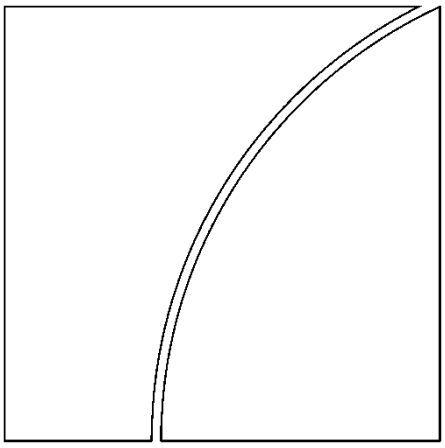
BIS

BIS Consultative Group on Innovation and the Digital Economy (CGIDE)



Report

A proposal for a retail central bank digital currency (CBDC) architecture

December 2024

BIS Representative Office for the Americas

This publication is available on the BIS website (www.bis.org).

ISBN 978-92-9259-825-9 (online)

Table of contents

Foreword

Central bank digital currencies (CBDCs) are a direct liability of the central bank which can be seen as a new digital payment instrument. They entail the development of new public infrastructure that offers multiple technical options and functionalities. They can be intended for use by households and businesses (retail CBDC) or for transactions by financial institutions (wholesale CBDC). This report focuses on the former. Potential roles for a retail CBDC, based on individual jurisdictions' policy objectives, include increasing financial inclusion, fostering innovation in financial services, enhancing the efficiency of domestic payment systems, responding to reductions in cash usage and more.

As each central bank explores the features that are most relevant for the policy goals of their own jurisdiction, it can be helpful to share experiences with peer institutions. This may be particularly relevant in the light of future interoperability between CBDC systems and other payment systems. In this context, this report introduces a proposal for a retail CBDC architecture. The proposal aims to serve as a basis to develop functional CBDC solutions, potentially working as a reference for member central banks in the Americas and around the world.

The Consultative Group on Innovation and the Digital Economy (CGIDE) was launched in February 2020 to meet the demand for greater cooperation in technological innovation and the digital economy by BIS member central banks in the Americas. It reports to the Consultative Council for the Americas (CCA), which brings together the central bank Governors of Argentina, Brazil, Canada, Chile, Colombia, Mexico, Peru and the United States (Board of Governors of the Federal Reserve System and Federal Reserve Bank of New York). This group provides a forum where senior central bank officials can cooperate towards the following objectives:

a. Analysing and developing public technological infrastructures geared towards tackling common shortcomings in all participating jurisdictions.

b. Promoting an environment suitable to open banking, potentially through the development of key application programming interfaces (APIs).

c. Analysing the implications of these public technological infrastructures in terms of market structure and regulatory implications.

The design proposed in this report represents one possible approach to the design of a CBDC. It acknowledges that different central banks and initiatives, including those by CGIDE members, may adopt alternative models tailored to their specific policy objectives and regulatory frameworks.

This report was prepared by a technical task force of central bank experts who participate in the CGIDE, which was launched in May 2022. Its main purpose is to open a conversation around technical considerations in the design of a CBDC. The report seeks feedback from central banks and the public on the proposal for a retail CBDC architecture. It also aims to serve as a useful general reference for central banks conducting research on CBDC or seeking to develop their own CBDC initiatives. Comments are welcome and should be addressed to americas@bis.org.

Othón Moreno	Renato Dias de Brito Gomes	Alexandre Tombini
Chair of the Technical Task Force	Chair of the CGIDE	Chief Representative for the Americas
Bank of Mexico	Central Bank of Brazil	Bank for International Settlements

Executive summary

As central banks explore retail central bank digital currencies (CBDCs), there is value in sharing experiences and working together on a proposed retail CBDC architecture. This architecture defines how a CBDC will be issued and circulated, and what roles the central bank and the private sector will play in operating the system. The choices around these items must flow from public policy considerations and user needs in a CBDC system. The early design choices made could have important consequences for the operation of a CBDC at a later stage, so it is crucially important to discuss these and get them right.

The Consultative Group on Innovation and the Digital Economy (CGIDE) launched a technical task force (TTF) in May 2022 to create a proposal for a retail CBDC architecture, guided by high-level technical requirements endorsed by CGIDE members. The TTF aims to deliver three outputs: (i) a definition of high-level technical requirements to identify core functionality and necessary elements; (ii) a business-level flow diagram for the core functionality; and (iii) a technical-level flow diagram with infrastructure components for CBDC implementation. This report is part of deliverables (ii) and (iii).

The proposed retail CBDC architecture is based on the *High-level technical requirements for a functional CBDC architecture* published by the CGIDE in December 2023. In that report, the CGIDE highlighted key requirements in five categories: (i) modular design; (ii) core functions; (iii) operational requirements; (iv) cyber resilience requirements; and (v) requirements related to third-party services.

This report discusses four main processes in the CBDC architecture: enrolling new users, creating CBDC, destroying CBDC and intra-ledger transfers. Enrolment involves user registration on the CBDC platform by creating a CBDC wallet. This occurs through a wallet application (on a smartphone app, feature phone interface or hardware) designed to display CBDC balances, initiate and receive transfers (to/from other wallets, the real-time gross settlement (RTGS) system or cash) and receive transaction notifications. Creating CBDC involves converting commercial bank money into CBDC, increasing balances in a user wallet registered on the platform through transfers from an account in the RTGS system or exchanges with local currency. Destroying CBDC is the opposite process: CBDC is withdrawn from the platform and converted back into balances in a commercial bank or other account, or cash, decreasing the balance in a CBDC wallet. This is done through deposits to an RTGS account or as cash withdrawals. The intra-ledger transfers involve movements of a certain value of CBDC from one wallet to another within the platform.

The architecture that this report lays out is for a hybrid model which allows for the division of labour between the central bank and private intermediaries. It allows for tiered know-your-customer (KYC) facilities, with wallets that use stricter KYC for individuals and businesses with higher transaction limits, and more basic wallets with simpler KYC requirements for more limited transaction sizes. Privacy can be guaranteed by separating transaction from identity information, such that the latter remains with private intermediaries and users. This helps to reduce risks and ensure greater privacy protections than in other models. The report lays out an operational workflow (with flow diagrams) for the four main processes that can guide the development of these functionalities in practice, by central banks or vendors.

As the CGIDE moves forward, several key technical questions arise for further exploration. For instance, how can the balance between centralised operation and decentralised access be optimised to ensure both security and accessibility? How can privacy be further protected while ensuring compliance with anti-money laundering (AML) and KYC regulations? To address these and other technical questions, the CGIDE will evaluate the potential of tokenisation and the development of integrated financial ecosystems where tokenised deposits and CBDCs coexist. This remains an important area for further work by central banks to help advance the development of payment and financial systems.

The report does not represent a policy position of CGIDE members and observers on the design, issuance or adoption of CBDC, or on technical standards for CBDCs. Instead, it is offered as a public good to advance the work on these issues and to share insights from a group of experts in the Americas region.

Introduction

Examining the technical features of central bank digital currencies (CBDCs) is crucial as central banks progress in their exploration of this new digital payment infrastructure. The design choice should align with clear policy objectives of each jurisdiction, depending on the local context and market requirements. Currently, some central banks are focusing work on retail CBDCs, some on wholesale CBDCs and some on both. Here, we focus on the former. Potential roles for a retail CBDC, based on varying policy objectives, include increasing financial inclusion, fostering innovation in financial services, enhancing efficiency of domestic payment systems and responding to a reduction in cash usage. The definition of these objectives might also determine the retail CBDC design, associated with central banks' approach to user data privacy, access, anonymity and individual protections and rights, CBDC remuneration and quantity and transaction limits, the division of responsibilities between the public and the private sector and the inclusion of broader features such as programmability and offline capabilities. The technology solutions available to jurisdictions should be evaluated considering how well they can contribute to achieving policy objectives.

The CGIDE published a report on high-level technical requirements for the design of the business diagrams of a retail CBDC architecture in December 2023 (BIS CGIDE (2023)). These technical requirements aim to address the main central bank concerns related to interoperability, scalability, user-centric design, security and data privacy, which are foundational to retail CBDC initiatives.

The proposed retail CBDC architecture aims to build on this and serve as a general reference for central banks conducting research on CBDC or developing their own initiatives. As used in this report, an architecture is defined as the design, issuance and distribution of a retail CBDC to end users, as well as the roles that the central banks and the private sector will play in operating this system. The report does not represent a policy position of CGIDE members and observers on the design, issuance or adoption of CBDC, or on technical standards for CBDCs more generally. Instead, it is offered as a public good to advance the work on these issues and to share insights from a group of experts in the Americas region.

This report has three sections. Section 1 describes some of the technical design approaches for a CBDC system. Section 2 briefly summarises the main technical design considerations agreed by the CGIDE for the proposed CBDC architecture. Section 3 presents and describes the main business diagram of the CGIDE's proposal for a CBDC architecture.

1 CBDC technical design approaches

The design of a CBDC should focus on promoting central banks' public policy goals and fulfilling users' needs. Different technical designs can align with public policy objectives of increasing financial inclusion, improving the efficiency and security of domestic payment systems, promoting low cost and greater accessibility, enhancing processing speed, increasing privacy and introducing additional functionalities such as programmability and offline payments. A focus on users' needs is very much complementary, targeting ease of use, low or no cost, high standards of privacy and data protection and integration with other payment instruments. This can guide key CBDC design choices, which typically involve the operational architecture, data management and access technology that will be used in a CBDC system (see Auer and Böhme (2020) and BIS Innovation Hub and Hong Kong Monetary Authority (2022)). Finally, the design could consider mimicking current physical means of payment (ie banknotes and coins) for easy and organic adoption by households and businesses.

A crucial choice in the architecture design is how the CBDC will be issued and circulated, and what roles the central bank and the private sector will play. One option is a direct model, where the CBDC represents a direct claim on the central bank, which maintains a record of all balances and updates them with each transaction. The central bank would handle all functions in the payment system, from issuing

the CBDC to distributing it and interacting with end users. A direct CBDC could eliminate reliance on intermediaries as it would entail a ledger fully operated by the central bank. However, this model would require substantial operational and technical capacity and potentially involve direct customer onboarding complying with KYC regulations by the central bank. There could also be a potential long-term impact on innovation associated with this model due to reduced competition and limited private sector involvement. Most central banks have therefore chosen not to pursue this model.

In a two-tier or indirect model, the central bank relies on private sector participants as intermediaries, which act as gateways between individual CBDC users and the CBDC system. This model is like today's financial system where commercial banks provide money to end users in the form of deposits. Customers have a claim on intermediaries, while the central bank only keeps track of wholesale accounts. Gateway service providers are crucial and perform various functions from operating the CBDC core system infrastructure to offering customised end user services. This model relieves the central bank of responsibilities such as dispute resolution and KYC activities. However, the central bank cannot maintain a record of individual claims, and there is no direct, cash-like proof of claims.

These models are not mutually exclusive, and central banks are also considering intermediated or "hybrid" models. In a hybrid model the issuance of the CBDC is a direct claim on the central bank and it keeps a full ledger of transactions (often without any user identity information), but some functions are delegated to intermediaries. This intermediate solution can vary depending on how functions are distributed between the central bank and private intermediaries. For example, the central bank could own the technical system necessary for a specific function, while the private sector executed the function (IMF (2022)). This model might offer better resilience than an indirect CBDC but requires more complex infrastructure for the central bank including interlinking with intermediaries' infrastructures. Yet the hybrid model is easier to operate than a direct CBDC and preserves the private sector's primary role in retail payments and financial intermediation. Of course, it also increases dependencies in the operational model on multiple participants, depending on the number of intermediaries enabled.

Data management infrastructure can be based on either a conventional centralised database or on distributed ledger technology (DLT). In a centralised model, transaction data are stored across multiple physical nodes controlled by one central entity. Again, identity information can be kept separately, eg by financial intermediaries to maintain privacy of transactions. In contrast, DLT systems allow the ledger to be jointly managed by different entities in a decentralised manner. In such systems, each ledger update must be harmonised among all entities' nodes through consensus mechanisms. There are practical challenges in reconciling the decentralised nature of DLT with the need for the central bank to maintain control of core CBDC infrastructure. Both DLT-based systems and conventional databases have drawbacks: the main drawback in a conventional architecture is the risk of failure of the central node, while in a DLT model it is the operational overhead of consensus mechanisms and reliability of technology. In either case, redundancy and replication of nodes are alternatives to tackle this particular vulnerability.

Another important consideration for central banks is the access technology for the CBDC. One option is an account-based model, where ownership is tied to an identity and claims are recorded in a database. The second option is a token-based model, where access and claims require users to know a private key and meet identity requirements. In this model users employ a cryptographic unique alias as their identity in CBDC transactions. While a token-based model can ensure broader access via digital signatures, it carries high risks of funds loss if users fail to keep their private key secure.

The design of a retail CBDC architecture should also consider safety, efficiency, openness to innovation, competition and interoperability. Safety involves ensuring the security, availability, privacy preservation, resiliency and robustness of the CBDC system. An efficient CBDC architecture provides fast and scalable payment solutions while keeping costs low. Openness to innovation is crucial to allow the system to evolve with the changing needs of users and central banks, and competition is crucial to ensure that the market remains efficient and innovative over time. This means the CBDC infrastructure should be modular, scalable and flexible to enable central banks to implement different models according to their

specific context and accommodate additional participants and new technological developments (BISIH and HKMA (2022)). Interoperability with other payment systems and agreements (eg fast payment systems (FPS)) is also key but remains at initial stages and faces challenges. For instance, interoperability between FPS and CBDC systems may require using common components such as address resolution services (World Bank (2024)).

Examples of current CBDC projects and experiments already launched and under evaluation by central banks worldwide include the Sand Dollar (Bahamas), JAM-DEX (Jamaica), eNaira (Nigeria), Project Aurum (Hong Kong SAR), e-CNY (China) and e-krona (Sweden). In July 2024, the Central Reserve Bank of Peru announced a CBDC pilot led by Bitel – a mobile network operator – focused on unbanked people and with offline capabilities (Box A). The main technical design features of these prototypes and live CBDCs are summarised in Table 1.

Main design features of CBDC projects and live CBDCs Table 1

		Operational architecture (direct, indirect or hybrid)	Data management (centralised or distributed model)	Access technology (account- or token-based)
Live CBDCs	Jurisdiction			
Sand Dollar	The Bahamas	Hybrid, where the central bank manages the issuing, validation and settlement ledgers	DLT system with identity infrastructure owned by the central bank	Token-based
JAM-DEX	Jamaica	Hybrid	Centralised model controlled by the central bank	Token-based
eNaira	Nigeria	Hybrid, with transactions handled and recorded by a system owned by the central bank	DLT system	Account-based
CBDC projects and experiments underway				
Project Aurum	Hong Kong SAR	Hybrid	Wholesale system built on DLT and retail built on a server-based system	Token-based
e-CNY	China	Hybrid, with the central bank owning and managing the issuing ledger	Hybrid architecture, where DLT is used only in limited areas	Account-based
e-krona	Sweden	Hybrid, where the central bank manages the issuing and validation ledgers	DLT system	Token-based
CBDC pilot	Peru	Hybrid	Hybrid/shared model where the participant shares anonymous data with the central bank	Account-based

Sources: IMF (2022); central bank websites.

Box A

Peru: a retail CBDC pilot designed to expand digital payments with offline capabilities

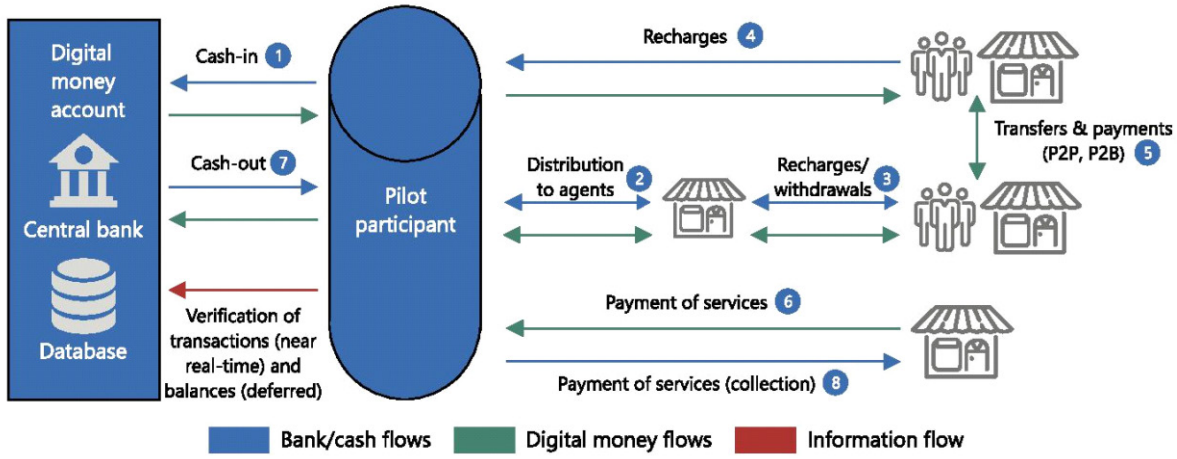
The Central Reserve Bank of Peru (BCRP) has made progress in exploring a retail CBDC. With technical assistance from the International Monetary Fund (IMF) since 2021, the BCRP published a white paper on the implementation of a CBDC in March 2023. The document highlighted the context, goals, challenges, target population, potential use cases and key design features for a CBDC in Peru.

In April 2024, the BCRP issued a regulation for retail CBDC pilots (Circular No. 0011-2024-BCRP) and launched a call for the private sector to participate in the first pilot. Some aspects to be considered by the interested institutions include: (i) offline payment functionality; (ii) fostering access to digital payments among the unbanked population; and (iii) non-interest bearing accounts, among others. Interested parties should also evaluate user experience and enrolment schemes, analyse the substitution effect between cash and CBDC, and evaluate the sustainability of business cases of digital cash distribution companies, among others.

In July 2024, after an exhaustive evaluation of the applications the BCRP selected the Vietnamese mobile network operator Viettel Perú S.A.C. (commercially known as Bitel) to lead the first CBDC pilot in Peru. Bitel's proposal was aligned with the specific objectives of the pilot, design and characteristics established in the regulation. Bitel has 7 million users in Peru, 2.5 million of which are in low-inclusion (eg rural) areas. Furthermore, Bitel has already registered a digital wallet application, BiPay, which will be used for the distribution of CBDC to end users in both online and offline contexts. This pilot will last one calendar year, which may be extended for up to one additional year, upon justified request.

The pilot is designed as a hybrid model, in which the central bank will provide CBDC (including RTGS account, issuance and monitoring modules) while the participant delivers user-facing services (eg distribution of CBDC among end users, KYC, digital wallet interface, payment services, account register). Graph A1 gives an overview of the design.

Design of the first pilot led by Bitel — Graph A1



Source: Vega and Andia (2024).

The first pilot will work as follows. First, the participant (Bitel) must deposit funds in the CBDC account at the BCRP (cash-in). In this stage, CBDC is issued for a value equal to the value of the funds received. Then, the participant is allowed to distribute CBDC to the agents and end users (ie individuals and businesses). The latter can recharge their CBDC accounts either by delivering cash to agents or through a deposit account (directly to the participant). Then, end users can make person-to-person (P2P) and person-to-business (P2B) payments, including utility payments and others associated with companies affiliated with the participant. When the participant converts CBDC into bank money, this reduces money from the CBDC ecosystem. Finally, with the funds obtained, the participant makes payments to the companies for whom it provides collection services (eg utility companies).

To strengthen the protection of end users' funds, the regulation established that the participant must maintain at the BCRP a balance at least 2% higher than the sum of the balances of the CBDC held by end users. Also, the participant must have a letter of guarantee for a value of PEN 500,000 (USD 130,000) from a bank with a rating of A+ or higher.

Two-factor authentication and secure session termination will also be applied. The participant is also required to implement the International Organization for Standardization (ISO) and International Electrotechnical Commission (IEC) 27001 standard on information security management during the pilot. This standard ensures that the participant establishes effective controls and commits to continually improving the security of end users' data.

In addition, the BCRP will receive anonymous transactional data in near real time and balances in CBDC accounts twice a day. To receive these data from the participant, the BCRP will establish a secure communication link using site-to-site virtual private network (VPN) and end-to-end encryption as an essential cyber security measure to protect information transmitted between the participant and the BCRP. Also, the BCRP will develop an application programming interface (API) infrastructure based on representational state transfer (REST) using microservices to handle participant authentication and information reception. The data will be stored in centralised databases within the BCRP, facilitating efficient monitoring and backup of the CBDC ecosystem.

The pilot will develop offline capabilities. The participant will implement an unstructured supplementary service data (USSD) solution for those users who do not have a smartphone or access to mobile data. This technology will allow customers to communicate with others on Bitel's network, without the need for a smartphone, mobile application or mobile data, as a long as the end user is in an area with at least 3G coverage. USSD technology will be particularly relevant in rural and remote areas where other banking access points are unavailable or costly, but where the participant's network coverage is widespread.

The USSD solution will implement various security measures. For example, universal subscriber identity module (USIM) cards to connect to the 3G/4G network. These cards use stronger algorithms than the SIM cards used in 2G networks. All USSD messages will be encrypted and packaged at the internet protocol (IP) layer. Other security measures include speed verification and enforcement of limits on USSD requests.

2 Key design considerations for the proposed CBDC architecture

The proposed retail CBDC architecture is based on the *High-level technical requirements for a functional central bank digital currency (CBDC) architecture* published by the CGIDE in December 2023.[1] The main technological considerations for the proposed architecture include:

- Hybrid model: the central bank provides the core CBDC infrastructure (eg issuance, settlement and governance modules), while the private sector delivers user-facing services. The core platform enables both the private sector and the central bank to build modular functionalities on top of it using APIs.
- Flexible approach: this approach considers alternatives to a fully centralised model, allowing for the integration of permissioned ledgers that exhibit some decentralisation (eg distributed transaction validation and node participation from regulated financial institutions). It aims to balance centralised control with broader access for specific institutions.
- Token-based model: this model offers an extensive and flexible programmable infrastructure, facilitating the use of smart contracts and atomic settlement. The architecture would support innovative solutions that maintain the benefits of tokenisation while ensuring sound identification practices. However, the architecture proposed in this report is generic in order to allow that an account-based model can be used with minimal changes.
- Modular framework: a flexible framework that supports either a pre-existing settlement mechanism or a newly developed one, accommodating the evolving needs of different jurisdictions regarding policy, legal, regulatory and governance considerations.

[1] The document is available at www.bis.org/publ/othp82.pdf (last access on 31 July 2024).

– Privacy safeguards: evaluation of different technological options to protect privacy and minimise personal data exposure, such as data aggregation, encrypted data processing and data minimisation.

– User-centric design: a focus on meeting the needs, preferences and usability requirements of end users.

– Scalable model: a design that efficiently handles a high volume of transactions.

These considerations are priorities for CGIDE members and align broadly with international experiences in the design and implementation of retail CBDCs. The technological requirements of interoperability, cross-border payment functionalities, risk management and business continuity are also crucial for a comprehensive CBDC architecture. These requirements will be addressed in future stages of the project by the CGIDE.

3 Description of the proposed CBDC architecture

The implementation of a CBDC involves a complex interplay of processes, participants and information flows to ensure a secure, efficient and user-friendly system. This chapter outlines the key processes involved in the operation of a CBDC platform, including user enrolment, creation and destruction of CBDC and intra-ledger transfers. Additionally, it details the chronological steps that users and intermediaries must follow, highlights the main participants in the CBDC ecosystem and describes the relevant information flows that support the functionality of the platform.

The key participants of the infrastructure are:

– Central banks: which provide the core CBDC infrastructure and governance.

– Intermediaries: financial institutions and certified third parties that offer user-facing services and perform necessary regulatory verifications (KYC, AML).

– End users: individuals or businesses using the CBDC for transactions with a variety of purposes.

– Third parties: private sector participants that offer IT services or software applications required by the final users.

Graph 1 illustrates the basic CBDC architecture diagram. The main components are:

– Core CBDC components: the set of scalable services that provide the base methods for the management and administration of the CBDC platform.

– Database CBDC: the data storage for the recording of transactions, wallet data, identification of participants and third parties, etc.

– CBDC Type 2: a token-based model, where access and claims require users to know a private key and meet identity requirements. It could be a CBDC Type 1, that is, an account-based model, where ownership is tied to an identity (even if held by a private intermediary, not the central bank) and claims/transactions are recorded in a database, but this could easily be achieved by showing only the balance to the users, and not the token itself.

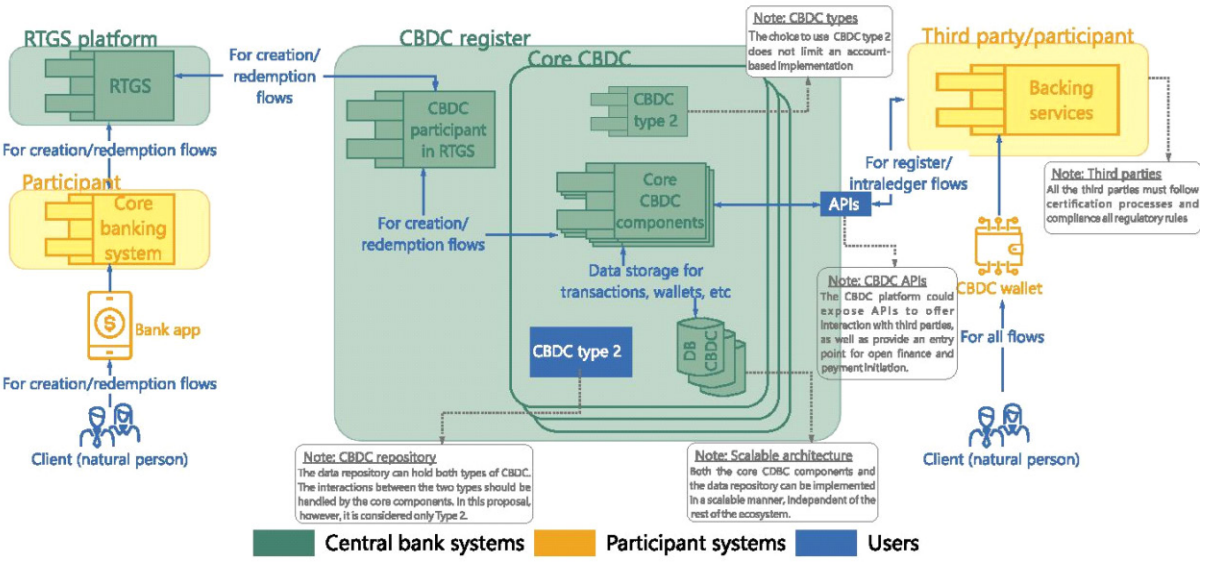
– RTGS: a continuous process of payment settlement on an individual order basis without netting debits and credits. This can occur in an RTGS system.

– CBDC participant in the RTGS system: in order for CBDC participants to receive funds from their corresponding RTGS account, the CBDC platform must be registered as a client of the same RTGS system.

– Participant core banking: the core system of a participant that provides banking services to its customers.

- Banking app: the application that a participant offers to its customers, in order to provide them with banking services. These apps are usually designed for smartphones and in some cases may include services associated with wallet application functionality.
- API: a software component that defines a set of rules in order to enable different software entities to communicate with the CBDC platform.
- Third-party backing services: the core system services of a third party to provide the services to its customers.
- CBDC wallet: an interface (eg app, hardware) that allows individuals to send and receive CBDC.

CBDC basic architecture diagram — Graph 1



Source: Authors' elaboration.

3.1 Main processes in the CBDC architecture

This section discusses four main processes in the CBDC architecture, namely the enrolment of new users, creation and destruction of CBDC, and intra-ledger transfers.

3.1.1 Enrolment

Users register on the CBDC platform by creating a "CBDC wallet" through an intermediary. In some jurisdictions this process may occur through a dedicated wallet application. This is a specialised application (smartphone app, feature phone interface or hardware) that is designed to display CBDC balances, initiate and receive transfers to/from other wallets, the RTGS system or cash, and receive transaction notifications. In particular, when the user is already a client of the intermediary, the KYC process has already been done and it is not necessary to do it again.

Personal information is required by certified third parties during the registration process. As with opening a bank account, this can involve eg a government-issued identity document or phone number to ensure compliance with AML and KYC regulations. Yet once this is collected, it should be kept private.

Depending on the jurisdiction, these verifications can be performed inside or outside the wallet application. Graphs 2.A and 2.B illustrate the enrolment complying with KYC requirements ("KYC-

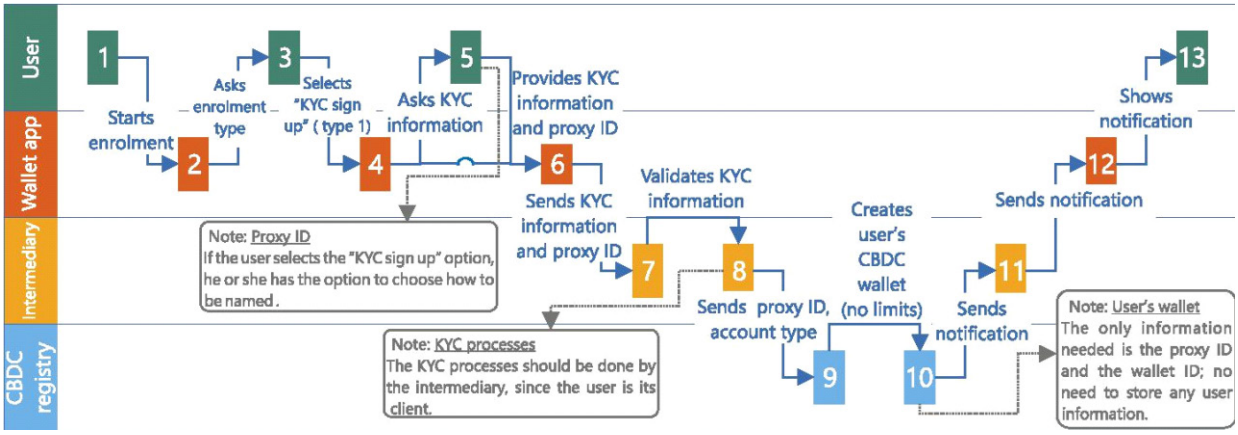
compliant") and anonymously, respectively. Like bank and transaction accounts today, the information could be kept private by the intermediary.

The main steps of the (generic) user enrolment process are as follows.[2] First, the user logs into the wallet application, either anonymously or using the KYC mechanisms provided by the intermediary. In the first case, a random proxy ID is generated. In the second, this proxy ID is provided by the user. Then the intermediary receives the request to enrol a user, and in the case of a non-anonymous customer, uses its KYC mechanism to validate the customer's identity. Next, a request is sent to the CBDC registry to create a CBDC wallet, either anonymous (in which case there are limits to the amount of currency that this wallet can transfer or hold) or owned by a user (in which case there may be higher or no limits). Finally, a notification is sent back to the user through the intermediary and the corresponding wallet application.

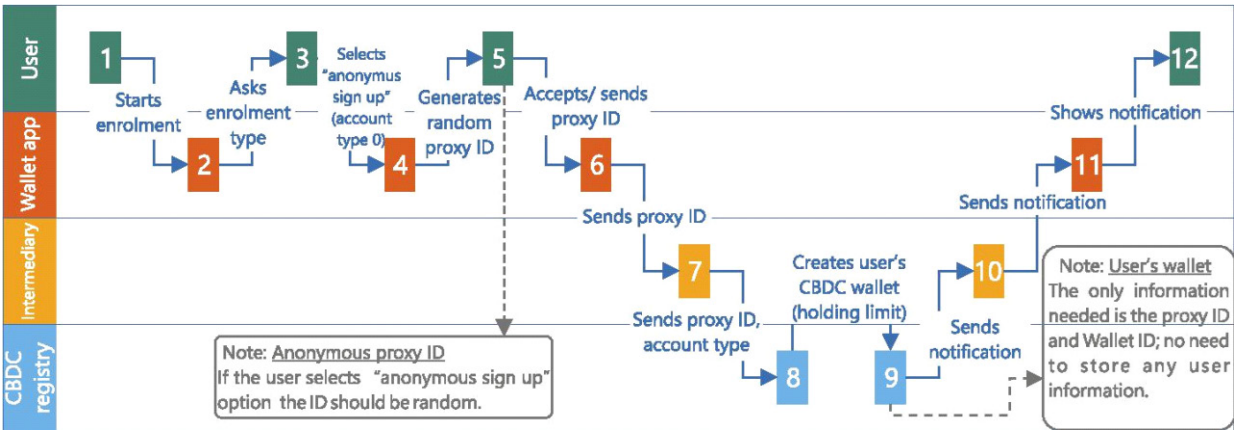
User enrolment in the CBDC

Graph 2

A. KYC-compliant wallet



B. Basic wallet



Source: Authors' elaboration.

[2] For the sake of simplicity, we assume here that KYC is done inside the wallet. Since the wallet is built by the participant and is intended to be built inside the banking app, here we draft only one of many paths where the KYC processes could be applied. Of course, every participant should apply these processes in line with the rules of their jurisdiction.

3.1.2 Creation of CBDC (cash-in process)

The next key process involves converting commercial bank money into CBDC tokens. This means increasing the balance in a user wallet registered on the platform through transfers from the client bank account to an account in the RTGS system or exchanges with local currency.[3] Graphs 3.A, 3.B and 3.C illustrate the CBDC creation process.

The process begins when the intermediary orders CBDC creation. With this, the operator requests the exchange of local currency for CBDC, through a funds transfer from the intermediary's account to the CBDC participant's account (wallet) via the RTGS system. The RTGS system sends a payment notification to the CBDC participant, which in turn instructs the CBDC registry to credit CBDC to the intermediary's CBDC wallet. Once the intermediary has established its CBDC wallet, users can request the CBDC cash-in with the following procedure. Users have to have a previously registered wallet, either named (with the corresponding KYC process) or anonymous. Also, they should have access to a wallet application provided by the financial intermediary that holds the user's bank account (for the first case) or a cash interface (for the second case).

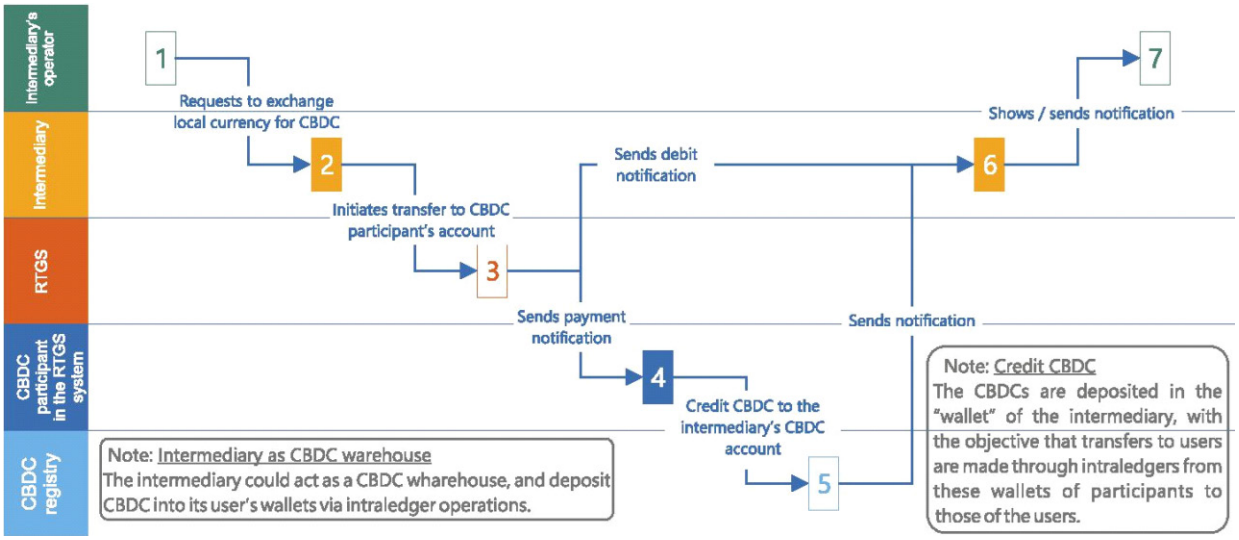
The main steps of the creation process are as follows. The user, either via a cash interface or the wallet application provided by the financial intermediary that holds the user's account, instructs the exchange of local currency for CBDC, by sending the amount to exchange and the proxy ID of the destination CBDC wallet. At this point, the intermediary could reserve the amount to exchange, from the user's account (in case it is a named wallet) to prevent an overdraft. The intermediary, after complying with AML processes, instructs the allocation of CBDC on behalf of the user. Within the CBDC registry, the amount of CBDC will be withdrawn from the intermediary's wallet, and deposited into the user's wallet once a limit validation has been performed. Finally, a notification is sent back to the user, via the intermediary and the corresponding wallet application or cash interface. At this point, the intermediary should debit the user's account for the value exchanged.

[3] One possibility is to initiate the transfer from a bank account into the CBDC platform via the RTGS system, but in this proposal the flow is to transfer from a user's bank account to a special account belonging to the intermediary (so it is an intrabank transfer), and then for the intermediary to instruct a transfer from their own account in the RTGS system to the CBDC account in the RTGS system (but not necessarily in that order). So, in order to generalise, we use the term "account in the RTGS system" and leave the details to the case in question.

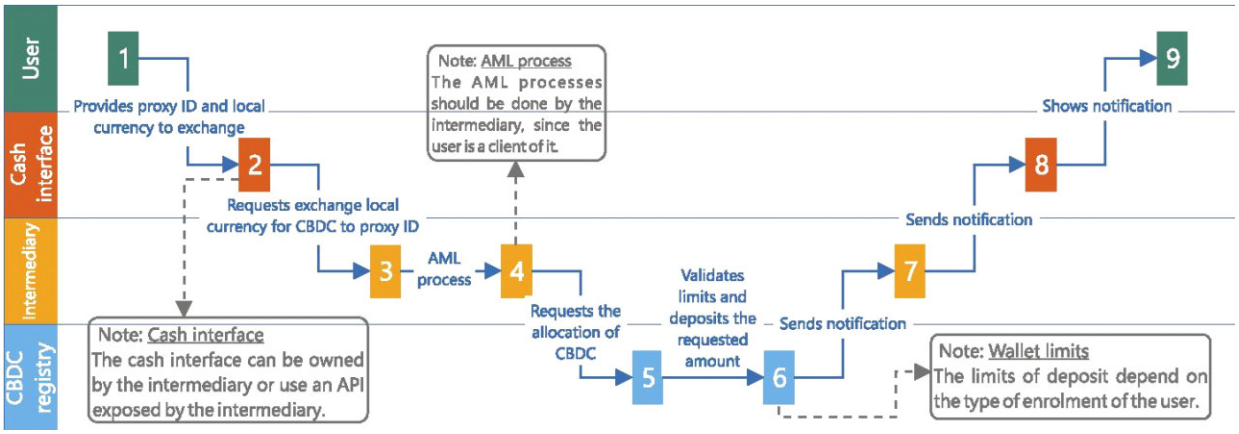
CBDC creation process

Graph 3

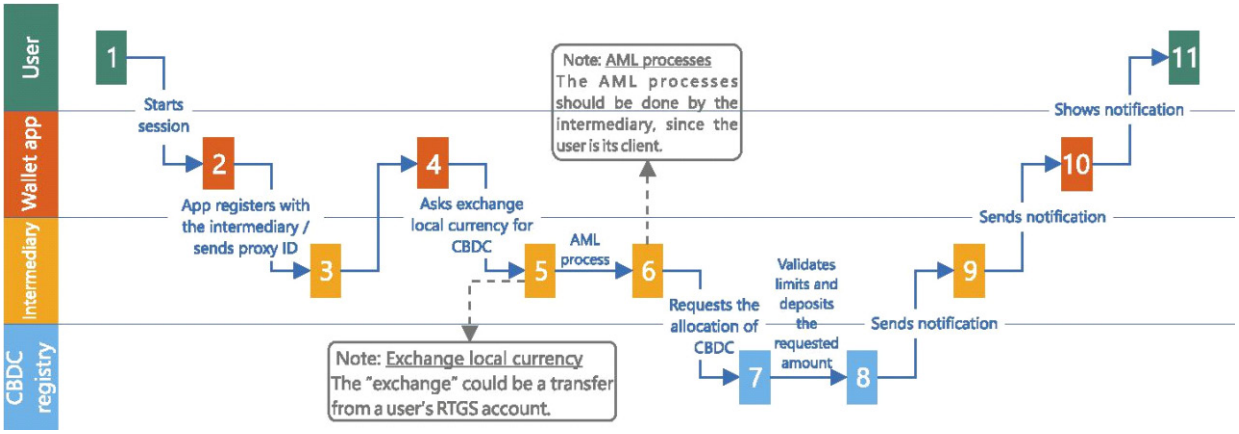
A. From the intermediary's point of view



B. Exchange local currency for CBDC



C. Load from the user's bank account



Source: Authors' elaboration.

3.1.3 Destruction of CBDC (cash-out process)

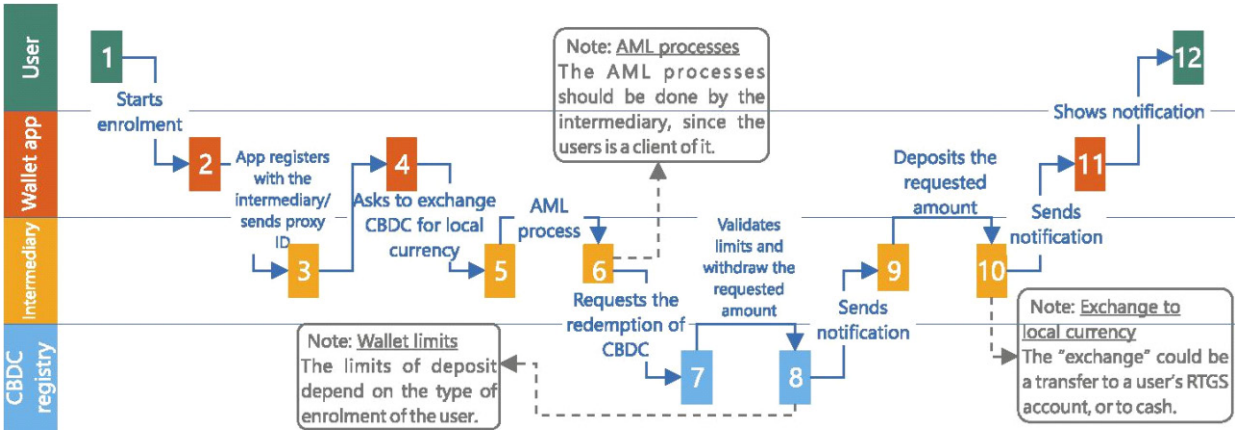
In this process, CBDC is withdrawn from the platform and converted back into balances in a commercial bank or other account, or cash. This decreases the balance in a CBDC wallet. Graphs 4.A and 4.B show the cash-out process.

The main steps of the CBDC destruction process are as follows. Users have to be previously registered to a wallet, which is either named or anonymous (with the corresponding KYC process for each). They should also have access to a wallet application provided by the financial intermediary that holds the user's bank account or a cash interface. The user logs into the wallet application (which in turn requests registration with the intermediary according to the defined policies and procedures) and instructs the exchange of CBDC for local currency, by sending the amount to exchange and the proxy ID of the originating CBDC wallet. After complying with AML processes, the intermediary requests the withdrawal of the given amount from the user's wallet. Then, the CBDC registry performs the required validations according to the user's enrolment type, withdraws the amount requested from the user's wallet and deposits it in the intermediary's wallet. It then notifies the intermediary, which then deposits the requested amount to the user's account (or in cash) and notifies the user. Finally, the wallet application notifies the user about the deposit or cash payment.

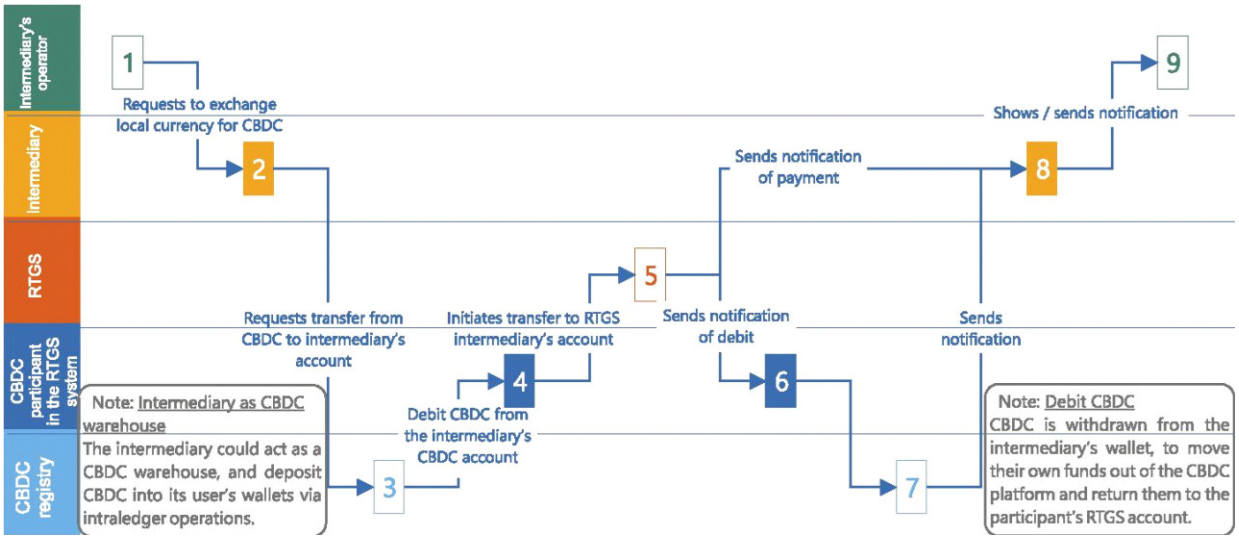
If the cash-out is requested directly by the intermediary, the operator requests the exchange of CBDC for local currency, through a funds transfer from the CBDC participant's account (wallet) to the intermediary's account via the RTGS system. To perform this operation, the following steps are required. First, the intermediary's operator requests to exchange CBDC for local currency. Then, the intermediary's back-end system translates this request to the CBDC registry, which debits CBDC from the intermediary's wallet, and instructs the CBDC participant in the RTGS system to perform a payment to the intermediary's account in the RTGS system. The RTGS system sends a debit notification to the CBDC participant and a payment notification to the intermediary. Finally, the CBDC registry sends the debit notification to the intermediary, which sends it to the intermediary's operator.

CBDC destruction process Graph 4

A. Exchange CBDC tokens for local currency



B. From the intermediary's point of view



Source: Authors' elaboration.

3.1.4 Intra-ledger transfers

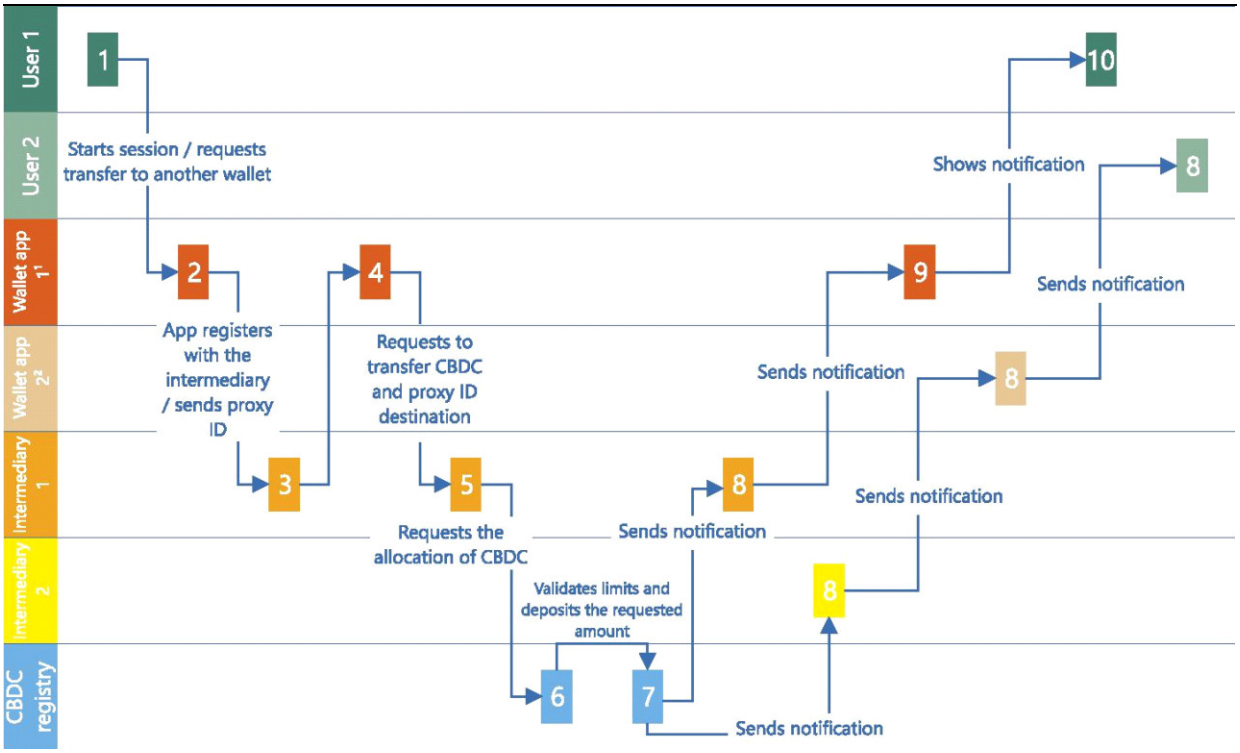
This final process transfers a certain value of CBDC from one wallet to another within the platform. Wallets may be from different tiers (higher-KYC or basic). Graph 5 illustrates the intra-ledger transfer process.

The main steps of the intra-ledger transfer are as follows. First, user 1 (the one initiating the payment) logs into their wallet application (app 1). Then, app 1 requests registration with its intermediary (intermediary 1) according to the defined policies and procedures. Intermediary 1 validates the request and sends a proxy ID to app 1. User 1, via app 1, requests the CBDC transfer to the beneficiary (user 2, who uses app 2). Intermediary 1 requests the registry to transfer the corresponding CBDC allocation to user 2's CBDC wallet. The CBDC registry performs the required validations according to the defined policies, then withdraws the requested CBDC amount from user 1's CBDC wallet and deposits it in user 2's wallet, and finally notifies the intermediaries of both users. Intermediaries 1 and 2 receive notifications of the transfer

and deposit operations and notify apps 1 and 2. Finally, the apps notify the users that the transfer has been done.[4]

Intra-ledger transfer process

Graph 5



[1] Belongs to intermediary 1, which provides services to user 1. [2] Belongs to intermediary 2, which provides services to user 2.

Source: Authors' elaboration.

3.2 Advanced payment capabilities offered by CBDCs

A CBDC could be the foundation for advanced functionalities as well as new types of arrangements and transactions. As new settlement assets, CBDCs have the potential to foster innovation, payment efficiency and security by supporting different financial solutions such as smart contracts, tokenisation and programmability. In a tokenised environment, CBDCs can act as a bridge between traditional and decentralised finance, enabling seamless transactions and enhancing liquidity. These functions could be offered for either wholesale CBDC or retail CBDC, or both.

If they use DLT, CBDCs can support the use of *smart contracts* to programme outcomes for a variety of use cases. Smart contracts enable the contractual terms of an agreement to be enforced automatically without the intervention of a trusted party (Zheng et al (2020)). These contracts may depend on events, identities and states, or time and reside on a computing environment able to verify and execute the contract using a programming language. Smart contracts can address coordination issues in financial markets and enable new digital economy applications with many potential benefits (BIS (2023)). Another use case is in supply chain financing, where delivery versus payment (DvP) problems could be solved with

[4] Here, funds are transferred directly into the wallet without intermediary 2 validating and accepting the request. This may vary depending on each jurisdiction and regulatory regime. For instance, intermediary 2 may also need to perform validation checks.

smart contracts. The technology underlying CBDCs can integrate smart contracts into existing payment processes, enhancing their functionality.

Tokenisation can simplify financial transactions by facilitating more direct actions. By removing the traditional separation of messaging, reconciliation and multi-asset atomic settlement, tokenisation could enhance the capabilities of the monetary and financial system and unlock new economic arrangements. With central banks and CBDCs at the core of the monetary system, tokenisation could enable composability, contingent payments and more efficient financial transactions (BIS (2023) and Carstens and Nilekani (2024)). For example, Project Helvetia, a joint experiment by the BIS Innovation Hub Swiss Centre, the Swiss National Bank and SIX Group, explored the integration of tokenised assets and central bank money into one settlement platform. The project found that a wholesale CBDC existing on a permissioned DLT platform and accessible to financial intermediaries opens up more functionalities enabled with tokenisation, eg instant and simultaneous settlement (BIS Innovation Hub et al (2020)). Moreover, tokenisation could link transactions and operations with money and assets residing on a programmable platform.

CBDCs could also unlock the potential of *programmable* payments to enable automatic transfers when pre-determined conditions are met. Automated transactions would offer functional benefits, enable new processes and foster new business models (Karaivanov et al (2023)). Programmable platforms would allow the transfer of money or assets through the execution of programming instructions issued by system participants without the intervention of an account manager. If a CBDC resides on the same ledger as other tokenised assets and claims, settlement would be done using the economy's unit of account (BIS (2023)).

CBDCs can be another policy tool to improve *cross-border payments*. Interoperability of CBDC systems and multi-CBDC arrangements could reduce the costs for payment service providers and simplify transaction chains, potentially leading to higher transaction speed and lower end user fees. CBDCs could also increase payment diversity, resilience, competition and efficiency (CPMI et al (2021)).

CBDCs could also support *offline payments*. With this feature, the payer and/or payee would not require a connection to any ledger system. This is particularly relevant in rural and remote areas with no internet or telecoms connectivity. In some jurisdictions, like Peru and Ghana, a potential retail CBDC is seen as a digital payment instrument for unbanked people and for use in remote areas. In Peru, the CBDC pilot will implement an USSD solution to reach out to these populations. In Ghana, the eCedi provides an offline solution through smartcards for merchant payments. The Bank of Canada also highlighted the need for a universal access device that could incorporate offline capabilities (Miedema et al (2020)).

Conclusion

The proposed CBDC architecture outlines four key processes that must be completed: user enrolment, creation (cash-in) and destruction (cash-out) of CBDC, and intra-ledger transfers. These four processes could involve other flows and vary depending on the CBDC design, regulatory framework, technological infrastructure and policy objectives of each jurisdiction. Of course, the introduction of other features such as offline and cross-border payments could also modify the reference diagrams of flows presented here.

As the CGIDE moves forward, several key technical questions arise for further exploration. For instance, how can the balance between centralised operation and decentralised access be optimised to ensure both security and accessibility? How can privacy be further protected while ensuring compliance with AML and KYC regulations? To address these and other technical questions, the CGIDE will evaluate the potential of tokenisation and the development of integrated financial ecosystems where tokenised deposits and CBDCs coexist. This remains an important area for further work by central banks to help advance the development of payment and financial systems.

Annex A: Members of the Technical Task Force of the Consultative Group on Innovation and the Digital Economy

Members

Central Bank of Argentina	Mara Misto Macias Fabian Pereyra Mariano Vázquez Silvina Ojeda
Central Bank of Brazil	Renato Gomes (Chair of CGIDE) Angelo Duarte Fabio Araujo
Bank of Canada	Alin Dan Sabir Husain Francisco Rivadeneyra
Central Bank of Chile	Enrique González Francisco Hidalgo Álvaro Merino
Central Bank of Colombia	Carlos Arango Yurly Sosa Samuel Gutiérrez John Ruiz
Bank of Mexico	Othón Moreno (Chair of Task Force) Ángel Salazar Daniel Garrido Carlos Hernández Ángel De León
Central Reserve Bank of Peru	Milton Vega
Central Bank of Uruguay	Adolfo Sarmiento
Board of Governors of the Federal Reserve System	Peter Lone Franklin Ervin Anders Brownworth
BIS Innovation Hub	Miguel Díaz
Eastern Caribbean Central Bank	Sharmyn Powell

Observers

Bank for International Settlements	Alexandre Tombini
	Jaime Cortina
	Christian Upper
	Jon Frost (oversight)
	Tara Rice
	Anneke Kosse
	Carolina Velásquez (secretariat)
	José Aurazo (secretariat)

References

Auer, R and R Böhme (2020): "The technology of retail central bank digital currency", *BIS Quarterly Review*, March.

Bank for International Settlements (BIS) (2023): "A blueprint for the future monetary system: improving the old, enabling the new", *Annual Economic Report 2023*, Chapter III.

BIS Consultative Group on Innovation and the Digital Economy (CGIDE) (2023): *"High-level technical requirements for a functional central bank digital currency (CBDC) architecture*", December.

BIS Innovation Hub (BISIH) and Hong Kong Monetary Authority (HKMA) (2022): *Project Aurum: a prototype for a two-tier central bank digital currency*, October.

BIS Innovation Hub, Swiss National Bank and SIX Group AG (2020): *Project Helvetia Phase I: settling tokenised assets in central bank money*, December.

Carstens, A and N Nilekani (2024): "Finternet: the financial system for the future", *BIS Working Papers*, no 1178, April.

Committee on Payments and Market Infrastructures (CPMI), BIS Innovation Hub, International Monetary Fund and World Bank (2021): *Central bank digital currencies for cross-border payments*, report to the G20, July.

International Monetary Fund (IMF) (2022): "Behind the scenes of Central Bank Digital Currencies", *Fintech Notes*, 9 February, www.imf.org/en/Publications/fintech-notes/Issues/2022/02/07/Behind-the-Scenes-of-Central-Bank-Digital-Currency-512174.

Karaivanov, A, B Mojon, L A Pereira da Silva and R M Townsend (2023): "Digital safety nets: a roadmap", *BIS Papers*, no 139, September.

Miedema, J, C Minwalla, M Warren and D Shah (2020): "Designing a CBDC for universal access", *Bank of Canada Staff Analytical Notes*, no 2020-10, June.

Vega, M and A Andia (2024): "Pilotos con CBDC: ampliando la frontera de los pagos digitales en Perú", *Revista Moneda*, no 198, July.

World Bank (2024): *Interoperability between central bank digital currency systems and fast payment systems: a technical perspective*, 26 June.

Zheng, Z, S Xie, H Dai, W Chen, X Chen, J Weng and M Imran (2020): "An overview on smart contracts: challenges, advances and platforms", *Future Generation Computer Systems,* vol 105, April.