Central Bank Digital Currencies – 1st Proof of Concept Experiments[1]

Disclaimer

The Bank of Korea (BOK) has not decided whether or not to issue a central bank digital currency (CBDC), nor has it selected any specific model or design features. A distributed ledger technology (DLT) based platform used in the experiments, in particular, does not take precedence over any other: system architecture and design features introduced in this note are NOT final and thereby subject to change over the course of follow-up research and experiments.

Context

The Bank of Korea (BOK) has not decided whether or not to issue a central bank digital currency (CBDC), nor has it selected any specific model or design features. Notwithstanding this current status, it has been noted that the recent payment landscape demonstrates an unprecedented evolution that has been accelerated by digitalization and technological innovation. Furthermore, the rise of Big Tech and new payment service providers (PSPs) suggests a series of policy implications to the BOK in the context of its roles in ensuring the safety and efficiency of financial market infrastructures including payment systems.

Against this background, the BOK undertook a series of proof-of-concept (PoC) experiments from August 2021 to June 2022 with the primary goal of testing the technical feasibility of a CBDC on a DLT based platform. The PoC experiments, in particular, were guided by the following objectives:

- Validate technical and institutional design features of a CBDC in a simulated virtual space;
- Test the feasibility and reliability of DLT in supporting baseline functions ranging from CBDC lifecycle management up to P2P, offline, and cross-border payments.

System architecture & design features

The BOK built its CBDC test system in the cloud on a hybrid model featuring a two-tier structure where the BOK manages the CBDC lifecycle while participant nodes[2] support CBDC circulation and provide end user services, including digital wallets and KYC[3] requirements. The test system comprises of four main components: the BOK system; a participant system; an end user support system; and, the ledger management system. Each of these were specifically designed to support the following key functions:

- **BOK system:** This module is tasked with managing the CBDC lifecycle, ranging from the creation

[1] This note was prepared based on the original Korean document published on Nov. 7, 2022 (press release), which was written by the department's e-finance division, to which the CBDC teams belong. Any questions or comments about the contents of this note can be delivered to bokcbdc@bok.or.kr.

[2] Note that the BOK undertook the PoC experiments without the participation of banks or of other PSPs, i.e., they were BOK solo projects. The participant nodes and other end user service elements are, in this respect, simulated, modelling a permissioned DLT network and its auxiliary service providers. In light of this, participant nodes in the test system can be viewed as banks.

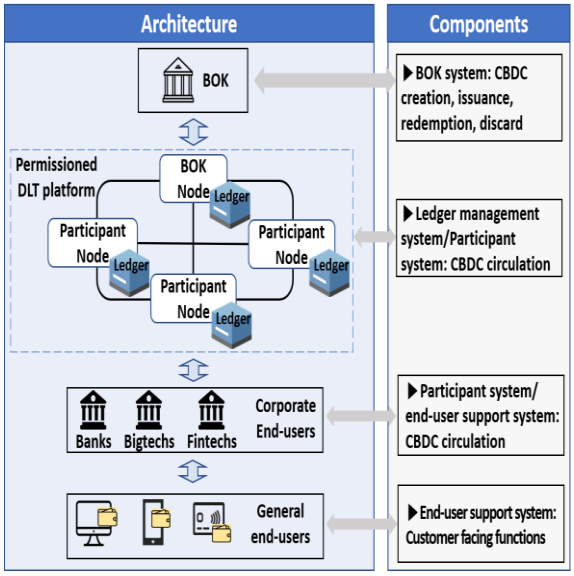
[3] "Central banks and payment service providers (PSPs) could continue to work together in a complementary way, with each doing what they do best: the central bank providing the fundamental infrastructure of the monetary system and the private PSPs using their creativity, infrastructure and ingenuity to serve customers." From "CBDC: An Opportunity for the Monetary System," BIS Annual Report (June 2021).

and issuance to the redemption and discarding, where the creation and discard operations are simulated to operate in a secure area of the BOK inaccessible from any internet connection. As for these functions, in addition, multiple rounds of authorization procedures with different private keys are required to execute relevant procedures in line with real-world security arrangements. This module serves as a gateway connecting participant nodes' virtual reserve balances with the BOK and the corresponding CBDC circulation in the simulated space.

- **Participant system:** Participant nodes are supported by this module when they transfer (redeem) a CBDC to/from an end user's wallet by decreasing/increasing the end user's corresponding account balance with the nodes.
- **End user support system:** This module supports the end user's payment initiation and generates a receipt of the CBDC using their mobile wallet apps.
- **Ledger management system:** CBDC payments and circulation are processed upon the permissioned DLT platform constructed by the BOK, whose design features share the Ethereum open-source protocols. The BOK system and its participant system, as stated above, were reflected on this DLT platform as "nodes" over the course of the CBDC experiments.

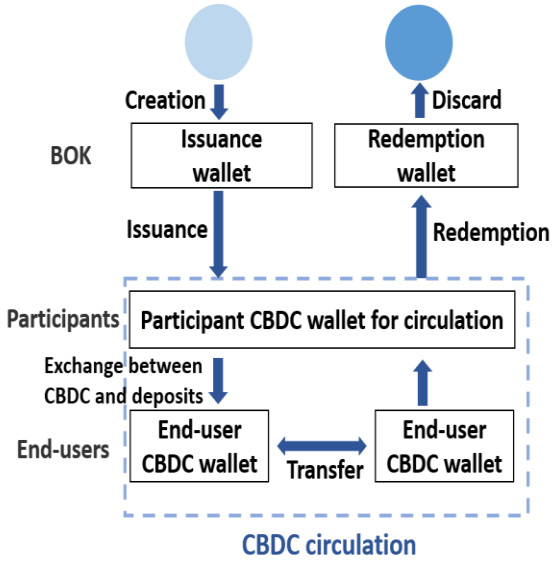
Figure 1. BOK's CBDC Test System – Architecture & Main Components

Main Architecture & Components



Source: BOK

A Snapshop of the CBDC Lifecycle, as Modelled by the Experiments



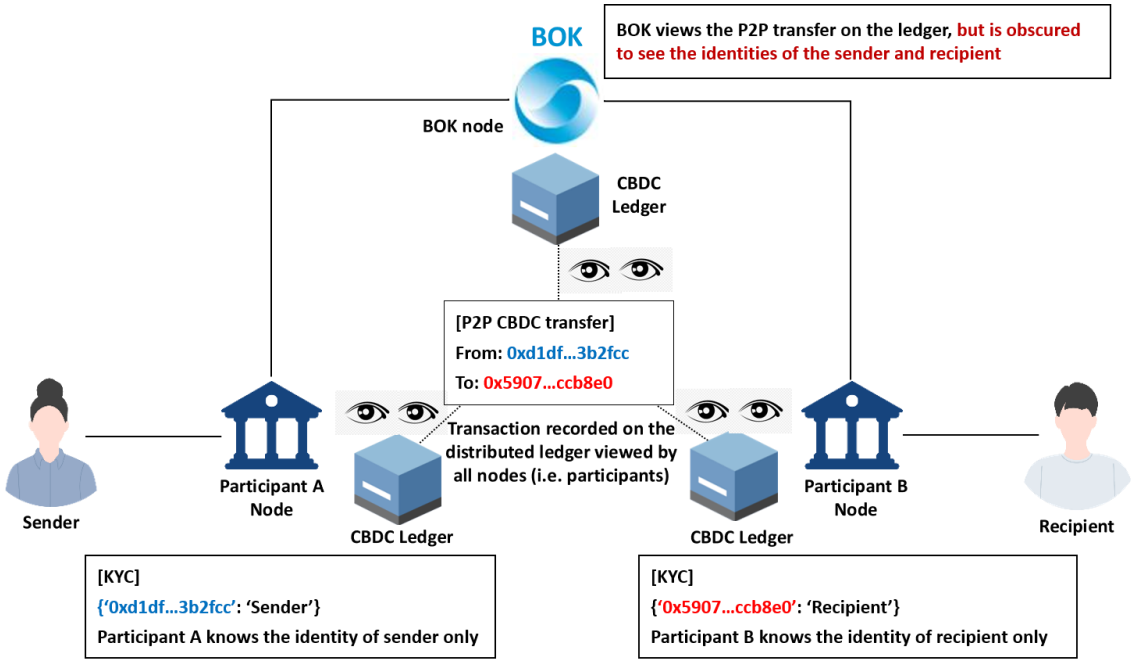
Source: BOK

Phase 1 experiments

Phase 1 experiments were conducted from August 2021 to December 2021, and were mainly dedicated to testing the operational feasibility of CBDC lifecycle management and of P2P transfers. The results showed that a test system in the cloud can be constructed in a robust manner, supporting the smooth functioning of baseline CBDC features, as designed. Specifically, all operations of the creation-issuance-circulation-redemption-discard cycle showed stable performance, and CBDC circulation on

the DLT platform demonstrated that end user P2P CBDC transfers can be processed smoothly by this emerging technology in the normal course of business.

Figure 2. Stylized Example of a P2P CBDC Transfer as Simulated in the Phase 1 Experiments



Source: BOK

Phase 2 experiments

Phase 2 experiments were undertaken from December 2021 to June 2022, and focused mainly on testing additional CBDC functions in the context of exploring potential use cases, as well as assessing performance enhancement measures and end user anonymity enhancement measures on the DLT platform.[4] Overall test results from this phase suggest that the following functions subject to the experiment are technically feasible, while some areas that require further analysis were identified, as well.

- **Offline payments:** The experiment tested the concept where end users make CBDC payments for their purchases of goods and services in brick-and-mortar stores without any internet access. (In the transaction, the merchant's CBDC apps perform the corresponding CBDC receipt.) End user CBDC apps equipped with near field communication (NFC) features are a key enabler supporting relevant communications between end user CBDC apps. This use case was considered mainly because a robust backup function in relation to CBDC operation is of critical importance considering the possibility of a cyber incident or a disaster disrupting internet communications.[5] Furthermore, the system was designed to leave no footprint over the course of the transaction

[4] Relevant modules tasked with supporting this additional area of experiments were added to the CBDC test system built in the phase 1 experiments.

[5] Recent meteorological observations suggest that the risk of there being a higher frequency and magnitude of natural hazards could rise around the Korean Peninsula.

flows, in consideration of modelling the anonymity of existing physical cash. Annex 1 shows a stylized example of this offline payment test flow.

- **Digital asset transactions:** This test executed the concept of a DvP settlement between a CBDC and a digital asset token using a smart contract by interlinking heterogenous CBDC and digital asset ledgers through a bridge system. Test transactions modelled an end user's general digital asset purchase by simultaneously paying off a CBDC to the seller. The transaction flows are normally composed of: digital asset registration (recorded on the digital asset ledger), transaction request by the buyer, transaction on a block, simultaneous exchange of the digital asset token and the CBDC supported by a smart contract (transactions are processed instantly). Annex 2 shows a stylized example of such a digital asset transaction flow.

- **Cross-border payments:** This test reviewed a USD-KRW cross-border payment model where a KRW intermediary transfers a KRW CBDC to a USD intermediary (recorded on a KRW ledger) and the USD intermediary transfers a USD CBDC to a KRW intermediary (recorded on a USD ledger) through a smart contract. The model assumes that the USD and KRW CBDCs are in circulation on the two distinctive distributed ledger networks, and that the intermediaries undertake pertinent currency conversions. Annex 3 shows a stylized example of such a cross-border payment.

- **Rollup:** This technology was tested as a potential measure to help DLT platforms overcome the scalability issue and enhance overall processing capacity and speed. Annex 4 shows the details of rollup technology and how it was tested by these experiments.

- **Zero knowledge proof:** The potential of zero knowledge proof was reviewed with the aim of exploring a measure that could strengthen the end user anonymity of CBDC payments.

Key findings and lessons learned[6]

All in all, the two rounds of PoC experiments suggest that circulating a CBDC on a permissioned DLT platform is technically feasible with a reasonable degree of stability and reliability. All CBDC functions subject to the experiments – conventional P2P payments, offline payments, digital asset transactions, and cross-border payments, for instance – showed performance in line with each of their concepts under normal business scenarios.

Nonetheless, a series of resilience implications was juxtaposed as well, along the lines of tests and interpreting the results, most of which were centred on the inherent limitations of scalability that are embedded in distributed ledger, as specified below:

- **Processing capacity:**[7] This test showed that the system is able to achieve peak throughput of

[6] BOK Governor Rhee shared his view on the juxtaposition of the potentials and limitations of DLT-based CBDC circulation in his keynote address delivered on Sept. 28, 2022,in the IMF STI webinar (https://www.bis.org/review/r221028b.htm). This section contains the relevant analytical details of some of the main points that Governor Rhee emphasised in his speech.

[7] The PoC experiment carried out performance evaluations of the DLT platform's processing capacity against the following two indicators:

- **Throughput:** the number of payment instructions successfully processed by the network
- **Latency:** the time required for the network to successfully process a payment instruction

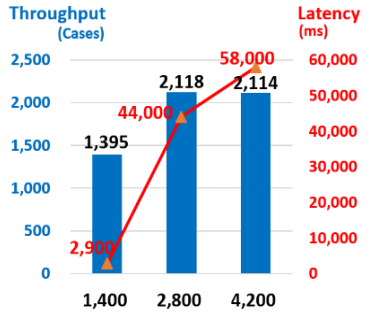
approximately 2,000 transactions per second on a continuous basis, suggesting that the CBDC test system is able to handle typical retail payment volumes through the normal course of business. (The daily average volumes per second are 486.6 and 220.4 in credit card networks and electronic banking networks, respectively, the two incumbent retail payment networks that are ranked first and second in terms of processing volumes.)

This test, however, also brought to light issues of concern under extreme but plausible scenarios. Specifically, the system's latency showed notable signs of increase up to 44 seconds when there were 2,800 requests per second, which was followed by far steeper latency increases from 44 seconds up to 60 seconds as transaction volumes were further upped to 2,800 and 4,200 per second, respectively.[8]

Moreover, the number of nodes on the DLT platform and the volume of end users' simultaneous access to payment services indicated operational concerns, as well. For instance, throughputs decreased by approximately 10% as the number of nodes was raised from 4 to 30,[9] or when that of simultaneously accessible end user accounts was risen from 500,000 to 10 million.

Figure 3. Performance Evaluations of the CBDC Test System

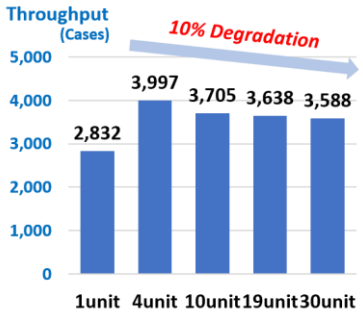
<Transaction Volumes per Second>



Transaction volumes per second

Source: BOK

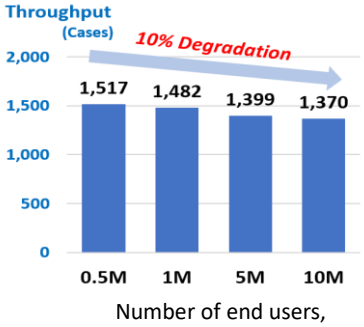
<Number of Nodes>



Number of nodes

Source: BOK

<Access Traffic>



Number of end users, simultaneous access

Source: BOK

- **Performance enhancement measures:** This test showed us that rollup can be considered as a potential measure to accelerate the processing speed of the DLT platform, as each sub-network supported by this measure showed throughputs of approximately 700 transactions per second, suggesting that there is enhanced processing capacity across the entire DLT platform. (Each sub-network's work is relayed to the main platform and recorded thereon.) The layered processing structure of the DLT platform, however, was not free from scalability constraints, as transactions

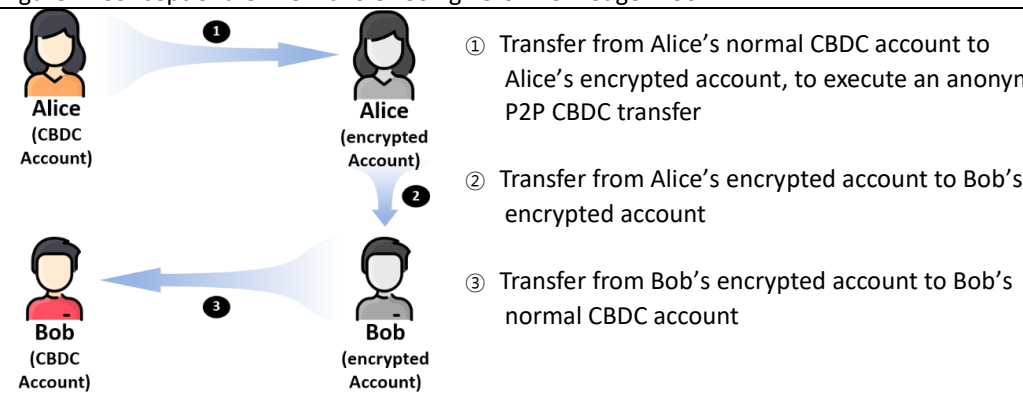
[8] The stress scenarios were based on BOK payment statistics data that show that during peak times, i.e., at the end of a month or on an IPO due date, payment traffic tends to soar three or four times higher than payment traffic in normal times.

[9] A counterintuitive observation is that a single consensus node model witnessed the least processing capacity in terms of throughput. Pertinent analysis suggests that processing volumes tend to overly concentrate on a single node breaching the threshold that that node is able to bear for timely processing.

between each sub-network exceeded certain capacity thresholds.

- **Anonymity enhancement measure:** This test showed us that zero knowledge proof, an experimental encryption technology regarded as a promising anonymity solution by the industry, should be accompanied by additional research and development. This conclusion is based on the observation that up to an additional 14 seconds are needed to process a single transaction when zero knowledge proof is applied to the processing cycle (including the setup time).

Figure 4. Concept of a CBDC Transfer Using Zero Knowledge Proof



Source: BOK

Aside from the technical analysis, one challenge in identifying potential use cases that can support CBDC adoption was also noted, in consideration of incumbent digital payment instruments. In light of this, determining which areas of existing payments can be most effectively addressed or enhanced by a CBDC was set as one of the key questions in the BOK's subsequent workplan.

Follow-ups and next steps

The BOK has been undertaking extended PoC experiments in partnership with major commercial banks since the conclusion of the phase 2 experiments in June 2022. One distinctive feature of the subsequent on-boarding experiments is that participant nodes of the BOK test system are filled in by each participating bank's actual test platform, thereby enabling the BOK to test CBDC functions in a more realistic setting, i.e., each participating bank's test platform is individually linked to the BOK's test system in the extended PoC experiments that are underway, as opposed to a single cloud environment of the previous experiments where all participant nodes were virtual and confined within the same cloud realm. The on-boarding experiment is running performance evaluations of the DLT platform against the incumbent indicators, i.e., throughput and latency, with the aim of providing the BOK with additional insights and reference points.

The BOK is, in parallel, considering furthering its CBDC research with a view to exploring more use cases and collecting additional technical information about CBDC circulation in a new test environment. Given any CBDC's multi-dimensional nature and the huge ripple effects it could have on the financial system as a whole, the BOK will explore heightened collaboration with the industry and at international forums, as well as with the government and legislative bodies, concerning the course of the new endeavours ahead.

Annex 1: Stylized example of the offline payment test flow

■ Offline P2P CBDC payments are composed of four steps: payment initiation, relay of the instructions, communication between CBDC wallets, and completion.

① Payment initiation: An end user wishing to transfer some CBDC to a merchant for payment initiates the payment instruction through a CBDC wallet app on their smartphone, which is executed through user authentication.

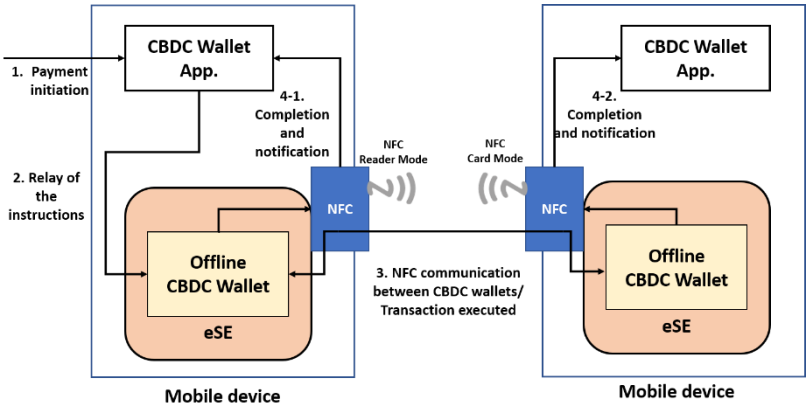
② Relay of the instructions: The instructions are relayed to the offline CBDC wallet app, transmitting NFC signals to the merchant's offline CBDC wallet app.

③ Communication between CBDC wallets: The preceding steps are processed and confirmed by the NFC between CBDC mobile wallet apps of the payer and the payee.

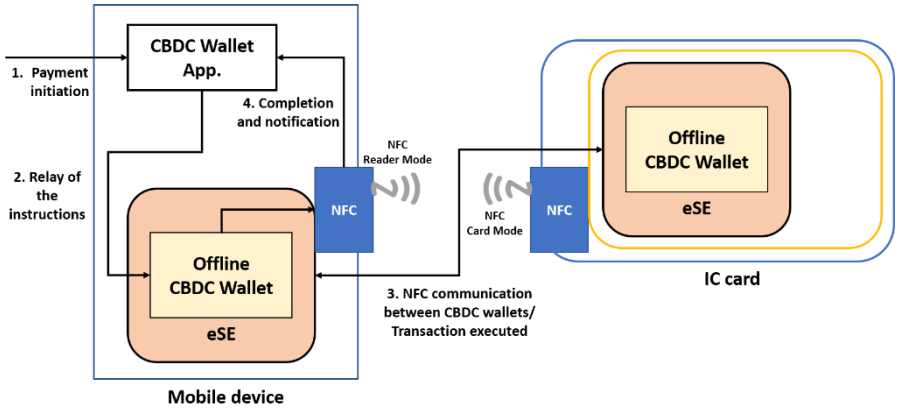
④ Completion: The offline CBDC wallet apps relay payment completion messages to the respective CBDC mobile wallet apps of the payer and the payee.

Offline CBDC Payment Using NFC

1. Mobile device → Mobile device



2. Mobile device → IC card



Source: BOK

Annex 2: Stylized example of the digital asset transaction flow

■ There are four steps to a digital asset transaction with a CBDC: digital asset registration, transaction request of the buyer, digital asset on the transaction block, and simultaneous exchange of the digital asset and the CBDC. A bridge system supports the linkages among the heterogenous distributed ledgers where the CBDC ledger executes the CBDC transfers, while the digital asset ledger processes the ownership transfer of the corresponding digital assets.

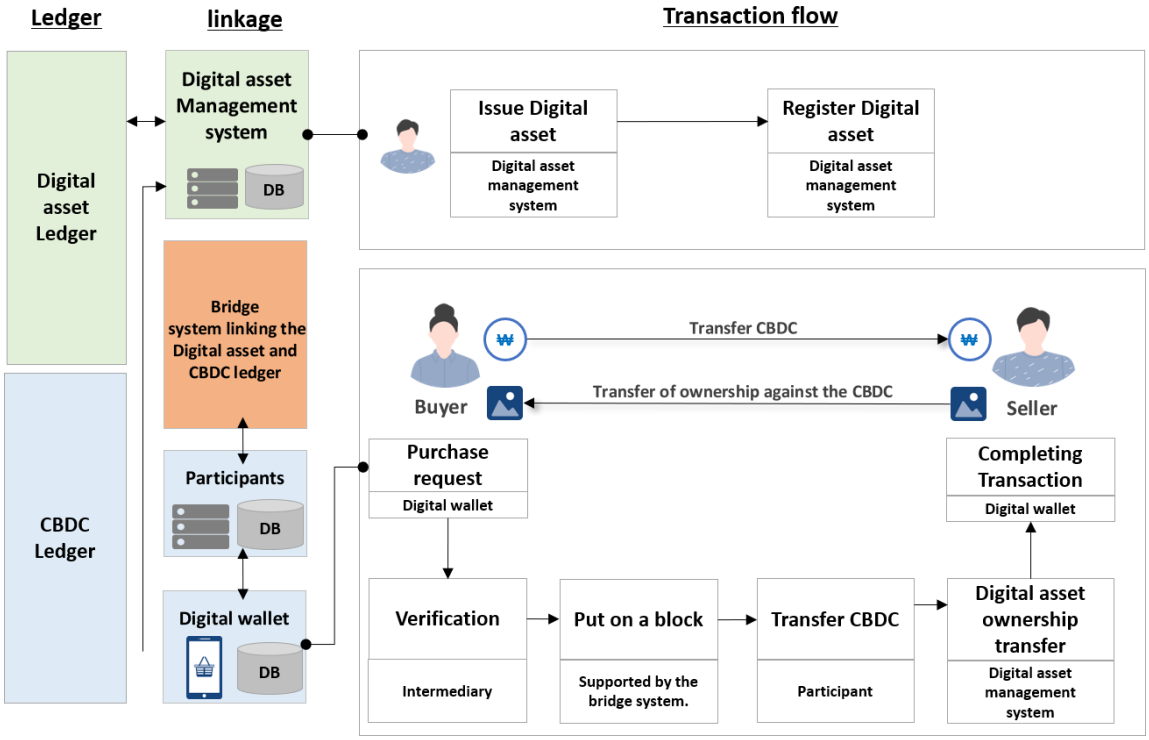
① Digital asset registration: A seller wishing to sell their digital asset registers tokenized images and videos on a digital asset management system.

② Transaction request of the buyer: A buyer submits a digital asset purchase request to the network using their mobile wallet app, followed by the participant node's confirmation of the buyer's ID, transaction information, and CBDC balance.

③ Digital asset on the transaction block: The network puts the digital assets on a block, disabling any potential purchase by other buyers of the same digital asset, which is completed by the distributed digital asset ledger.

④ Simultaneous exchange of the digital asset and the CBDC: The CBDC ledger executes the CBDC transfers from the buyer to the seller in concurrence with the transfer of the digital asset ownership from the seller to the buyer on the digital asset ledger.

Digital Asset Transactions by Linking Heterogenous Distributed Ledgers



Source: BOK

Annex 3: Stylized example of KRW-USD cross-currency transfers

■ The model assumes that USD and KRW CBDCs are in circulation on the two distinctive distributed ledger networks, and that the intermediaries undertake the required currency conversions. Note that step 2 and 3 below are executed instantly by a smart contract based on a pre-arranged exchange rate and relevant terms and conditions between the USD and KRW intermediaries.

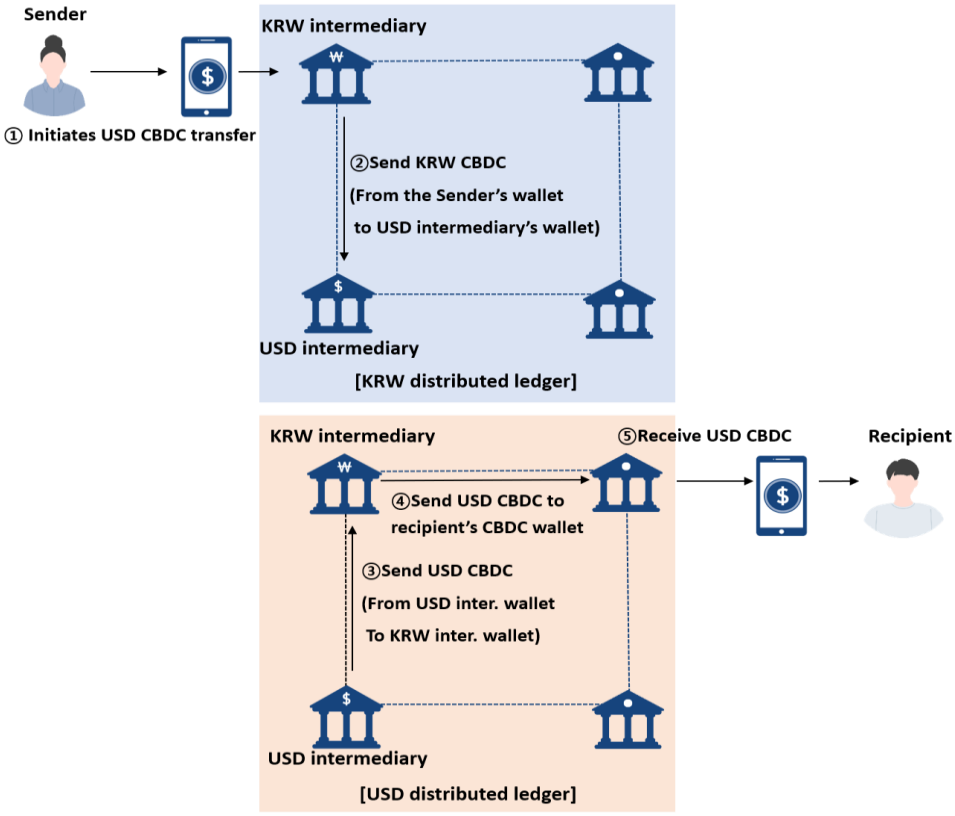
① A sender initiates a USD CBDC transfer to a recipient by executing an equivalent KRW CBDC amount transfer from their wallet.

② The KRW intermediary sends the KRW CBDC from the sender's wallet to the USD intermediary's KRW CBDC wallet. The transfer is executed and recorded on the KRW distributed ledger.

③ The USD intermediary, in concurrence with step 2, above, sends the corresponding USD CBDC from its wallet to the KRW intermediary's USD CBDC wallet. The transfer is executed and recorded on the USD DLT ledger.

④ The KRW intermediary, upon completion of step 2 and 3, above, sends the corresponding USD CBDC from its wallet to the recipient's CBDC wallet.

⑤ The recipient takes the USD CBDC and the payment is completed.



Source: BOK

Annex 4: Rollup as a performance enhancement measure for a DLT platform

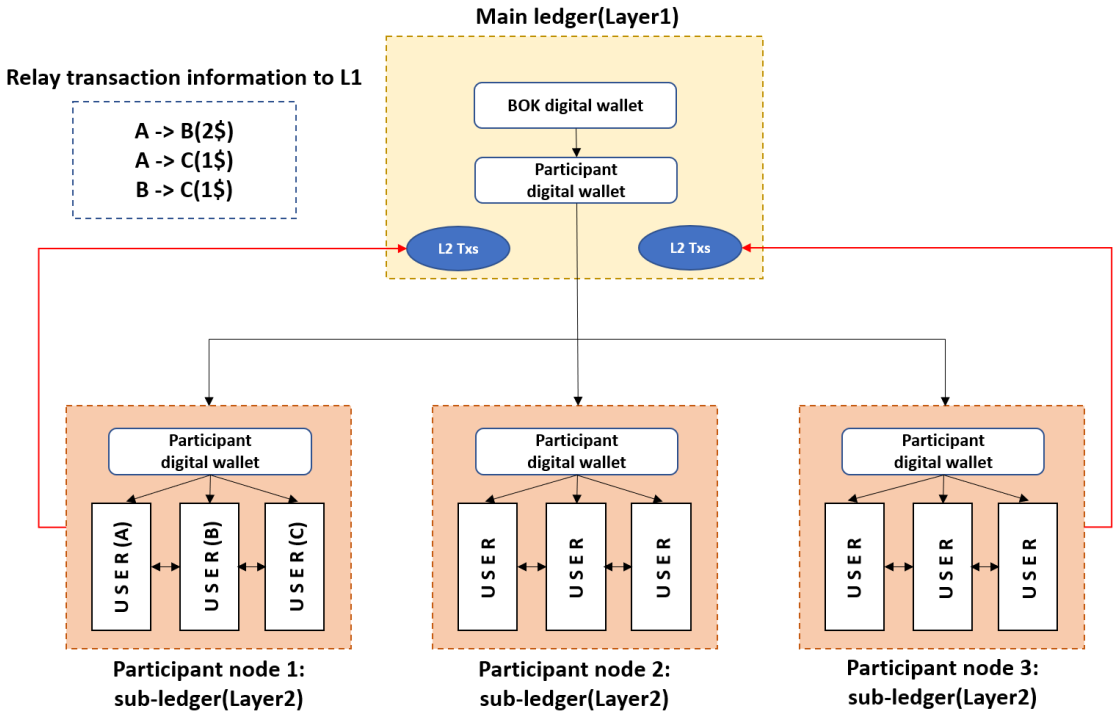
- Rollup refers to technology that processes instructions on a distributed ledger by layered structures composed of the main ledger (layer 1) and its network of sub-ledgers (layer 2), where the former aggregates and records the work of the latter in processing instructions. Rollup is considered to be a potential catalyst that could address (or circumvent) scalability constraints of a DLT platform in an environment where there is a large volume of relatively small-value payments. The PoC experiment tested its technical feasibility in supporting retail payments using a CBDC.

- The PoC, in particular, tested both an optimistic rollup and a zero knowledge rollup, the two typical variants that are widely recognized by the industry. The results provide the following observations:

  - **Optimistic rollup:** In layer 1, assuming that no fraudulent transactions take place, such as double spending, aggregates and records of transactions are submitted by layer 2, followed by subsequent validations of the transactions recorded. This methodology allowed each layer 2 ledger to process about 728 transactions per second in the experiment. Nonetheless, it took about a week for the layers to substantiate the validity and integrity of the transactions in the pertaining blocks, thereby putting end users' access to their CBDCs in their wallets on hold during this period.

  - **Zero knowledge (ZK) rollup:** Each node, i.e., each network participant, encrypts their transaction records in layer 2 using ZK encryption methodology, and relays them to layer 1. The ZK encryption enables nodes to anonymize their transaction records on the network. This experiment showed us that a ZK rollup enables each layer 2 ledger to process roughly 590 transactions per second, which is significantly slower than other general cases.

Scalability Experiments With Rollup



Source: BOK