

Discussion Paper Series

RIEB

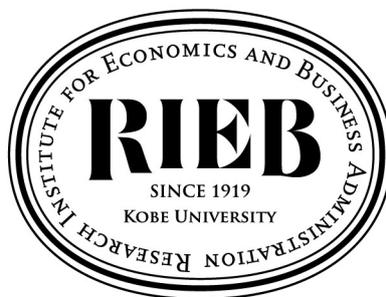
Kobe University

DP2026-06

**Possible Network Infrastructure Securely
Transferring Data Having Value,
such as CBDCs**

**Wataru TAKAHASHI
Taiji INUI**

March 5, 2026



Research Institute for Economics and Business Administration

Kobe University

2-1 Rokkodai, Nada, Kobe 657-8501 JAPAN

Possible Network Infrastructure Securely Transferring Data Having Value, such as CBDCs

Taiji Inui, ISO/TC68, ISO20022 Payments & Securities SEG, Citron Systems, taiji.inui@home.email.ne.jp
Wataru Takahashi, Research Fellow, RIEB, Kobe University, wtaka.oue@gmail.com

Abstract—Central Bank Digital Currencies (CBDCs) are planned in many countries (central banks) and implemented in some countries. CBDCs issued as legal tender by central banks must guarantee both security and anonymity. This paper discusses network infrastructure requirements for securely transmitting digital assets having value themselves like CBDCs. For this purpose, a method to implement an infrastructure to securely transmit CBDCs using Public Key Infrastructure (PKI) is discussed.

Keywords—CBDC, ADCC, central bank, two-tier system, PKI, DLT, CA, digital device

I. INTRODUCTION

When sending paper-based information to a remote location, methods such as letters and postcards which do not have extra security measures can generally be used. On the other hand, when sending physical banknotes such as ten-thousand-yen bills, a special envelope called "cash registered mail (Figure 1)" is required in Japan. More specifically, Japanese yen banknotes (currency) need to be sent using a special envelope to be sealed securely preventing it from unauthorized opening as well as each mail to be identified by registering it to Japan Post. Even if something such as losing the envelope with the banknote inside because of natural disaster, robbery, accident etc. happened, the amount of banknotes to be sent will be guaranteed up to 500,000 yen by the Japan Post.

Figure 1. Cash registered mail



Currently, financial transactions to send money (funds transfers) are conducted by transferring only information (payment instructions) through payment and settlement systems (networks) and/or banking systems to move (change) the ownership of the "money" which is stored within a database protected by robust security. In case of the Bank of Japan Financial Network System (BOJ-NET) which is known as one of the most secure payment and settlement systems

since it is the largest value payment system in the world as far as authors know and also keep the money (Japanese yen) within the most secure database from the viewpoint of physically and information technology perspective as far as I know. As such the money (value) itself never goes outside the secure environment (the database). It is also true for the faster payment systems such as Zengin system processing messages (payment instructions) about 6 million transactions a day in average where the value itself is stored in the database managed by individual banks from the retail payment perspective. In this case the money (value) from wholesale perspective will move (to be settled) later within the database managed by the Bank of Japan (reference [1]). Therefore, money (value) itself never goes through the network in terms of current payment system perspective. Talking about digital form of money, electronic money has been popular and used a variety of occasion since around 2000 in Japan. One of the authors proposed electronic money issued by central banks (reference [2]), which may be referenced when discussing CBDCs. In case of electronic money, value (figure) recorded in a digital wallet (device) is when transferring ownership instead of transferring money. It is different from transferring (handing over) banknotes. Whereas, taking look at recent trends, Central Bank Digital Currencies (CBDCs) which may need to transfer value itself through networks are planned in many countries (central banks) and implemented in some countries. As a matter of fact, the Bank of Japan conducted proof of concept (POC) for digital yen phase 1 and phase 2 in 2022 and 2023, respectively. The results of POC Phase 1 and Phase 2 are reported in reference [3] and [4], respectively. After completing POC Phase 1 and Phase 2, the Bank conducted Pilot Program on CBDC and published a report (reference [5]). The Program discussed a variety of issues including (i) privacy, (ii) process flow for credit transfers, (iii) performance, and (iv) functional scalability. The Program also established working groups with stakeholders to discuss CBDC issues such as (i) connection between CBDC systems and external systems, (ii) CBDC ecosystem, (iii) KYC and authentication/authorization, (iv) new technologies, (v) user devices and interfaces, (vi) coexistence of CBDC and other payment instruments, (vii) operational flow, etc.

In case of Europe a Pilot Program started in 2021. After completing the Pilot Program, the ECB Governing Council decided that the Eurosystem will move to the next phase of the digital euro project, then, recently European Central Bank (ECB) announced that if EU lawmakers adopt the regulation in the course of 2026, the digital euro could be issued during 2029 (reference [6]). Not only ECB but also other central banks including People's Bank of China (PBOC), Reserve Bank of India (RBI), Sveriges Riksbank, and Banco Central do Brasil (BCB) are also trying to introduce CBDCs which are possibly e-CNY (reference [7]), E-Rupi or eIND, e-krona, and DREX, respectively. Also, it is said that CBDC may already be introduced in Bahamas, Jamaica, Nigeria, and Cambodia.

The Bank of Japan published a report “The Bank of Japan’s Approach to Central Bank Digital Currency” in 2020 and posted on the Bank of Japan website followings are pointed out.; (i) there is a possibility of a sudden increase in societal demand for CBDCs in the future, (ii) while there are currently no plans to issue a CBDC, thorough preparation is deemed essential, and (iii) pilot experiments and institutional designs are being explored to develop a payment system suited for the digital era. The report also referenced a survey of central banks worldwide, noting that more than half foresee the possibility of issuing retail CBDCs in the near future.

In general, CBDCs issued as legal tender by central banks must guarantee both high security and full anonymity. This paper discusses network infrastructure requirements for securely transmitting valuable digital assets like CBDCs. Moreover, the system should provide mechanisms to swiftly detect counterfeit or altered CBDCs. When issuing CBDCs, the central bank should generate a set of authentication keys, securely storing the private key within a physically and digitally protected environment.

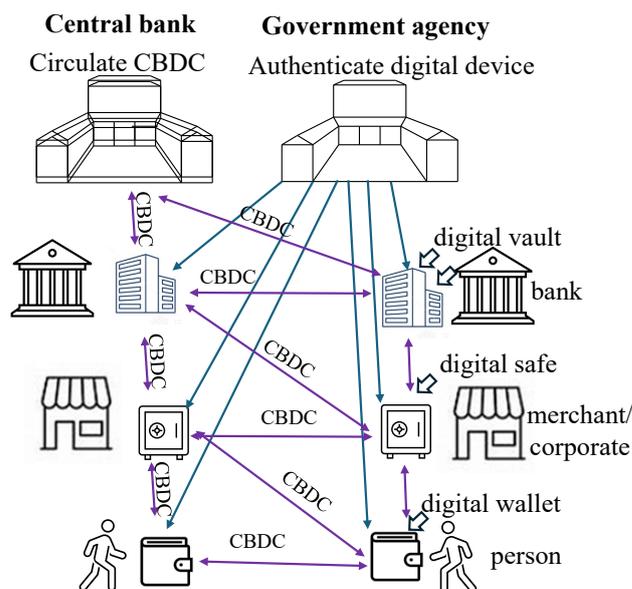
Each CBDC should have a unique alphanumeric serial number similar to the serial number of physical Bank of Japan notes, ensuring traceability. However, whether denominations of CBDCs similar to those for banknotes will be applied or not remains uncertain. Additionally, CBDCs should feature a digital seal encrypted with the central bank’s private key, allowing verification using the public key.

Besides central banks, government agencies responsible for digital devices (vaults, safes and wallets) will be established to manage security measures. PKI should be employed to authenticate digital devices with relevant government agencies serving as certification authority (CA). Encryption keys (both private and public keys) must remain strictly within the designated network infrastructure without external exposure.

Similarly, digital devices should carry a seal encrypted with the respective government authority’s private key, ensuring authentication via the public key. Given that digital devices may use less secure networks, such as the internet, secure transmission methods should be implemented. Devices should perform mutual authentication using private and public keys while generating and sharing sufficiently strong encryption keys. For further details, refer to the document “Electronic Money and Electronic Money Systems Issued as Legal Tender by Central Banks or Equivalent Institutions” by the author (reference [2]). The institutional framework to issue CBDC is shown in Figure 2.

Given this context, unlike existing payment systems, CBDCs—representing money itself—are expected to go outside secure databases and be transmitted across networks. This scenario is comparable to sending actual cash through registered mail but in digital form. Consequently, a security framework equivalent to “cash registered mail” must be established for transmitting CBDCs over networks. Hereinafter a method to securely transmit CBDCs using Public Key Infrastructure (PKI) is discussed. An image of distributing CBDCs is as “An image of two-tier network architecture”.

Figure 2. Institutional framework to issue CBDC

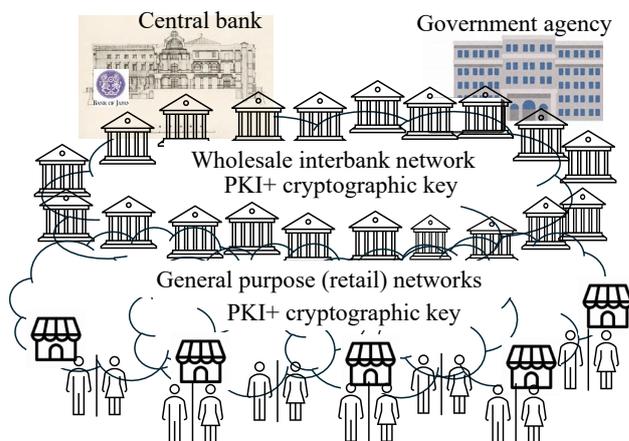


Just like conventional payment and settlement systems, two-tier system will be applied. More specifically, CBDCs are issued by central banks and distributed via financial institutions (through banks as the intermediary before distributed to the public including merchants and people) for retail payment perspective.

II. NETWORK INFRASTRUCTURE FOR TRANSMITTING CBDCS

In order to securely transfer data having value themselves such as CBDCs, CBDCs need to be protected by encryption with keys having sufficient strength as well as authenticated by using PKI. In this case two-tier network architecture will be adopted just like the current architecture for banknote distribution. An image of two-tier network architecture for CBDC distribution is shown in Figure 3.

Figure 3. An image of two-tier network architecture



1. Domestic transferrer network for CBDCs

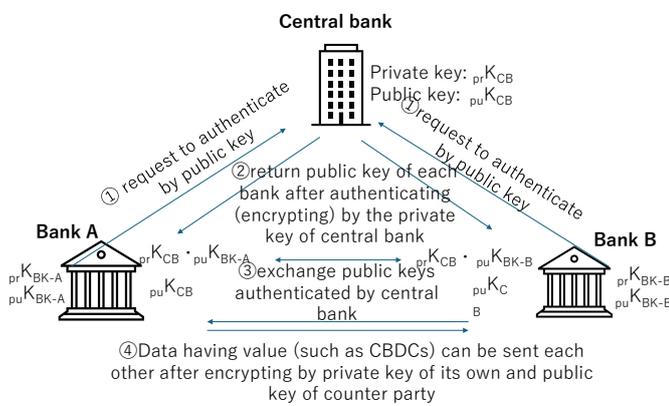
Wholesale CBDC transferrer between two commercial banks in a country (domestically) is discussed here. A shared strong encryption key can be exchanged between Bank A and

Bank B by using PKI. More specifically Bank A send a strong encryption key to Bank B after encrypting it using its private key and public key of Bank B. Bank B decrypt it by its private key and public key of Bank A when received it. To increase security level, Bank B send back the shared strong encryption key to Bank A after encrypting its own private key and public key of Bank A, which makes mutual authentication more secure. The wholesale CBDC transfer is shown in Figure 4.

With respect to the strong encryption key, Triple Data Encryption standard (DES) or Advanced Encryption Standard (AES) may be applicable though it should be decided by the banks.

Bank A and Bank B can also be authenticated each other by using private key and public key as explained the above. CBDCs are transferred by encrypting by the shared strong encryption key. Wholesale (domestic) CBDC transfer is shown in Figure 4.

Figure 4. Wholesale CBDC transfer



Private keys and public keys for digital devices such as digital vaults, digital safes, and digital wallets are issued and managed by government as shown in Figure 2.

2. Cross-border network for CBDCs

Then, cross-border network infrastructures will be an important issue. Also, CBDCs may be used for cross-border payments. Then, there will be some initiatives to implement regional digital common currency such as Asia Digital Common Currency (ADCC) or even Global Digital Common Currency (GDCC) for cross-border payments and settlements. With respect to the ADCC, refer to the Appendix “Outline of Asia Digital Common Currency (ADCC)” as well as references [8], [9] and [10] for GDCC.

As already discussed, CBDC can be issued by the central bank. Also, digital devices such as digital vaults, digital safes, and digital wallets can be authenticated by the government agency in each country.

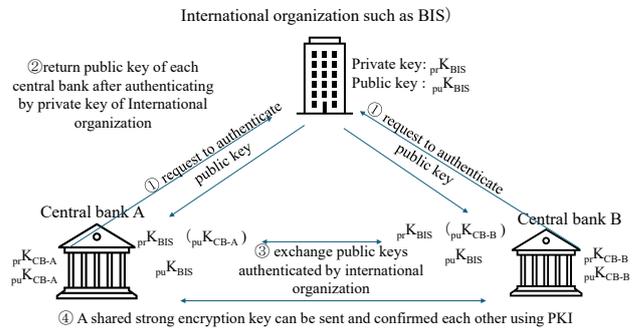
With respect to the model for international (cross-border) transfer of CBDCs including and digital common currency (ADCC for example) an image of cross-border transfer is shown in Figure 5.

Central banks may not want to be authenticated by the international organization established by governments of

member countries. Digital devices owned by the central banks may be authenticated each other under the BIS framework.

Cross-border transfer of CBDC is shown in Figure 5.

Figure 5. Cross-border transfer of CBDC



With respect to actual implementation, there may not be such a system or network directly transferring CBDCs or data with value (money) as far as authors know for the time being. Having said that, there is an example which may better be reported here for reference, which is “Cross-border DVP Linkage between Japan and Hong Kong”. More specifically, “the Bank of Japan Financial Network System (BOJ-NET) Japanese Government (JGB) Services” and “Hong Kong Monetary Authority (HKMA) Hong Kong dollar Clearing House Automated Transfer System (CHATS)” are directly connected each other to provide DVP services in 2020. In this case, each central bank generated private key and public key and exchange public key, then a shared encryption key with sufficient strength is exchanged. Specific characteristics of such keys are not disclosed for security purposes. Considering the nature of digital common currency such as ADCC, a network infrastructure needs to connect related central banks as a final goal. Also, considering the possibility of CBDCs to be implemented regionally or globally, a network infrastructure securely connecting not only central banks but also commercial banks as well as related government agencies may need to be established with appropriate granularity.

3. Retail network

One of the most important user requirements for the retail payments using CBDC may be offline payment by touching digital wallets each other and/or digital wallet and POS machine without using remote network, as well as the remote transfer of CBDC between mobile devices. Such retail payments are out of scope of this paper. Having said that since this is an important issue to keep interoperability of payments among retail payment devices such as POS machines and mobile devices, international cooperation framework to discuss this kind of issues may need to be established. Not only technological interoperability but also interoperability in terms of legal framework, operating practices, market practices, etc. may also be important. The experience by “Cross-border DVP Linkage between Japan and Hong Kong” described above may help in this perspective. Though it is not for CBDCs but for electronic money, plastic card with contactless IC chip inside is widely used globally in particular in Japan since 2000. Mobile phones (smart phones) with contactless IC chips are also used. These currently used devices may be a convenient candidate to be used as an electronic wallet for CBDCs.

III. CONCLUSION

This paper discusses network infrastructure requirements for securely transmitting digital assets having value themselves like CBDCs. For this purpose, a method to securely transmit CBDCs using Public Key Infrastructure (PKI) is discussed. In addition to that, followings may be pointed out.

CBDCs are being planned in many countries (central banks) and already implemented in some countries, then could be developed globally. Considering current technological advancement and cost of handling paper banknotes digital form of money as the legal tender will be issued and prevail soon or later. Also, issuing money is an important issue to keep monetary sovereignty as well as seigniorage. As such, central bank of each country may need to keep its own national currency even for the digital form of money. Also, money used for cross-border transactions (international currency) may be regarded as a global public good considering the proposal by Mr. John Maynard Keynes and recently by Mr. Mark Carney. Therefore, a reasonable international institutional framework may need to be established.

It should be noted that the opinions and content presented in this report represent the personal views of the authors and do not reflect the official stance of central banks, international institutions, or any other organizations.

IV. ACKNOWLEDGMENT

The authors express their heartfelt gratitude to Mr. Masayuki Mizuno of Hitachi, Ltd. Mr. Shinya Kitajima of Fujitsu Limited, Mr. Yusuke Yanagida and Mr. Zen Kawada of NTT Data, Mr. Tetsuya Inoue of Nomura Research Institute, and Mr. Noritaka Akamatsu of International Monetary Fund. Last but not least, the authors would like to express deepest appreciation to Mr. Moayad Z. Alouqalily and his team for their advices and comments to improve this paper.

REFERENCES

- [1] Current Status and Future Prospects of Payment & Securities Settlement Systems in Southeast Asia, Taiji Inui, Ministry of Finance, 2022
- [2] Electronic Money Issued by Central Banks or Equivalent Institutions as Legal Tender, Taiji Inui, 2009, Google site
- [3] Central Bank Digital Currency Experiments: Results and Findings from “Proof of Concept Phase 1”, Bank of Japan, 2022
- [4] Central Bank Digital Currency Experiments: Results and Findings from “Proof of Concept Phase 2”, Bank of Japan, 2023
- [5] Central Bank Digital Currency Experiments Progress on the Pilot Program, Bank of Japan, 2025
- [6] Progress on the preparation phase of a digital euro, European Central Bank, 2025
- [7] Theories and Practice of exploring China’s e-CNY, Changchun Mu, People’s Bank of China, 2022
- [8] A Proposal for an Asia Digital Common Currency (ADCC) Applying Distributed Ledger Technology (DLT) and Blockchain Technology (BCT) from Part III - The Power of Distributed Ledgers in Payments, by Taiji Inui and Wataru Takahashi, edited by Sabrina Leo and Ida Claudia Panetta, Cambridge University Press, 2023

- [9] Asia Digital Common Currency as a Global (International) Currency, Wataru Takahashi, Taiji Inui, RIEB, Kobe University, 2022
- [10] On Possible Measures and Processes to Issue Digital Common Currency in ASEAN+3 Including Challenges and Opportunities, Taiji Inui, Wataru Takahashi, Mamoru Ishida, RIEB, Kobe University, 2020

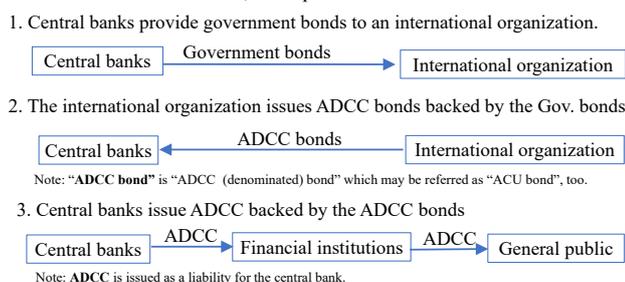
Appendix: Outline of Asia Digital Common Currency (ADCC)

Asia Digital Common Currency (ADCC) is to be issued by each country in Asia (ASEAN+3) coexisting with local currency in each country.

1. Basic Concept

Basic concept for issuing ADCC is (i) central bank in each country provides government bonds in each country to an international organization, (ii) the international organization issues Common currency denominated bonds (ADCC bonds) and returns the bonds to the international organization in accordance with the government bonds provided, (iii) the central bank received (returned) ADCC bonds from the international organization issues ADCC as the liability of the central bank backed by the ADCC bonds as assets. ADCC is utilized as the common currency mainly for cross-border trades, payments, and settlements as well as those for domestic purposes at local markets as well.

Chart A1, Concept to issue ADCC



ADCC is distributed for cross-border payment and settlement.

An image for each central bank in the region provides local currency denominated government bonds to the international organization is shown in Chart A2. The ADCC does not bear interest just as banknotes doesn't.



ADCC bond is a bond denominated with currency ADCC. (Appendix)

Firstly, issuing ADCC bonds is highly related with the stability of ADCC as a currency. Also, issuing ADCC bonds may have an equivalent role with the European

Monetary Union established the conditions for joining the union (convergence criteria), Maastricht Treaty though there may have big differences from the conditions in Europe including historical background, scale of economy of each country, impact to the region, etc.

As such, issuing ADCC bonds has an important meaning, particularly to be used for cross-border trade and settlement. Tokenized bonds can be issued and distributed without having specific Central Securities Depository (CSD) utilizing DLT. In other words, the advantage of the ADCC bonds may be that the bonds can be issued without relying on local CSDs. The ownership of the bonds can be secured by having the tokenized bonds. More specific issues such as issuance of the ADCC bonds by the international organization, distribution to central banks, are discussed as follows:

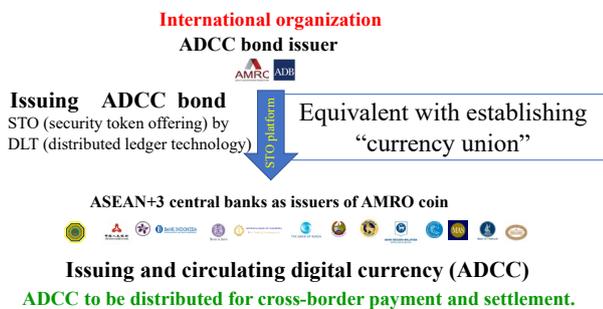
Issuing digital securities (security token) may already be a proven technology having actual implementation such as securities issuance of the World Bank (bond-i) for example. In Japan, the law enforced in May 2020 "Amendment of Financial Instruments and Exchange Act" stipulated "Electronically Recorded Transferable Rights to Be Indicated on Securities, etc." and "Electronically Recorded Transferable Rights" which made the legal position of digital securities clear. More specifically, "Electronically Recorded Transferable Rights to Be Indicated on Securities, etc." may correspond to the "securities" defined by Article 2 (1) of the "Financial Instruments and Exchange Act" positioning security token as digital securities. "Electronically Recorded Transferable Rights" may correspond to "Assets deemed to be money" of Article 2-2 of the Act.

Issuing digital securities (security token) can generally be issued with same way as normal securities. An issuer (possibly an international organization) issues securities and investors (central banks in this case) purchase the securities (ADCC bonds). Paying agent assigned the role may take care of principal and interest payment. Also, the digital securities in this case may not be issued by public offering considering the characteristics of the securities. The difference from the conventional securities issuance may be that it can be issued without central securities depository (CSD). Therefore, creditors (owners) of securities are recorded in the bond ledger, which guarantees (secures) ownership of the securities. The bond ledger is managed by blockchain infrastructure (platform). Also, a variety of matters such as rating of the securities, paying agency, etc. may be discussed at the international organization and decided by

member central banks (or possibly including related government agencies). Since the operator (provider) of the blockchain infrastructure should play a very important role, the decision needs to be done carefully after sufficient survey and discussions by the members.

The international organization and member central banks are to be connected by P2P network technologically. The international organization returns ADCC bonds each central bank. The amount of ADCC bonds to be returned may be equivalent with the government bonds received from each central bank. The ADCC bonds can be transferred each other through the distributed ledger technology (DLT). A possible image of issuing ADCC bonds is shown in Chart A3.

Chart A3, Possible image of issuing ADCC (denominated) bonds backed by government bonds utilizing DLT such as STO

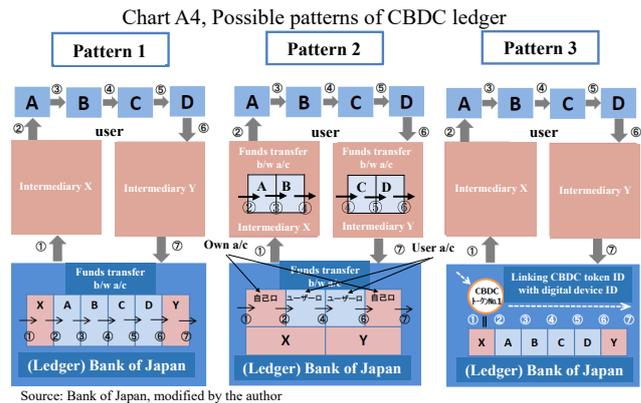


Brief description on Common (metal) common currency in Ming Dynasty, Asia Digital Common Currency (ADCC), issuing methods including procedures of ADCC, exchange rate calculation of ADCC, are discussed in references [a1], [a2], [a3], and [a4].

2. Issuance and circulation of ADCC

With respect to the issuance and circulation of ADCC, firstly, the central bank in each country issues ADCC as the liability of each central bank backed by the ADCC bonds as assets. Regarding the circulation of ADCC, it is expected to utilize infrastructures for CBDC in each country and for cross-border as well. Therefore, it may be essential to standardize and harmonize related infrastructures in each country for cross-border interoperability of ADCC and CBDC. For such a purpose, it is very important for central banks to cooperate each other together with the international organization. During the first stage, it may be possible to start from online type of issuance and circulation just like the Bank of Japan is planning for its CBDC (digital yen). Implementation of online ADCC/CBDC may need less investment compared to the case

including offline ADCC/CBDC. Possible image of ADCC/DBDC ledger is shown on Chart 4.



With respect to the wholesale side of infrastructure supporting ADCC/CBDC, connecting central banks and intermediaries (banks) blockchain/DLT platform may be adopted just like for distributions of ADCC bonds. On the other hand, regarding retail side of ADCC/CBDC, one of the most possible case may be using tamper resistance type of digital wallets such as smart phones with contactless IC chip inside as mobile wallets for offline payment and settlement. In such a case, blockchain/DLT platform may not be applicable considering technological features of the blockchain/DLT. Inter connection between wholesale and retail ADCC/CBDC which may be handled by central banks and intermediaries (banks, financial institutions, and payment service providers) may also be very important. It is one of the most important issues to secure interoperability between central banks to issue and circulate ADCC in terms of standardization and harmonization of specifications and user requirements including methods, framework, systems, regulations, etc. In any case, it is essential, for the international organization and central banks to discuss this kind of issues seriously.

References

- [a1] The Revival of Yongle Coins: The Future of Currency and the Asia Digital Common Currency, Wataru Takahashi, Kyoto Bank, 2020
- [a2] The Asia Digital Common Currency as an International Currency, Taiji Inui, Wataru Takahashi, Nissei Research Institute, 2022
- [a3] Issuance Methods, Procedures, and Considerations for the Asia Digital Common Currency, Taiji Inui, Wataru Takahashi, Mamoru Ishida, Kobe University Research Institute for Economics & Business Administration, 2023
- [a4] The Value (Exchange Rate) of the Asia Digital Common Currency (ADCC), Taiji Inui, Wataru Takahashi, Japan Finance Association, 2024