience and, sometimes, for user privacy considerations, the decoupling of the wholesale and retail layers poses challenges for cross-ledger synchronisation. A robust design is necessary to guard against the possibility of over-issuance and double spending by an intermediary. The decoupling of the two layers poses challenges to maintaining congruence of the respective ledgers, especially, when all the communications between the two layers depend solely on the intermediaries. In order to minimise the central bank's supervisory burden of implementing oversight on the intermediaries, a technology solution is needed to ensure that the intermediaries follow the rule and protocol, specifically, to prevent an intermediary from over-withdrawing CBDC as CBDC moves from the wholesale layer to the retail layer, or over-issuing e-money without adequate CBDC backing in the retail layer. In addition, it is also necessary to prevent double spending of CBDC or e-money by an intermediary or user in the retail system to maintain ledger integrity.

3.1.3 Privacy-preserving transaction traceability

To correctly identify the rightful owners of CBDC in the wholesale layer, and ensure correct accounting and redemption of e-money with multiple issuers, traceability of retail transactions is necessary but needs to be done in a privacy-preserving manner. Issuance of CBDC can only take place in the wholesale layer by the central bank. As CBDC moves to the retail layer or is used to back e-money issuance in the retail layer, the central bank may not be able to keep the latest records of the owners of the CBDC, especially in the intermediated model or CBDC-backed e-money. Should an intermediary become insolvent, the central bank could lack information to honour claims on the CBDC itself or as the backing assets from the general public. A traceability

solution is therefore needed to provide the central bank with the needed information. Besides, the same traceability capability is also needed for e-money if there are multiple issuers. When e-money is issued by multiple issuers, for correct accounting and redemption of e-money, it is necessary to identify the issuers and the corresponding backing assets of the e-money used in a transaction. For the CBDC or e-money to be widely accepted as a payment means, user anonymity should be preserved if transactions are traceable. Privacy-preserving transaction traceability is therefore sought.

3.1.4 Flexible and reconfigurable

A flexible, and preferably reconfigurable, technology architecture that supports multiple instantiations of the two-tier distribution models, including both CBDC and CBDC-backed e-money, is desirable. Some of the two-tier models may be more suitable than the others in a given jurisdictional context or scenario. Flexibility to instantiate different models would considerably increase the applicability of the technology design to different contexts. This flexibility is especially important, given the uncertainty about the final form of the rCBDC that would be widely accepted and the outcome of the ongoing debate on CBDC.

3.2 Key design questions

In summary, technological solutions are being sought to address three main design issues, namely, over-issuance prevention, privacy-preserving transaction traceability and a flexible architecture to support different models of rCBDC. More detailed design questions are given in Table 2.

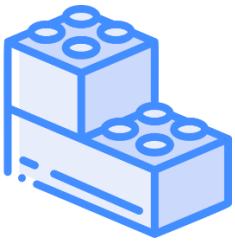
Design Issues	Key Design Questions
 **Over-issuance Prevention**	• With minimised interaction between the wholesale and retail ledgers, can a design be certain that the two levels of ledgers are always congruent? • Can technology help ensure that an intermediary follow the rule and protocol? • With intermediaries being the only channel for cross-ledger communications, can over-issuance of e-money and double spending of CBDC by an intermediary be prevented with a suitable design of transaction structure? • Can the same structure allow detection of the traitor?
 **Privacy-preserving Transaction/Asset Traceability**	• Can transaction traceability be supported while preserving user privacy? • Can a design tell who is the issuer for a given amount of e-money held by a user? • Can the design tell which CBDC backing asset should be released when e-money is redeemed? • Can transactions be designed in such a way that they can provide sufficient information for the central bank to honour claims when an intermediary becomes insolvent?
 **Flexible Architecture**	• Is it possible to have a flexible architecture which can support different two-tier distribution models, including hybrid CBDC, intermediated CBDC, and CBDC-backed e-money? • Can a design be modularised such that different two-tier distribution models can be instantiated through configuration of components? • Can the design support different types of arrangements (e.g. token vs. account) with minimal design changes? • Can the design be extensible for new services or innovation to be built on?

Table 2. Key design questions for two-tier distribution infrastructure for rCBDC

4. Principles guiding solution ideation

The solution ideation process of this whitepaper is guided by the key principles of safety, efficiency, and openness to change, innovation and competition. Figure 5 depicts an exposition to stipulate the desirable properties and characteristics that an ideal CBDC system and infrastructure should exhibit in order to fulfil these three principles. However, in practice, it is impossible to achieve all these properties in one design as the actual instantiation would inevitably involve trade-offs between them.

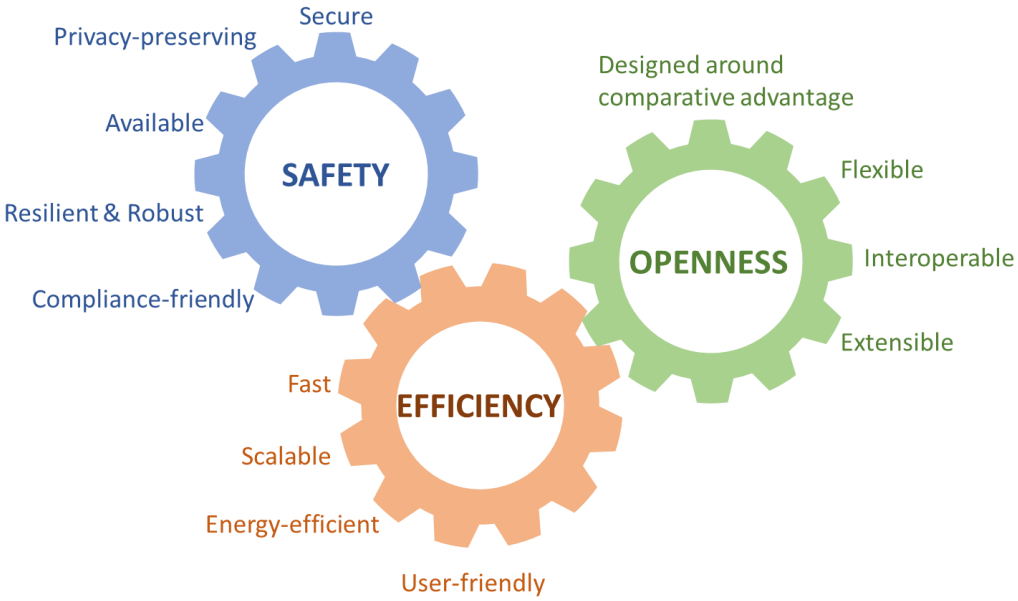


Figure 5. Design principles for the two-tier distribution infrastructure for rCBDC

4.1 Safety

The safety consideration is about ensuring that CBDC, as a payment system, performs reliably as planned at all times in order to build up user confidence. For any rCBDC that can be used as a safe payment instrument, the design of its infrastructure is required to be:

- **Secure** — A CBDC payment infrastructure should follow the highest level of standard against frauds and cyber-attacks. While a silver bullet solution that is unconditionally secure may not exist in practice, the design should be based on a well-articulated adversarial model, with potential attack vectors systematically enumerated. Whenever possible and affordable, the **defence-in-depth** strategy should be adopted such that multiple layers of defence or protective means should be in place against a given attack in order to safeguard the integrity of the ledger and system of CBDC.
- **Privacy-preserving** — A CBDC system should be compliant to relevant privacy protection regulations. Ideally, the **privacy-by-design** approach should be adopted to embed user privacy protection in the system design and operation of CBDC (Information and Privacy Commissioner of Ontario, 2018). The system should be designed in such a way that only necessary data are disclosed to relevant parties as needed for processing transactions and

fulfilling relevant compliance requirements. Personally identifiable information (PII) should be restricted to authorized parties only.

- **Available** — A CBDC system should be highly available with minimum service downtime. Ideally, it should provide 24/7 payment services.
- **Resilient and robust** — Ideally, a CBDC system should be robust to known operational issues and resilient to unknown operational disruption. It should be able to recover from unknown operational disruption such as connectivity outages whenever practically feasible.
- **Compliance-friendly** — A CBDC system should support CBDC to be compliant with regulations around AML/CFT and sanctions.

4.2 Efficiency

The efficiency consideration is about ensuring that CBDC offers benefits to users and the industry while keeping the cost incurred in setup and operation at a reasonable level. An efficient CBDC infrastructure that brings benefits to households and businesses needs to be:

- **Fast** — The process from the initiation of a payment by a payer to the receipt of funds by a payee should be completed as quickly as possible with certainty of completion. In technical terms, the end-to-end latency of a payment transaction should be reasonable for the typical user, with reference to the waiting time they typically find acceptable.
- **Scalable** — As the uptake increases, the number of users and volume of transactions will increase. Therefore, the technology on which a CBDC infrastructure is built should be able to handle the increased demand through the addition of a reasonable amount of hardware resources. The additional hardware resources required should be linearly proportional to the increased transaction volume and user base.
- **Energy-efficient** — The energy required to process a transaction should be as little as possible to reduce the emission of greenhouse gases. Proof-of-work based protocols, which demand a disproportionately high level of power consumption, should therefore be avoided.
- **User-friendly** — The user interfaces for making payments should be intuitive to typical users, requiring the lowest level of technical literacy and minimum number of steps whenever practically feasible. Ideally, user-friendliness should include accessibility for the widest group of users, including those who might be physically challenged and face barriers in access to hardware or data networks.

4.3 Openness to change, innovation and competition

The openness consideration is about ensuring that the CBDC system as a whole remains open to change, innovation and competition, and evolves with the changing needs of users and central banks. This means that the CBDC infrastructure would need to be:

- **Designed around comparative advantage** — The issuance and distribution infrastructure of a CBDC should be developed based on the respective strengths and expertise of the central bank and the private sector, so long as the infrastructure provides a level-playing field for the private sector and does not compromise safety, security, and resilience of the payment system.

- **Flexible** — The issuance and distribution infrastructure of a CBDC should be modular and designed as a composition of reconfigurable components, in order to allow a certain degree of flexibility for central banks to implement different two-tier models according to the respective jurisdictional contexts, and accommodate changes as informed by new policy research findings. If practically feasible, the design of the infrastructure should also be flexible to support the issuance and settlement of different asset embodiments (CBDC and CBDC-backed e-money).
- **Interoperable** — A CBDC infrastructure should be designed in a manner that avoids creating a closed-loop payment system wherein users can only make payments to users of the same provider. Instead, it should allow CBDC payments to be freely made between users of different banks and PSPs, and ideally, easy payments between a CBDC account and a bank deposit account. While a certain, minimum set of standards and rules for cross-provider payments, such as transaction structures and cryptographic schemes, is inevitable, the CBDC system should allow banks and PSPs a reasonable degree of autonomy in choosing the respective technology platforms and interfaces for providing services to their customers. This would imply that the interface between providers and the core infrastructure should preferably be based on common, conventional technology. In addition, the CBDC infrastructure should be designed to allow future extensions to support interoperability with other countries' CBDC payment systems. This requirement would mean interfaces for unseen software connectors should be part of the design considerations.
- **Extensible** — Recognising that the functionality of the CBDC infrastructure would need to evolve over time, the design should not limit the range of services that can be provided in the future. Rather, it should include sufficient room for enhancements or extensions to allow private sector innovators to build additional services on top of the CBDC platform, and support innovative use cases.

5. Architecture of one possible design

While the HKMA is opened to different architecture designs, based on the three guiding principles in Chapter 4, and taking reference from the interim results from Project Aurum, one possible design is proposed. The design consists of two layers: (1) wholesale CBDC issuance and redemption system (called the interbank layer or, simply, the wholesale system) and (2) an rCBDC/e-money distribution and circulation system (called the wallet layer or, simply, the retail system). The former should only be accessible to intermediaries (commercial banks and PSPs) and the central bank, whereas the latter could only be accessed by intermediaries and an ecosystem of users in the general public equipped with mobile wallet applications. CBDC issuance only takes place in the wholesale system. The retail system is supposed to be operated by the intermediaries with minimum involvement of the central bank. The wholesale and the retail systems should be adequately decoupled with minimum information exchange to minimise the attack surface and exposure of the CBDC issuance process. The intermediaries, serving as gateways, facilitate the communication and synchronisation between the wholesale and retail systems. This chapter will describe the design of this architecture and how the design would avoid the intermediaries from deviating from established protocols and rules.

5.1 Tier 1 – wholesale system

The wholesale system for issuance and redemption of CBDC, and settlement of interbank transactions is based on DLT. The wholesale system is used only for transactions among the central bank and intermediaries, among the intermediaries themselves as well as for the deposit of CBDC to an omnibus account (Bank of England, 2021) to move CBDC to the retail system.[4] The wholesale system is jointly operated by a number of selected intermediaries, such as those permitted to issue CBDC-backed e-money. The group of pre-selected intermediaries can operate validating nodes that run the DLT consensus. The central bank operates a node for CBDC issuance and redemption but does not participate in the DLT consensus. In this way, the central bank could be freed from the task of settling interbank transactions, resulting in better decoupling.

5.1.1 Technology employed

The technology architecture is agnostic to the state representation of the underlying DLT platform although a UTXO implementation would allow the central bank to have more explicit control on CBDC issuance. CBDC held by the intermediaries in the wholesale system can be represented as either account balances or unspent transaction outputs (UTXOs), depending on the DLT platform adopted. Examples of the former include Hyperledger Fabric and Enterprise Ethereum, whereas, Corda is an example of the latter. The proposed design works well for both implementations. The only requirement is that a transaction processed by the chosen DLT platform can be exported with its signatures to the retail system, in order to prove the authenticity of the transaction and attest that the concerned CBDC has been issued by the central bank and locked up in the wholesale system.

The presence of malicious validating nodes would have similar effects on CBDC supply in both UTXO-based platforms and platforms based on account balances. It seems that, in the DLT platforms based on account balances, the validating nodes have to be trusted to a certain extent to maintain correct CBDC balances. Notwithstanding, the required level of trust on the DLT validating nodes should be similar in both UTXO-based platforms and platforms based on account balances since the presence of malicious DLT validating nodes has a similar impact in the two cases. Malicious validating nodes in the UTXO-based platforms, while unable to issue new units of CBDC, can still assist in double spending the same issued unit of CBDC to increase the money supply. This would achieve similar effects as maliciously adjusting CBDC balances in the platforms based on account balances. However, it is usually easier to notice double spending of the same UTXO than a wrongly adjusted account balance if the ledger is open for inspection (Chan, 2021).

5.1.2 Cybersecurity considerations

It is possible to isolate the CBDC issuance process from the wholesale system to improve cybersecurity. If manual operation is allowed, the redemption process of CBDC can also be decoupled from the wholesale system. A key consideration of the architecture is whether the CBDC issuance process can be sufficiently isolated from other activities (that is, transactions among banks and among users) on the basis of the principle of privilege separation and network segmentation (Provos et al., 2003; Australian Cyber Security Centre, 2019). Since the central bank node is not involved in the DLT consensus by design, it can be placed in separation from other nodes in the wholesale system, say, through a data diode (Okhravi & Sheldon, 2010). This would enhance

[4] The omnibus account is in essence a custodian account jointly controlled by DLT validating nodes that locks up fund or backing assets in the wholesale system as CBDC is moved to the retail system or used to issue e-money in the retail system. The fund or backing assets will be released when CBDC is moved back from the retail system.

cyber resilience and the security of the central bank's private key, which is used to authorize CBDC issuance. Data diodes allow data traffic to flow in one direction only and are the only approach attaining EAL-7 assurance (Common Criteria, 2017). However, the redemption of CBDC would require the involvement of the central bank node in receiving requests from intermediaries, unless a manual process is allowed. There is a trade-off between cyber resilience, ease of operation and the level of process automation.

Difference between UTXO-based and Account-based CBDC issuance

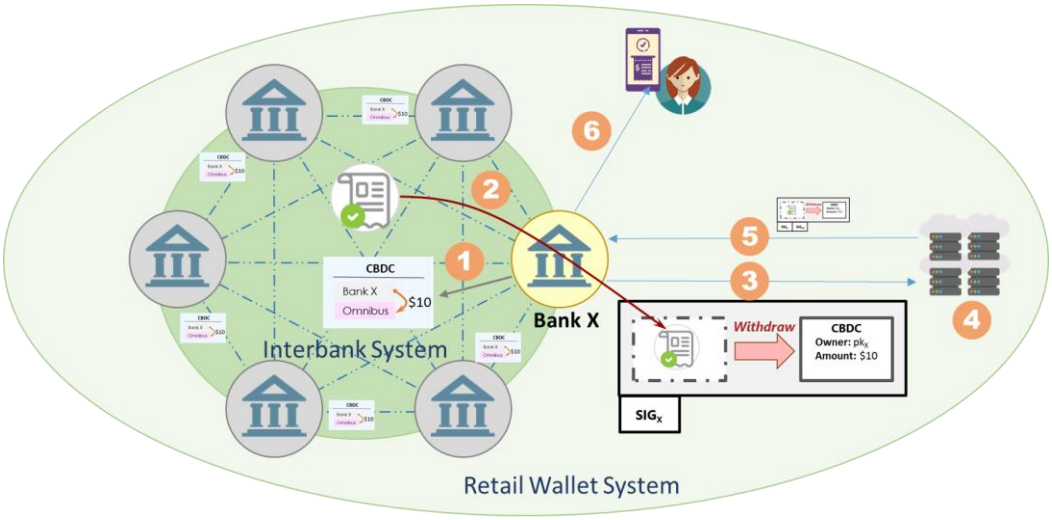
The difference between a UTXO-based and an account-balance-based platform lies in how the global state of the DLT system is represented and updated when a transaction is processed. In the case of CBDC, the global system state corresponds to a representation of the CBDC holdings of all the participants.

In the UTXO implementation, the system state is represented by a list of ownerships of all units of assets, and a transaction explicitly specifies the resulting state (i.e. ownerships) of the concerned units of assets. In this way, the right to issue a new unit of an asset is a prerogative of the respective asset issuer (as assured by public key cryptography), and the DLT (i.e. its nodes responsible for validating transactions) can only update the ownership of an already issued unit of asset, but has no capability to issue new units (Chan, 2021). In other words, the central bank in this case would have sole control of the issuance of new CBDC units on a UTXO-based DLT platform even if it does not participate in managing the platform. This is analogous to cash or other token-based arrangements.

In the account balance implementation, the system state is represented by a list of all participants' account balances of different assets, and a transaction does not carry full information that can allow the determination of the end state or resulting account balances of the participants involved. A transaction has to be combined with the current state or account balances of the involved participants in order to determine the resulting account balances (Chan, 2021). In other words, repeatedly replaying a transaction could possibly lead to wrong account balances. In the context of CBDC issuance on DLT, all the current account balances are maintained by the DLT, and the central bank submits a signed issuance transaction for the DLT to process in order to update the account balances of the respective recipients of the newly issued CBDC. Most DLT platforms use unique transaction references and establish mechanisms to prevent transaction replays.

5.2 Tier 2 – retail distribution and circulation system

A two-tier distribution model is adopted wherein the central bank issues CBDC to intermediaries, which then help distribute and circulate CBDC among households and businesses in the general public. In this model, only the central bank can create and destruct CBDC. Intermediaries serving as gateways are the only communication channels to relay transactions and messages between the wholesale and retail systems (Figure. 6). These intermediaries also help protect the wholesale system and fend off cyber-attacks from the retail system, in turn protecting the central bank node and the CBDC issuance process from potential attacks. *Without loss of generality, the following discussion assumes that the wholesale system is based on a platform implemented with account balances. The discussion for a UTXO-based platform should be similar but simpler.*



(1) To distribute CBDC from the wholesale system to the retail system, the requesting intermediary (Bank X in this case) initiates a CBDC deposit transaction at the wholesale ledger to move funds into an omnibus account which is administered collectively by the intermediaries.
(2) Bank X then exports the validated wholesale CBDC deposit transaction (i.e. signed by a quorum of DLT validating nodes hosted by the intermediaries) from the wholesale, interbank system to the retail wallet system.
(3) Bank X then forms an rCBDC coinbase transaction (in the form of a UTXO) with the wholesale transaction embedded in it for the validator infrastructure of the retail wallet system to verify and endorse by signing on it. The embedded wholesale transaction not only gives a proof of authenticity for the respective rCBDC coinbase, but also allows subsequent rCBDC transactions to be traced back to its backing assets held in the wholesale system as recorded by the wholesale transaction. By defining the coinbase transaction and the claim on the associated wholesale deposit, a coinbase transaction can instantiate a CBDC or CBDC-backed e-money.
(4) The validator infrastructure checks whether the wholesale transaction has been used to back other rCBDC coinbase transactions previously. If it has not been reused, the validator registers the rCBDC transaction as newly created in its UTXO database and sign on the rCBDC coinbase transaction to endorse its validity.
(5) The validator can pass the signed coinbase transaction or simply its signature on the coinbase transaction to Bank X. The rCBDC is now owned by Bank X.
(6) Bank X can distribute a certain amount of rCBDC to an end user by transferring its ownership through forming a new UTXO transaction to consume the output of the coinbase transaction.

Figure 6. Distribution Model of rCBDC

5.2.1 Method of distribution from wholesale to retail layer

Intermediaries distribute or move CBDC from the wholesale system to the retail system by forwarding the concerned wholesale transactions to the retail system and embedding them in the respective coinbase transactions. An intermediary deposits CBDC to an omnibus account[5] (Bank of England, 2021) in the wholesale system in order to withdraw an equivalent amount of CBDC (or issue an equivalent amount of e-money for the case CBDC-backed e-money) in the retail system. The intermediary then passes the confirmed wholesale transaction with the respective signatures (including the intermediary's and those of the needed quorum of DLT validating nodes) to the retail system, and forms a new retail transaction embedded with this wholesale transaction to withdraw the same amount of rCBDC or e-money in the retail system. This retail transaction is called a coinbase transaction (based on the terminology of Narayanan et al. (2016)), marking the first transaction which does not inherit any monetary value from other transactions in the retail system.

The coinbase transaction inherits its monetary value directly from the wholesale transaction embedded in it. No new money is created in the withdrawal process as CBDC is moved from the wholesale system to the retail system. The CBDC spent or deposited in the wholesale transaction is rendered unusable while CBDC is withdrawn from or e-money is issued in the retail system. The monetary value of the newly created coinbase transaction in the retail system

[5] For UTXO-based DLT platform, an intermediary spends a UTXO with a specially crafted transaction to move CBDC to the retail system.

is directly inherited from the embedded wholesale transaction, which in turn originates from an issuance transaction initiated by the central bank. A retail user can verify the authenticity of CBDC or e-money represented by the coinbase transaction through verifying the signatures of the embedded wholesale transaction, which has deposited an equivalent amount of CBDC in the wholesale system. In other words, cross-ledger asset recognition is achieved through signed transactions.

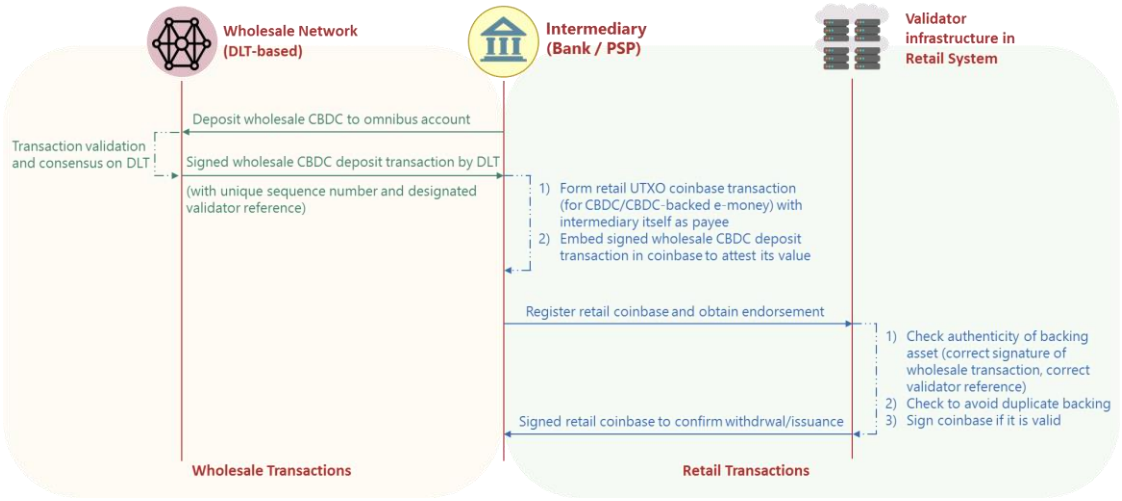


Figure 7. Transaction flow for distribution from wholesale to retail system

5.2.2 Synchronisation and validation of the decoupled ledgers

The synchronisation of the wholesale and retail ledgers is achieved through the exchange of signed transactions channelled through intermediaries. A validator infrastructure is designed in the retail system to ensure that each wholesale transaction is used once only for CBDC withdrawal or e-money issuance. The communications between the wholesale and retail systems are strictly limited to the transactions relayed by the intermediaries to ensure decoupling of the two systems for the sake of cyber resilience. While digital signatures allow the authenticity of a wholesale transaction to be verifiable in the retail system (thereby achieving cross-ledger asset recognition), they cannot prevent an intermediary from repeatedly using the same wholesale transaction to create multiple coinbase transactions to withdraw CBDC or issue e-money multiple times in the retail system. A system-wide validator infrastructure is introduced in the retail system to keep track of wholesale transactions that have been used. When an intermediary creates a new coinbase transaction, it has to obtain a signature on the transaction from the validator infrastructure, which would verify the wholesale transaction and make sure it is a new one before signing on the coinbase transaction. For the sake of prudence, the wholesale transaction should include a reference specifying the validator infrastructure designated to verify it.

A payment transaction takes a coinbase transaction as its input and the value of transfer is inherited from that of the coinbase transaction. A coinbase transaction is valid only if the wholesale transaction is valid and the signature of the validator infrastructure is available and valid. Recipients of the rCBDC and e-money would need to verify that these two conditions are fulfilled. Usually, an intermediary puts itself as the owner of the UTXO of a coinbase transaction. When a user requests CBDC or e-money, the intermediary would then transfer the money through a payment

transaction paid to the user. The value to be transferred with the payment transaction is inherited from the coinbase transaction. To prevent double spending,[6] the validator infrastructure's signature on the payment transaction is required for a valid payment. The validator infrastructure keeps a list of valid UTXOs and would remove all UTXOs that have been spent from the list.

5.2.3 Redemption mechanism

To move CBDC back to the wholesale system or redeem e-money, an intermediary forwards a retail redemption transaction with the validator infrastructure's signature to the wholesale system to release CBDC locked up in the omnibus account. An intermediary may exchange CBDC or e-money accumulated in the retail system for CBDC in the wholesale system through a redemption transaction. A redemption transaction is a special payment transaction with no output UTXO. As in the processing of typical payment transactions, the validator infrastructure's signature on the redemption transaction is required. The validator infrastructure will sign on the transaction only if all its input UTXOs are in the valid list, and then remove them from the valid list. The intermediary then passes the redemption transaction with the needed signatures to the wholesale system and embeds it to form a new wholesale transaction to request a top-up of its account balance. In order for this wholesale top-up transaction to be valid, the signatures of the intermediary and the validator infrastructure on the embedded retail redemption transaction are required and will be verified by the DLT validating nodes. These signatures are needed by the wholesale system to confirm that the concerned CBDC or e-money has been removed from circulation in the retail system before the CBDC is released into the wholesale system. Again, no new money is created.

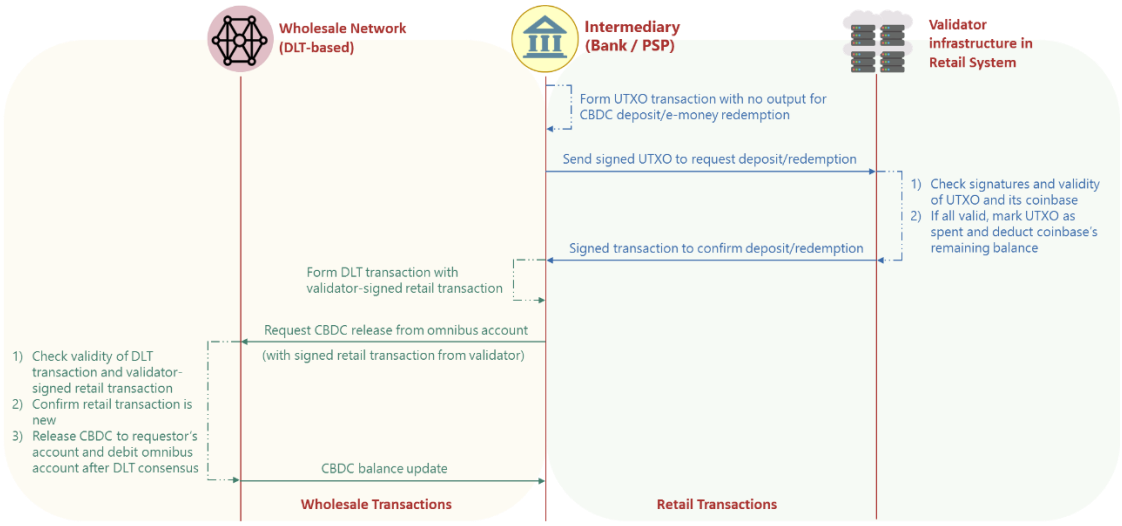


Figure 8. Redemption transaction flow

For readers' interest, the transaction flows for (1) distribution from an intermediary to a user and (2) retail payments between two users are illustrated on the next page. The underlying mechanism is similar to those described in the above paragraphs.

[6] In double spending, a payer pays the same UTXO to two distinct parties. In this way, the same amount of money represented by the UTXO is spent twice.

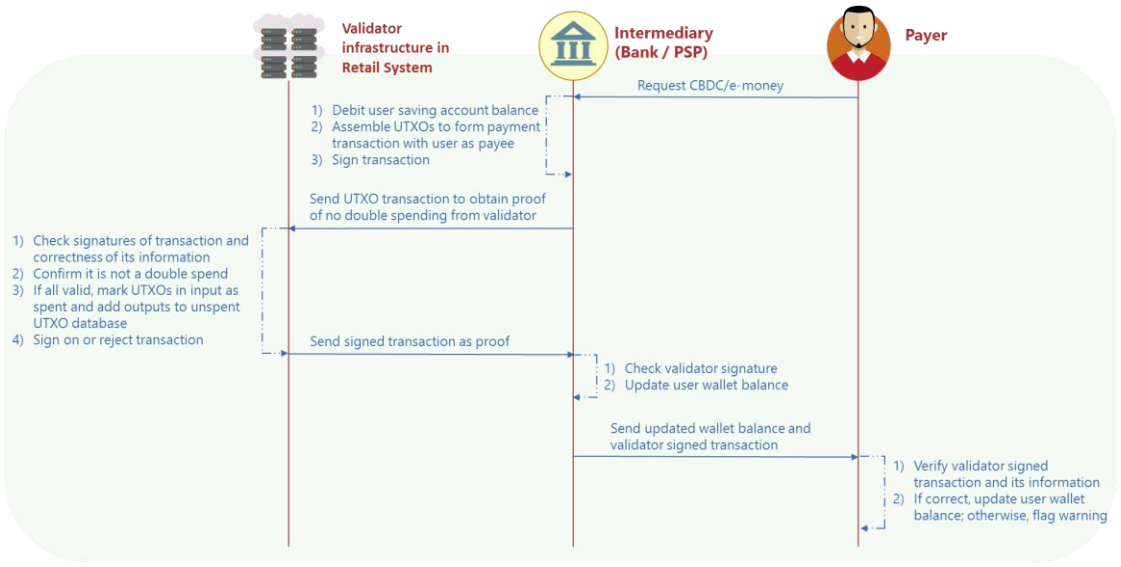


Figure 9. Transaction flow for distribution from intermediary to user

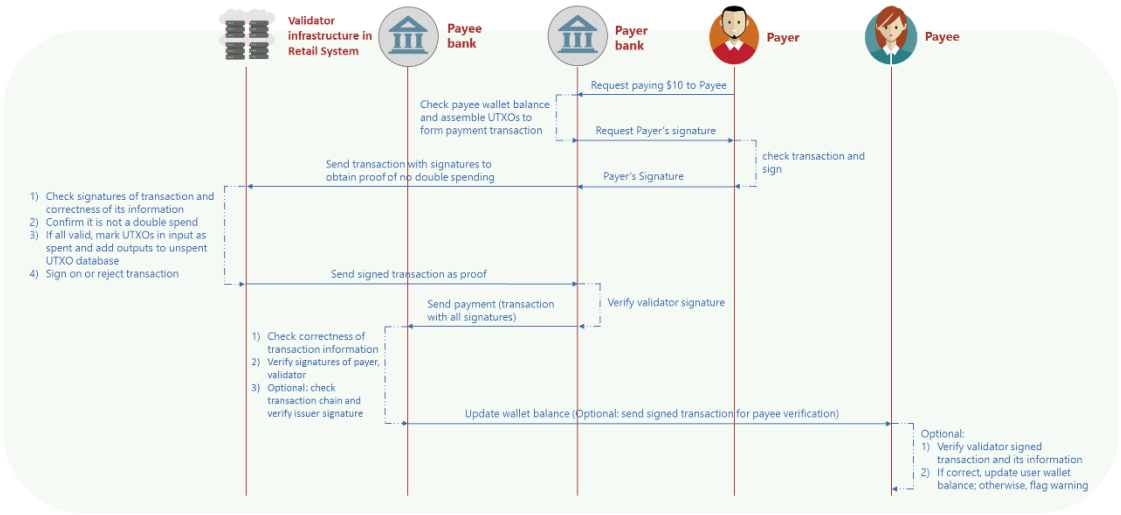
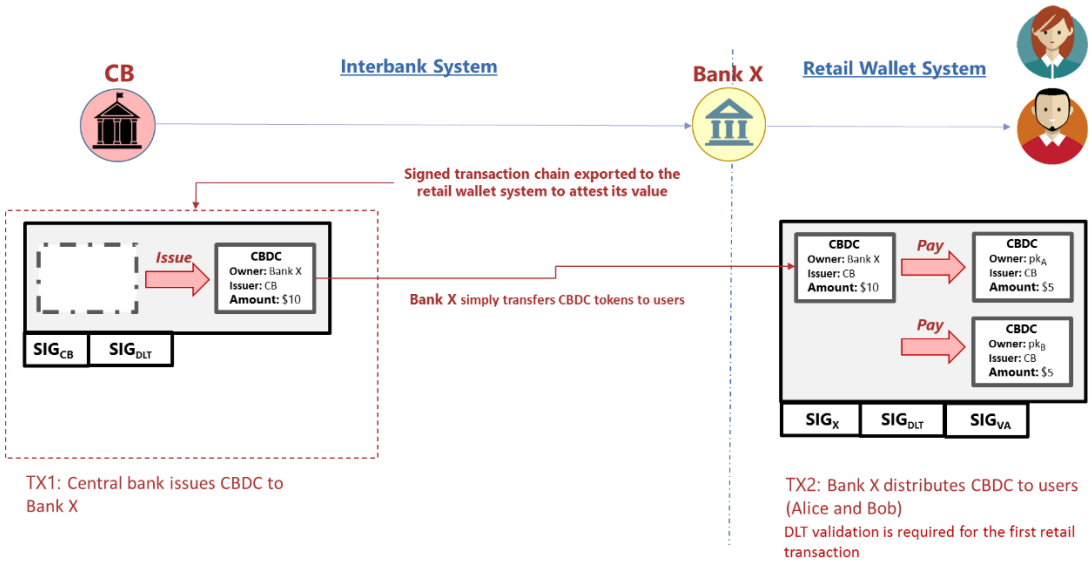


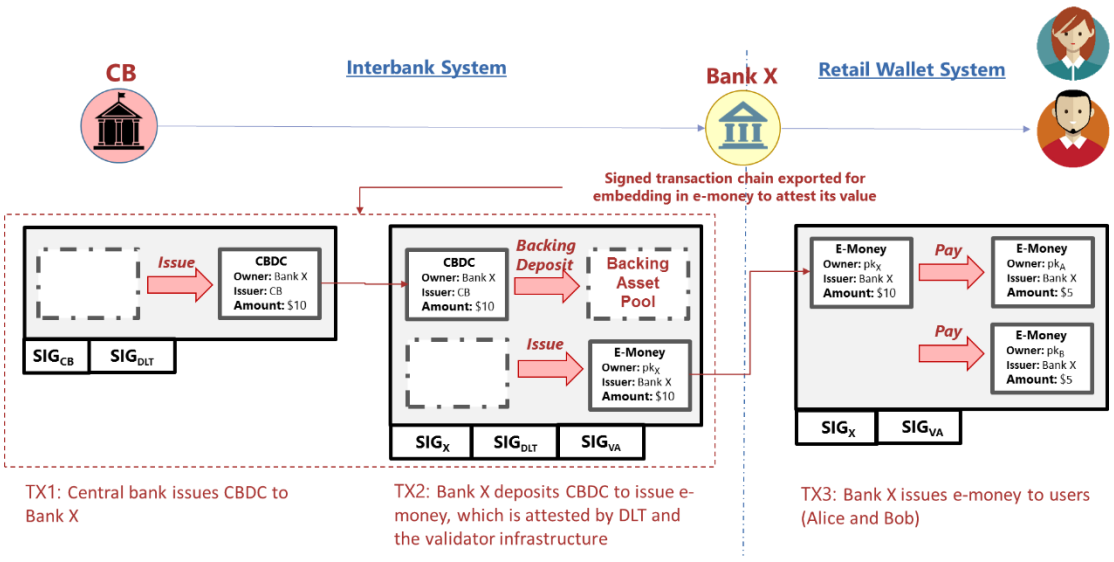
Figure 10. Transaction flow for retail payment transaction between users

5.3 Alternative tier 2 distribution and circulation system with a UTXO-based tier 1 wholesale system

The CBDC distribution model described in Chapter 5.2 is based on a wholesale system implemented with a DLT platform based on account balances. Figure 11 shows how the distribution can be done if a UTXO-based DLT platform is adopted for the wholesale system. The flow should be simpler given both the wholesale and retail systems use UTXO as the basic transaction structure.



(a) Transfer of CBDC from the wholesale system to the retail system



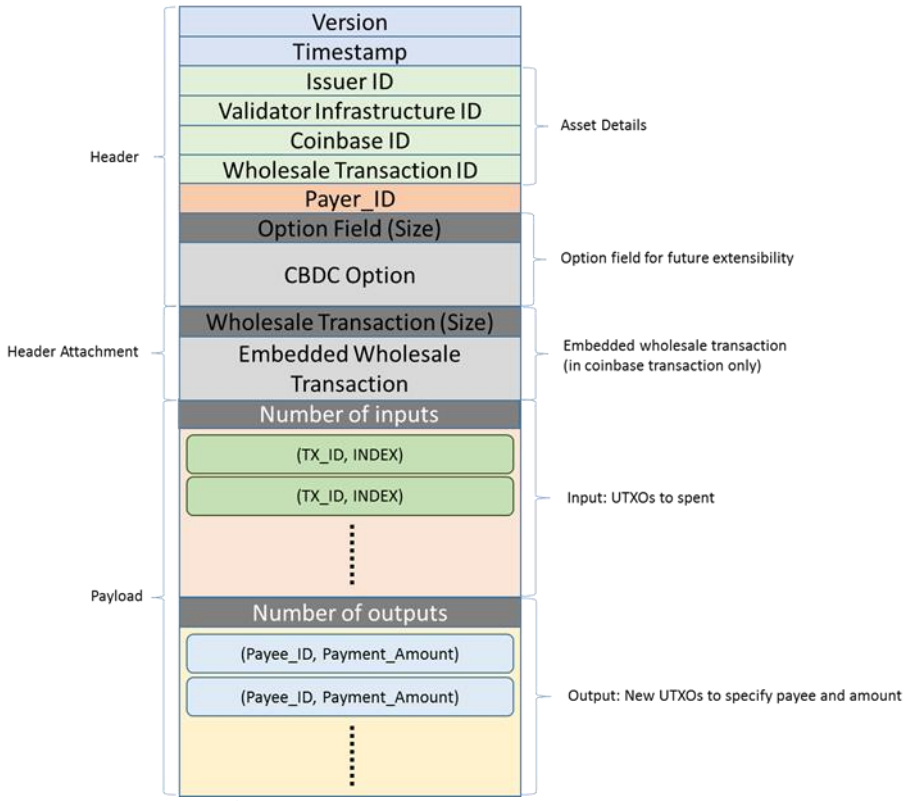
(b) Issuance of e-money in the retail system with full backing of CBDC held in the wholesale system

Figure 11. Cross-ledger synchronisation with UTXO-based DLT Platform (Corda) for the Wholesale System

5.4 rCBDC based on UTXOs with account balances

Users in the general public hold rCBDC in the form of account balances at intermediaries, with the formation of UTXO transactions (signed by the owner and the validator infrastructure) required for the actual value transfers in payments. As shown in Figure 6, a typical coinbase transaction — through which an intermediary (Bank X) moves CBDC from the wholesale system to the retail system — has no input and only one output or UTXO that specifies the payee (the intermediary itself) and the amount of CBDC the payee owns. For preserving user

anonymity to a certain extent, the payee's public key, rather than his real identity or PII, is used in the UTXO. In order to spend this UTXO, the intermediary as its rightful owner has to form a payment transaction that includes an input and new outputs. The input is the output or UTXO of the coinbase transaction that is to be spent by the payment transaction and new outputs or UTXOs are created to specify the payees and amounts of the payment. The payer and the validator infrastructure have to sign on this payment transaction before it is finalised and valid. The payee or his bank will need to verify the validity of the payment transaction through verifying its content and the attached signatures. If the payee's bank is also the payer, the payee has to verify the payment transaction.[7] Depending on how much the validator infrastructure can be trusted, the verification of a payment transaction might also need to include the verification of the inheritance chain of previous payment transactions up to the coinbase transaction. If all the verification goes well, the payee's bank can then update the CBDC account balance of the payee accordingly. Usually, users would only see CBDC account balances and their banks or PSPs would form, manage and receive UTXO transactions for them. Similarly, for Alice to spend the received payment, she has to form a payment transaction with an input referencing the UTXO she received in a previous a transaction and new outputs.



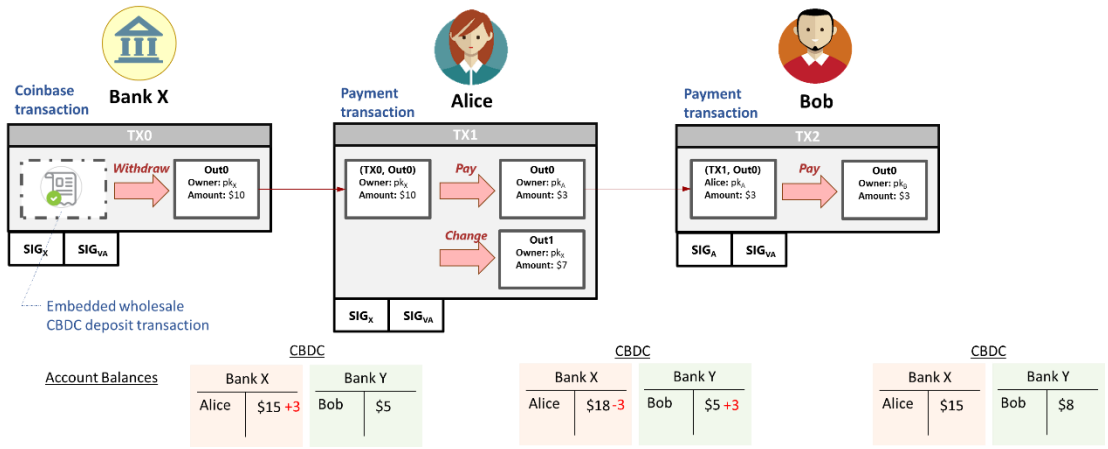
1) The issuer ID refers to the central bank in CBDC and issuing intermediary in CBDC-backed e-money.
2) The Payer_ID and Payee_ID include the public key of payer/payee and a reference to his bank or PSP

Figure 12. A sample UTXO transaction

[7] If the payer is simply the payee's bank, the payee has to verify the transaction because it is the bank that will update the payee's CBDC account balance accordingly when all the verification went well. The payee's verification of the payment transaction is necessary to safeguard against the scenario where the payer creates an empty transaction (without valid inputs) and skips verification by the validator infrastructure to deceive the payee.

5.4.1 Benefits

This design leverages on the strengths of both UTXOs and account balances, that is, the traceability of UTXO transactions, and the intuitiveness of account balances for people to conceptualise money. Since each UTXO transaction has an explicit reference to a previous transaction and inherits its monetary value from it, transactions inheriting their values from the same portion of a coinbase transaction can be readily linked up to form an inheritance chain.[8] This inheritance chain would allow the latest ownership of CBDC or e-money to be traced back to the respective portions of coinbase transaction(s), which in turn explicitly point to the wholesale transactions (and therefore the backing assets for e-money) that the monetary values in the retail system originated from. This traceability of UTXO transactions would allow an intermediary to distinguish e-money issued by different issuers. Should an issuer become insolvent, an e-money owner (possibly with the help from the validator infrastructure) showing a transaction chain could prove his ownership of the backing assets, thereby allowing the central bank to honour claims. The same would apply to CBDC in the intermediated model. However, it could be relatively difficult for people to work directly on UTXO transactions. To improve the user friendliness of this model, users would only see account balances at intermediaries serving them, and the intermediaries would manage UTXO transactions for the users.



Alice is a customer of Bank X and holds a CBDC account balance at Bank X. Bob is a customer of Bank Y and holds a CBDC account balance at Bank Y. If Alice pays to Bob, Bank X will help her form a payment transaction in UTXO format and send it for endorsement signature by the validator infrastructure. Then Bank X will debit Alice's CBDC account balance and send the validated payment transaction to Bank Y. Bank Y will help Bob to verify the content and signatures of the received payment transaction. If the verification goes well, Bank Y will update Bob's CBDC account balance.

Figure 13. Account balance/UTXO Hybrid Model

In practice, UTXO transactions have the flexibility to instantiate account-based or token-based implementations while explicitly supporting transaction traceability.[9] Table 3 compares UTXO with account balances and tokens with respect to their effectiveness in addressing the design

[8] More precisely, each transaction (be it a coinbase or payment transaction) has a transaction number which is usually a hash value of its content, an output of a previous transaction is usually referred by a pair consisting of the transaction number and the index of the output.

[9] A UTXO transaction can implement a token or account, based on whether the public keys used in a UTXO represent the identity of a user (as in Bitcoin) or that of a token (as in Chaum (1983), Chaum et al. (1988), Chaum et al. (2021)).

issues of the two-tier distribution infrastructure for rCBDC.[10] Typical transactions used in account-based ledgers lack information for asset or transaction traceability. When an account balance is updated, information of a transaction is subsumed into the new balance. This not only makes it difficult to trace transactions, but also poses challenges for cross-ledger asset recognition. Besides, implementation of anonymity protection in an account-based ledger is non-trivial, whereas, a pseudonym system is easy to implement and effective for a UTXO-based ledger.[11] While a pure token implementation (Chaum, 1983; Chaum et al., 1988; Chaum et al., 2021, Camenisch et al., 2005; Camenisch et al., 2007) does not have the same inefficiencies as in account balances, transaction traceability is not supported as each token can only be used once and the central bank has to re-issue a new token each time a payment is made. On the contrary, traceability is native in UTXO transactions.

	Account balance	UTXO	Token (e.g. Chaum 1983, Chaum et. al. 1988)
Cross-ledger synchronisation & asset recognition	Difficult	Easy	Easy
Transaction traceability (esp. for backing asset)	No	Yes	No
Token based or Account based	Account based	Both	Token based
Implementation of transaction anonymity	Difficult	Easy	Easy

Table 3. Comparison of accounts, tokens and UTXOs for solving the design issues of two-tier distribution infrastructure for rCBDC
Source: Adapted from Chan (2021)

5.4.2 Different coinbase transaction definitions under UTXO

Depending on the definition of a coinbase transaction and the associated legal arrangement for the underlying asset, the financial asset it represents could be CBDC or CBDC-backed e-money. The monetary value transferred in any payment transaction is ultimately inherited from one or more coinbase transactions, of which the underlying assets are represented by

[10] The distinction between token-based systems and account-based systems is based on the definitions of Bank for International Settlements (2021). Unlike a physical token as defined in Kahn & Roberds (2009) and Kahn (2016), a digital token still needs intermediation during ownership transfer. Although the authenticity of a digital token can be guaranteed through public key cryptography, a digital token can be easily copied, which implies that a malicious owner of a digital token could double spend it by giving different copies of the digital token to different payees. Intermediation through a trusted party is therefore necessary to uniquely determine the rightful ownership of a digital token.

[11] Transactions to a particular account would always cause an update of balance to that account would also mean implementing anonymity is non-trivial. If pseudonyms are implemented in an account-based system, the size of the system state or the number of accounts in the system could grow fast as payments are made to become practically unmanageable. In contrast, the system state of a token-based or UTXO-based implementation is proportional to the number of active UTXOs and independent of the number of existing pseudonyms.

the wholesale transactions embedded in them. Besides, different legal arrangements can be made on the claim of ownerships of these underlying assets, which are CBDC issued by the central bank in the wholesale system. As a result, the same coinbase transaction structure could be used to instantiate CBDC or CBDC-backed e-money by adjusting the definition of the coinbase transaction and respective legal arrangements (Chan et al., 2017).[12]

5.4.3 Trade-offs of speeding up UTXO tracing

The tracing of an inheritance chain of transactions could possibly be speeded up by including in payment transactions explicit references to the coinbase transaction, but this may increase the overhead of payment transactions. In the most primitive form, one has to trace and verify each transaction in an inheritance chain in order to verify the possession of the backing assets when given a payment transaction. As payments are made, this inheritance chain could grow to a practically unmanageable length. Including the transaction numbers of the coinbase transaction(s) in each subsequent payment transaction would greatly reduce the tracing complexity to a constant factor. Since the transaction number is usually implemented as a hash value of the content of a transaction, the integrity of the coinbase transaction can be verified easily. However, if merging of UTXOs from different previous transactions in a payment transaction is allowed, the size of these coinbase references could grow considerably, increasing the transaction processing complexity on the part of the validator infrastructure and intermediaries. The trade-off needs careful investigation.

5.5 Validator infrastructure designed as a UTXO database

5.5.1 Purpose

A designated validator infrastructure is needed in the retail system to prevent duplicate use of the same wholesale transaction to create multiple coinbase transactions by an intermediary, and double spending of the same UTXO to pay multiple payees by a user or intermediary. While public key cryptography can allow anyone to verify the authenticity of a transaction, thereby supporting cross-ledger asset recognition and peer-to-peer payments,[13] it cannot prevent an intermediary from using the same wholesale transaction to create multiple coinbase transactions to withdraw CBDC or issue e-money multiple times without adequate backing in the wholesale system. Neither can it prevent a user or an intermediary to use the same UTXO to pay multiple payees, that is, double spending. Without counter-checking with other payees, a payee would not be able to notice such an over-withdrawal/over-issuance or double spending. A system-wide function is therefore necessary to preserve the integrity of the retail ledger and maintain a unique, temporal order of payment transactions to prevent double spending. A designated validator infrastructure is designed as a UTXO database to be the single source of truth for the status of all transactions in the retail system. It records the first appearances of all valid wholesale transactions in the retail system and retail transactions (including coinbase and payment transactions), and rejects subsequent, repeated appearances of transactions that have been recorded in its database.

[12] The same coinbase transaction structure could be used to instantiate rCBDC or CBDC-backed e-money by adjusting the coinbase definition, as demonstrated in Chan et al. (2017) which redefines and uses the coinbase of the genesis block of a Bitcoin-based blockchain to manage the administration privilege rights of the blockchain and turn it into a permissioned blockchain.

[13] Fully peer-to-peer payments without any intermediation by a third party cannot be achieved in practice. Some form of intermediation, be it by a single trusted party or all participants of a system, is inevitable to ensure that a token is not double spent.

5.5.2 One implementation of the validator infrastructure

A simple implementation of the validator infrastructure consists of two databases, with one keeping track of valid coinbase transactions and UTXOs, and the other storing all valid, raw transactions. Any database technology can be utilised. As shown in Figure 14, the first database consists of two tables: the first table uses the transaction ID of the wholesale transaction (embedded in a coinbase transaction) as its primary key, while the second table uses the pair referencing UTXOs (i.e. the transaction ID of the payment transaction containing a UTXO and the output index of the UTXO) as its primary key.

One of the databases consists of two tables, with the first table recording coinbase transactions and their remaining monetary values, and the second table recording active UTXOs. When a new coinbase transaction with valid signatures is received, the validator infrastructure uses the transaction ID of the embedded wholesale transaction to search for a match in the first table. A match means that this coinbase transaction is an over-issuance. The validator infrastructure will reject it. Without the validator infrastructure's signature, no payee would accept the coinbase transaction or any of its subsequent payment transactions. If there is no match, the coinbase transaction will be added to the first table, and its UTXO added to the second table. When CBDC is moved to the wholesale system or CBDC-backed e-money is redeemed, the monetary value will be deducted from the corresponding coinbase entries in the first table.

As payment transactions are processed, old UTXO entries are erased from the second table, with new ones added to it. When a new payment transaction with a valid payer signature is received, a search in the second table for each input of the received transaction (which should consist of the transaction ID of a previous transaction and the output index of the UTXO to be spent) will be conducted. If a match can be found for all these inputs, the matched entries will be erased from the second table, and the new UTXOs of the payment transaction added to it. Otherwise, the payment transaction would be rejected. The validator infrastructure's signature on a payment transaction is necessary for the confirmation of payment.

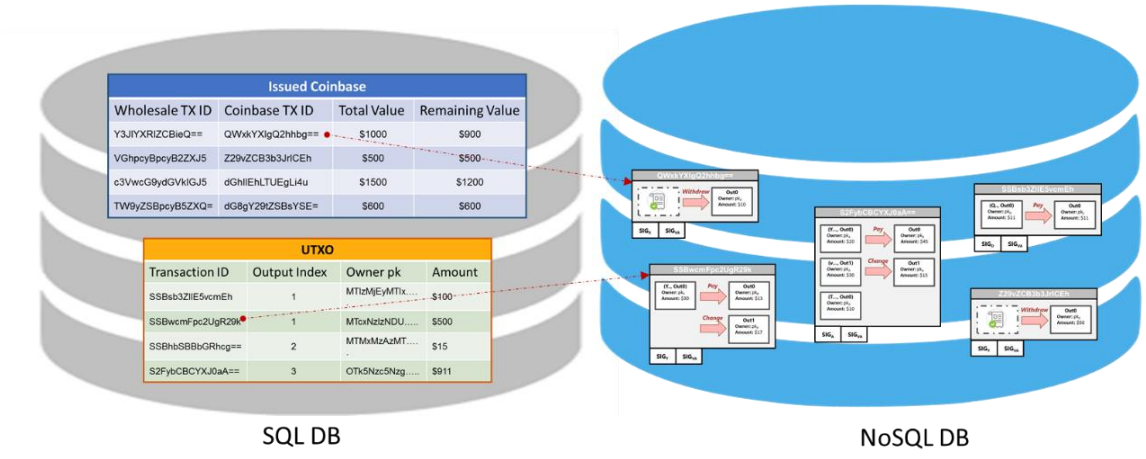


Figure 14. Validator's UTXO database stores unspent transaction outputs in a relational database and signed transactions in a NoSQL database

5.5.3 Other design considerations

The role of the validator can be played fully by a single party or collectively by multiple parties in a DLT setting. While a conventional, centralised database implementation for the

validator infrastructure is preferable for performance and governance considerations, the current architecture does not preclude other implementations, for instance, DLT. A centralised database implementation does not necessarily imply a lower level of resilience compared to DLT.[14] The distinction between a centralised database and DLT lies mainly in whether the infrastructure (which could be composed of multiple machines for both cases) is in full control by a single entity or jointly controlled by multiple entities with decision made through a voting-like process (i.e DLT consensus). DLT would be particularly useful for implementing the validator infrastructure if a suitable entity (that is unlikely to collude with potential adversaries against the ledger integrity) cannot be practically identified. But the implication of such an arrangement on potential breaches of privacy regulations would need careful evaluation.

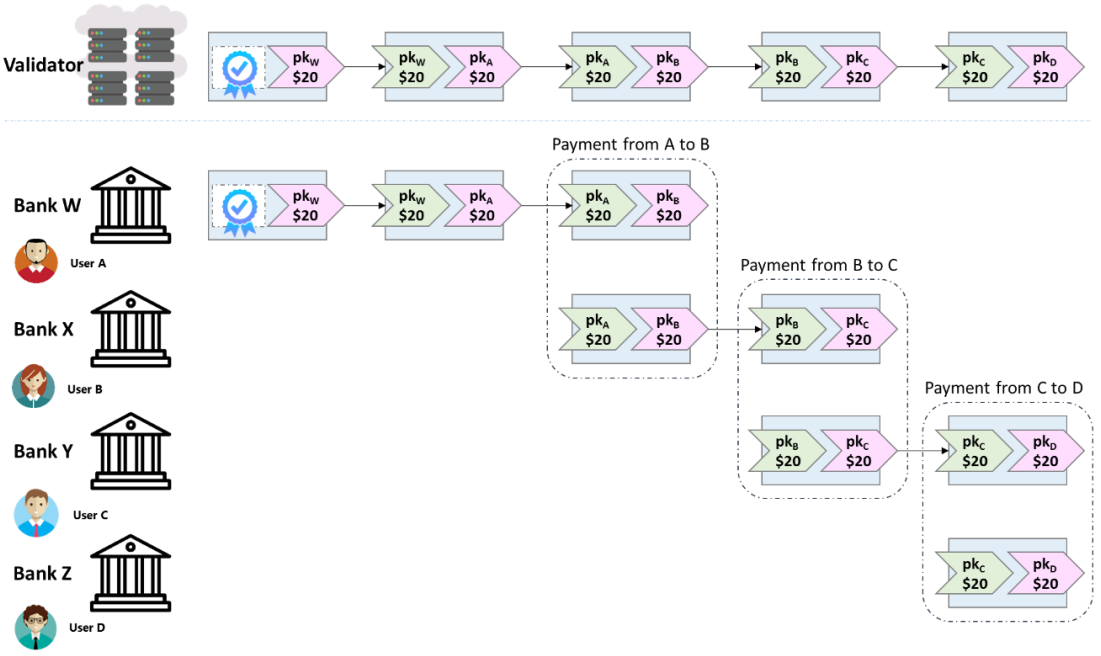
For the case of a single party implementing the validator infrastructure, the processing power can be scaled up through database sharding. Database sharding (Corbett et al., 2012) is a well-established technique that partitions table entries across multiple database servers in order to parallelise operations through splitting them across multiple servers. In this way, the workload of the validator infrastructure can be split across multiple database servers by simply assigning each database with the responsibility to handle a range of coinbase transaction IDs. Operations can hence be scaled up to handle tens of thousands of transactions by adding hardware proportionately. In contrast, it would be more complex to scale up the processing capability of DLT as the communication overheads in running the consensus protocols are usually the bottleneck.

If a highly trustworthy party can be identified for hosting the validator infrastructure, it is possible to optimise the transaction validation process and alleviate the privacy issues associated with UTXO transactions. To a large extent, a UTXO is designed to facilitate peer verification of a payment transaction. UTXO transactions are therefore designed in such a way that the payee of the current transaction would see the payment details of other payees in the previous transactions of an inheritance chain in order to verify his transaction.[15] Similarly, a bank may need to access transaction data of customers of other banks while processing a transaction for its customer. If the validator infrastructure can be entrusted with the verification of the inheritance chain of a payment transaction, a payee or his bank would not have to access the payment details of previous transactions, therefore avoiding the privacy issues of typical UTXO transaction processing. In this way, a bank would only need to keep a portion of the inheritance chain for each transaction it processes, that is, the payment transactions it receives and sends. Shortened transaction chains would also mean a lower storage complexity and transaction latency in relation to the download of the transaction chains. A slight increase in computing overhead on the part of the validator infrastructure is possible with crafted optimisation. The key trade-off is that a higher level of trust and availability of the validator infrastructure is required. The impact of a malicious validator infrastructure on the supply of money should be similar although the attacks could differ in nature. In the event of insolvency of an intermediary, if the validator infrastructure is also unavailable, all the intermediaries would need to work collectively to reconstruct the inheritance chains in order to provide the central bank information to honour claims from users.

[14] In typical industrial configurations, a centralised database also implements redundancy at different levels, for example, RAID at the hardware level and database replication at the system level, with resilience comparable to typical DLT settings. On the other hand, DLT usually works in a non-uniform environment, and maintaining network connectivity in such an environment is more challenging with implications on the overall resilience.

[15] In order to fully verify the authenticity of the CBDC underlying a payment transaction, a payee has to verify the chain of all previous payment transactions that link up the coinbase or issuance transaction to the current transaction.

(a)



(b)

Figure 15. The two cases how the transaction chain of a coinbase is stored
In case (a), besides the validator, banks of users also store the complete transaction chain, therefore able to see previous transactions in the chain initiated by users who are not their customers. In case (b), the complete transaction chain is kept at the validator only, with banks of users only keeping portion(s) of the transaction chain corresponding to transactions of their own customers only.

5.5.4 Two-tier architectures based on different validator infrastructures

Depending on the party/parties hosting the validator infrastructure, different two-tier architectures can be achieved. The design of the validator infrastructure, in particular, with the centralised database approach, is simple, and access can be merely implemented with conventional application programming interfaces (APIs). This implies that it is very flexible to implement the validator infrastructure with different hosting configurations, which, as a result, could lead to the instantiation of different two-tier architectures, including the hybrid and intermediated models, as well as CBDC-backed e-money (Table 4). CBDC-backed e-money would have greater flexibility in adopting different configurations for the validator infrastructure. It should be noted that different configurations of the validator infrastructure have implications on its capability to prevent different types of frauds and robustness against different adversarial coalitions.

Two-tier Architecture	Host of validator infrastructure		Prevention					Tolerable Collusion Size
	Verification of issuer's transactions	Verification of users' transactions	Over-issuance by intermediary	Repeated redemption by intermediary	Double-spending by intermediary	Double-spending by user	Double-spending by collusion of bank and user	
Hybrid	Central Bank		✓	✓	✓	✓	✓	-
Intermediated	Joint Venture (e.g. interbank clearing house)		✓	✓	✓	✓	✓	N
CBDC-backed e-money	Joint Venture + Issuer		✓	✓	✓	✓	✓	N
	Joint Venture	Issuer	✓	✓	✓	✓		N
	Issuer + Another Intermediary		✓	✓	✓	✓	✓	2
	Another Intermediary	Issuer	✓	✓	✓	✓		2

Table 4. Comparison of different hosting configurations of the validator infrastructure and their fraud prevention capability

5.6 Pseudonym system with evolving public keys

Payment transactions contain no PII of users. Users transact with their public keys only, and the mapping between public keys and the real identities of users is kept and known to the users' banks only. In order to address the privacy issues of typical UTXO designs and preserve user anonymity from the validator infrastructure and others, transactions are designed to work on users' public keys only and contain no information that can uniquely identify any user. An observer who is able to access all transactions, say, at the UTXO database of the validator infrastructure, would only see payments made between public keys. This is similar to the use of pseudonyms or confidential identities (Monetary Authority of Singapore, 2017). However, if static public keys are used, the payment pattern of users is preserved. When the real identity of the owner of a public key is discovered, say, through external data sources, his privacy would be totally breached with all his transactions revealed. This is a realistic threat because when a user makes a payment, say, to pay tax, he usually needs to submit the transaction reference with his real identity, and the mapping is therefore known to the payee and can possibly be used to look up other transactions of this user if access to the validator infrastructure is also possible.

5.6.1 Improved privacy with dynamic public keys

Better privacy protection could be achieved by evolving the public key that a user uses for receiving and making payments. In order to anonymise the ownership of CBDC or e-money as represented by a UTXO owned by a publicly recognised public key, the owner of the public key can spend the UTXO and pay it sequentially to a number of randomly selected public keys. If other

users also use different, anonymised public keys, it is practically difficult to distinguish between the two cases: (1) the owner paying to himself, and (2) the owner paying to another user. Subsequent payments made by the anonymised public key therefore cannot be linked to the owner. Since the owner needs to go through his bank to initiate these anonymised payments, his bank would know the real identity of the owner of these public keys. A bank can therefore keep the mapping between the real identities and public keys to keep track of the holdings of its customers. If necessary and with proper authorisation, the bank can also reveal all the public keys of a given identity for investigation.

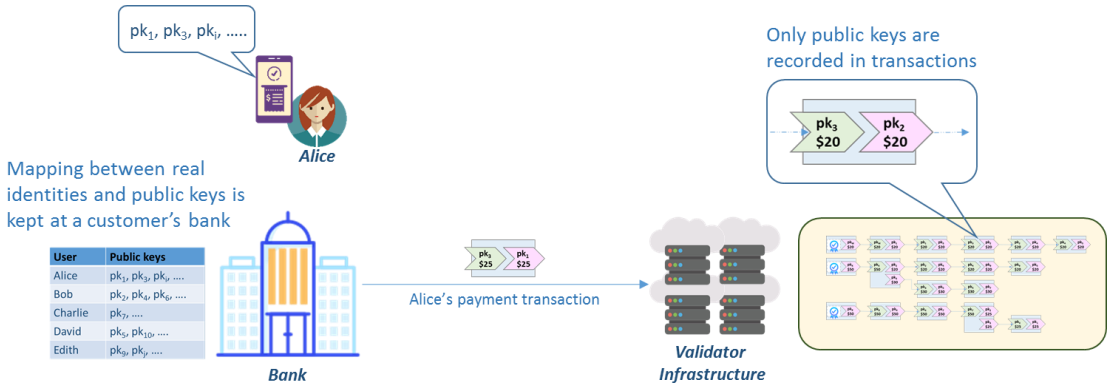


Figure 16. Pseudonym system for transactions with mapping between real identities and pseudonyms (or public keys) kept at intermediaries only

To anonymise the receipt of payment, a payee can randomly select a new public-private key pair and ask the payer to pay to this public key. If each public key is used once only and a new public key is used for each payment, the anonymity of a user is reasonably protected. In order to instruct his bank to process payments on his behalf, the payee would have to register this new public key with his bank. Banks therefore would be aware of all public keys that each of its customers owns, and could fulfil the KYC/AML rules. For usual payments, after a payer obtains the public key of a payee with the first payment, subsequent payments to the same payee do not require any setup and can be made without the involvement of the payee. However, to anonymise the receipt of payment, a payee needs to inform the payer of his new public key and register it with his bank each time he receives a payment even though the payer has made prior payments to him. A registration phase is required for each payment.

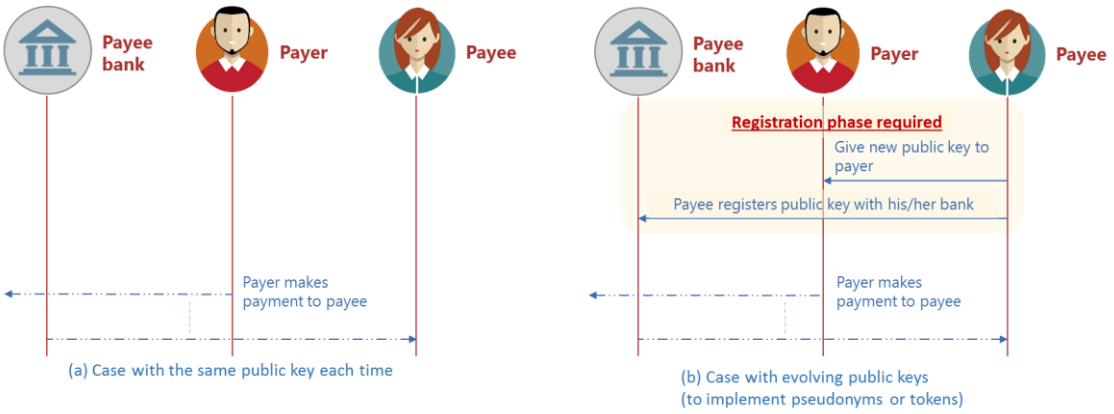
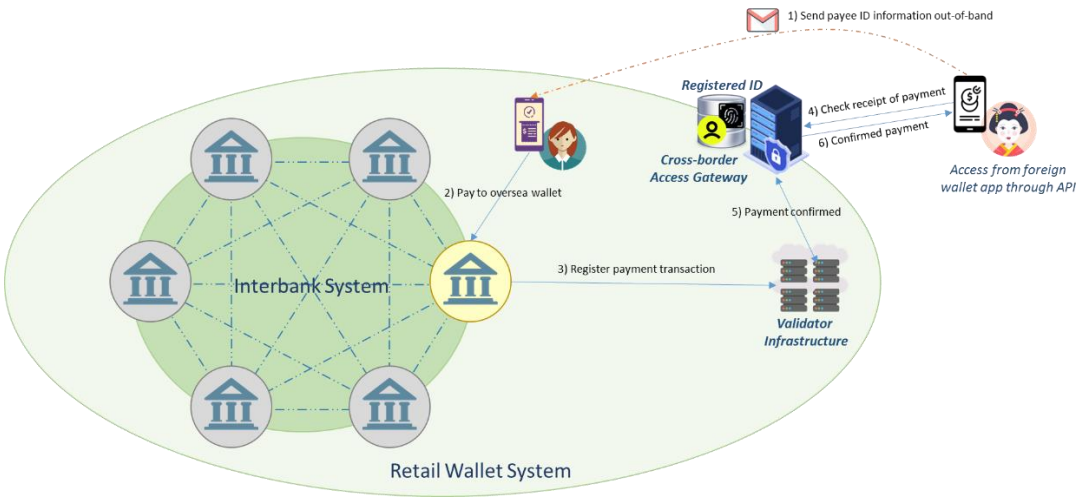


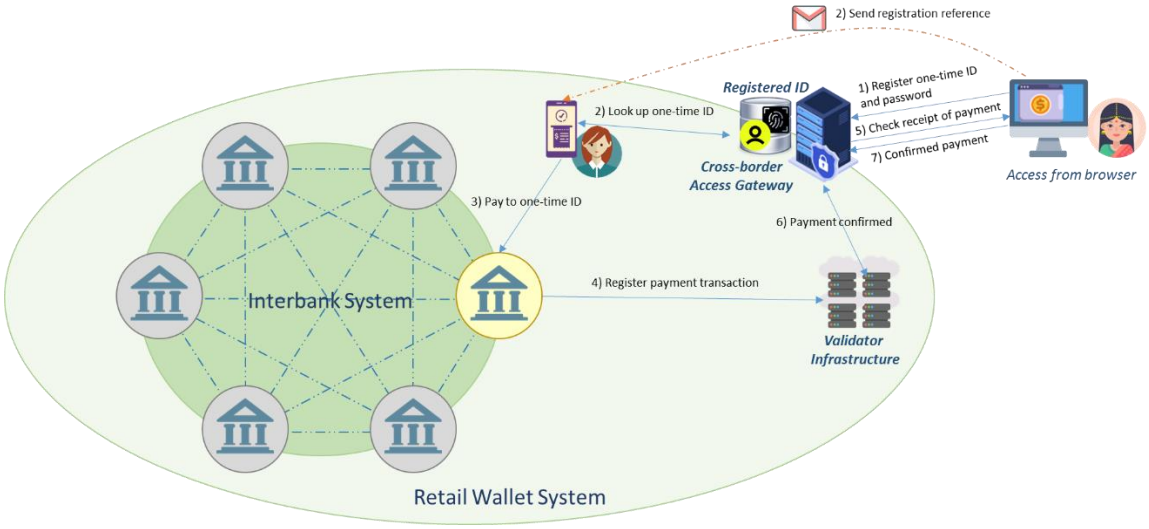
Figure 17. Normal payment process versus payment process with pseudonym system requiring public key registration

5.7 Support for cross-border interoperability

To support cross-border uses, a proxy server is required to connect overseas users to the validator infrastructure for cybersecurity reasons. The validator infrastructure, as a store of retail transactions, provides a single source of truth in the retail system. For cybersecurity and resilience considerations, in the current design, user wallets cannot access the validator infrastructure directly and have to initiate transactions through their banks or PSPs. On one hand, because of the use of UTXO-based transactions, payments could be made to any public key (even unseen before) with little setup required. Cross-system interoperability and support for foreign users to receive payments and hold CBDC or e-money are relatively simple. A foreign user only needs to have his public key set up and share it with the payer in order to receive payments. Purely from the technological perspective, pre-registration of the public key with the validator infrastructure is not required. Yet, pre-registration is desirable for compliance with KYC/AML regulations. In order to make payments from CBDC or e-money received, an overseas user needs an application that can form and sign a payment transaction with a prescribed UTXO format. On the other hand, for sake of cybersecurity and resilience, a designated gateway server to connect foreign users to the validator infrastructure is preferred. This gateway would play a role similar to a bank or PSPs for local users. With the implementation of a UTXO token, it is possible for a foreign user to receive and make payments through a web browser and password.



(a) Architecture for supporting overseas users with a mobile app



(b) Architecture for supporting overseas users without a mobile app

Figure 18. Extensions of the architecture with a server gateway to support overseas users

6. Preliminary analysis

Chapter 6 looks at how the proposed architecture discussed in Chapter 5 fares with reference to the key design questions raised in Chapter 3, as well as the three key principles, i.e. safety, efficiency, and openness raised in Chapter 4.

6.1 Over-issuance prevention

The validator infrastructure, which could be instantiated by a centralised database or DLT, could help to prevent over-issuance and double spending in the retail system. However, there will be trade-offs in terms of performance and availability. A highly available online service and database server is required to implement the validator infrastructure in the retail system. As rightly noted by Chaum et al. (2021), only online checks can effectively prevent double-spending to fully eliminate the risk. The same observation would apply to over-withdrawal of CBDC or over-issuance of e-money as these processes could be seen as double spending of the wholesale transaction. But online checks imply that transactions will be impossible if network connectivity to the validator infrastructure is unavailable, especially if it is implemented with a centralised database. While a DLT-based validator infrastructure has the benefit of better resilience, it is inevitably accompanied with a loss in performance. More rigorous experimentation would be needed to compare its performance with database replication or distributed database (e.g. Cassandra). Besides, a highly available DLT arrangement has to trade off data consistency between different copies of the ledger in the presence of network partitioning (Brewer, 2012; Gilbert & Lynch, 2012). As future work, novel techniques to reduce the reliance on the validator infrastructure without sacrificing performance need to be researched.

The UTXO transactions kept at the validator infrastructure can readily form inheritance chains, which can be used as an audit trail. Each transaction requires the signatures of a number of parties to authorise it, and the validator infrastructure forms a store of all signed transactions. If some fraud such as an over-issuance, which cannot be promptly caught and prevented by the

validator infrastructure, occurs, the signed transactions kept in the validator infrastructure's UTXO database could readily form inheritance chains to provide an audit trial. This could possibly be seen as a form of defence-in-depth against over-issuance.

6.2 Asset and transaction traceability

Explicit references to previous transactions in a UTXO transaction allows easy traceability of transactions and assets, in turn supporting correct redemption when there are multiple e-money issuers. The UTXO design requires each payment transaction to specify the source(s) of the CBDC/e-money used to make the payment concerned by explicitly referencing the previous payment transactions. An inheritance chain of transactions can therefore be formed readily to link up the current ownerships of CBDC or e-money with the coinbase transactions from which the CBDC/e-money inherits its monetary value. The identified coinbase transaction would directly refer to the wholesale transactions which can trace back to the original issuance of CBDC by the central bank. This helps distinguish e-money issued by different intermediaries while allowing e-money to constitute a single balance in a user's wallet. If necessary, an inheritance chain can be used as a proof of ownership of the backing assets held in the wholesale system. However, access to an inheritance chain by a user would have privacy implications. Although the proposed pseudonym system could preserve user anonymity to a large extent even if an inheritance chain is made public, more study is necessary to enumerate different ways to store and reconstruct inheritance chains of UTXO transactions. Specifically, if explicit references of coinbase transaction are included in each payment transaction, traceability could possibly be achieved without forming an inheritance chain. The trade-off of different metrics would require more in-depth experimentation and investigation.

6.3 Flexibility

The proposed architecture can flexibly instantiate different two-tier distribution models, based on different configurations of the validator infrastructure, and support both CBDC and CBDC-backed e-money through suitable coinbase definitions. The current architecture is designed with modularity and flexibility in mind, with system and user functions cleanly delineated. On one hand, different configurations of the validator infrastructure can result in different two-tier distribution models. For example, if the validator infrastructure is hosted by the central bank, the hybrid model can be instantiated. Likewise, if the validator infrastructure is hosted by a designated joint venture of all the intermediaries, the intermediated CBDC model can be instantiated. In the case of CBDC-backed e-money, the validator infrastructure could possibly be hosted by another intermediary other than the issuer. On the other hand, through different definitions of a coinbase transaction and the legal arrangement of the underlying assets held in the wholesale system, the same infrastructure could be used to support both CBDC and CBDC-backed e-money. The properties above would greatly maximise the usability of an infrastructure constructed based on this proposed design, especially when the outcome of the debate on CBDC remains uncertain.

Since cross-ledger communications are minimised in the proposed architecture, the designs of the wholesale and retail systems could be made independent. Currently, the wholesale, interbank system is based on DLT. In case a centralised database similar to the RTGS is preferred in accordance with the local context, this change in preference would have minimum impact on the design of the retail system. Integration of the two systems would only require the same transaction

format and digital signature scheme for cross-ledger messages or transactions, and most translations could be done at the systems of the intermediaries. Cross-ledger synchronisation is largely achieved through signed transactions relayed by intermediaries.

6.4 Safety

Cross-ledger synchronisation merely based on signed transactions exchanged via intermediaries enhances separation of the wholesale and retail ledgers, potentially leading to better cyber resilience. CBDC issuance is restricted to the wholesale system only. The cross-ledger synchronisation design ensures sufficient decoupling between the wholesale and retail ledgers to implement the principle of privilege separation and network segmentation (Provos et al., 2003; Australian Cyber Security Centre, 2019). The intermediaries (banks and PSPs) would play the role of security gateways for the wholesale system against potential attacks from the retail system. Besides, the transaction flows have been designed to minimise interactions between retail payment activities and wholesale functions so as to minimise the attack surface. This would greatly reduce the probability of compromise of the central bank's private key, which is used to issue CBDC in the wholesale system. Security of the central bank's private key can be further strengthened through the installation of a data diode. But this would require a manual process of CBDC redemption in the wholesale system. While the central bank may possibly run the validator infrastructure (e.g. in the hybrid model), the processes of CBDC issuance and the validator could be placed on separate machines, with the former in the protected wholesale system and the latter in the more open retail system.

Only the owner can spend his CBDC or e-money to ensure payment safety, but this also brings up user-friendliness issues related to losing private keys. The principle of segregation of duty is embedded in the proposed architecture. While the validator infrastructure verifies and confirms each transaction in the retail system, without the private key of a user, it is still unable to spend any CBDC/e-money belonging to the user. That is, a successful payment requires the involvement of the CBDC/e-money owner, his bank, and the validator infrastructure. However, this brings up a potential user-friendliness issue in the sense that if a user loses his private key, he cannot spend his CBDC/e-money for good. As a backup, a user may use a password-based encryption scheme to encrypt his private key and store the encrypted copy at his bank or PSP. But this does not fully eliminate the risk of losing a private key since the user may still forget the password used for encryption.

The proposed architecture preserves user anonymity from the validator infrastructure and other users through a pseudonym system, which only uses public keys in transactions and evolves public keys for new transactions, while making the mapping between real identities and public keys known to the respective intermediaries only. All transactions are designed to use public keys only and refrain from using personally identifiable information, which could be seen as an embodiment of privacy by design. However, this does not guarantee adequate privacy in practice since the public keys used are static, and there is reasonable probability to infer the real identities of users when combined with external data sources. Dynamic public keys are necessary to make inference of user identities difficult. In the proposed architecture, a new public-private key pair is randomly selected each time a new payment is received. The privacy of payees is preserved because, when given two payment transactions paid to different public keys, practically, nobody would be able to tell whether the two payments belong to the same payee. In other words, if an adversary knows the real identity of the payee of a payment transaction, if given another payment

transaction paid to a different public key of the same payee, he would not be able to tell for sure whether this payment transaction also belongs to the payee. In terms of anonymising existing holdings of CBDC/e-money, the process of generating a sequence of payment transactions paid to newly generated public keys is of the same nature as Bitcoin mixing (Bonneau et al., 2014). Nobody can tell for sure whether one of the payment transactions is paid to the original owner or to another user.

Additional research is necessary to refine the design of the pseudonym system to introduce dynamic, evolving public keys. The drawback of this pseudonym system with evolving public keys is the need on the part of a user to handle a large number of private keys. Yet, it is possible to generate multiple public keys from a single private key, through private key derivation from a root key with inputs from the data fields of transactions (Chan, 2013), or a pseudonymous signature scheme generating incomparable public keys from the same private key (Waters et al., 2003; Kutylowski et al., 2016). Additional functionalities, such as traceability, are included in more advanced pseudonymous signature schemes, including the one used in eIDAS tokens (BSI TR-03110 eIDAS Token Specification). Besides, the protection of the pseudonym system against different attacks and statistical analysis methods needs to be evaluated.

Maintaining availability of the validator infrastructure is crucial for the availability of service of the retail system. Each transaction in the retail system has to be verified and endorsed by the validator infrastructure before the payee can accept it. In order to minimise the possibility of a successful denial-of-service attack against the validator infrastructure, user devices cannot connect to the validator infrastructure directly, instead they have to go through an intermediary. Since intermediaries are considered more trustworthy, the attack surface is reduced. Replication or additional redundancy commonly used in conventional databases, not necessarily DLT, could be adopted to increase the availability of the validator infrastructure. Evaluation of its effectiveness has to be based on experimentation and proper scientific measurements.

6.5 Efficiency

The proposed architecture is expected to be energy-efficient and scalable even in the event of an increasing number of users and transaction volume. The system-wide bottleneck is at the validator infrastructure, with the conventional, centralised database technology being the preferred implementation. The key processing load of a transaction is largely on verifying the digital signatures of the inheritance chain of transactions, most parts of which only need to be performed once given the verification is done by a single server. The verification process of the validator infrastructure could be very energy-efficient and fast, compared with the proof-of-work consensus of Bitcoin. With increasing number of users and transaction volume, a proportionate increase of hardware resources with conventional database sharding should suffice to scale up the processing capacity of the validator infrastructure.

Typically, a user needs to have a mobile wallet app in order to access the retail system and user friendliness should be moderate. In order to hold CBDC or e-money and make payment transactions, a dedicated mobile app is required. Most of the tasks needed to initiate a transaction, such as the formation of a UTXO transaction, would be carried out by the intermediary's server to minimise the number of steps required of the user before a transaction can be made. However, the proposed architecture does not have support for users with limited access to hardware or network connectivity. Since most of the processing of a transaction is in the backend server, it is possible to design a web-browser version to allow a foreign user to receive and make payments with a single

password if a UTXO-token is used. However, the user-friendliness of setting up a one-time password for receiving and making a payment is unclear.

6.6 Openness to innovation

Structures are included in the proposed architecture to accommodate service extensibility and interoperability. An option field is included in the transaction structure to support future extensions of services and functionalities. This approach is similar to the TCP option field which, as past experiences have shown, is reasonably flexible for testing out new services and features in TCP/IP (RFC791, RFC793). As an example, the option field can be used to specify the conditions for spending a particular UTXO of a transaction to implement programmable money or payments. However, it should be noted that programmable money is generally seen as a voucher, rather than currency. Besides, the current architecture has made provision to support overseas users or wallets through a dedicated server gateway as a bridge to route the requests of these users to the validator infrastructure while maintaining the protection for the validator infrastructure. This demonstrates one possible way to support interoperability with CBDC systems of other jurisdictions. Since connectivity to the validator infrastructure is largely based on conventional APIs, building a software connector to support a foreign or overseas user to receive and make payments from his mobile app — which could possibly be developed by a third party vendor — should be straightforward once the common interface can be agreed on.

From a protocol stack perspective, similarities could be drawn between the proposed architecture and the TCP/IP protocol stack. The design of UTXO transactions could be seen as a thin protocol layer, alike the Internet Protocol (IP) layer in the TCP/IP protocol stack, that can be built on different configurations or technologies of the validator infrastructure below it and flexibly support different application services above it. It is reasonably envisioned that this thin, standardised layer of the CBDC protocol stack could serve as the basis for fostering payment innovation. Similar to the TCP/IP protocol suite which supports the connectionless UDP (RFC768) and the connection-oriented TCP (RFC793) in the transport layer built on the IP layer, the proposed architecture builds on the UTXO transaction format to support both accounts and tokens. Besides, a UTXO-based account is similar to UDP in that it does not require the payee's pre-registration of his public key with the payer (that is, connectionless). Whereas, a UTXO-based token is similar to TCP in that it is connection-oriented and requires the payee to pre-register his new public key with the payer each time a payment is made. On top of the UTXO transaction format, a host could implement an account balance or token view for its wallet or database. For instance, in the proposed architecture, a user wallet only implements an account balance view, the validator infrastructure only implements a token view (in the form of the UTXO database), and an intermediary implements both.

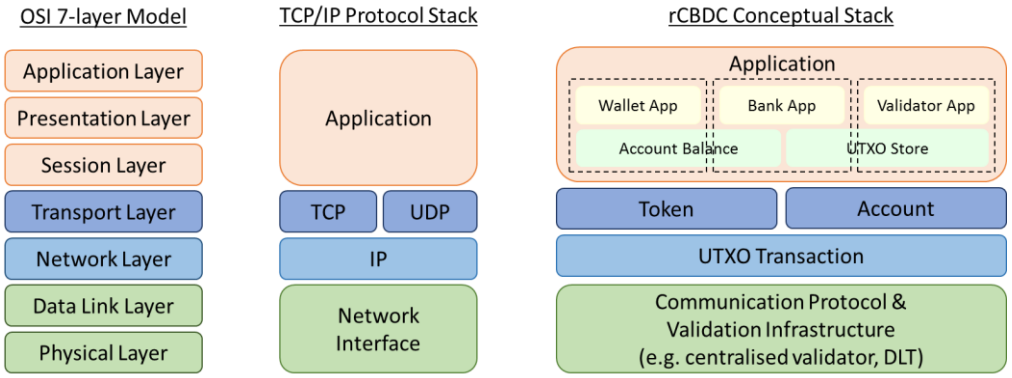


Figure 19. UTXO transaction structure and the related token/account implementation as the key anchor layer for applications built on it and the underlying infrastructure arrangement

7. Future work

This whitepaper studies two-tier distribution models for rCBDC and illustrates how the proposed technology architecture can respond to the three design questions raised in Chapter 3: (1) cross-ledger synchronisation and over-issuance prevention can be achieved by the presence of separate, decoupled wholesale and retail ledgers; (2) transaction and asset traceability to enable correct accounting and redemption of CBDC-backed e-money with multiple issuers, and to support the central bank to honour claims when intermediaries become insolvent; and (3) a flexible design to support different two-tier architectures of rCBDC and CBDC-backed e-money with minimum design change required. In addition, the paradigm of privacy by design is applied in the proposed architecture. A pseudonym system with evolving public keys is designed to ensure better privacy protection.

Some components of the proposed architecture have different design options, involving different trade-offs. To gain a better understanding of these trade-offs, a more thorough investigation through experimentation is necessary. To enhance the flexibility of the proposed architecture to suit different application contexts, different options are available for a few components of the design. For example, these include different configurations of the validator infrastructure, and whether to allow users to have access to the whole inheritance chain of previous transactions. These options involve a trade-off between security, privacy, and performance. The evaluation of these different options and fine tuning of the design would require rigorous experimentation and measurements.

New findings of technology research, especially in cryptography and distributed systems, could possibly inform CBDC research. In particular, new insights, techniques, and tools may be offered by the academia and industry to help achieve a better trade-off and refine the proposed architecture in this whitepaper. While the proposed architecture has reasonably addressed some of the main issues of rCBDC to a large extent, it is believed that better designs or techniques could always be possible, as informed by the latest advances in academic and industry research. Based on an initial, preliminary analysis of the proposed architecture, the HKMA has identified a number of areas for further discussion, which are summarised as seven problem statements (Table 1). The academia and industry are invited to comment on the proposed architecture by making reference to the seven problem statements. It is believed that input to these

problem statements have a great potential to lead to optimised designs of CBDC. New ideas and project proposals are also solicited.

Security modelling and analysis for the proposed design, as well as ideas for novel use cases and capabilities that can be uniquely enabled by rCBDC are especially solicited. In view of the adversarial conditions that an rCBDC infrastructure is anticipated to operate in and the importance of maintaining its resilience and robustness as a critical infrastructure, a deeper understanding of the attack surface and potential malicious actions against an rCBDC infrastructure is essential. Equally important is a rigorous security analysis of the design based on a well-defined threat model. Security analysis of the proposed design based on widely accepted frameworks (e.g. STRIDE, PASTA, attack tree, etc.) is sought. In addition, while benefits of rCBDC have been identified in the literature, not many are unique that cannot be delivered through other means which are more efficient and introduce fewer risks. New ideas of use cases and capability that can only be delivered by rCBDC are therefore sought.

Feedback on the proposed architecture and improvement proposals on rCBDC and CBDC-backed e-money in general are solicited from the academia and industry. In view of the deep and broad expertise of the academia and industry, this whitepaper is published as a Request For Comments (RFC) document — following the practice of the Internet community in the conception of the Internet — to invite academics, technologists, and the wider industry community to provide feedback on the initial architectural design of rCBDC presented in this whitepaper. Besides, suggestions and ideas of better designs are also solicited. Submissions are to be sent to fintech@hkma.gov.hk .

8. Acknowledgement

The HKMA thanks Prof. K. P. Chow (University of Hong Kong), Prof. Sherman Chow (Chinese University of Hong Kong), Dr. C. D. Shum (Logistics and Supply Chain MultiTech R&D Centre) and Prof. S. M. Yiu (University of Hong Kong) for comments and suggestions.

9. Bibliography

Adrian, T. & Mancini-Griffoli, T. (2019), 'The rise of digital money', IMF Fintech Note 19/01.

Agur, I., Ari, A. & Dell'Ariccia, G. (2019), 'Designing central bank digital currencies', IMF Working Paper 19/252.

Allen, S., Čapkun, S., Eyal, I., Fanti, G., Ford, B. A., Grimmelmann, J., Juels, A., Kostiainen, K., Meiklejohn, S., Miller, A., Prasad, E., Wust, K. & Zhang, F. (2020), 'Design choices for central bank digital currency: Policy and technical considerations', National Bureau of Economic Research (NBER)Working Paper, No. 27634.

Auer, R. & Böhme, R. (2020), 'Technology of retail central bank digital currency', BIS Quarterly Review pp. 85–96.

Auer, R. & Böhme, R. (2021), 'Central bank digital currency: the quest for minimally invasive technology', BIS Working Papers, No. 984.

Auer, R., Cornelli, G. & Frost, J. (2020), 'Taking stock: Ongoing retail CBDC projects', BIS Quarterly Review pp. 97–98.

Australian Cyber Security Centre (2019), 'Implementing network segmentation and segregation', Australian Signals Directorate, Australian Government.

Bank for International Settlements (2021), 'CBDCs: an opportunity for the monetary system', BIS Annual Economic Report pp. 65–95.

Bank of Canada (2020), 'Contingency planning for a central bank digital currency'.
URL: https://www.bankofcanada.ca/2020/02/contingency-planning-centralbank-digital-currency/

Bank of England (2020), 'Central bank digital currency: Opportunities, challenges and design', Discussion Paper.

Bank of England (2021), Bank of England omnibus accounts - access policy.

Bech, M. & Garratt, R. (2017), 'Central bank cryptocurrencies', BIS Quarterly Review pp. 55–70.

Berentsen, A. & Schar, F. (2018), 'The case for central bank electronic money and non-case for central bank cryptocurrencies', Federal Reserve Bank of St. Louis Review 100(2), 97–98.

Bindseil, U. (2020), 'Tiered CBDC and the financial system', ECB Working Paper, No. 2351.

BIS Innovation Hub (2020), 'Project Helvetia: Settling tokenised assets in central bank money'.

Blaskiewicz, P., Hanzlik, L., Kluczniak, K., Krzywiecki, L., Kutylowski, M., Slowik, M. & Wszola, M. (2019), 'Pseudonymous signature schemes', in K. Li, X. Chen & W. Susilo (eds) Advances in Cyber Security: Principles, Techniques, and Applications, Springer, pp. 185–255.

Boar, C., Holden, H. & Wadsworth, A. (2020), 'Impending arrival - a sequel to the survey on central bank digital currency', BIS Papers, No. 107.

Bonneau, J., Narayanan, A., Miller, A., Clark, J., Kroll, J. A. & Felten, E. W. (2014), 'Mixcoin: Anonymity for Bitcoin with accountable mixes', in N. Christin & R. Safavi-Naini (eds) Financial Cryptography and Data Security - 18th International Conference, FC 2014, Vol. 8437 of Lecture Notes in Computer Science, Springer, pp. 486–504.

Bordo, M. D. & Levin, A. T. (2017), 'Central bank digital currency and the future of monetary policy', National Bureau of Economic Research (NBER) Working Paper, No. 23711.

Brainard, L. (2021), 'Private money and central bank money as payments go digital: an update on CBDCs', Speech at the Consensus by CoinDesk 2021 Conference, Washington, D.C., 24 May, 2021.

Brewer, E. A. (2012), 'Pushing the CAP: strategies for consistency and availability', IEEE Computer 45(2), 23–29.

Brunnermeier, M., James, H. & Landau, J.-P. (2021), 'The digitalisation of money', BIS Working Papers, No. 941.

Brunnermeier, M. & Niepelt, D. (2019), 'On the equivalence of private and public money', Journal of Monetary Economics 106, 27–41.

Bullmann, D., Klemm, J. & Pinna, A. (2019), 'In search for stability in crypto-assets: are stablecoins the solution?', European Central Bank Occasional Paper Series, No. 230.

Camenisch, J., Hohenberger, S. & Lysyanskaya, A. (2005), 'Compact e-cash', in Advances in Cryptology: Proceedings of EUROCRYPT 2005, Springer-Verlag Lecture Notes in Computer Science 3494, pp. 302–321.

Camenisch, J., Lysyanskaya, A. & Meyerovich, M. (2007), 'Endorsed e-cash', in Proceedings of IEEE Symposium on Security and Privacy (SP'07), pp. 101–115.

Chan, A. C.-F. (2013), 'On optimal cryptographic key derivation', Theoretical Computer Science 489-490, 21–36.

Chan, A. C.-F. (2021), 'UTXO in digital currency: Token-based or account-based? Or both?', arXiv preprint arXiv:2109.09294.
URL: *https://arxiv.org/abs/2109.09294*

Chan, C. F., Shum, C. D. & Makhlouf, A. B. (2017), 'System and method for controlling a ledger of transactions'. US Patent App 20200082361A1.
URL: *https://patents.google.com/patent/US20200082361A1*

Chaum, D. (1983), 'Blind signatures for untraceable payments', in Advances in Cryptology: Proceedings of CRYPTO'82, pp. 199–203.

Chaum, D., Fiat, A. & Naor, M. (1988), 'Untraceable electronic cash', in Advances in Cryptology: Proceedings of CRYPTO'88, pp. 319–327.

Chaum, D., Grothoff, C. & Moser, T. (2021), 'How to issue a central bank digital currency', SNB Working Papers 3/2021.

Committee on Payments and Market Infrastructures (2015), Digital currencies.

Committee on Payments and Market Infrastructures and Markets Committee (2018), Central bank digital currencies.

Common Criteria (2017), Common methodology for information technology security evaluation, rev. 5 (ISO/IEC 18045).

Corbett, J. C., Dean, J., Epstein, M., Fikes, A., Frost, C., Furman, J., Ghemawat, S., Gubarev, A., Heiser, C., Hochschild, P., Hsieh, W., Kanthak, S., Kogan, E., Li, H., Lloyd, A., Melnik, S., Mwaura, D., Nagle, D., Quinlan, S., Rao, R., Rolig, L., Saito, Y., Szymaniak, M., Taylor, C., Wang, R. & Woodford, D. (2012), 'Spanner: Google's globally-distributed database' in Proceedings of 10th USENIX Symposium on Operating Systems Design and Implementation (OSDI 12), pp. 261–264.

Duffie, D. (2019), 'Digital currencies and fast payment systems: Disruption is coming', Asian Monetary Policy Forum.

European Central Bank (2019), 'Exploring anonymity in central bank digital currencies', Focus, Issue, No. 4.

European Central Bank (2021), Eurosystem report on the public consultation on a digital euro.

Garratt, R., Lee, M., Malone, B. & Martin, A. (2020), 'Token- or account-based? A digital currency can be both', Liberty Street Economics, Federal Reserve Bank of New York, August 12, 2020.

German Federal Office of Information Security (2016), Technical guideline BSI TR-03110: eIDAS token specification.

Gilbert, S. & Lynch, N. A. (2012), 'Perspectives on the CAP theorem', IEEE Computer 45(2), 30–36.

Green, E. J. (2007), 'Some challenges for research in payments', in S. Millard, A. Haldane & V. Saporta (eds) The Future of Payment Systems, Routledge, Oxford, pp. 75–85.

Group of Thirty (2020), Digital currencies and stablecoins: Risks, opportunities, and challenges ahead — A report published by Group of Thirty, Washington, D.C.

IETF (1980), 'User Datagram Protocol', RFC 768.
URL: *https://rfc-editor.org/rfc/rfc768.txt*

IETF (1981a), 'Internet Protocol', RFC 791.
URL: *https://rfc-editor.org/rfc/rfc791.txt*

IETF (1981b), 'Transmission Control Protocol', RFC 793.
URL: *https://rfc-editor.org/rfc/rfc793.txt*

Kahn, C. M., McAndrews, J. & Roberds, W. (2005), 'Money is privacy', International Economic Review 46(2), 377–399.

Kahn, C. M. (2016), 'How are payment accounts special?', Talk at the Payments Innovation Symposium, Federal Reserve Bank of Chicago, October, 2016.

Kahn, C. M., Rivadeneyra, F. & Wong, T.-N. (2020), 'Should the central bank issue e-money?', Journal of Financial Market Infrastructures 8(4).

Kahn, C. M. & Roberds, W. (2009), 'Why pay? An introduction to payments economics', Journal of Financial Intermediation (18), 1–23.

Kumhof, M. & Noone, C. (2018), 'Central bank digital currencies — design principles and balance sheet implications', Bank of England, Staff Working Paper, No. 725.

Kutylowski, M., Hanzlik, L. & Kluczniak, K. (2016), 'Pseudonymous signature on eIDAS token - implementation based privacy threats' in J. K. Liu & R. Steinfeld (eds) Information Security and Privacy - 21st Australasian Conference, ACISP 2016, Vol. 9723 of Lecture Notes in Computer Science, Springer, pp. 467–477.

Libra Association (2020), Libra white paper v2.0.
URL: *https://libra.org/en-US/white-paper/*

Mancini-Griffoli, T., Peria, M. S. M., Agur, I., Ari, A., Kiff, J., Popescu, A. & Rochon, C. (2018), 'Casting light on central bank digital currency', IMF Staff Discussion Notes 18/08.

Mavroudis, V., Wüst, K., Dhar, A., Kostiainen, K. & Čapkun, S. (2020), 'Snappy: Fast on-chain payments with practical collaterals', in Proceedings of the 27th Annual Network and Distributed System Security Symposium (NDSS 2020).

Merkle, R. C. (1987), 'A digital signature based on a conventional encryption function' in C. Pomerance (ed.) Advances in Cryptology - CRYPTO '87, August 16-20, 1987, Proceedings, Vol. 293 of Lecture Notes in Computer Science, Springer, pp. 369–378.

Milne, A. (2018), 'Argument by false analogy: The mistaken classification of bitcoin as token money', Available at SSRN: *https://ssrn.com/abstract=3290325*.

Monetary Authority of Singapore (2017), Re-imagining interbank real-time gross settlement system using distributed ledger technologies — Project Ubin, Phase 2.

Nakamoto, S. (2008), 'Bitcoin: A peer-to-peer electronic cash system'.
URL: *https://www.bitcoin.com/bitcoin.pdf*

Narayanan, A., Bonneau, J., Felten, E., Miller, A. & Goldfeder, S. (2016), Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction, Princeton University Press, New Jersey.

Ng, L. K. L., Chow, S. S. M., Wong, D. P. H. & Woo, A. P. Y. (2021), 'LDSP: Shopping with cryptocurrency privately and quickly under leadership', in Proceedings of the 41st IEEE International Conference on Distributed Computing Systems (ICDCS 2021).

Okhravi, H. & Sheldon, F. T. (2010), 'Data diodes in support of trustworthy cyber infrastructure' in Proceedings of CSIIRW'10, pp. 1–4.

Provos, N., Friedl, M. & Honeyman, P. (2003), 'Preventing privilege escalation', in Proceedings of 12th USENIX Security Symposium (USENIX Security 03), USENIX Association, Washington, D.C.

Quarles, R. K. (2021), 'Parachute pants and central bank money', Speech at the 113th Annual Utah Bankers Association Convention, Sun Valley, Idaho, 28 June, 2021.

Sveriges Riksbank (2020), The Riksbank's e-krona project.
URL: *https://www.riksbank.se/globalassets/media/rapporter/e-krona/2019/theriksbanks-e-krona-pilot.pdf*

Waller, C. J. (2021), 'CBDC: A solution in search of a problem?', Speech at the American Enterprise Institute, Washington, D.C., 5 August, 2021.

Waters, B. R., Felten, E. W. & Sahai, A. (2003), 'Receiver anonymity via incomparable public keys' in S. Jajodia, V. Atluri & T. Jaeger (eds) Proceedings of the 10th ACM Conference on Computer and Communications Security, CCS 2003, ACM, pp. 112–121.