BANK OF KOREA

A step toward new financial market infrastructure: Bank of Korea's initiative

October 2023

Contents

Foreword

The Bank for International Settlements (BIS) has a central role to play in fostering responsible innovation within the central banking community. It works closely with central banks as they respond to the growing challenges presented by an increasingly digitised world. It is against this background that the BIS is accompanying the Bank of Korea in its exploration of the future of central bank money. Drawing on its extensive research and experiments in the area of CBDC, the BIS is providing advice to the Bank of Korea and looks forward to learning from the implementation of this ambitious project.

Innovation and technology are central to the BIS's efforts to support central banks' pursuit of monetary and financial stability in the context of an increasingly digital financial environment. The BIS Innovation Hub (BISIH), established in 2019, seeks to contribute to these efforts by (i) identifying and developing in-depth insights into critical trends in financial technology of relevance to central banks; (ii) exploring the development of public goods to enhance the functioning of the global financial system; and (iii) serving as a focal point for a network of central bank experts on innovation. The BISIH's work programme focuses on the development of technological solutions – typically proofs of concept (PoCs) and prototypes – to solve financial sector problems of importance to central banks.

The speed of innovation in the financial system poses a significant challenge for central banks. On the one hand, they need to integrate technological and financial considerations into the solutions they put forward, and, on the other, they need flexibility in how they go about responding to the social demands they face. Central banks are in the process of understanding these changes and developing the flexibility to adapt quickly and respond appropriately to them in the public interest. To this end, it is vital for central banks to experiment with new technologies and accumulate expertise. Building and testing PoCs, prototypes and pilots is characterised by uncertainty and complexity.

While the products generated in this process may not be the ultimate solutions, they are valuable as part of a learning process. Some of these lessons relate to the feasibility of the particular technology or the viability of the ideas that are being tested. Others relate to the innovation process itself. Failure can bring about lessons that lead to better solutions. "Failing forward" – although a cultural change for traditional central banking – is essential for experimenters if they are to usefully explore different ways of serving society in the new digital economy. The BISIH is a partner to the central banking community in this role, seeking to make the process of experimentation as efficient and constructive as possible.

The Bank of Korea's pilot is an important example of how central banks are testing the boundaries of technology. In support of this initiative, the BIS is pleased to provide advice to the Bank of Korea on the design and implementation of the pilot. Such advice is being provided through a series of technical exchanges and seminars that seek to improve the design of the system, based on the lessons learned from other projects. At the same time, the BIS recognises that the ultimate design and policy choices remain entirely the Bank of Korea's discretion. The report below represents the Bank of Korea's own approach to CBDC after considering the BIS's input.

It is envisaged that this pilot will generate important lessons and useful insights with respect to the technology proposition, the policy implications, the underlying economic architecture, and the viability of the solution for the Korean ecosystem. The pilot will be a valuable tool for the Bank of Korea as it seeks to identify and refine the functions needed to reshape the country's monetary system for the digital economy. The pilot will also serve the broader global community by providing insights on the singleness of money within a CBDC ecosystem, and the integration efforts that will be necessary to keep all participants in the financial system operating efficiently.

Any experimentation with CBDC must recognise that no technology is superior to all others from a global perspective, and it may be the case that no optimal technology exists. The technologies, architecture, and design choices outlined in this report represent one approach, out of multiple options, that was designed

to operate within a specific environment. Its desirability for the Korean financial system must be validated by the country's institutions and society, based on the Bank of Korea's experience with the pilot.

The quest for the optimal technology in most jurisdictions is a dynamic endeavour, influenced as it is by the ecosystem and the evolving requirements of stakeholders. Uncertainty during the experimentation and piloting phases is only to be expected, given the system's complexity and its interactions. These conditions can take the form of an unexpected feedback loop between technological and policy implications or the contributions of system participants. What matters is to learn from these situations with the aim of building a robust foundation for the future monetary system through the provision of new services.

The pilot is a testament to the key role that CBDC might play as monetary anchor in such a future ecosystem. While the adaptation of the domestic requirements and restrictions of this pilot remain to be validated, several features show promise. These include public-private participation, innovative use cases, and integration between different issuers in the ecosystem using separate ledgers. The pilot also aims to integrate different existent tokenisation initiatives to take full advantage of the current efforts and plans of the participants.

Tokenisation is the process of representing claims digitally in a way that allows for their use on a programmable platform. As set out in Chapter III of the BIS's 2023 Annual Economic Report, this is a possible next step in digital recordkeeping and asset transfer. In a tokenised setting, money and assets become "executable objects" that can be transferred through the execution of programming instructions issued by system participants, potentially without the intervention of third parties. This does not mean that financial intermediaries are eliminated. On the contrary, trusted intermediaries will play an essential role in the operation and governance of tokenised systems.

The pilot explores an architecture that aims to reap the full benefits of tokenisation, which can only be realised with the existence of a monetary unit of account that denominates transactions. It is therefore essential that central bank money is the basis of any ecosystem based on tokenised claims. CBDC provides a tokenised representation of the unit of account and is essential for maintaining the singleness of money.

A financial market infrastructure underpinned by central bank money, such as the concept of a unified ledger, does not imply a sole ledger that overshadows all other systems in the economy. A key aspect of the Bank of Korea project is its broad systemic scope, which encompasses a central bank-operated core infrastructure and satellite interconnected systems operated by other entities. This interconnection provides the functionality needed for a wide variety of use cases, making the platform more flexible and open to market developments.

Another interesting element of the pilot is its approach to leveraging existing regulatory frameworks by finding equivalences with the functions in the proposed architecture. This basis simplifies the identification of new elements that need to be developed. A third feature is the voucher approach, which allows for simple conditionality for the currency issued within the system. Each of these features has the potential to enhance our general understanding of a CBDC ecosystem.

Previous work has been essential. Central bank institutions around the world, including the BISIH, are already working on CBDC-related projects. To make new advances, it is important to incorporate both the learnings from previous experiments and guidelines from standard-setting bodies (eg CPMI-IOSCO, NIST). The BISIH's thinking and its work on CBDC can feed into CBDC implementations across the globe, including this pilot.

Several aspects could be further explored. These include the onboarding of new and diverse participants, the reduction of intermediate steps in some use cases, the assurance of quantum-resistant encryption, the exploration of offline capabilities for certain use cases, and the exploration of cross-border functionalities.

Through public-private collaboration and experimentation, the Bank of Korea's pilot will facilitate a deeper understanding of technical issues, and of the policy and regulatory implications. On the technical side,

testing the chosen platform will increase clarity on how to achieve an optimal implementation. Yet beyond meeting core requirements the experiment will highlight the potential for testing other functionalities. At the same time, policy and regulatory requirements may change when real-world scenarios are implemented.

The desired output of any pilot is to learn before implementing a fully operational solution. As such, the question whether the proposed technology will ultimately be the one implemented is less important than the Bank of Korea's learning process in making informed policy decisions on the relevant technical issues. The project will also help the Korean society to gain trust in Bank of Korea's digital capabilities by witnessing the technological features of the experiment. The BIS and central banking community stand ready to learn and gain from this experience.

1 Introduction

With the launch of a new CBDC pilot project along with the regulatory bodies of Korea, the Financial Services Commission (FSC) and the Financial Supervisory Service (FSS),[1] Bank of Korea will broaden its CBDC research scope to encompass a wholesale CBDC. The Bank of Korea is set to establish a CBDC network that will enable financial institutions to issue digital currencies, including tokenised deposits and CBDC-backed tokenised e-money. Furthermore, the Bank of Korea intends to identify innovative use cases and to test them through distinct stages, each tailored to specific use cases.[2]

In this section, the discussion will encompass three main areas: (i) providing an overview of the Bank of Korea's progress on CBDC research, (ii) clarifying the reasoning behind the extension of CBDC research to encompass a wholesale CBDC in light of evolving internal and external conditions, and (iii) unveiling the objectives of this project.

1.1 Progress on CBDC research and lessons learnt

In an anticipatory response to the rise of the digital economy, the Bank of Korea established a dedicated CBDC research unit in 2020. A series of comprehensive experiments, with a primary focus on a retail CBDC, has been conducted. These experiments included a simulation project designed to assess basic and extended functionalities of CBDC, conducted from August 2021 to June 2022. Additionally, the Bank of Korea carried out an extended project in collaboration with 14 commercial banks from July to December 2022. Over the course of the simulation project, a mock CBDC system was developed utilising distributed ledger technology (DLT) within a cloud-based virtual testing environment in order to test the core CBDC lifecycle operations such as minting, issuance, circulation, redemption and destruction. The testing scope was subsequently expanded to include additional operations, including offline payments, digital asset transactions, and cross-border payments. Moreover, the experiment encompassed an assessment of the feasibility of integrating advanced IT technologies to enhance DLT's transaction processing capabilities and strengthen privacy protection. Upon the completion of the simulation project, the extended project was subsequently conducted. This follow-up project entailed interconnecting the Bank of Korea's mock system with the test servers hosted at commercial banks, thereby creating an environment resembling a real CBDC network. The outcome of this exercise indicated the seamless performance of the mock system. This multifaceted research has significantly enhanced the Bank of Korea's technical understanding of retail CBDC.

While conducting a comprehensive assessment to chart a path for future research, it was considered that there is currently no immediate need for Korea to embark on preparations for the introduction of a retail CBDC. Korea has a well-developed payment infrastructure, including a fast payment system, and conveniently accessible private payment services,[3] such as mobile banking services offered by banks and those provided by IT companies. Consequently, retail CBDC could face challenges in presenting any distinct advantages over the established private services, which could potentially impede its successful adoption. Moreover, considerations also included the examination of potential outcomes, including the possibility that the widespread adoption of a retail CBDC may encourage bank disintermediation, along with existing apprehensions regarding possible privacy infringements. Perspectives opposing the direct application of programmability, a feature that

---

1 This pilot project does not presuppose the official issuance of a CBDC by the Bank of Korea. Additionally, the architecture of the CBDC network may evolve in response to future technological advancements and changes in the economic and financial landscape.

2 These stages include the proof of concept (PoC) conducted within a virtual environment, alpha testing involving the participation of employees from financial institutions, and (closed) beta testing that extends to the general public.

3 As of 2022, the average daily use of internet banking, mobile banking, and "convenient" payment services in Korea stood at KRW 19.7 million, KRW 16.8 million, and KRW 23.4 million, respectively.

distinguishes digital currencies from conventional private payment instruments, into retail CBDC[4] have also been taken into consideration.

Nevertheless, as a central bank, the Bank of Korea maintains that it is necessary to be prepared for scenarios in which the introduction of a retail CBDC becomes necessary due to changes in the financial and economic landscape. Considering the diminishing use of cash in Korea,[5] the introduction of a retail CBDC may eventually become essential to guarantee the general public's continued access to central bank money. Furthermore, in the event of a market failure within the payment services market, the urgency of the introduction of a retail CBDC could intensify. In alignment with these considerations, the Bank of Korea plans to conduct advanced research into key technological aspects of retail CBDC in parallel with the pilot project. This research will include areas such as offline transactions[6] and privacy enhancing technologies.

1.2 Advance of tokenisation and wholesale CBDC

Tokens and tokenisation, originally popularised by Bitcoin, have extended their reach beyond the cryptocurrency domain. They have now permeated various real-world assets, garnering the attention of financial institutions, including securities companies. In Korea, tokenisation has facilitated fractional investments in various unconventional assets such as music copyrights, Korean beef, and artworks, although these innovative services have thus far operated exclusively within the confines of the financial regulatory sandbox. However, a pivotal transition is currently in progress. In February 2023, the FSC, the regulatory authority in Korea, announced its plan to authorise the issuance and circulation of security tokens. This plan involves a comprehensive overhaul of the regulatory framework. In response to the government's initiative, consortia led by prominent securities companies have been formed. These consortia are proactively gearing up to develop their own platforms to provide trading services for security tokens.

In line with the trend of asset tokenisation, the tokenisation of money as a payment instrument is advancing rapidly. Bitcoin was initially introduced as a digital substitute for cash. However, it does not effectively serve the three functions of money: serving as a store of value, as a unit of account, and as a medium of exchange. Bitcoin is rarely used as a unit of account, and its high price volatility make it an inappropriate store of value or medium of exchange.[7] Consequently, stablecoins have gradually emerged and have assumed the roles that Bitcoin struggled to fill. However, as demonstrated by the Terra/Luna incident in 2022, stablecoins have the potential to give rise to numerous challenges concerning user protection and financial stability. Additionally, even with the establishment of a regulatory framework in the future, stablecoins are subject to inherent limitations. Notably, the issue of seigniorage being allocated to the private sector remains, and addressing the adverse effects of bank disintermediation is challenging. Furthermore, there exists uncertainty regarding the feasibility of effectively regulating stablecoins on public blockchains to ensure safe operation in terms of operational risk, governance, and compliance with AML/CFT standards.

A notable trend has emerged as global banks display heightened interest in tokenising their deposits. While some banks have already initiated the provision of commercial services built upon tokenised deposits for their corporate clients, other prominent financial institutions are accelerating their research and development efforts. These entities are investigating the potential of tokenised deposits in facilitating delivery-versus-payment (DvP) in conjunction with tokenised assets. Furthermore, these institutions are exploring how programmability can be harnessed to develop innovative financial services.

---

4 See Panetta (2023)

5 According to a recent survey by the Bank of Korea, the share of cash among all payment instruments used by consumers fell from 17.4% in 2019 to 14.6% in 2021 based on value and from 26.4% to 21.6% based on the number of transactions.

6 In May 2023, the Bank of Korea signed an MOU with Samsung Electronics to strengthen research into an offline CBDC.

7 See BIS (2022).

Central banks and international organisations are showing substantial interest in endorsing a wide array of tokenised assets and tokenised deposits through the issuance of wholesale CBDCs. This eagerness arises from their recognition of the evolving landscape toward a tokenised economy. Tokenised deposits offer the advantage of addressing concerns associated with bank disintermediation, while still being subject to the same rigorous user protection and AML/CFT regulations that are currently applied to banks. However, a potential challenge arises when individual banks develop their independent systems without establishing seamless interoperability between them. In such a scenario, the advantages of programmability would be confined within each isolated system, potentially resulting in a fragmented or siloed financial infrastructure. BIS (2023) introduced the concept of unified ledger that encompasses both tokenised assets and tokenised deposits, centred on CBDC. The Federal Reserve Bank of New York (New York Fed) and the Central Bank of Brazil have embarked on research and development efforts aimed at developing a platform that establishes a connection between tokenised deposits and CBDCs.

1.3 Objectives of the Bank of Korea's CBDC project

The first objective of the CBDC project is to redirect the public's considerable interest in cryptoassets toward more innovative, constructive, and responsible channels. Koreans are widely known for their active involvement in crypto trading.[8] Furthermore, there exists an active interest and significant investment in the field of blockchain technology from both large enterprises and start-ups. The CBDC project is anticipated to serve as a testing ground for financial institutions to implement innovative payment and financial services on the Bank of Korea's infrastructure and assess their effectiveness.

The second objective is to support the integration of the emerging concept of tokenisation into the realm of assets. While the tokenisation of assets is gaining ground in Korea, discussions and preparations concerning the use of tokenised money as a payment method for these tokenised assets are still far behind. By leveraging the Bank of Korea's infrastructure, initiatives will be launched to explore methods to enable DvP in transactions involving tokenised assets.

The third objective encompasses exploring and assessing a means to significantly enhance payment system efficiency by introducing programmable digital currencies issued by banks. The distinctive feature of digital currencies lies in their programmability. Nevertheless, it remains uncertain which specific services can be realised and to what extent payment efficiency can be improved through this inherent programmability, as opposed to conventional payment methods. This project aims to garner more definitive insights by applying programmable currencies to specific use-cases (eg tokenised voucher[9] for subsidies, initial public offerings (IPOs), and settlement for asset transactions).

The fourth objective lies in the realisation of the unified ledger concept proposed by the BIS. Although issuing and circulating all tokenised assets on a single network operated by the Bank of Korea may be impractical, there is still a need to prevent the adverse effects of fragmentation that could occur if individual banks or operators of tokenised asset networks independently establish their own systems. The CBDC network, which is designed to empower commercial banks to issue digital currencies and ensure secure, instant, and simultaneous asset settlement on an external platform, could be viewed as a variation of the unified ledger concept.

The following sections are organised as follows. Section 2 provides a thorough exploration of the CBDC network in this project. Section 3 examines the implications of this project, encompassing both technical and policy perspectives. Section 4 focuses on considerations pertaining to legal and regulatory aspects, as well as personal information protection. Section 5 concludes.

---

8 According to a survey by the Korea Financial Intelligence Unit, the number of active users is 6.3 million (double counted) as of the end of 2022.

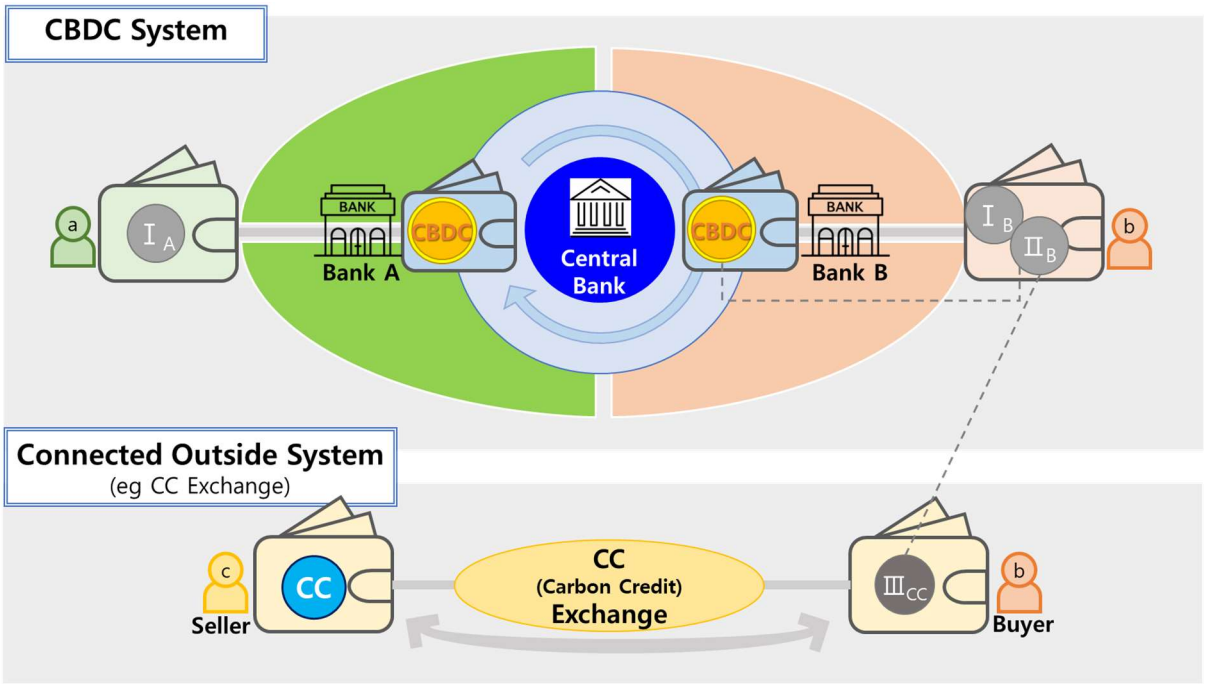
9 Tokenised voucher will be covered in Box A.

2 Bank of Korea's CBDC network design and architecture

2.1 CBDC network

Graph 1 illustrates the structure of the CBDC network, comprising of a CBDC system and connected outside systems. Within the CBDC system, CBDCs, tokenised deposits (DC-I) and tokenised e-monies (DC-II) will be issued and circulated. CBDCs take on the pivotal role of an anchor in the CBDC ecosystem by facilitating seamless exchanges at par between tokenised deposits and tokenised e-monies. The CBDC system will be interlinked with several connected outside systems,[10] each tailored to cater to specific use cases (eg carbon credit exchange). In connection with the tokenised e-monies (DC-II) within the CBDC system, specialised digital currencies[11] (DC-III) that are exclusively designed for use as payment instruments will be issued within the connected outside system. Table 1 summarises the key characteristics of the digital currencies to be issued within the CBDC network.[12]

CBDC network Graph 1



Source: The Bank of Korea.

[10] In Korea, various financial institutions are actively advancing their plans to develop their own security token trading platforms, driven by the recent announcement of the FSC allowing for the issuance and circulation of security tokens. Furthermore, individual banks may consider establishing their own dedicated networks in order to employ smart contracts with restricted visibility.

[11] Another approach to contemplate involves the issuance of DC-III using CBDC as collateral, replacing the use of DC-II. This approach has the potential to streamline processes related with DC-III and enhance the system's efficiency compared to the current design. Nonetheless, there arises a concern regarding potential limitations on the issuance of DC-III by non-banks, which cannot hold current accounts with the Bank of Korea.

[12] On-ramp and transfer process for digital currencies will be covered in Appendix 1.

Digital currencies within the CBDC network Table 1

Types	Roles/characteristics	Issuance platform	Issuer	Collateral asset
CBDC	Serving as settlement asset for interbank funds transfers	CBDC system	The Bank of Korea	—
DC-I	Tokenised deposits	CBDC system	Commercial banks	CBDC (partial)
DC-II	Tokenised e-money	CBDC system	Commercial banks	CBDC
DC-III	Serving as specialised payment instrument	Connected outside system	Commercial banks	DC-II

Source: The Bank of Korea.

2.2 CBDC system

The Bank of Korea will supervise both the development and implementation of the CBDC system, which will be established as a permissioned programmable platform. Designated financial institutions will participate as node operators for the system's operation. Moreover, they will be able to hold CBDCs for inter-bank settlement and as collateral for issuing CBDC-backed digital currencies (DC-II). In order to issue DC-II, banks are required to hold an equivalent amount of CBDC as reserve assets. Note that precautionary measures may be required to address the possibility of default, ensuring that DC-II is legally backed by the CBDC. For instance, the CBDC could be transferred to a segregated account specifically earmarked for securing CBDC and maintained by the Bank of Korea.

Initially, exclusive participation rights in the CBDC network and the authorisation to issue digital currencies (DC-I and DC-II) will be granted to commercial banks. Indeed, considering the imperative of upholding intermediation and credit creation roles of banks within the current two-tier monetary system, banks will be allowed to issue tokenised deposits[13] (DC-I) backed by fractional reserve banking. In this design, each bank will introduce its own digital currencies (DC-I and DC-II) that conform to a common technical standard.

In addition to issuing their own digital currencies, banks will provide a digital wallet service through a smartphone app, enabling users to efficiently manage their digital currency holdings. Once users initiate the digital wallet registration process, banks will verify their identity through an ID verification agency[14] and subsequently assign a simplified wallet address (alias)[15] to them.

On the other hand, dependent upon discussions with regulatory authorities, the inclusion of non-bank institutions, such as payment service providers (PSPs), in the CBDC network could be considered. While non-banks could gain access to participate in the CBDC network and issue digital currencies, they would be limited to issuing tokenised e-monies (DC-II), which should be fully backed by CBDC within the CBDC system.[16]

[13] The Bank of Korea will require banks to hold a certain amount of CBDC as reserves. The ratio of CBDC to DC-I will be set by the Bank of Korea.

[14] In Korea, mobile carriers providing ID mobile verification services can serve as ID verification agencies.

[15] The alias, serving as a unique identifier for a user's digital wallet, will be linked to the public key held by the financial institution that issued the digital wallet. Consequently, in the event that a user decides to switch to a different service provider, the new provider will undertake KYC/AML procedures on the user, resulting in the assignment of a new alias to the user.

[16] CBDC network with non-banks will be covered in Appendix 2.

2.3 Connected outside system

As previously stated, connected outside systems for specific purposes (eg a carbon credit exchange) can be interlinked with the CBDC system. To ensure smooth functioning of the payment process in the transactions involving tokenised assets (eg carbon credits) on the outside distributed ledger platform, the issuance of the payment token (DC-III) solely for use within the designated ledger could be allowed. By having both payment token and tokenised assets within the same platform, the delivery and payment process can be executed simultaneously in a DvP manner.

The designated financial institution, participating in both the CBDC system and the connected outside system, will play an exclusive role in issuing a payment token (DC-III). Consequently, within each connected outside system, DC-III will be issued by a single financial institution. In order to maintain the singleness of money, an equivalent amount of DC-II will be secured as collateral within the CBDC system for the issuance of the payment token (DC-III).

2.4 CBDC system architecture

Graph 2 illustrates the CBDC system architecture under the project. The architecture comprises two main areas: the common ledger[17] area at the bottom and the application area at the top.

The common ledger area consists of a platform layer, a currency layer, and a program layer. In the case of the platform layer, the participating nodes will communicate with each other on a peer-to-peer (P2P) basis utilising a virtual private network (VPN) to create a firewall between them and the public internet. Digital currency transactions will undergo a validation process carried out by participating system members, and then be linked to an existing chain of blocks. Essential information, such as digital currency balances, will be stored in the state database. To maintain confidentiality, particularly since each participant stores and shares transaction information on the shared ledger, it is essential to implement additional security measures. One effective approach could entail the introduction of private enclave nodes to encrypt transaction data, providing access exclusively to the relevant banks for detailed transaction information.

The currency layer encompasses CBDC and digital currencies that are issued and circulated within the CBDC system. The Bank of Korea will transfer CBDCs to commercial banks that, in turn, will issue DC-I through smart contracts and credit them to their customers. Each digital currency must adhere to the technical standards set by the Bank of Korea.

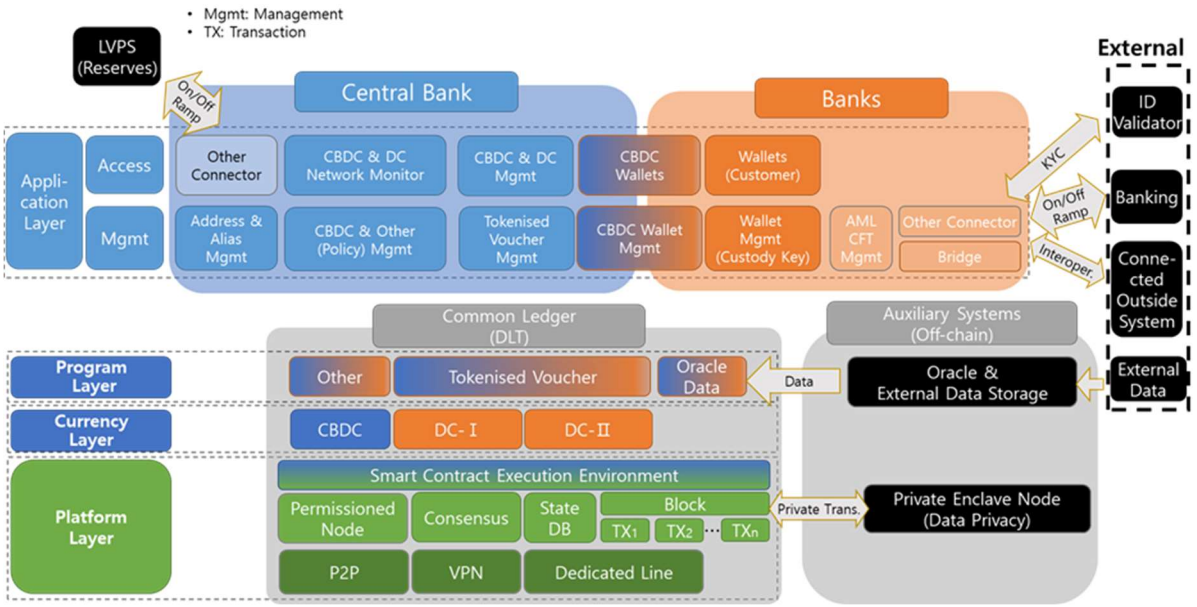
Within the program layer, commercial banks can integrate secure and efficient programmable functions facilitated by smart contracts based on digital currencies. A tokenised voucher will be issued based on digital currency to program payment conditions and provide functions such as automatic payment to the recipient when predetermined conditions are met, enabling commercial banks to offer creative and innovative program features. Additionally, this layer allows for the issuance of other types of assets, such as NFTs. If the execution of smart contracts is dependent on external data, an oracle in the auxiliary system will fetch this external data and input it into the common ledger.

To ensure that the CBDC network operates seamlessly, the Bank of Korea and commercial banks must integrate the common ledger with their existing financial systems using external applications. This integration is intended to supplement functionalities that are not supported by DLT and facilitate smooth interaction with the common ledger. Various functionalities need to be implemented through these applications, including providing user interfaces for end-users in the form of digital wallets, managing digital currency circulation policies, establishing connection and communication with external systems, and ensuring regulatory compliance.

---

[17] The common ledger is a distributed ledger where digital currency transactions and ownership changes are recorded. Both the Bank of Korea and commercial banks participate in this distributed ledger network as node operators.

CBDC system architecture Graph 2



Source: The Bank of Korea.

Box A Tokenised voucher

Tokenised voucher refers to a protocol that specifies the conditions upon which an underlying digital currency can be used (MAS, 2023). Within the CBDC network, commercial banks can issue digital currency which is essentially tokenised money. This tokenised money can then be wrapped into a tokenised voucher, which is intended for exclusive use for designated purposes based on programmed conditions. Once the conditions are met, the tokenised money is released.

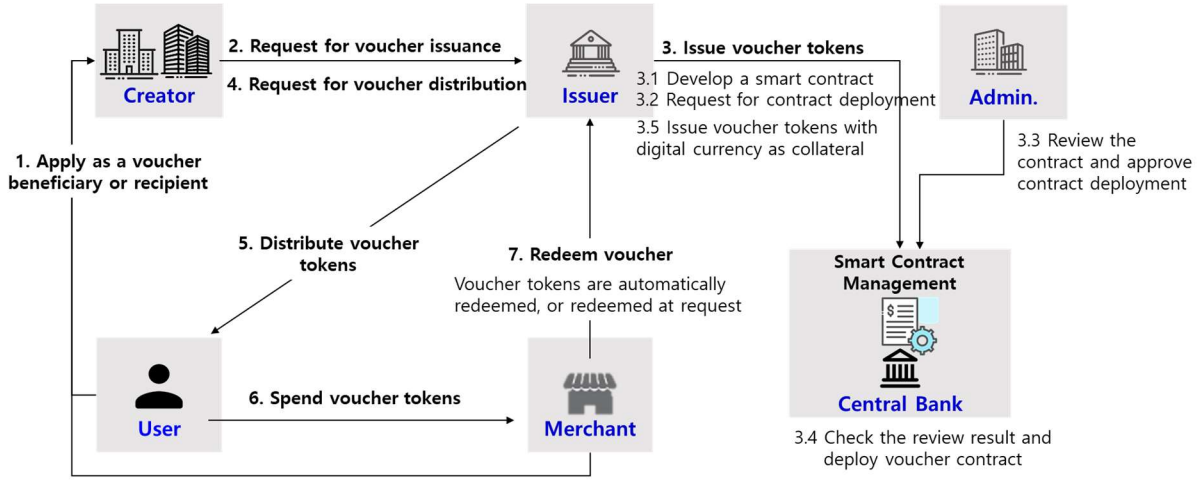
There would be several potential benefits to providing a tokenised voucher service[18] within the CBDC network. From the perspective of the voucher creators (eg government and corporations), they can easily issue vouchers without the need for a separate system. This leads to quicker implementation and reduced costs, enhancing the overall efficiency of voucher programs. Furthermore, a tokenised voucher service provides the creators with more flexibility to set various payment conditions for the vouchers. They can tailor voucher usage to specific needs, such as imposing time restrictions or spending limits. The tokenised voucher service allows users to access diverse vouchers through a single digital wallet application, simplifying voucher management. Lastly, merchants can benefit from the convenience of instantly receiving their funds.

Graph 3 briefly outlines the business process for a tokenised voucher service. Note that the issuer, which is typically represented by banks, will develop a smart contract and request its deployment through the smart contract management system. Subsequently, the administrator[19] will review the internal logic of the smart contract to ensure the system's integrity and reliability. Upon verifying the review results, the Bank of Korea, as the operator of the CBDC system, will proceed to deploy the smart contract within the CBDC system.

[18] A tokenised voucher service refers to a service that issues tokenised vouchers to be used only for specific purposes, using underlying digital currency as collateral on the CBDC network, and distributes these vouchers to users and merchants.

[19] Either the Bank of Korea or the Korea Financial Telecommunications & Clearings Institute (KFTC), which operates the retail payment systems, is expected to take on the role of administrator.

Business process for a tokenised voucher service Graph 3



Source: The Bank of Korea.

Box B Two mechanisms for final settlement in central bank money

Through this project, the Bank of Korea intends to assess the technical validity of diverse methodologies aimed at achieving final settlement for transactions involving tokenised assets through central bank money, even when tokenised assets and money exist on separate platforms. Hence, the Bank of Korea intends to explore designs for two different channels in the CBDC network that ensures interoperability among diverse programmable platforms: an asset transfer mechanism involving the transfer of either assets or money to the alternate platform to facilitate DvP within that platform; and, an asset exchange mechanism, which entails exchanging ownership of assets and money on distinct platforms.

The Bank of Korea plans to create a unified ledger for tokenised asset settlement in the connected outside system by issuing DC-III on the connected outside system and utilising the asset transfer mechanism. Furthermore, in order to assess the feasibility of this mechanism, the Bank of Korea intends to carry out tests involving the exchange of assets and central bank money that are issued on separate ledgers, utilising the asset exchange mechanism. The outcomes of these tests will serve as a reference point for comparison with the results obtained from testing the asset transfer mechanism.

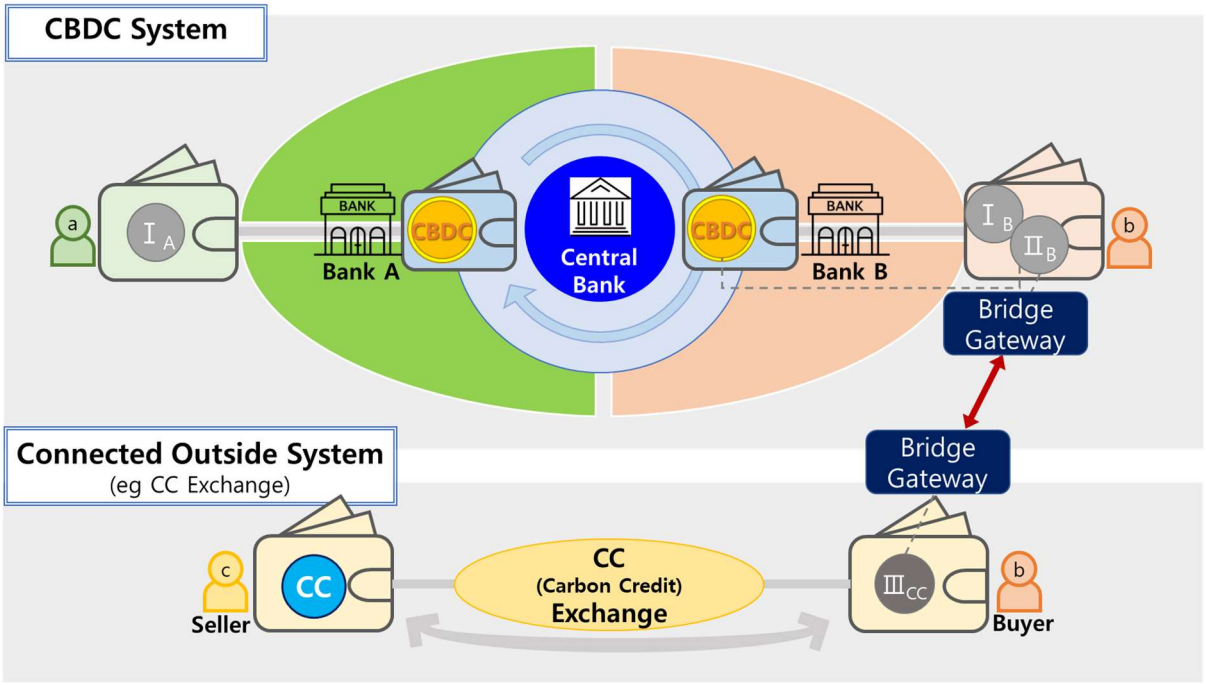
Specifically, the asset transfer mechanism predominantly relies on a common smart contract known as the bridge, to transfer assets across different networks. A noteworthy example of the asset transfer mechanism is the Secure Asset Transfer Protocol (SATP)[20] standard, which has been actively researched and developed by the Internet Engineering Task Force (IETF). This standard is particularly well-suited for permissioned[21] ledgers. Furthermore, one of its features is to have a gateway application through which multiple distinct distributed ledgers are interconnected. Specific architectures and use cases have already been demonstrated.

20 https://datatracker.ietf.org/wg/satp/about/

21 Utilising platforms such as COSMOS and Polkadot, which are designed to enhance interoperability within permissionless blockchain networks where transaction details are publicly accessible, may not be suitable for a permissioned blockchain network that prioritises transaction confidentiality and privacy.

Asset transfer mechanism

Graph 4



Source: The Bank of Korea.

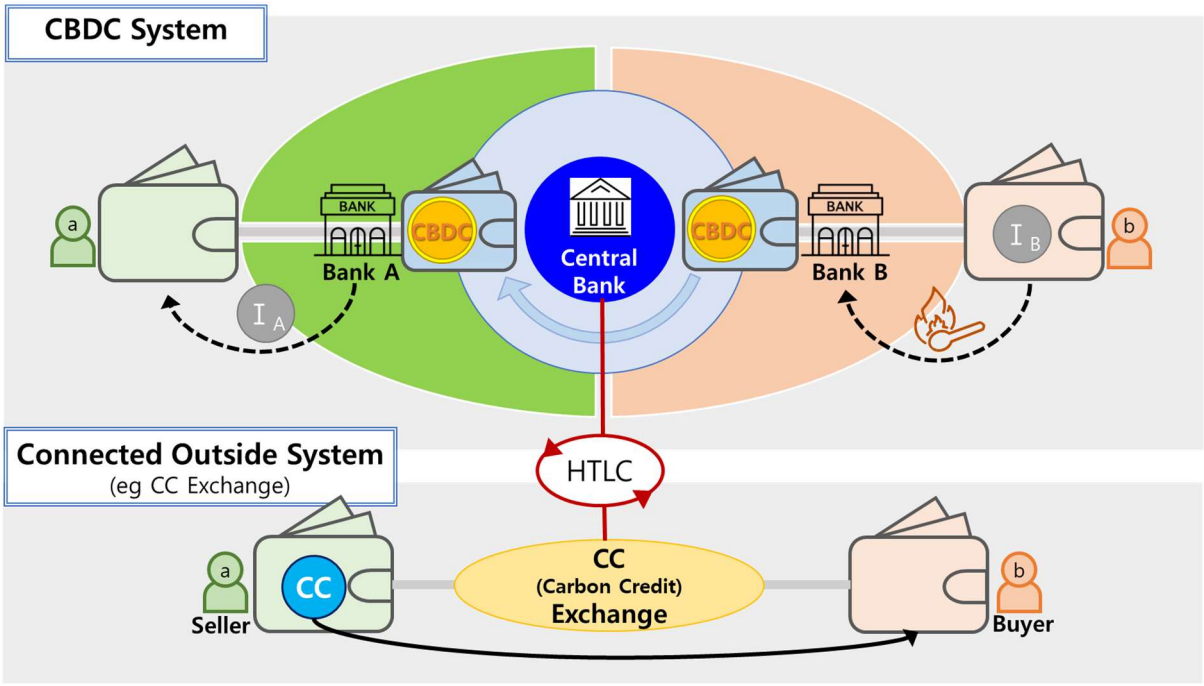
On the contrary, the asset exchange mechanism involves the exchange of assets and money issued on separate ledgers between participating parties in transactions. This approach primarily employs atomic swap-type smart contracts, for example, Hashed TimeLock Contracts (HTLC). This mechanism does not necessitate a direct linkage between the asset ledger and the money ledger.[22] At present, research and experimentation on HTLCs are underway.[23] Nevertheless, it is worth noting that the asset exchange mechanism could prove challenging to implement for transactions involving three or more parties.[24] Moreover, the processing speed for transactions, by utilising this mechanism, may be relatively moderate. Consequently, its applicability may be restricted, especially in cases involving substantial transaction volumes with smaller amounts per individual transaction.

22 Indeed, the off-chain information exchange remains crucial for transactions between trading parties.

23 In Project Cedar x Ubin+, the New York Fed and the Monetary Authority of Singapore (MAS) have recently explored potential approaches to enhance wholesale cross-border multi-currency payments and settlements, involving the utilization of HTLC.

24 While some ideas (eg Generalized HTLC for Cross-Chain Swapping of Multiple Assets with Co-Ownerships) have been proposed, there have been no actual implementations to date.

Asset exchange mechanism Graph 5



Source: The Bank of Korea.

3 Considerations

3.1 Law and regulations

In the early phases of the project, extensive deliberations took place with the regulatory bodies of Korea, the FSC and FSS, concerning the legal status of tokenised deposits and tokenised e-money. While these tokens might seem to align with the existing financial regulatory framework, their unique technical attributes warrant a more comprehensive assessment. If any discrepancies arise, it becomes necessary to undertake efforts aimed at developing an updated legal framework specifically tailored to accommodate these innovations.

Within the scope of the project, the design of digital currencies has been driven by the consideration of where new technologies and use cases could be tested relatively easily without any need for complex or time-consuming institutional overhauls, such as legislative amendments. Consequently, digital currencies are structured to closely align with their regulated counterparts that already exist within the current financial regulatory framework. Wholesale CBDCs will be recognised within this project as central bank reserves without amendments of the Bank of Korea Act in consultation with the relevant authority. Furthermore, tokenised deposits (DC-I) have been designed to closely resemble traditional deposits in structure, with the only difference being the technical form factor utilising blockchain technology.[25] For example, applying the burn and issue transfer process, similar to the existing fast payment system, and having a private key under a bank's custody, both mirror the current operation of deposits. Moreover, to eliminate any legal uncertainty, the FSC plans to apply its financial regulatory sandbox regimes to the issuance and circulation of DC-I by banks. These

[25] This design principle has been previously applied in the Bank's retail CBDC simulation, with the aim of closely emulating the life cycle of traditional cash as much as possible, from CBDC manufacturing and issuance to distribution, redemption, and disposal.

activities will be recognised within the financial regulatory sandbox regimes as the services that can be conducted under the Banking Act. Additionally, the FSC plans to protect the property rights of DC-I holders by mandating continuous synchronisation of transaction records, so-called mirroring, between the CBDC network and participating banks' databases.

Similarly, tokenised e-money (DC-II) is designed to closely resemble current e-money in that it cannot create credit, particularly because it is required that the issuer hold 100% as safe reserve assets, wholesale CBDC issued by the Bank of Korea in this project. However, it is essential to conduct a thorough examination to ensure that no issues arise from the fact that the new tokens may not match perfectly with existing e-money, considering the differences in underlying technology and the form factor of the tokens. Regarding DC-II and DC-III, after this project ends, the Bank of Korea and FSC will review their legal status in accordance with the Electronic Financial Transaction Act, the Act on Reporting, and Using Specified Financial Transaction Information and any future legislation related to virtual assets.

Currently, there are diverse approaches to how tokenised deposits should be categorised and regulated across countries, and there appears to be a range of opinions even within single countries. Europe has explicitly excluded deposits from the scope of the Markets in Crypto-Assets Regulation (MiCA) and efforts are underway to incorporate tokenised deposits into the existing regulatory framework, while Singapore is developing a regulatory framework where tokenised deposits and stablecoins are treated differently. In the U.S., there is a perspective that banks can issue tokenised deposits on permissioned platforms under the existing regulatory system.

Indeed, given the shift toward a tokenised financial ecosystem and the rise of diverse payment and settlement mechanisms, such as cryptoassets, particularly stablecoins resembling tokenised e-money, it may be essential to contemplate the formulation of a new regulatory structure for future financial systems. This entails the notion of constructing an entirely new regulatory framework from scratch rather than adapting tokenised deposits or electronic money into the current framework. This approach involves bestowing them with a new legal status and incorporating them within a new regulatory framework. This "blank slate" strategy could offer greater adaptability than the existing framework, enabling the full utilisation of the innovative potential of emerging technologies.

In addition to this, to establish a solid legal foundation that empowers central banks to enhance their research and development efforts related to financial market infrastructures (FMIs), it is prudent to explore the implementation of a dedicated sandbox framework. This specialised sandbox would specifically cater to the advancement of the FMIs, distinct from the conventional regulatory sandbox structure designed for commercial financial services.

3.2 Personal information protection

Within the CBDC network, essential data, such as user account details and payment transactions, will be securely stored. To facilitate the seamless and widespread adoption of both CBDC and digital currencies, it becomes imperative for the central bank and regulatory bodies to establish robust privacy standards that prioritise user confidentiality, while ensuring transparency in the methodologies employed for privacy-preserving measures. Aligned with this objective, the Bank of Korea recognises the utmost importance of protecting personal information. Consequently, the Bank of Korea in collaboration with relevant government authorities is actively engaged in ongoing initiatives that encompass the exploration of personal information protection management systems and policies, as well as proactive research into privacy-enhancing technologies. These initiatives will encompass diverse perspectives from stakeholders, various regulatory frameworks, and relevant technologies.

Particularly, the use of digital currencies is anticipated to introduce a range of innovative services and engage new institutions (eg government and corporations as tokenised voucher creators) as stakeholders. This entails a thorough evaluation of the amount of information required for these services, clarification of the roles

and responsibilities of newly involved stakeholders, and the identification of appropriate technologies and guidelines to enhance personal information protection. Furthermore, in the process of formulating use-case test scenarios and designing a CBDC system along with its related IT infrastructure, the Bank of Korea will seek to safeguard users' own data control rights while maintaining the system's convenience and distinctive functionalities.

Nevertheless, while the adoption of privacy-enhancing technology could potentially augment the security, transparency, and stability of personal data safeguards, it is important to recognise that the computational demands of this technology might impose adverse effects on the CBDC system's performance. Striking a judicious balance is imperative. Therefore, it is vital to understand that relying solely on privacy-enhancing technology may not comprehensively address all challenges. It becomes essential to concurrently develop robust and effective personal information protection policies. These policies should be accompanied by a clear delineation of responsibilities among involved parties and participating organisations, as well as the establishment of a resilient personal information protection management system.

4 Conclusion

The role of central banks in addressing the evolution of payment instruments and services encompasses broadening the domain of secure and sustainable innovation and competition, while vigilantly monitoring the potential for swift and disruptive changes that could pose risks to financial stability. In line with this objective, the Bank of Korea plans to continue its technical and institutional research, thereby contributing to the development of a payment ecosystem that promotes innovative progress. This endeavour entails various tasks such as refining the architecture and design of the CBDC network, as well as examining relevant legal and institutional aspects based on close cooperation with the regulatory bodies.

This report has presented a blueprint for the CBDC network that encompasses the issuance and circulation of both CBDC and private digital currencies. The Bank of Korea and regulatory bodies plan to conduct practical experiments involving a variety of innovative payment services, utilising the CBDC network in collaboration with financial institutions and relevant entities. The objective of this project is to stimulate innovative initiatives from the private sector and harness advanced information technology to promote constructive and responsible innovation. Furthermore, the issuance of programmable private digital currencies is expected to foster growth in the tokenised asset market and act as a catalyst for the introduction of various innovative payment services.

The Bank of Korea and regulatory bodies will establish a working group that includes other relevant institutions, and participating banks in order to successfully execute the project and reduce legal uncertainty. Additionally, the Bank of Korea will strengthen its cooperation with the BIS and other central banks. Moreover, upon the project's completion, the Bank of Korea plans to publish a comprehensive report detailing the project's outcomes, insights gained, and future directions.

References

Bank for International Settlements (BIS) (2022): "The future monetary system", *Annual Economic Report 2022*, June, Chapter III.

_____ (2023): "Blueprint for the future monetary system: improving the old, enabling the new", *Annual Economic Report 2023*, June, Chapter III.

Committee on Payments and Market Infrastructures and Market Committee (CPMI-MC) (2018): "Central bank digital currencies", March.

Monetary Authority of Singapore (MAS) (2023): "Purpose Bound Money (PBM) Technical Whitepaper", June.

Panetta, F (2023): "The digital euro: our money wherever, whenever we need it", Introductory statement at the Committee on Economic and Monetary Affairs of the European Parliament, 23 January.

Authors and acknowledgements

Authors

Foreword by Bank for International Settlements:

Miguel Díaz (Head of Toronto Centre, Innovation Hub)

Codruta Boar (Adviser, Innovation Hub)

Italo Borssatto (Adviser, Innovation Hub)

Rodney Garratt (Senior Adviser, Monetary and Economic Department)

Priscilla Koo Wilkens (Senior Economist, Monetary and Economic Department)

General content by Bank of Korea:

Digital Currency Research Division members

Acknowledgements

Financial Services Commission

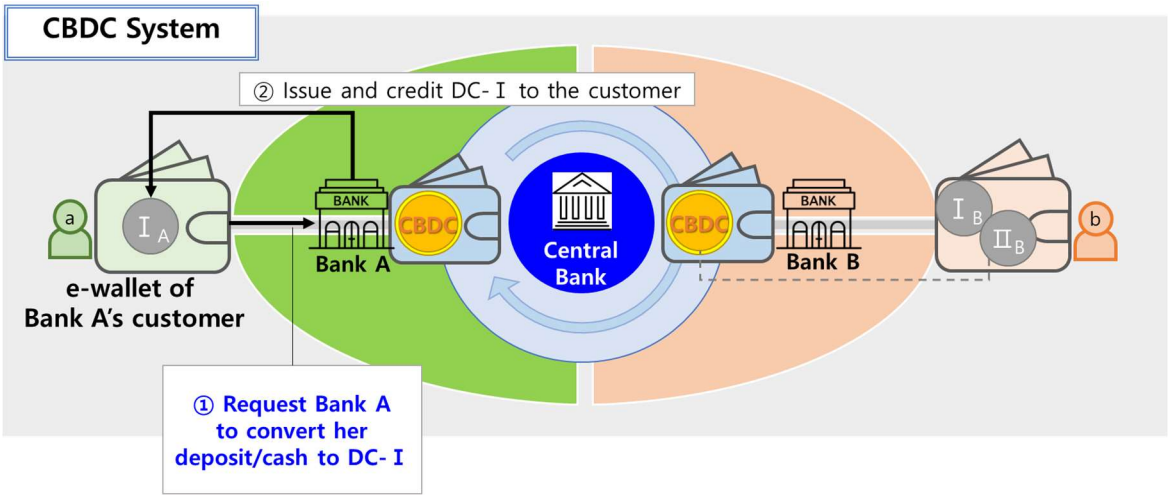
Financial Supervisory Service

Ministry of Economy and Finance

Appendix 1: On-ramp and transfer process

Graph 6 illustrates the on-ramp process for DC-I. When a user requests that bank A convert her deposit into DC-I through a smartphone app, the bank deducts the customer's deposit balance and issues DC-I to the user's wallet.

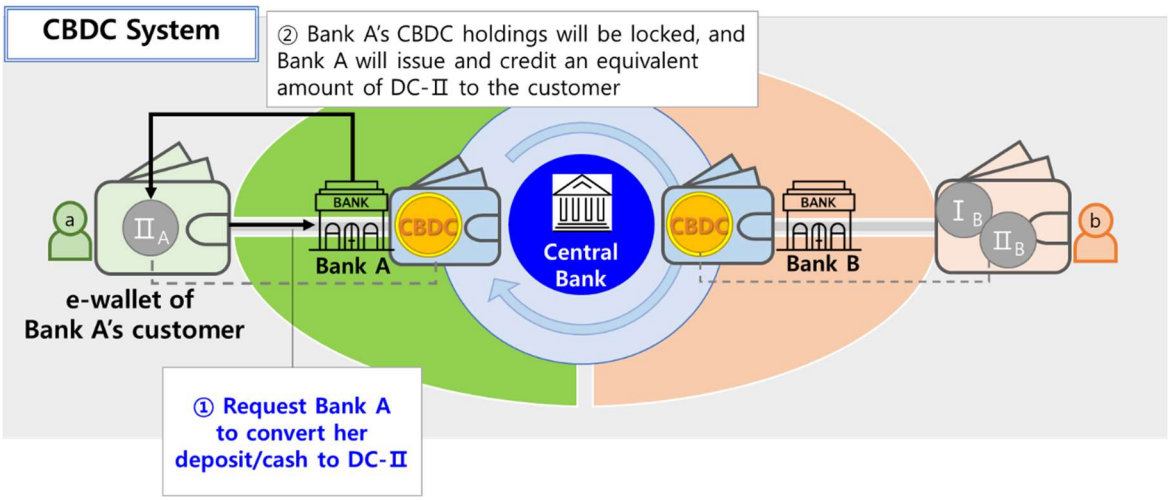
On-ramp process for DC-I — Graph 6



Source: The Bank of Korea.

Graph 7 illustrates the on-ramp process for DC-II. When a user requests that bank A convert her deposit into DC-II through a smartphone app, the bank deducts the customer's deposit balance and issues DC-II to the user's wallet. During the issuance of DC-II, an equivalent amount of CBDC will be secured as reserve assets.

On-ramp process for DC-II — Graph 7

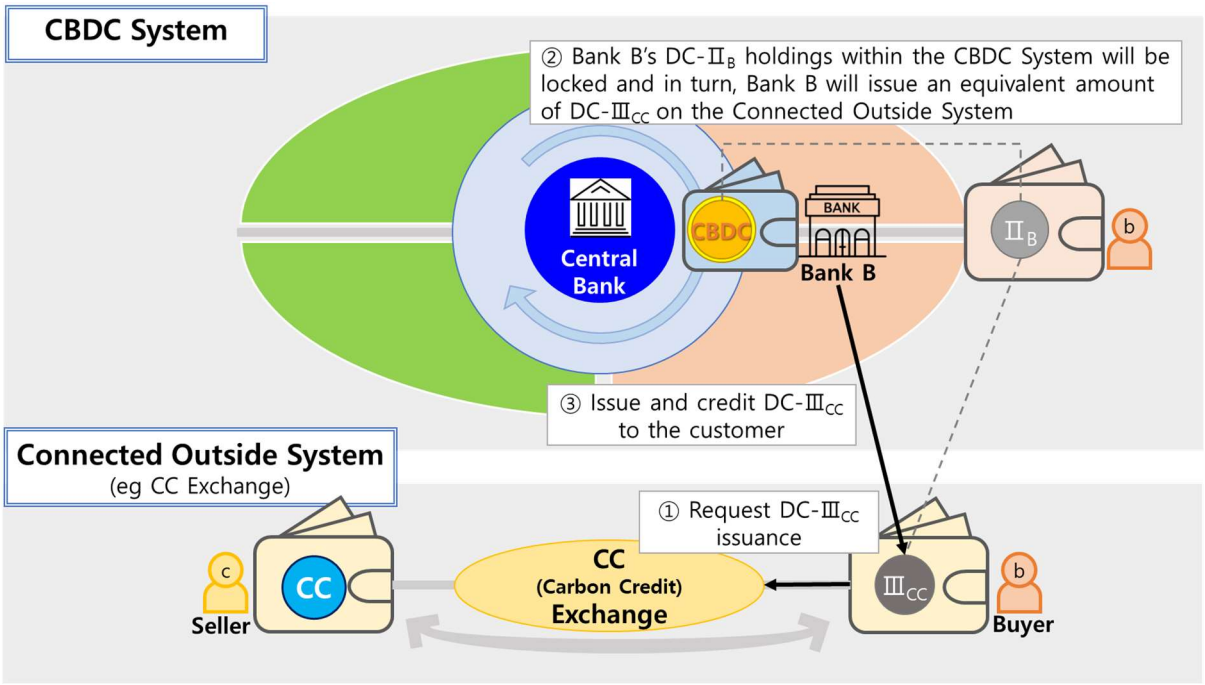


Source: The Bank of Korea.

Graph 8 illustrates the on-ramp process for DC-III. To issue digital currency (DC-III) that circulates within a connected outside system (eg carbon credit exchange), participating banks provide an equivalent amount of DC-II issued in the CBDC system as collateral. The system automatically locks this collateral to prevent potential any double creation of DC-III.

On-ramp process for DC-III

Graph 8



Source: The Bank of Korea.

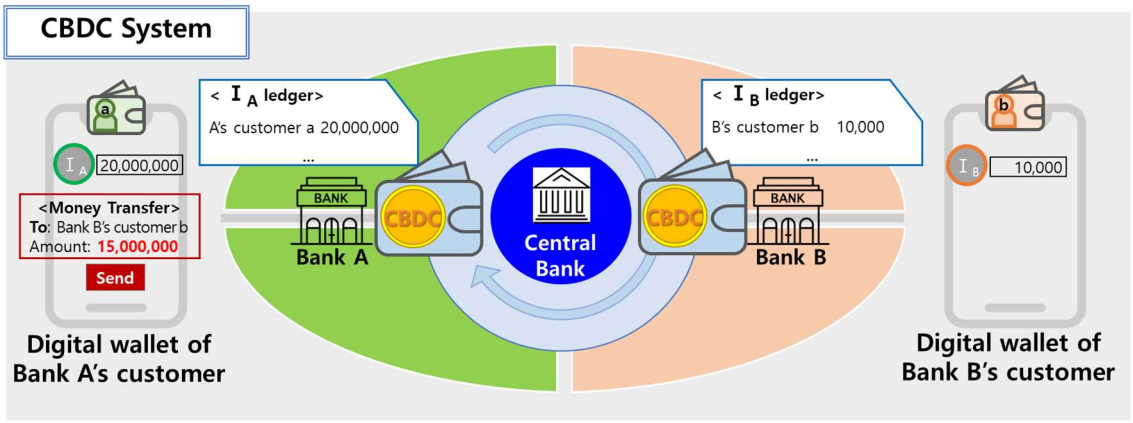
In the case of DC-I, liabilities are not transferred between banks in the same manner as with commercial bank deposits.[26] When DC-I issued by one bank is transferred to a receiver at another bank, the sender's tokenised deposit (DC-I) issued by the sender's bank is burned, and a new tokenised deposit (DC-I) is issued to recipient at the recipient's bank. Graph 9 illustrates the scenario where DC-I worth KRW 15 million is transferred from person a to person b. Note that DC-I_A held by person a is burned, and DC-I_B is issued to person b by the bank B. Simultaneously, the transfer of CBDCs between the banks takes place for settlement.

[26] When it comes to DC-II transfers, the Bank of Korea is considering employing the digital bearer instrument model within a limited scope.

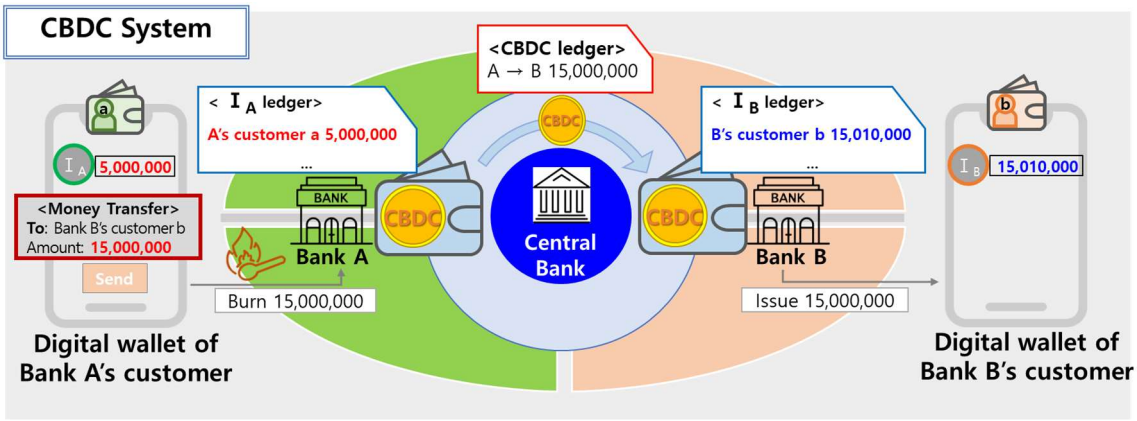
Transfer process (DC-I): Burn & Issue

Graph 9

Before



After



Source: The Bank of Korea.

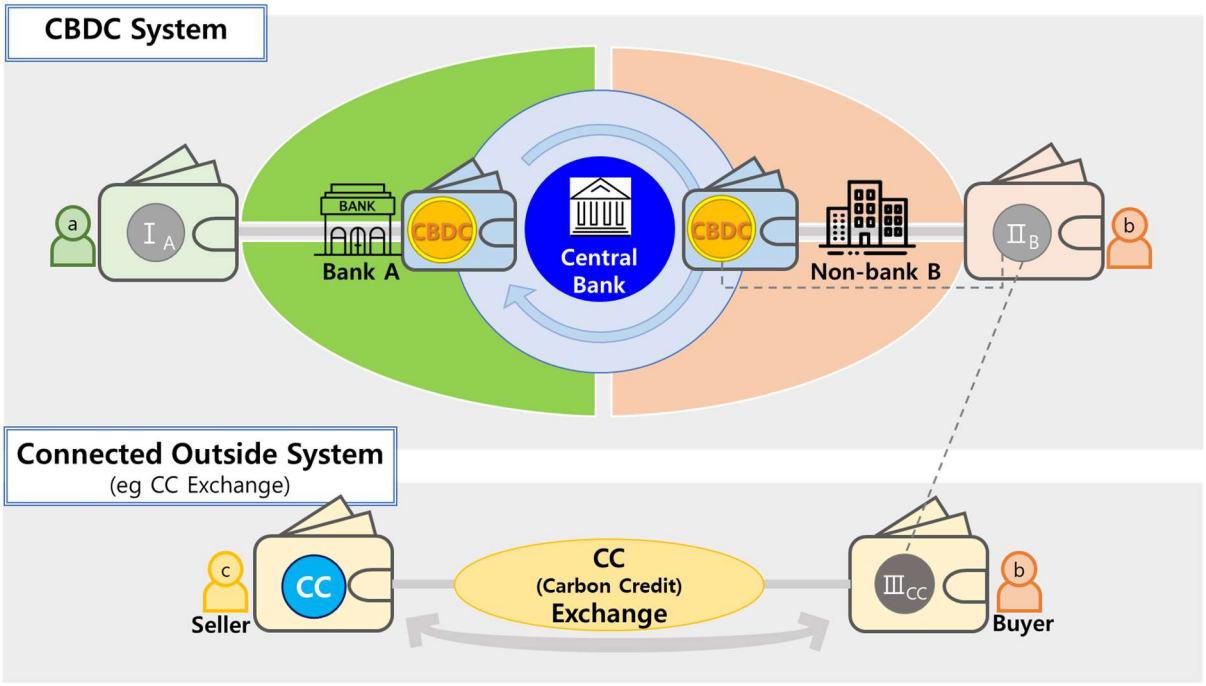
Appendix 2: CBDC network with non-banks

While only banks will be allowed to participate in the CBDC network over the course of the project, it is probable that this project will trigger discussions about[27] whether and to what extent non-banks will be allowed to participate in the CBDC network. As a rationale, non-banks could be allowed to issue digital currencies within the CBDC system in order to promote competition in the payment services market and the financial industry, and to provide a more stable and trustworthy alternative to private stablecoins.

However, strict requirements and regulations should be imposed on the non-bank institutions participating in the CBDC network, considering the need to ensure user protection and maintain financial stability, as well as the fact that non-banks are typically subject to much less stringent regulations compared to banks. These requirements may include requiring non-banks to exclusively issue tokenised e-money (DC-II) fully backed by CBDC within the CBDC system, along with implementing capital requirements and establishing a monitoring and supervisory system.

Graph 10 illustrates the structure of the CBDC network with non-banks. To issue tokenised e-money (DC-II) to end-users, a non-bank would need to request CBDCs from the commercial bank where it holds deposits. Then, the bank will debit the non-bank's account and transfer CBDCs from its CBDC wallet to the non-bank's CBDC wallet. The non-bank will provide these CBDCs as collateral, which will be automatically locked by the system. Once the Bank of Korea approves the issuance of DC-II, the non-bank can then credit DC-II to users' wallet.

CBDC network with non-banks — Graph 10



Source: The Bank of Korea.

[27] Given the significant implications of this issue for both payment and financial systems, it calls for a comprehensive examination of the scope and participation criteria from legal and payment policy perspectives. This entails in-depth discussions among central banks, government entities, and supervisory authorities to ensure a well-informed approach.

Glossary

For the purposes of the report presented we consider the following definitions:

Atomic settlement: Instant exchange of assets, such that the ownership transfer of each occurs only upon transfer of the others.

Central bank digital currency (CBDC): A digital form of central bank money, denominated in the national unit of account.

Central bank money: A liability of a central bank which can be used for settlement purposes.

Digital wallet: An interface that allows users to make transfers or otherwise transact in digital money and assets.

Distributed ledger technology (DLT): A means of saving information through a distributed ledger, ie a repeated digital copy of data available at multiple locations.

Delivery-versus-payment (DvP): A settlement mechanism that links an asset transfer and a funds transfer in such a way as to ensure that delivery occurs if and only if the corresponding payment occurs.

End-users: Individuals, households and firms that are not participants in a platform.

Fast payment system: An infrastructure focused on clearing and/or settlement of payments, in which the transmission of the payment message and the availability of "final" funds to the payee occur in real time or near-real time on as near to a 24-hour and seven-day basis as possible.

Hashed TimeLock Contracts (HTLC): A type of self-executable application that creates a time-based escrow that requires a cryptographic passphrase to unlock it, usually used to reduce counterparty risk.

Oracle: A service that provides outside ("off-chain") information for use by smart contracts in a DLT system.

Programmability: A feature of programmable platform and other technologies whereby actions can be programmed or automated.

Programmable platform: technology-agnostic platform with an execution environment and a ledger and governance rules.

Public key: A cryptographic key used with a cryptographic algorithm (known as public-key) that is uniquely associated with an entity and that may be made public. The public key has a corresponding private key. The public key may be known by anyone and, depending on the algorithm, may be used: 1. To verify a digital signature that is signed by the corresponding private key, 2. To encrypt keys that can be decrypted using the corresponding private key, or 3. As one of the input values to compute a shared secret during a key agreement transaction.

Smart contract: Self-executing applications of programmable platforms that can trigger an action if some pre-specified conditions are met.

Stablecoin: A tokenised asset that aims to maintain a stable value relative to a specified asset, or a pool or basket of assets, usually issued against the reception of the represented assets.

Token: A digital representation of value that is cryptographically secure, usually binding a data content that gives information on the asset to a digital signature created by the issuing entity.

Tokenisation: The process of recording claims by representing them through a token.

Tokenised asset: A digital representation of a claim of an asset using a token form.

Tokenised deposit: A digital representation of a bank deposit using a token form. A tokenised deposit represents a claim on a commercial bank, just like a regular deposit.

Tokenised e-money: A digital representation of e-money using a token form. A tokenised e-money represents a claim on an issuing institution.

Tokenised securities: Tokens that provide rights and obligations similar to traditional financial instruments such as shares, debt instruments or units in a collective investment scheme, as defined in securities regulation.