BIS Innovation Hub

Project Aurum

A Prototype for Two-tier Central Bank Digital Currency (CBDC)

October 2022

HONG KONG MONETARY AUTHORITY
香港金融管理局

Contents

The prototype is built in collaboration with:

ASTRI

Introduction

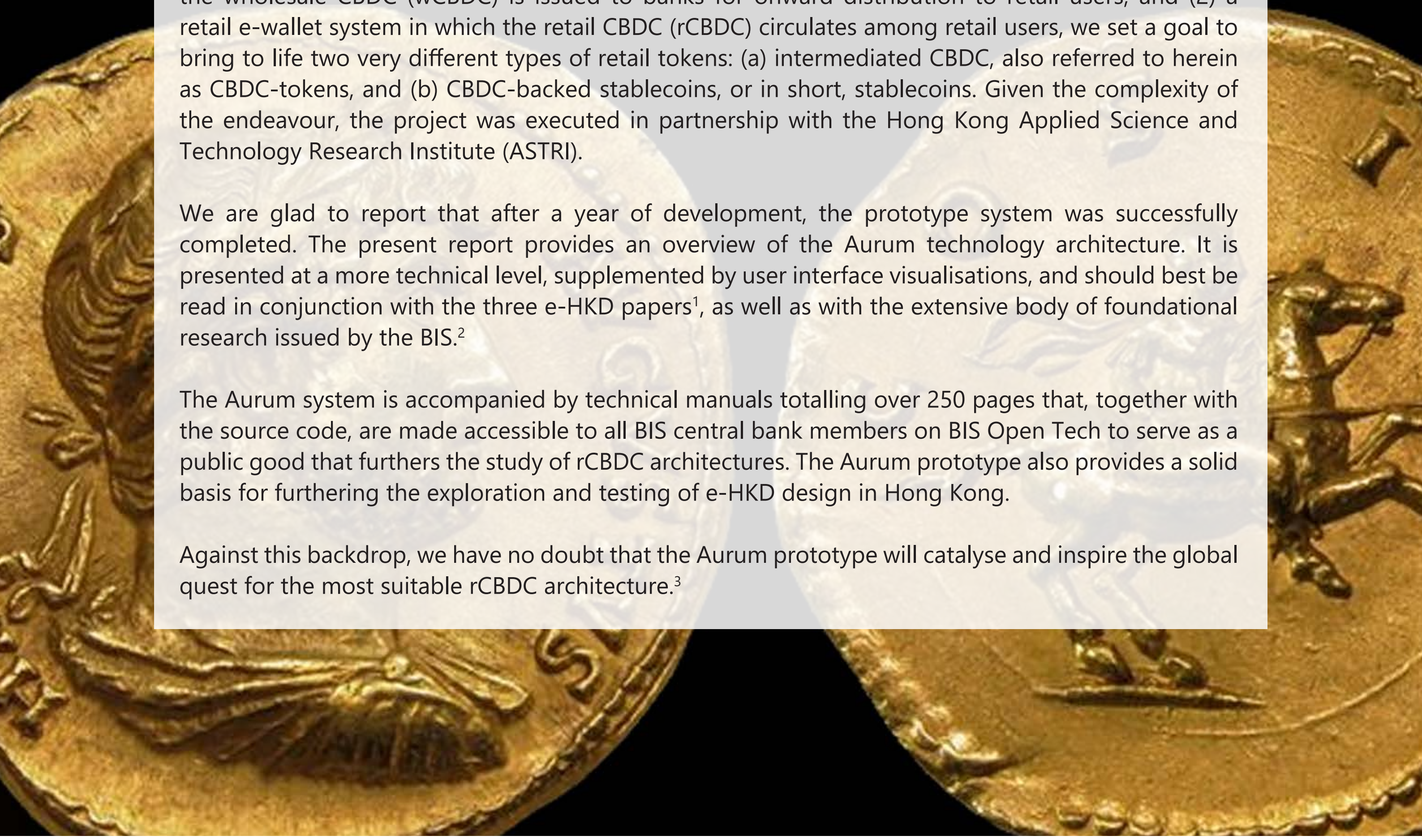
In the era of digitisation, central banks stand before a choice: does retail central bank money need to go digital and, if so, how? Jointly embarking on the challenge to design a full-stack central bank digital currency (CBDC) system, the Bank for International Settlements (BIS) Innovation Hub Hong Kong Centre and the Hong Kong Monetary Authority (HKMA) dubbed the project "Aurum", the Latin word for gold, reflecting our starting premise that digital currency issued under the auspices of a central bank must be as robust and trustworthy as gold.

Through the creation of a technology stack comprised of: (1) a wholesale interbank system in which the wholesale CBDC (wCBDC) is issued to banks for onward distribution to retail users, and (2) a retail e-wallet system in which the retail CBDC (rCBDC) circulates among retail users, we set a goal to bring to life two very different types of retail tokens: (a) intermediated CBDC, also referred to herein as CBDC-tokens, and (b) CBDC-backed stablecoins, or in short, stablecoins. Given the complexity of the endeavour, the project was executed in partnership with the Hong Kong Applied Science and Technology Research Institute (ASTRI).

We are glad to report that after a year of development, the prototype system was successfully completed. The present report provides an overview of the Aurum technology architecture. It is presented at a more technical level, supplemented by user interface visualisations, and should best be read in conjunction with the three e-HKD papers[1], as well as with the extensive body of foundational research issued by the BIS.[2]

The Aurum system is accompanied by technical manuals totalling over 250 pages that, together with the source code, are made accessible to all BIS central bank members on BIS Open Tech to serve as a public good that furthers the study of rCBDC architectures. The Aurum prototype also provides a solid basis for furthering the exploration and testing of e-HKD design in Hong Kong.

Against this backdrop, we have no doubt that the Aurum prototype will catalyse and inspire the global quest for the most suitable rCBDC architecture.[3]



1. See Hong Kong Monetary Authority: e-HKD: A technical perspective (hkma.gov.hk), October 2021; e-HKD: A Policy and Design Perspective (hkma.gov.hk), April 2022; and e-HKD - Charting the Next Steps (hkma.gov.hk), September 2022.
2. See R Auer and R Böhme, Central bank digital currency: the quest for minimally invasive technology (bis.org), June 2021; III. CBDCs: an opportunity for the monetary system (bis.org), *BIS Annual Report*, June 2021; Auer, Frost, Gambacorta, Monnet, Rice and Shin, Central bank digital currencies: motives, economic implications and the research frontier (bis.org), November 2021; *BIS*, Report 2 in a series of collaborations by central banks, CBDC - System design and interoperability (bis.org), September 2021; *BIS*, Report 1 in a series of collaborations by central banks, Central bank digital currencies: foundational principles and core features (bis.org), 2020; and Auer, Cornelli and Frost, Rise of the central bank digital currencies: drivers, approaches and technologies (bis. org) August 2020.
3. A special thank you to Codruta Boar, Daniel Eidan, Jack Ho and Benedicte Nolens from the BIS Innovation Hub, to Aldar Chan, Frederick Cheung, Nelson Chow, Brian Lam and Yvonne Tsui of the HKMA and to Chan Fai Lam and the ASTRI development team.

Section 1: Scope of Experimentation

1.1. Different types of retail CBDC

BIS research distinguishes between different types of rCBDC. The first level of distinction the BIS draws is between direct rCBDC, where customers are directly onboarded with the central bank, and different forms of intermediated rCBDC, where customers are onboarded by intermediaries.

In terms of the latter category, BIS research further distinguishes between three types of architectures:[4]

1. **Hybrid CBDC**, where the central bank keeps the full ledger and the instrument distributed by the commercial bank is a liability of the central bank;

2. **Intermediated CBDC**, where the central bank only keeps the wholesale ledger and the instrument distributed by the commercial bank is a liability of the central bank; and

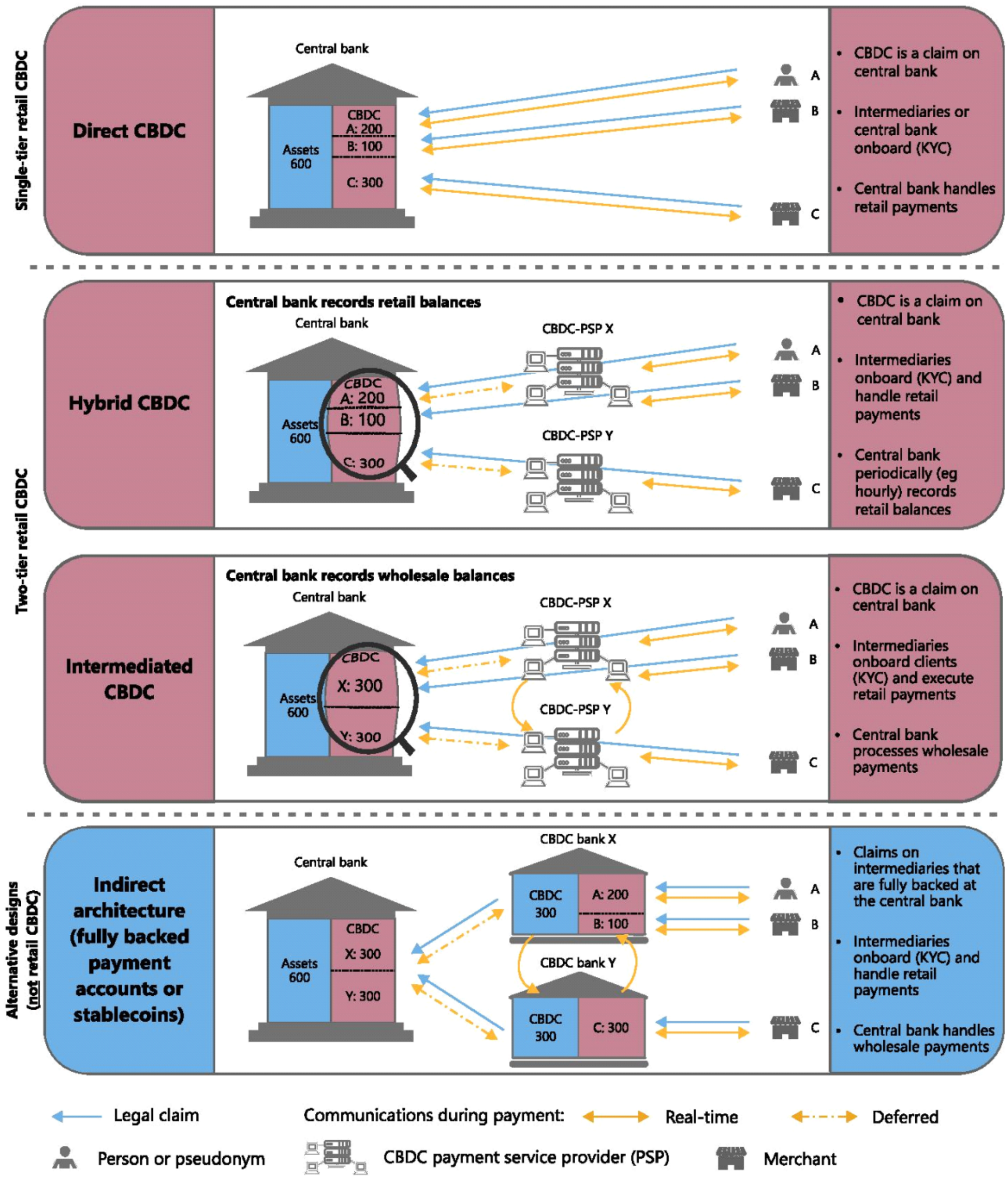
3. **Indirect architectures**, where the central bank keeps the wholesale ledger, but the instrument issued by the commercial bank is not a liability of the central bank and instead more akin to e-money or a stablecoin.

Each of these models is represented in the figure 1 below (Auer and Böhme) and is further explained in *e-HKD: A technical perspective* issued in 2021.[5]

> As the customer-facing side of retail payments is arguably better handled by the private sector than the central bank, the underlying question is how an operational architecture can balance direct claims on the central bank with the operational involvement of private sector payments services providers.
>
> **Auer and Böhme**[6]

4. See R Auer and R Böhme, Central bank digital currency: the quest for minimally invasive technology (bis.org), June 2021: "In hybrid designs, the central bank hosts a database of retail balances (even if anonymised), whereas in intermediated designs, it would keep track only of wholesale balances."
5. See e-HKD: A technical perspective (hkma.gov.hk), HKMA, October 2021, which referred to "CBDC-backed e-money". In the present report we use the wording "CBDC-backed stablecoin" or, in short "stablecoin."
6. See footnote 4.

Figure 1: rCBDC Architectures and fully-backed alternatives



In the "Direct CBDC" model (top panel), the CBDC is a direct claim on the central bank, which also handles all payments in real time and thus keeps a record of all retail holdings. Hybrid CBDC architectures incorporate a two-tier structure with direct claims on the central bank while real-time payments are handled by intermediaries. Several variants of the hybrid architecture can be envisioned. The central bank could either retain a copy of all retail CBDC holdings (second panel), or only run a wholesale ledger (third panel). In the indirect architecture (bottom panel), a CBDC is issued and redeemed only by the central bank, but this is done indirectly to intermediaries. Intermediaries, in turn, issue a claim to consumers. The intermediary is required to fully back each claim with a CBDC holding at the central bank. The central bank operates the wholesale payment system only.

Sources: elaboration based on R Auer and R Böhme, "The technology of retail central bank digital currency", *BIS Quarterly Review*, March 2020, pp 85–100.

1.2. Aurum studies intermediated CBDC and CBDC-backed stablecoins

Aurum, being the BIS Innovation Hub's first rCBDC project, decided to focus on the two architectures shown in figure 1: (a) intermediated CBDC, also referred to herein as CBDC-tokens, and (b) CBDC-backed stablecoins, or in short stablecoins.

1.2.1. Intermediated CBDC

The rationale for exploring intermediated CBDC is because, according to BIS research, many central banks are looking at intermediated CBDC and wishing to preserve the private sector's primary role in retail payments and financial intermediation.[7]

> If a CBDC is provisioned through a one-tier system fully operated by a central bank, such an arrangement would face various operational and policy challenges. There are also privacy concerns and potential impact on long-term innovation associated with the direct CBDC model. A CBDC 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.
>
> **eHKD: A Technical Perspective.**[8]

As such, we concluded that performing technology-driven experimentation in the space of intermediated CBDC by creating a code base that can be accessed by BIS member central banks for further study and experimentation would be very valuable and could help foster progress on the development of rCBDC.

In Aurum, we refer to intermediated CBDC issued to end-users as the CBDC-token, as distinct from the stablecoin, because while the CBDC-token constitutes a central bank liability, the stablecoin does not and instead constitutes a bank liability, be it one fully backed by wCBDC holdings in the interbank system.

7. See footnote 4.
8. See e-HKD: A technical perspective (hkma.gov.hk). HKMA, October 2021, p 10.

1.2.2. CBDC-backed stablecoins

While Auer and Böhme do not label CBDC-backed stablecoins as CBDC given that they do not constitute a liability of the central bank, Aurum decided to explore CBDC-backed stablecoins because, conceptually, they are the closest to the current Hong Kong SAR currency system where the physical bills are issued by the three note-issuing banks rather than by the central bank. In other words, CBDC-backed stablecoins are the digital equivalent of the current Hong Kong note-issuing bank system.

Bringing CBDC-backed stablecoins to life has never been done before and we therefore felt that doing so may supplement the growing body of research on private sector stablecoins. Indeed, what distinguishes Aurum from private sector stablecoins is that Aurum's stablecoin balances are reconciled, versus real time gross settlement (RTGS) balances of the issuing bank with the central bank. In this regard, the system developed for the CBDC-backed stablecoins is unique and can be useful as central banks look toward designing regulatory approaches with regard to private sector stablecoins, especially while seeking to design methods to verify the backing of the stablecoins, a highly topical matter.[9]

1.3. Trade-offs between different models

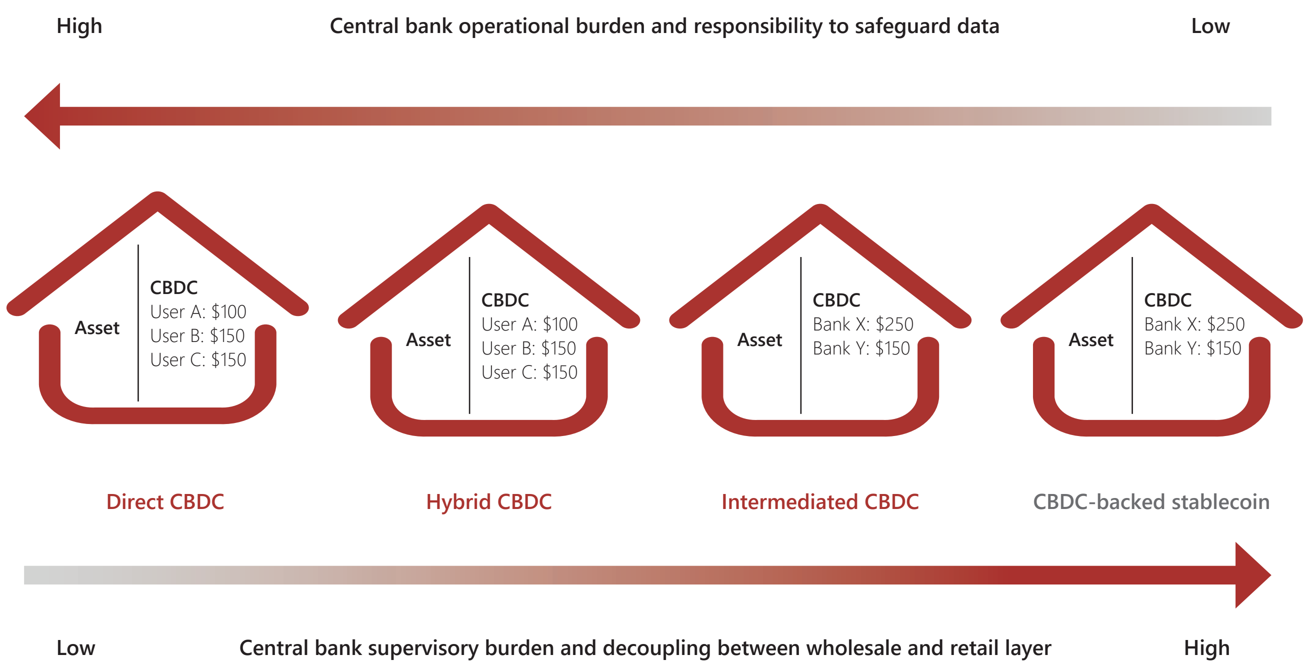
As noted by Auer and Böhme (2021), different trade-offs can be observed in the different two-tier distribution models illustrated in figure 1, namely: the central bank's operational burdens; the level of decoupling between the wholesale and retail ledger; the central bank's responsibility to safeguard 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 for 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 stablecoins 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 and as illustrated in figure 2, 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.

> The central bank has to operate either a complex technical infrastructure or a complex supervisory regime.
>
> **Auer and Böhme.**[10]

9. See US Department of the Treasury, *The Future of Money and Payments Report Pursuant to Section 4(b) of Executive Order 14067*, September 2022: "Failure of a stablecoin to maintain a stable value, or loss of confidence in a stablecoin's ability to maintain a value, could result in a run."

10. See footnote 4.

Figure 2: Illustration of trade-offs



1.4. Environmental considerations

As noted in *Principle 8. Energy and Environment Energy of the G-7 Public Policy Principles for Retail Central Bank Digital Currencies* (2021) environmental impact should be factored into the design and implementation of any CBDC from the outset.[11]

Based on data of the Cambridge Centre for Alternative Finance and Statista, we calculated the Bitcoin carbon footprint for 2021 to be over 600,000 gCO2.[12] In comparison, Aurum gCO2 stands at 0.0110, or less as TPS rises.

11. See G7_Public_Policy_Principles_for_Retail_CBDC_FINAL.pdf (publishing.service.gov.uk), G7, 2021
12. See Cambridge Centre for Alternative Finance, ccaf.io/cbeci/index and Statista, www.statista.com/statistics/730806/daily-number-of-bitcoin-transactions/

Section 2: Guiding principles

As part of embarking on the project, safety, flexibility and privacy were chosen as the guiding principles.[13]

2.1. Safety

One of the principal risks with digital currency is the double-spend problem. The double-spend problem describes the difficulty of ensuring digital money is not easily duplicated. In other words, double-spend refers to the incidence of an individual spending a balance of a particular digital currency more than once, effectively creating a disparity between the spending record and the amount of that digital currency available, as well as the way in which it is distributed. The issue of double spending is a problem that cash does not have: if you pay for a coffee with a $5 bill, turning that bill over to the Barista, you cannot turn around and spend that same $5 elsewhere.

The Aurum system is designed such that the wholesale interbank system can detect and prevent banks from:

1. **Over-issuance:** the system prevents banks from issuing more rCBDC than the wCBDC asset that bank owns

2. **Double-issuance:** the system prevents banks from using the same wCBDC asset to issue rCBDC repeatedly

3. **Double-redemption:** the system prevents banks from using the same rCBDC to exchange for wCBDC repeatedly.

The Aurum system achieves this through the validator mechanism that can help prevent over-issuance and double-spending in the retail system. However, there are 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 stablecoins as these processes could be seen as double spending of the wholesale transaction.

Another safety feature of the system is that transactions recorded as unspent transaction output (UTXO) allow the validator infrastructure to prove ownership of rCBDC even if its issuing bank has stopped operation. The UTXO design requires each payment transaction to specify the source(s) of the CBDC-token or CBDC-backed stablecoin 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 the CBDC-token or stablecoin with the coinbase transactions from which the CBDC-token or CBDC-backed stablecoin inherits its monetary value. The identified coinbase transaction would directly refer to the wholesale transactions which can trace back to the original issuance of wCBDC by the central bank.

13. See e-HKD: A technical perspective (hkma.gov.hk), HKMA, October 2021, including, but not limited to, pp 38-42.

What is a UTXO?[14]

An unspent transaction output (UTXO) is the technical term for the amount and ownership of digital currency that remains after a transaction, ie the unspent transaction amount.

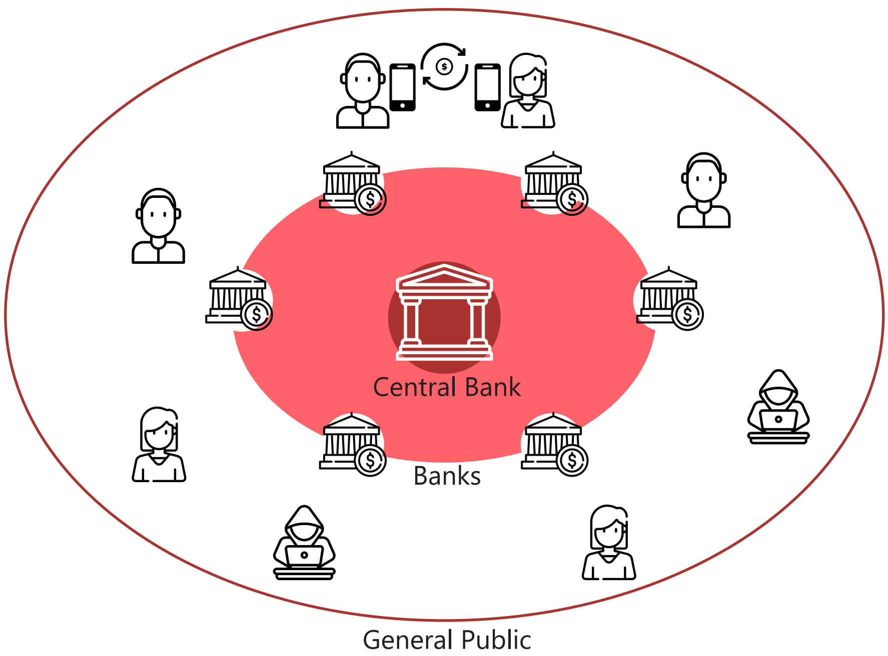
The UTXO model is used in many digital currencies because it allows users to track ownership of all portions of that digital currency through the chain of pseudonymous addresses that completed such transactions.

The identity of the user cannot be identified based on the chain, unless the user advertises that he/she owns a certain address.

Similarly in the case of Aurum the user can see the UTXO chain without knowing the identity of the prior users.

Furthermore, the system also achieves greater cyber security, wCBDC issuance is restricted to only the wholesale system. 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 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.

Figure 3: Resilience through de-coupling



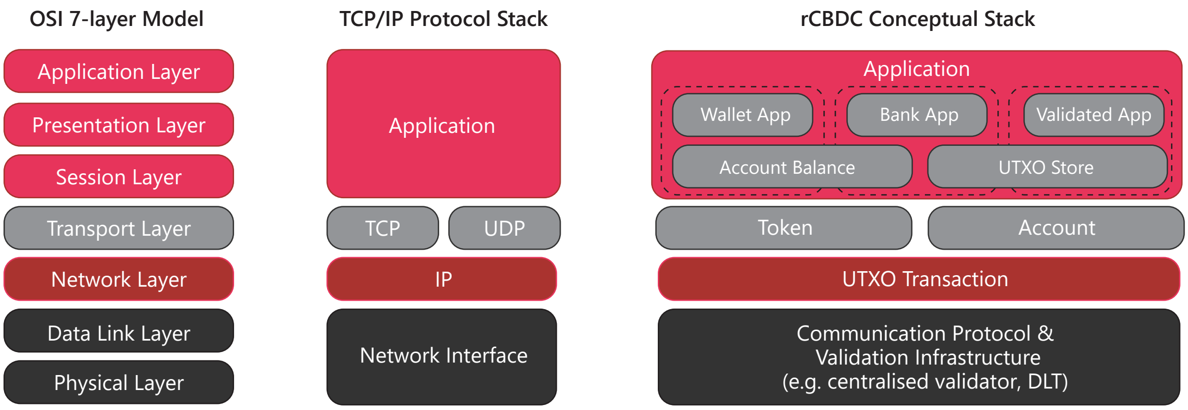
14. See www.r3.com/blog/what-is-a-uxto.

2.2. Flexibility

The architecture is designed with modularity and flexibility in mind, with system and user functions cleanly delineated. 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 *(a) the CBDC-token* and *(b) the CBDC-backed stablecoins.*

In addition, the designed architecture enables private sector flexibility and innovation. The design of UTXO transactions could be seen as a thin protocol layer, similar to 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.

Figure 4: UTXO transaction structure in comparison to TCP/IP protocol stack



2.3. Privacy

The system is comprised of *(1) a wholesale interbank system* and *(2) a retail e-wallet system*, i.e. an e-wallet system with an associated smartphone UI for the retail user.

This two-layered system architecture means that only the intermediaries who perform the Know-your-Customer (KYC) verification and who handle the rCBDC transactions can access the identity of the token owner. The central bank does not obtain such information, enabling retail user privacy. In addition, users use a cryptographic unique alias as identity in rCBDC transactions.

In other words, the proposed architecture preserves user anonymity from the validator infrastructure and other users through a pseudonym system, which only uses public keys in transactions, while making the mapping between real identities and public keys known to the respective intermediaries only. All transactions are designed to use pseudonymous public keys only and refrain from using personally identifiable information, which could be seen as an embodiment of privacy by design.

This feature is important as user privacy is often raised as a principal area to resolve for rCBDC to be adopted by users.

Figure 5: Design principles of Aurum

Safety:

- The wholesale interbank system can detect and prevent banks from:
  1. over-issuance: issue more retail rCBDC than the wholesale wCBDC asset the bank owns
  2. double-issuance: using the same wholesale wCBDC asset to issue retail rCBDC repeatedly
  3. double-redemption: using the same retail rCBDC to exchange for wholesale wCBDC repeatedly
- Users can still prove ownership of retail rCBDC even if the issuing bank has stopped operation.
- The system achieves increased cyber resilience through decoupling between the wholesale interbank system and the retail e-wallet system.

Flexibility:

- The Aurum system can be adopted for different CBDC models: intermediated CBDC and CBDC-backed stablecoins.
- It controls the amount of information disclosed by the retail e-wallet system to the wholesale interbank system while still guaranteeing system safety.
- The wholesale interbank system is separated from the retail e-wallet system.

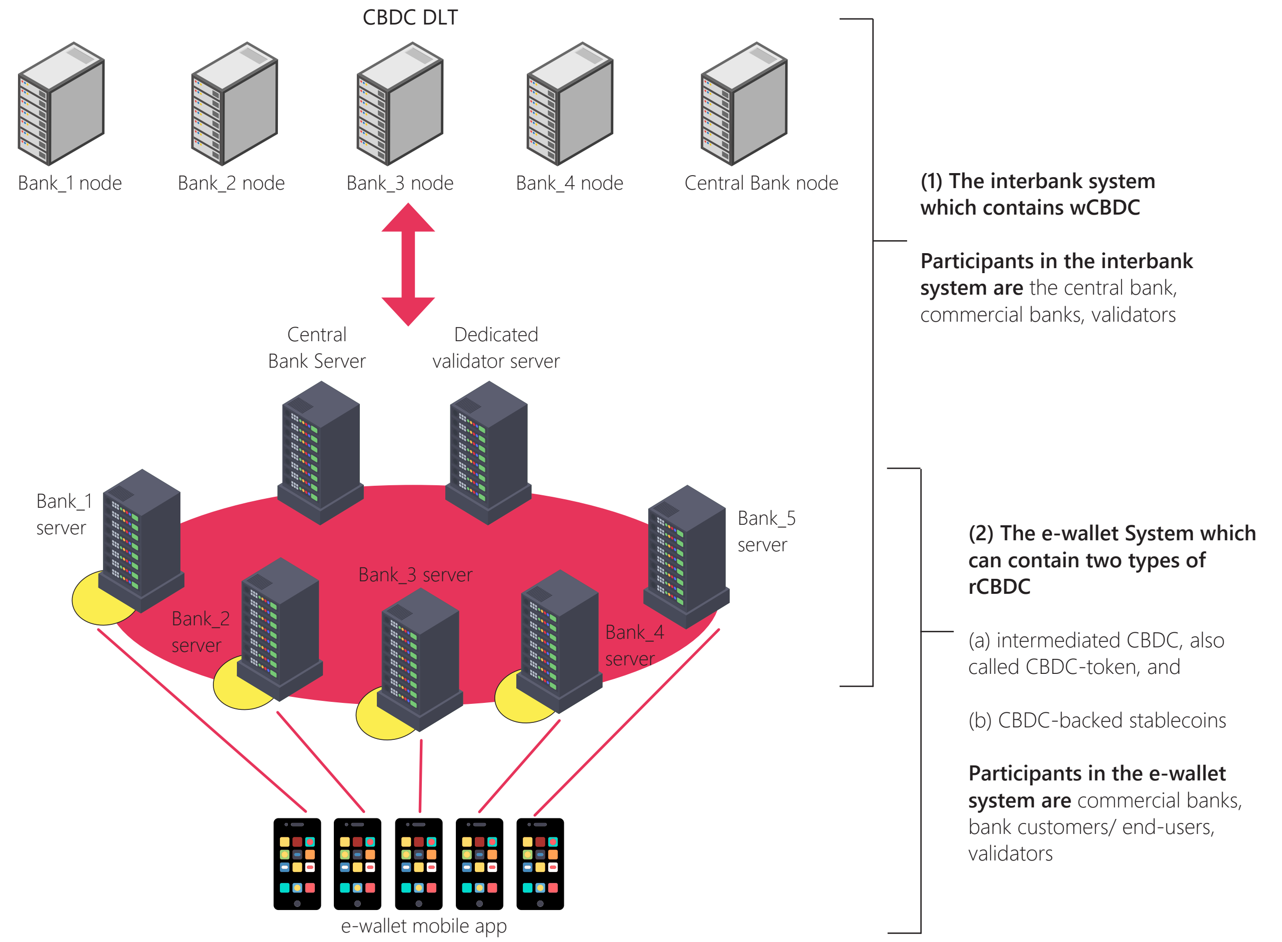
Privacy:

- Retail rCBDC transactions are not disclosed to the wholesale interbank system.
- Users use cryptographic unique alias as identity in CBDC transactions.

Section 3: High-level architecture

As noted above, the system is comprised of: *(1) a wholesale interbank system*, and *(2) a retail e-wallet system, ie an e-wallet system with an associated smart phone UI for the retail user.*

Figure 6: High-level architecture of Aurum



Notes: *Represents DLT validator server service run by issuing bank server, bank_5 is a non-issuing bank*

As shown in figure 6, in the network there are two types of validators:

1. **A DLT validator**, operated by an issuing bank. An issuing bank can serve as a validator for operations of another bank.

2. **A dedicated validator** which performs only the function of a validator and plays no other role.

Each bank owns the following accounts:

1. **A RTGS account** that is managed by the central bank.

2. **A wCBDC account** in the interbank system that is managed through DLT.

3. **An e-wallet account**. A bank may receive stablecoins issued by other banks. It may also receive CBDC-tokens. Hence, it will create its own e-wallet account to store such CBDC-tokens and stablecoins.

We elaborate on the wholesale interbank system and the retail e-wallet system in further detail below.

3.1. Wholesale interbank system

The wholesale interbank system is built on DLT and is an interbank network in which the participants are the central bank, commercial banks, and validators. The digital currency that circulates in this interbank system is called wCBDC.

The three types of participants in the wholesale interbank system are:

1. **Participants that are running the blockchain nodes**. In the prototype there are four issuing banks that each run a node as can be seen in figure 6. They also serve as endorser nodes to endorse DLT transactions.

2. **The central bank that may host a DLT node**, as also shown in figure 6. However, it does not serve as an endorser node, ie it does not endorse DLT transactions.

3. **All other commercial banks**. Commercial banks other than the four issuing banks do not host DLT nodes. They are only users of the DLT system. They have their own wCBDC accounts in the interbank system because all of them need to be able to access the DLT system to access their wCBDC accounts.

There are five types of wCBDC transactions recorded on the wholesale DLT network:

Transaction 1	Issuance from central bank to a commercial bank.
Transaction 2	Transfer between commercial banks.
Transaction 3	Redemption at central bank by a commercial bank.
Transaction 4	Deposit by a commercial bank for stablecoin issuance or CBDC-token distribution (to the e-wallet platform).
Transaction 5	Release to a commercial bank in response to stablecoin or CBDC-token redemption by the bank (from the e-wallet platform).

A shared custodian account is implemented in the wholesale interbank system. It is managed by a smart contract. When a bank requests the issuance of rCBDC from the interbank system, the smart contract will transfer an equivalent amount of wCBDC from the bank's wCBDC account to the custodian account to serve as the backing asset. The reverse is done when the bank requests redemption of the rCBDC.

3.2. Retail e-wallet system

The retail e-wallet system is a bank-based wallet network in which the participants are commercial banks, bank customers, and validators. As shown in figure 6, the digital currency that circulates in the retail e-wallet system takes two forms*: (a) intermediated CBDC, also referred to as CBDC-token*, and *(b) CBDC-backed stablecoins, also referred to as stablecoins*.

Each bank, regardless of whether it is an issuing bank or non-issuing bank, implements and operates its own retail e-wallet system. Its customers, ie the end-users, interact with the bank server through this e-wallet system. The customer conducts all e-wallet activities, eg payment, through his/her bank.

The retail e-wallet system is not built on DLT and is instead a server-based system. The bank operates an e-wallet system by running a bank server service that serves various participants.

The four types of participants in the e-wallet system are:

1. **The bank hosting the retail e-wallet system**. This is the bank operating the retail e-wallet system.

2. **The validator**. 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.

3. **End-users**. They are the retail customers of the bank. They have a savings account and an e-wallet account with the commercial bank. The e-wallet account stores only the CBDC-token or the CBDC-backed stablecoin. The customer may withdraw fiat from his/her savings account and deposit the equivalent amount into his e-wallet account in the form of the CBDC-token or the CBDC-backed stablecoin and vice-versa.

4. **Other commercial banks**. They participate in this e-wallet system to perform transactions between their end-users and the end-users of the other commercial banks.

The following are the three main rCBDC transactions in the retail e-wallet system:

Transaction 1	The end-user can exchange fiat currency for e-wallet currency (the CBDC-token or CBDC-backed stablecoin), and vice versa.
Transaction 2	The end-user can pay in or receive payment in the e-wallet currency (the CBDC-token or CBDC-backed stablecoin).
Transaction 3	The end-user can process a request to trace the UTXO history of the e-wallet currency (the CBDC-token or CBDC-backed stablecoin).

Below are examples of a bank's e-wallet operations that are confirmed/attested by validators:

1. Upon CBDC-token or CBDC-backed stablecoin issuance the validator signs on the generated coinbase UTXO.

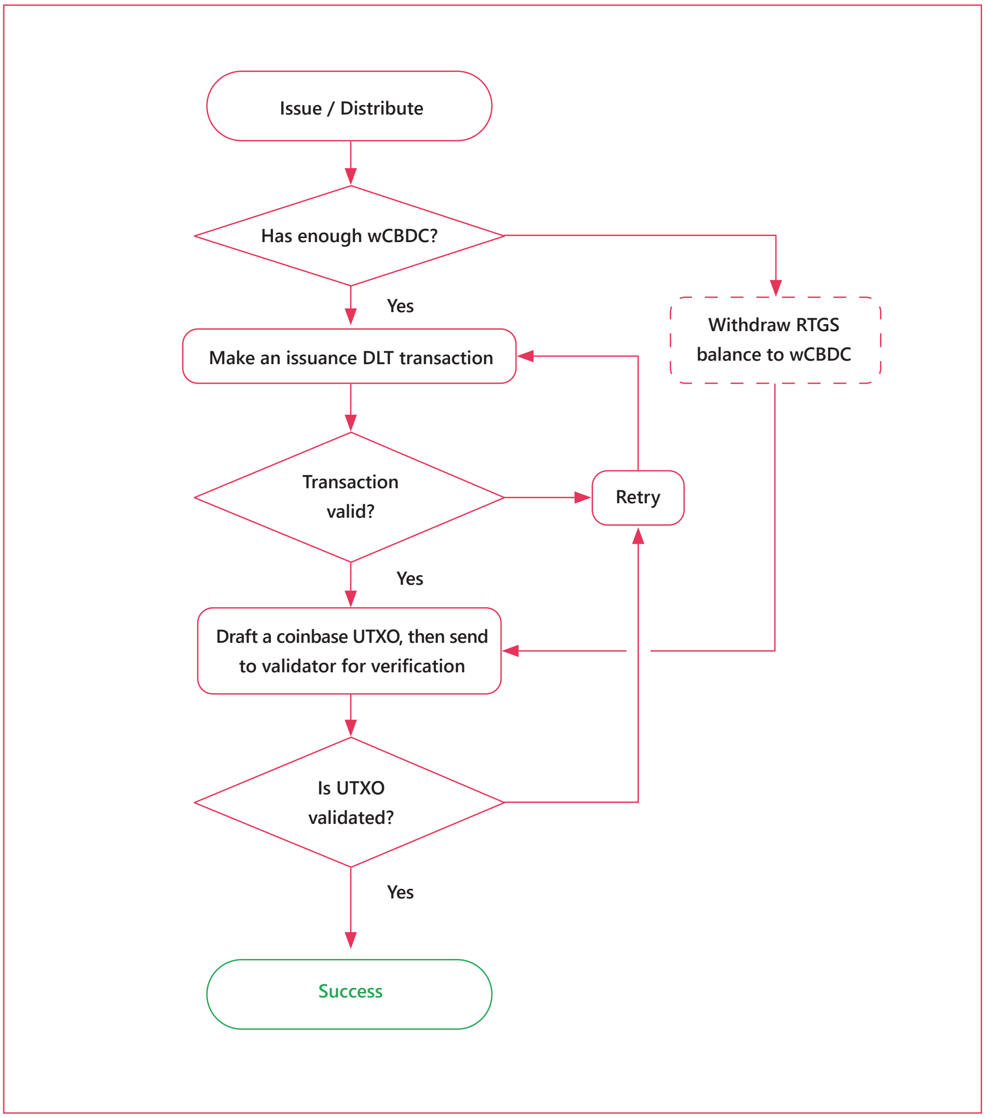
2. Upon e-wallet currency payment, the validator signs on the generated UTXO.

3. Upon redemption of the e-wallet currency, the validator signs on the UTXO that is marked for redemption.

Section 4: CBDC Operation

The bank can request the central bank to interact with the RTGS system (for testing purposes a RTGS simulator) to transfer money from its RTGS account to wCBDC in its wCBDC account. The bank then obtains rCBDC and can pass it in the form of a CBDC-token or CBDC-backed stablecoin to its end-users. The end-users can pass their CBDC-token or the CBDC-backed stablecoin to other end-users.

Figure 7: Issuance in the wholesale interbank system



The reverse process, called redemption, happens when the end-user exchanges his/her rCBDC back to his/her savings account. The bank in such case exchanges such CBDC-token or CBDC-backed stablecoin back to wCBDC in its wCBDC account. The bank can further exchange the wCBDC back to currency in its RTGS account.

4.1. Currency in the wholesale interbank system

The characteristics of wCBDC are:

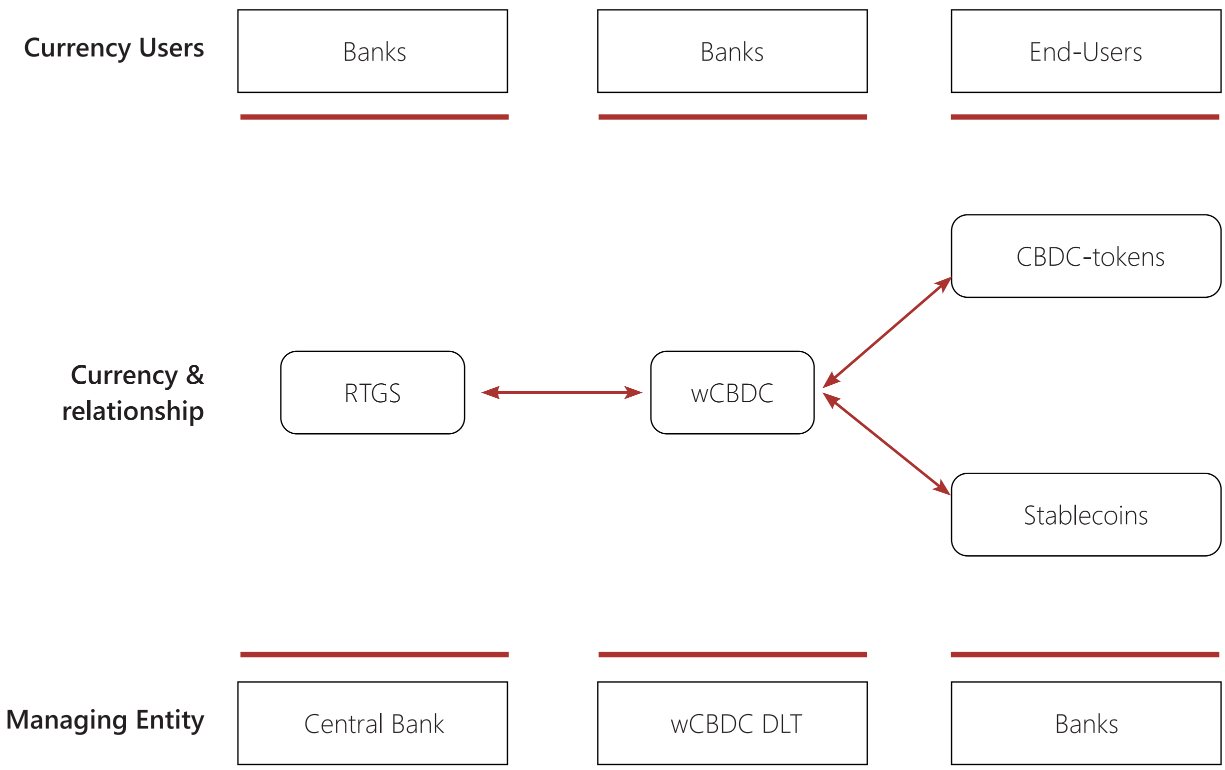
1. It is issued by the central bank to the requesting banks.
2. wCBDC transactions, including issuance, are processed by DLT.
3. Each unit of wCBDC value is equivalent to 10 cents of one Hong Kong dollar.

To obtain wCBDC, the bank sends a request to the central bank to withdraw the money from its RTGS account and to deposit the equivalent amount of wCBDC into its wCBDC account. As noted above, the action of deposit of the wCBDC into the bank's wCBDC account is executed through a DLT transaction. The DLT transaction is endorsed by a specified number of DLT endorser nodes. The endorsed DLT transaction serves as confirmation of the authenticity of the wCBDC in the bank's wCBDC account.

4.2. Retail e-wallet currencies

As noted above, there are two types of e-wallet currency: *(a) intermediated CBDC, also called CBDC-token* and *(b) CBDC-backed stablecoins.*

Figure 8: End-users can have two types of e-wallet currency



The CBDC-token is issued by the DLT on behalf of the central bank. The bank has to obtain the CBDC-token from the DLT through a process known as CBDC-token distribution. The stablecoin on the other hand is issued by issuing banks.

Both the CBDC-token and the CBDC-backed stablecoin exist in the form of a UTXO. The output of the UTXO pays to one or more payees. A payee can display the UTXO as proof of the CBDC-token or CBDC-backed stablecoin he/she owns. The payment of a CBDC-token or CBDC-backed stablecoin involves using an output of an UTXO to pay someone. It results in the creation of a new UTXO.

Since the CBDC-backed stablecoin is issued by an issuing bank, all its subsequent transactions are also processed by that issuing bank and validated by an authorised validator. In contrast, as the CBDC-token is distributed on the central bank's behalf, its transactions are processed and validated by the dedicated validator only.

The retail e-wallet contains only UTXOs of CBDC-tokens and CBDC-backed stablecoins that:

- √ Are paid to the e-wallet, and
- √ Have not been spent (ie not used in paying others), and
- √ Have not been redeemed.

We include below more detail on the respective process flows for the CBDC-token and the CBDC-backed stablecoin.

4.2.1. Flow of the CBDC-token

A CBDC-token is issued by the central bank and distributed to a commercial bank. *All banks* can obtain from the central bank the issuance of a CBDC-token from the central bank through the following steps:

1. The bank executes a CBDC-token distribution DLT transaction that transfers the equivalent amount of money from the bank's wCBDC account to the common custodian account (see 3.1.). This action is endorsed by the endorsing nodes in the DLT. These endorsing nodes add their signatures to the DLT transaction as proof of their endorsement.
2. The bank creates the CBDC-token UTXO. The DLT transaction generated in the previous step is embedded in this UTXO. This UTXO is called CBDC-token coinbase UTXO. The payee of this UTXO is the bank itself.
3. The bank then requests an authorised validator to validate the CBDC-token coinbase UTXO draft.
4. The validator verifies the UTXO. If it finds the UTXO to be valid, it will sign the UTXO draft. The UTXO draft now becomes a formal UTXO ready for usage.

After obtaining a CBDC-token, the bank may use it to pay the following entities:

- √ Other banks
- √ End-users who are the bank's customers
- √ End-users of other banks

Instead of using it for payment to others, the bank may also choose to redeem the CBDC-token UTXO. This action will nullify the CBDC-token and transfer the equivalent amount of wCBDC from the common custodian account to the bank's wCBDC account.

4.2.2. Flow of the CBDC-backed stablecoin

The CBDC-backed stablecoin on the other hand *can only be issued by issuing banks* through the following steps:

1. The bank executes a CBDC-backed stablecoin issuance DLT transaction on the wholesale interbank system. This involves a wCBDC deposit which transfers the equivalent amount of money from its wCBDC account to the custodian account (see 3.1.). The transaction is endorsed by the endorsing nodes in DLT (the endorsing nodes are the issuing banks). These endorsing nodes add their signatures to the DLT transaction as proof of their endorsement.

2. The bank then generates a draft of the CBDC-backed stablecoin UTXO and embeds in it the DLT transaction generated in the previous step. This UTXO is called stablecoin coinbase UTXO. The payee of this UTXO is the issuing bank itself.

3. The bank signs the UTXO.

4. The bank then requests an authorised validator to validate the stablecoin coinbase UTXO draft.

5. The validator verifies the UTXO. If it finds the UTXO to be valid, it will sign the UTXO draft. The UTXO draft now becomes a formal UTXO ready for usage.

After issuing the CBDC-backed stablecoin, the issuing bank may use it to pay the following entities:

- √ Other banks, including both issuing banks and non-issuing banks
- √ End-users who are the bank's customers; and
- √ End-users of other banks

Instead of using it for payment to others, the bank may also choose to redeem the CBDC-backed stablecoin. This action will nullify the stablecoin and transfer the equivalent amount of wCBDC from the common custodian account back to the bank's wCBDC account.

The redemption of a CBDC-backed stablecoin to recover the wCBDC from the custodian account can only be carried out by the issuing bank of that particular stablecoin. If a bank wants to redeem a CBDC-backed stablecoin issued by another bank, it has to perform the redemption through that issuing bank.

4.2.3. Need for the backing asset for both the CBDC-token and the CBDC-backed stablecoin

In order to obtain CBDC-token distribution from the interbank system or to issue a CBDC-backed stablecoin, a bank needs to submit a backing asset to the DLT.

The backing asset submission is carried out by the bank through transferring wCBDC from its wCBDC account to the common custodian account and attaching information about the purpose of transaction. The submission and the attached information will be examined by the DLT validating nodes and added as a backing asset record in wCBDC DLT ledger.

The backing asset record contains the following information:

wCBDC deposit amount	a. For the CBDC-token, this is the wCBDC that the bank deposits to the custodian account to obtain CBDC-token distribution from the DLT. b. For the CBDC-backed stablecoin, this is the wCBDC that the issuing bank deposits to the custodian account to issue the stablecoin.
Purpose of the wCBDC deposit	a. CBDC-token distribution b. CBDC-backed stablecoin issuance
Depositor identity	ID of the bank
Designated validator identity	ID of the validator

4.3. Server functions

Different servers have different functions in the overall system:

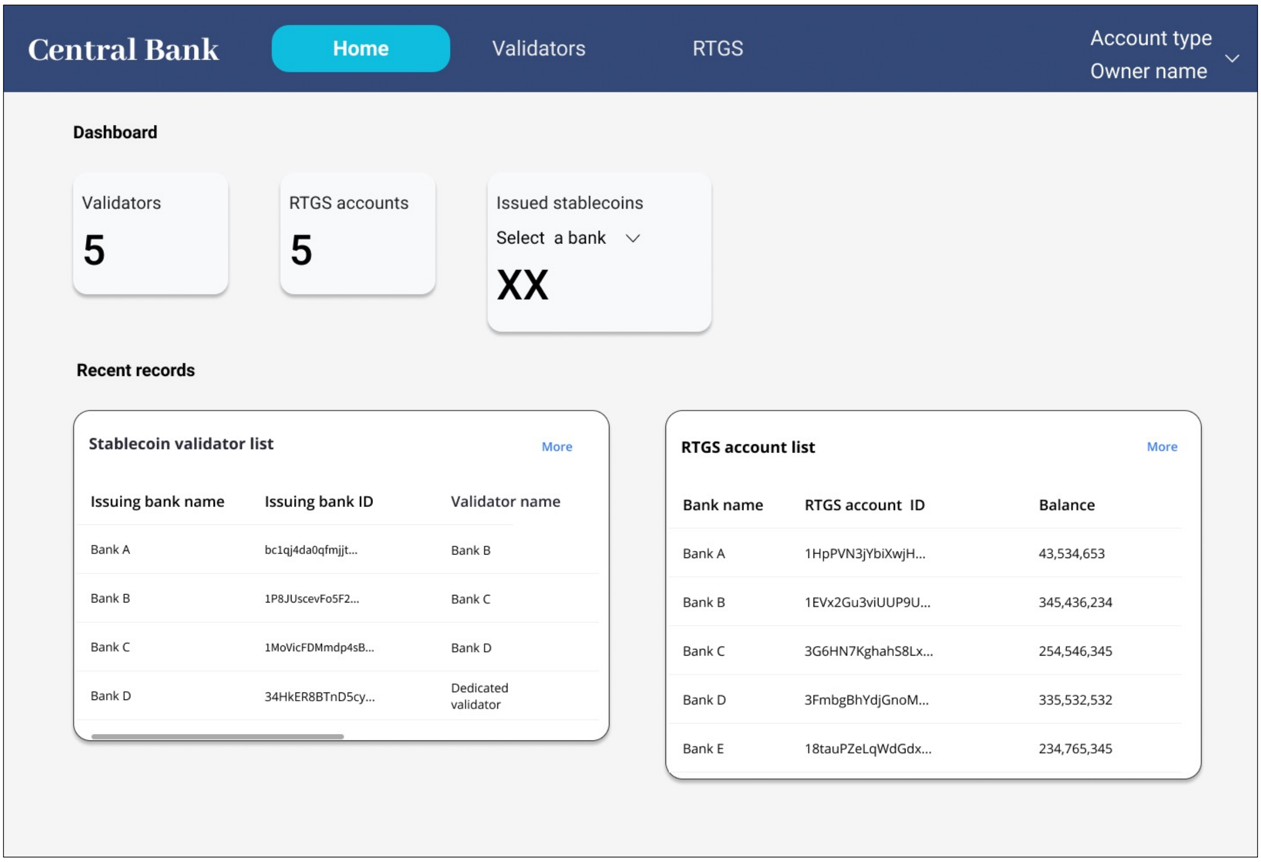
Functions of the central bank server	√ The central bank server interacts with the RTGS simulator to manage the RTGS account balances. It processes bank server requests to issue wCBDC out of the RTGS account, and vice versa.
Functions of the bank server	√ The bank server interacts with the central bank server for RTGS account transactions. √ It interacts with wCBDC DLT for wCBDC transactions and e-wallet currency issuance/redemption. √ It responds to e-wallet customer requests for: • e-wallet currency operation; and • savings account deposit/withdrawal. √ It interacts with the validator for e-wallet transaction validation. √ It services bank staff operations, for example where the bank staff requests the bank server to issue the stablecoin.
Functions of the validator server	√ The validator server responds to bank requests to validate an e-wallet currency UTXO.
Functions of the e-wallet	√ The e-wallet provides a savings account and an e-wallet account operation after sign-up by the customer. √ It also self-generates identity (ie a keypair and a user name) and stores the account information. √ It is used for: • Requesting e-wallet currency from the bank, this is done by withdrawing an equivalent amount of money from the savings account; • Redeeming e-wallet currency. Through this operation the e-wallet returns currency to the bank and in return the customer receives the equivalent amount of money in their savings account. • Paying e-wallet currency to other end-users. • Receiving e-wallet currency from other end-users.

Section 5: User interfaces

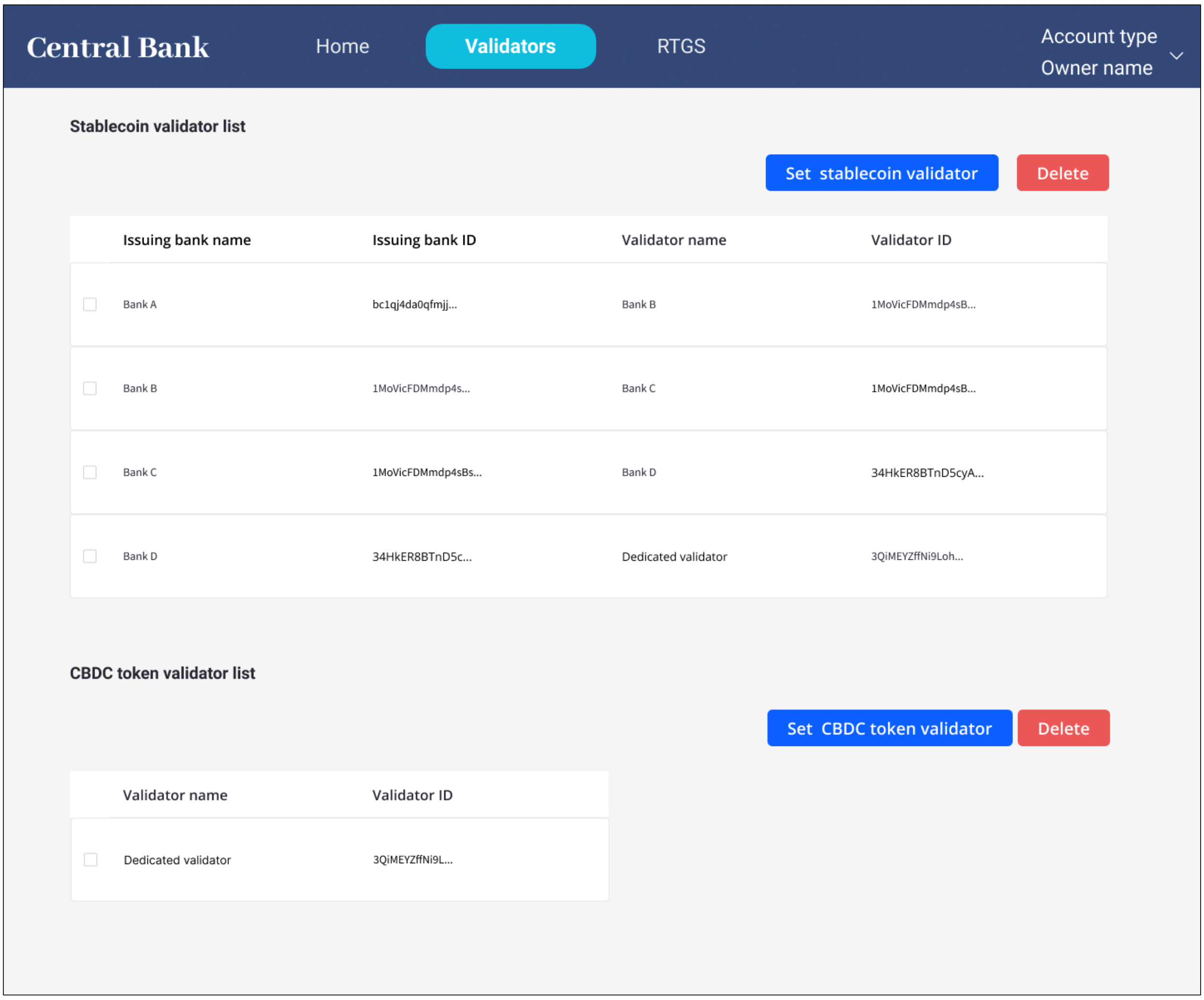
For ease of understanding, we share below a series of visualisations of the user interfaces (UI) by user type below.

5.1. Central bank user

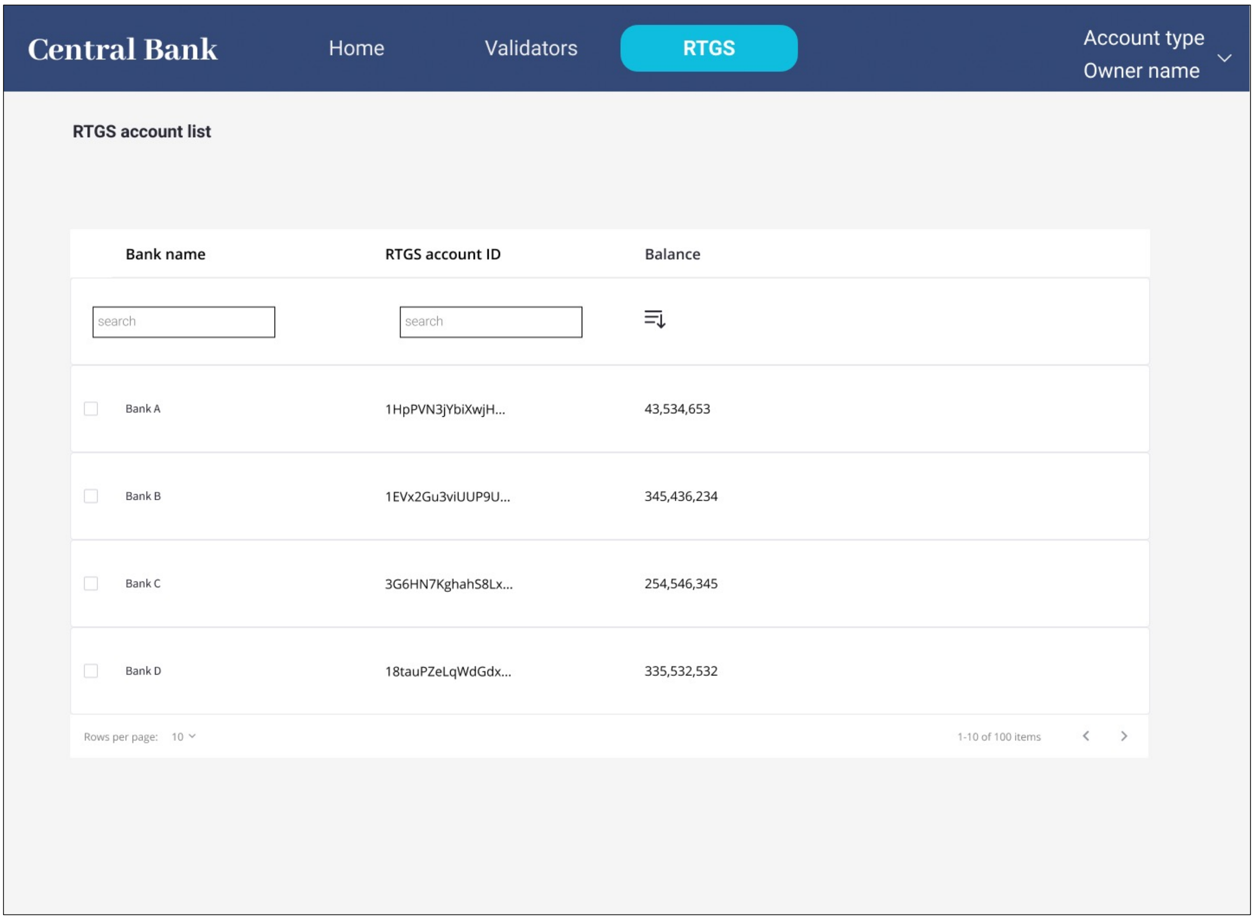
Visualisation 1: This is the central bank user dashboard that provides a summary of the number of validators, the number of RTGS accounts, and the number of CBDC-backed stablecoins issued by each issuing bank. Details of each validator and of each RTGS account are also displayed.



Visualisation 2: This is the central bank validator page on, which the central bank staff are able to see and manage the validators.

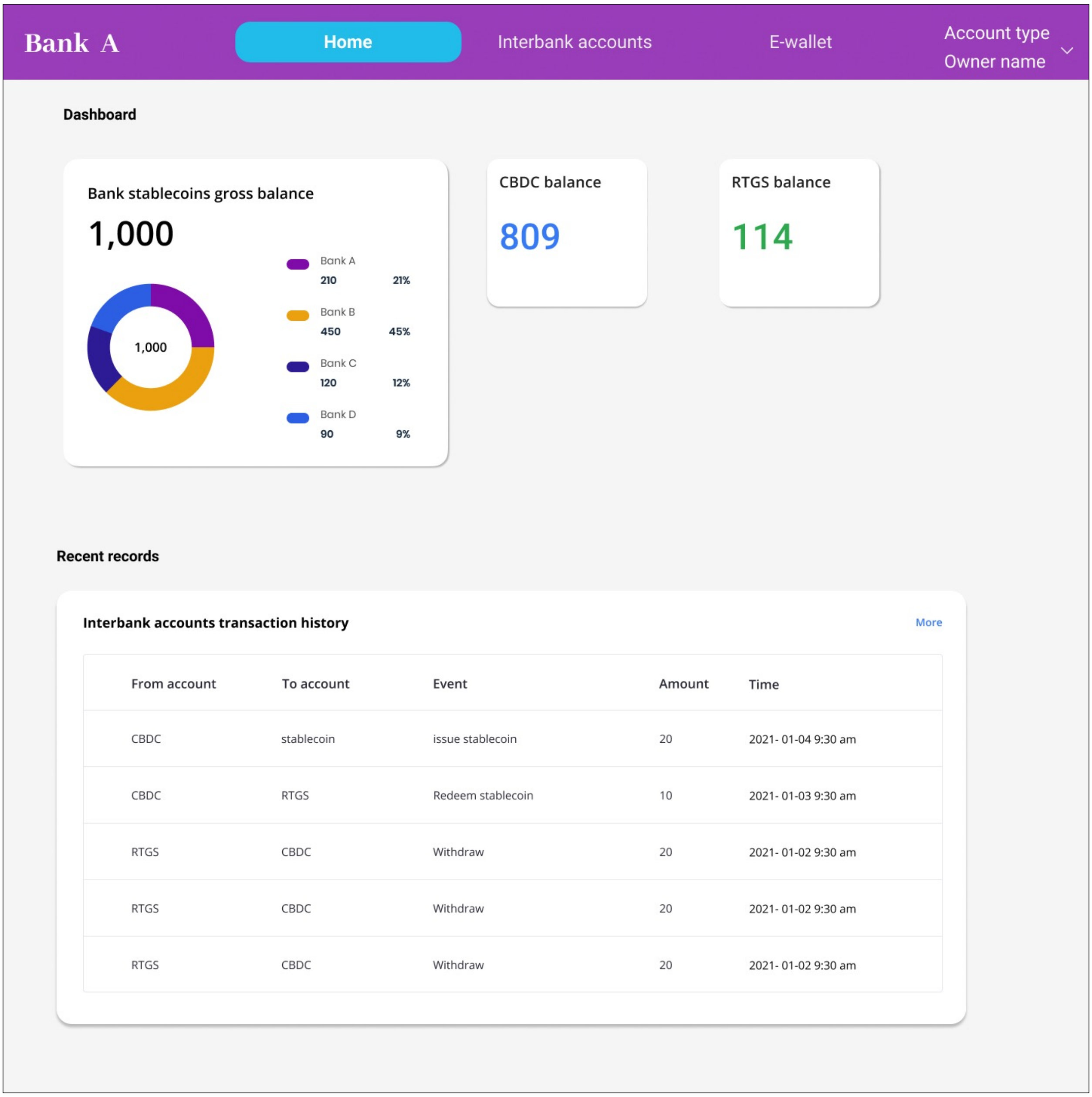


Visualisation 3: This is the central bank RTGS page on which central bank staff can review the RTGS accounts and click each row to review credit balances to the RTGS account.

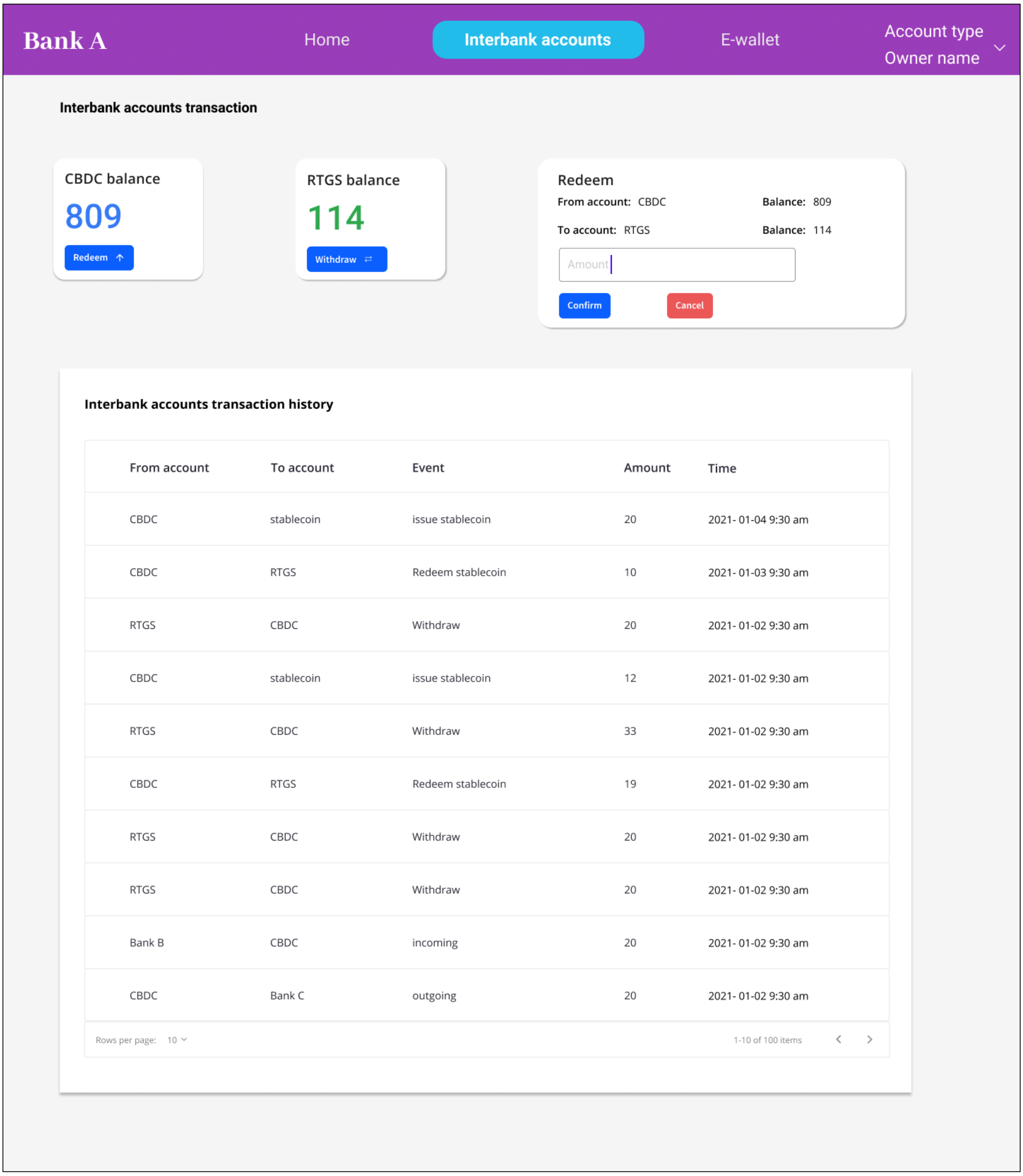


5.2. Bank user

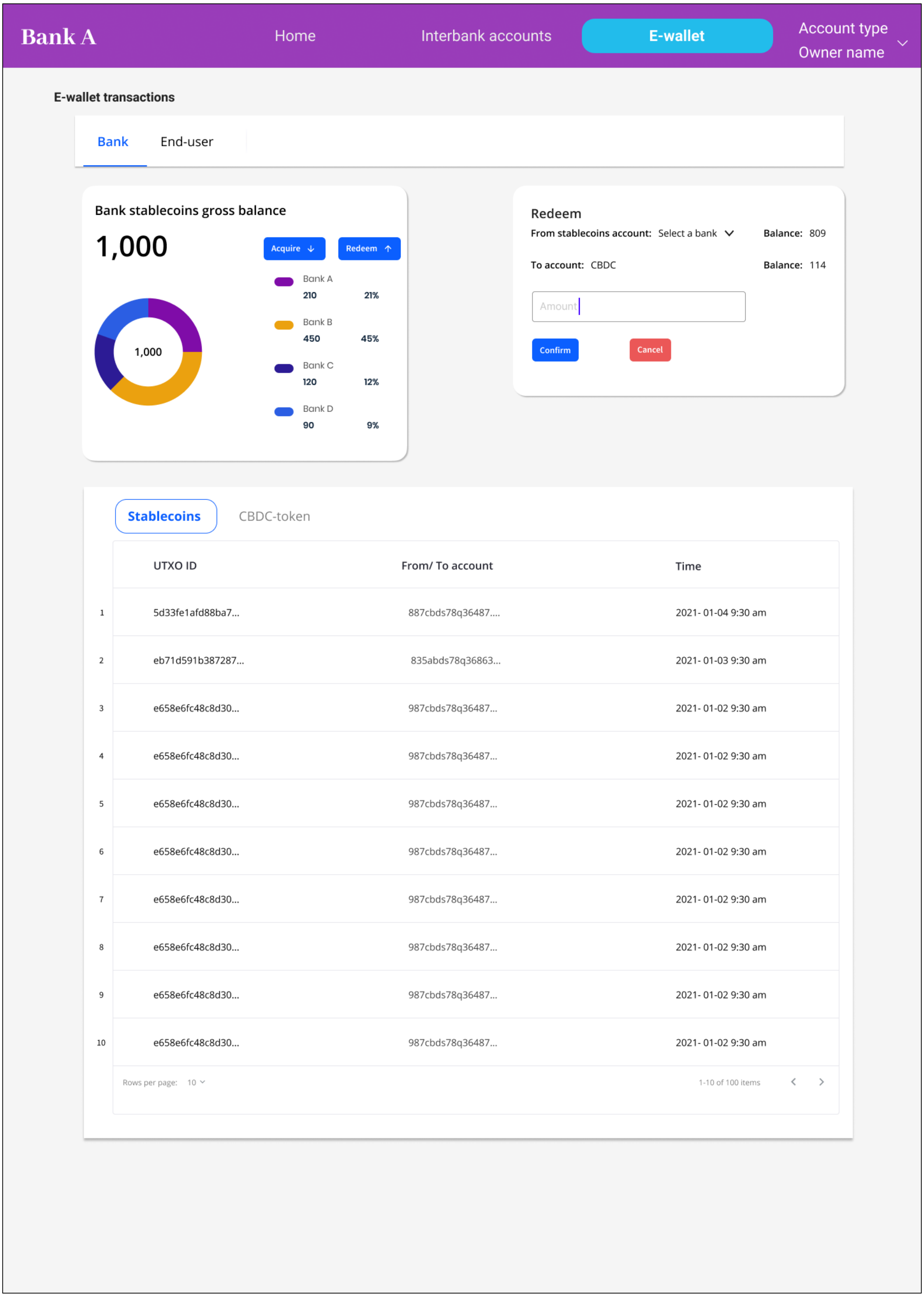
Visualisation 4: This is the bank user dashboard on which the bank user can see their RTGS, wCBDC and CBDC-backed stablecoin balance.



Visualisation 5: This is the bank user interbank accounts page on which bank staff can perform the wCBDC and RTGS currency transfers. The dashboard is divided into a display of the wCBDC and RTGS balance and an action box to process redeem and withdraw functions between the wCBDC and RTGS accounts. The table lists the transfer history with event details.

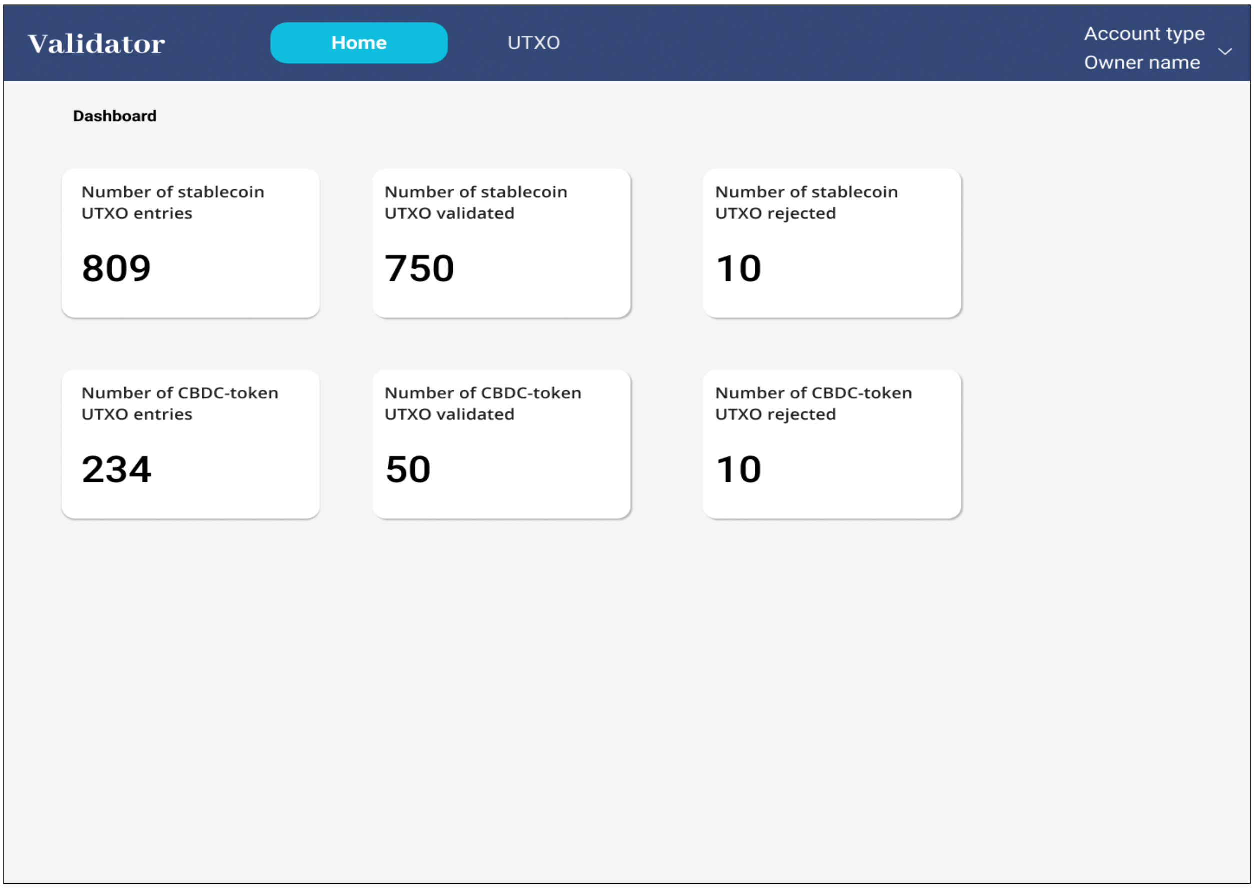


Visualisation 6: This is the bank user retail e-wallet page on which the bank staff is able to process the CBDC-backed stablecoin acquisition and redemption. The table shows the transaction history of the bank.

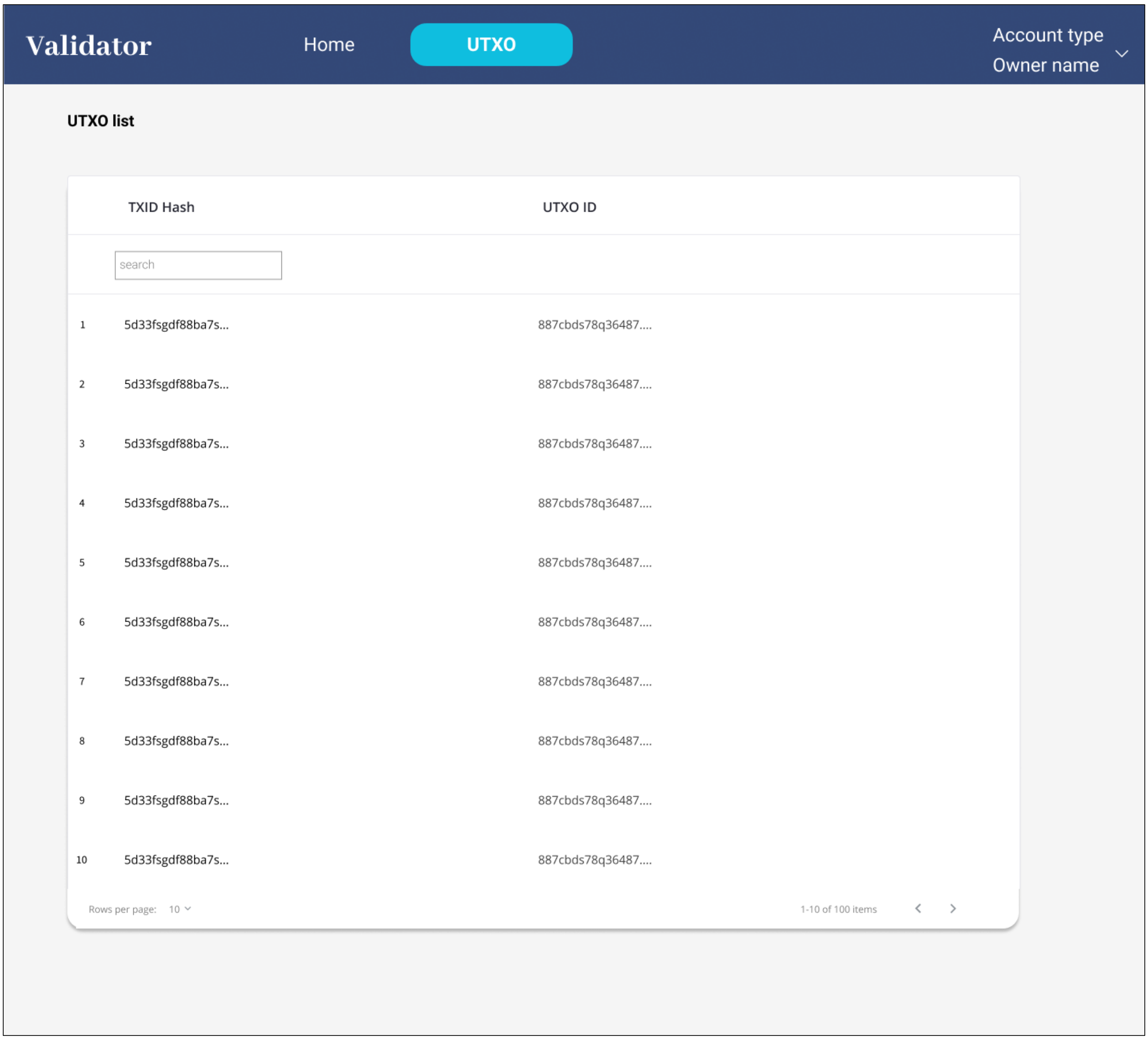


5.3. Validator

Visualisation 7: This is the validator user dashboard on which the validator can see validation/ rejection statistics.

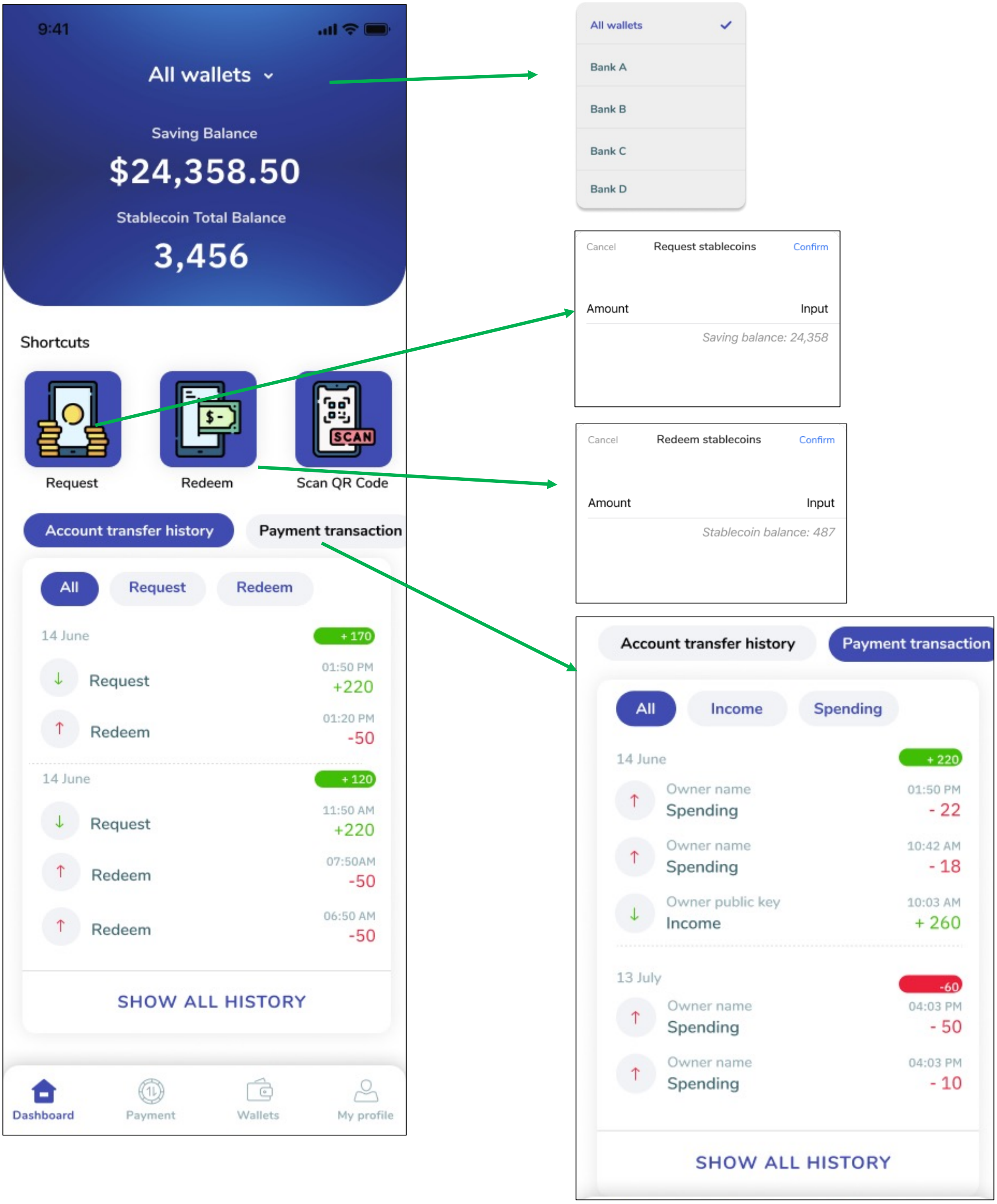


Visualisation 8: This is the validator UTXO list that shows the validated UTXO storage. Clicking each row will show the transaction detail.

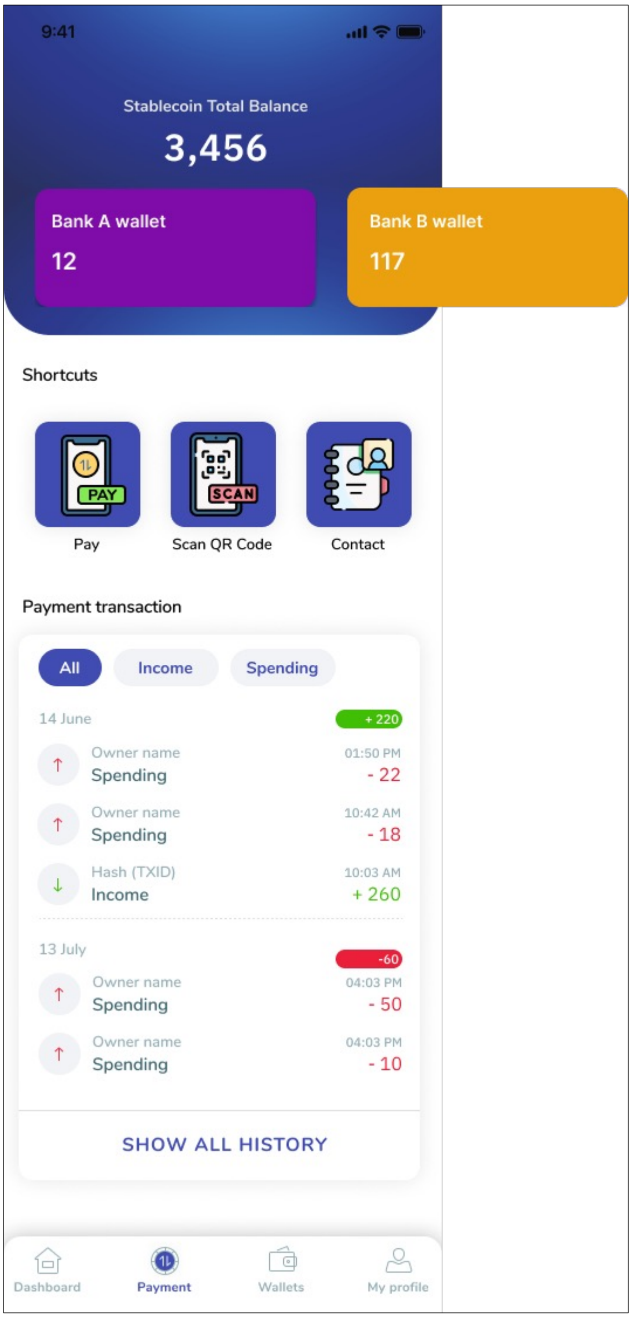


5.4. End-user

Visualisation 9: This is the retail end-user and smartphone-compatible UI, showing wallet balances. This includes the rCBDC request and redeem functions, and the QR code function for payment.



Visualisation 10: On the payment page, the end-user can see shortcuts to the payment process which include pay, scan QR code for payment, and add payee to contact. When the end-user has processed or received payments, all the transactions can be viewed in the transaction list.



Conclusion

Project Aurum was initiated to develop a working prototype that would serve as a public good for the central banking community. Adhering to the principles of safety, flexibility and privacy, Project Aurum has developed a two-tier rCBDC system comprising of a wholesale interbank system and an e-wallet system, in which the validator mechanism helps prevent over-issuance and double-spending.

Project Aurum has made a number of ground-breaking achievements. First, it has implemented two types of rCBDC architecture, intermediated CBDC and CBDC-backed stablecoins after considering trade-offs among different CBDC architectures. Second, the use of UTXO enables the traceability of the tokens to the backing assets, therefore providing safety to end-users in the case of commercial bank bankruptcy. Third, the two-tier architecture provides additional privacy for the end-users as the interbank system does not record any personal data. Lastly, the decoupling of the wholesale and e-wallet systems strengthens the cyber resilience based on the principle of privilege separation and network segmentation, by minimising the interactions between retail and wholesale activities.

We hope that Project Aurum could contribute to the central banking community as a foundation for further study on CBDC.

Glossary

- **Bank:** refers to the commercial bank. There are two types of banks: issuing and non-issuing banks. Issuing banks can issue CBDC-backed stablecoins, whereas non-issuing banks cannot.

- **CBDC-backed stablecoin:** one of the two types of digital currency in the retail e-wallet system. It is issued by an issuing bank and is thus a liability of the issuing bank.

- **CBDC-token:** one of the two types of digital currency in retail e-wallet system. Banks obtain CBDC-tokens from the interbank system through a process called CBDC-token distribution. The CBDC-token is a liability of the central bank. It is also referred to as intermediated CBDC per figure 1.

- **Custodian account:** as explained in 3.1., is an account in the interbank system. It stores wCBDC taken from banks as backing asset when such banks perform CBDC-token distribution or CBDC-backed stablecoin issuance. It is an account shared by all banks.

- **DLT:** acronym for Distributed Ledger Technology/blockchain.

- **End-user:** refers to the commercial bank customer or retail user of the rCBDC.

- **Fiat currency:** refers to the paper cash or physical cash, such as the Hong Kong dollar

- **Issuing bank:** is a commercial bank that is authorised to issue CBDC-backed stablecoins, in the prototype system as shown in figure 6 there are four issuing banks.

- **Non-issuing bank:** commercial banks that are not authorised to issue CBDC-backed stablecoins. In the current prototype, they can request such CBDC-backed stablecoin issuance from one of the four issuing banks.

- **rCBDC:** there are two types of retail e-wallet currency: (a) the intermediated CBDC, also referred to as CBDC-token, and (b) the CBDC-backed stablecoin, also referred to as stablecoin.

- **Redemption/redeem:** refers to the action in which one returns one form of currency to receive the original form of currency in return. For example, a bank first exchanges its wCBDC to issue a CBDC-backed stablecoin. When it eventually redeems the CBDC-backed stablecoin to get back the wCBDC in the wCBDC account, that action is called redemption or redeeming. Another example is for an end-user to redeem a CBDC-backed stablecoin to receive fiat currency in his savings account.

- **RTGS:** acronym for Real-Time Gross Settlement. It refers to a funds transfer system that already exists and allows for the instantaneous transfer of money and/or securities. Each bank has a RTGS account holding fiat currency that it owns.

- **UTXO (Unspent Transaction Output):** the representation for the CBDC-token and the CBDC backed stablecoin. Each UTXO contains input and output.

- **wCBDC:** is the digital currency in the wholesale interbank system. It is issued by the central bank.

- **wCBDC deposit:** refers to the action where a bank transfers wCBDC from its wCBDC account to the custodian account to: (a) receive a CBDC-token distribution from the DLT, or (b) issue a CBDC-backed stablecoin.

- **Validator:** refers to a trusted entity that validates transactions executed by the banks. There are two types of validators: (1) a dedicated validator which is an independent trusted entity, and (2) a DLT validator which is a role performed by an issuing bank which is also a member of the interbank DLT system as shown in figure 6.

Appendix 1: Users and their attributes

The ID of the entities are cryptographic public keys. Each public key has a matching private key. The generation of the keypair is based on the elliptic curve cryptography algorithm.

Central bank	√ **ID:** the central bank is identified through a public key. √ **Mechanism of ID assignment:** Pre-assigned and well-known, meaning the public ID of the central bank is well-known. It is to be generated at the very beginning and before any other operations are performed. √ **Trust-worthiness:** The system assumes 100% honesty on the part of the central bank; hence, the central bank's operation does not need validation by a third party √ **Currency system created and managed by central bank:** The central bank manages the RTGS system.
Banks	√ **ID:** each bank is identified through a public key. √ **Mechanism of ID assignment:** Pre-assigned and well-known. √ **Trust-worthiness:** The system does not assume 100% honesty on the part of the bank; hence, the bank's operation needs validation by the validator.
Validators	√ **ID:** each validator is identified through a public key. There are two kinds of validators, namely, the DLT validator and the dedicated validator. DLT validators are run by issuing banks. √ **Mechanism of ID assignment:** Pre-assigned and well-known. √ **Trust-worthiness:** The system assumes 100% honesty of the dedicated validator. As for a DLT validator, the system assumes it is honest in validating transactions of another bank, but the system also adds measures to countercheck the operation of the DLT validator, such as requiring the issuing bank's signature in addition to the validator signature in the stablecoin UTXO.
End-users	√ **ID:** each customer is identified by a 1 byte bank code + a public key. The purpose for adding a bank code to the ID is to indicate to which bank the end-user belongs. √ **Mechanism of ID assignment:** Requires sign-up to the bank to begin using this ID. √ **Trust-worthiness:** The end-user is untrusted. For the stablecoin operation, all e-wallet transactions must be signed by the issuing bank and validated by the validator. For the CBDC-token, all e-wallet transactions must be validated by the dedicated validator.

Appendix 2: Illegal operations and controls

The Aurum system is designed such that illegal operations can be identified and prevented as shown in the table below.

Illegal events	Commited by	Detected by	Remarks
Bank over-issuance	bank	validator	The validator can detect insufficient balance in bank's wCBDC account to cover the issuance.
Bank double-redemption	bank	validator	The validator rejects duplicate redemption request from the bank.
Bank double-redemption	bank + validator	DLT	Even if the bank and validator are dishonest, the double-redemption can be detected by the DLT system.
Bad end-user signature	end-user	bank	The bank does not accept user transaction without proper signature by respective public key.
End-user double-spending /double-redemption in payment	end-user	bank	The bank does not accept duplicate user transaction.
End-user double-spending /double-redemption in payment	end-user + bank	validator	Even if the bank and end-user are dishonest, the validator does not accept duplicate transaction.

Appendix 3: Complexities and solutions

Architecture

Complexity of two-tier CBDC architecture	Due to the two-tier design, an e-wallet transaction may be lengthy and may trigger interbank transactions. Hence, the protocol becomes lengthy and complex, especially with the need to handle exceptional cases.	**Current solution:** Since this is a necessary complexity to support the required system features, we developed and tested code to verify that such operations are processed correctly.
Complexity of the stablecoin operation	A transaction may involve stablecoins of multiple issuing banks, increasing the complexity of processing. Each transaction may involve sending multiple UTXOs to different banks for processing.	**Current solution:** We developed code to ensure correct handling when some of the UTXO processing fails. We simulate such failure cases with schemes such as bringing down validator and UTXO with bad signature.

Security

UTXO traceability	The traceability of an UTXO requires the storage of the whole chain of transactions, starting from the coinbase (issued UTXO) up to the UTXO. The chain may be long and hence increasing both the chain transmission time and the storage size.	**Current solution:** The bank server will send the chain to the requestor one segment at a time, so the requestor can see the segment quickly. **Solution for consideration:** It is possible to consider forcing the redemption of the UTXO for a long UTXO chain.
DLT processing overhead	DLT is utilised in the interbank system to ensure the security and reliability of transactions. However, as DLT processes transactions of each account serially, it processes one transaction per account, per block time.	**Current solution:** The transaction rate is increased by dividing each account into sub-accounts. Hence, DLT can process transactions of these sub-accounts in parallel.
Mutual checking between the stablecoin issuing bank and the validator	Stablecoin transactions need to be signed by both the issuing bank and the validator. This increases the processing overhead of such stablecoin transactions.	**Solution for consideration:** If the validator can be fully trusted, the requirement for the issuing bank's signature can be waived. This would reduce processing overhead.

Processing overhead

Storage of UTXO of end-users	An end-user phone device has limited storage capacity and may not be suitable to store copies of all of the end-user's UTXOs.	**Current solution:** The current design is for the end-users to store all their UTXOs in their bank servers. **Solution for consideration:** If the end-user desires to keep all the UTXO copies and all the relevant UTXO chains, a solution may be introduced in the future such that the end-user may redeem all his UTXOs and replace it with a single UTXO.
Signature signing and verification	Signature signing and verification have high overheads. Different processors have different levels of capability to perform such operations.	**Current solution:** We selected a cryptographic library that allows a specific make of CPU to achieve a higher signature processing rate. **Solution for consideration:** Use servers with CPUs capable of higher signature processing speeds.
Database server	The bank server originally used a network-based SQL database server to store client wallet information but found that access latency was high.	**Current solution:** The bank server uses a local file-based database instead of a network-based database server. **Solutions for consideration:** Using high speed networks between bank servers and network-based database servers. Using high-performance network-based database servers and database sharding techniques.

Management of large pool of UTXO	As there are large amount of UTXOs to be maintained by bank servers and validator servers, the search for the specific UTXO and the fields of the UTXO (eg input & output) will be lengthy.	**Current solution:** Multiple database tables are created for different search purposes. For example, one table is created with UTXO ID as the search key, another table with UTXO output as the search key. This results in a larger database in exchange for faster processing.
Large number of end-users	Banks are expected to process transactions of a large number of end-users simultaneously. Hence, parallel processing should be optimised to support this.	**Current solution:** Design databases such that different end-user wallets in bank servers are separated from each other and can be updated in parallel. Other similar measures are also adopted in other processing. **Solution for consideration**: Improve horizontal scalability by adding load balancing servers to the system to provide better parallel processing.

Bank for International Settlements (BIS)