# Cos-CBDC: Design and Implementation of CBDC on Cosmos Blockchain

Jungsu Han[1], Jeongheon Kim[1], Aram Youn[2], Jinhee Lee[2], Yunsuh Chun[2], Jongsoo Woo[3], and James Won-Ki Hong[1,3]

[1]Department of Computer Science and Engineering, POSTECH, Korea.
{saw1515, kjheon1118, jwkhong}@postech.ac.kr
[2]Hana Financial Group
{younaram, leejinhee, yunsuh.chun}@hanafn.com
[3]Center for Crypto Blockchain Research, POSTECH, Korea.
woojs@postech.ac.kr

***Abstract*— With the advent of e-commerce and electronic payment systems, the use of paper currency is decreasing. Therefore, it is sufficiently predictable that most paper currencies will disappear and digital currencies will become the mainstream. This phenomenon is further accelerated by advances in blockchain technology and COVID-19. This is why the Central Bank Digital Currency (CBDC) has recently begun to attract attention. Currently, there are studies on CBDC with a blockchain-based distributed ledger. In this paper, we propose Cosmos blockchain based CBDC (*Cos-CBDC*) that enables communication between blockchains using Inter-Blockchain Communication (IBC) protocol to ensure interoperability. We not only analyze the requirements of *Cos-CBDC* but also design and implement it using Cosmos-SDK. Furthermore, we propose a Group Key Management system in *Cos-CBDC*. It can give different user privileges, and privacy-preserving is possible in the key generation process.**

***Index Terms*— Blockchain, Central Bank Digital Currency, Inter-chain Communication, Key management, Privacy**

## I. INTRODUCTION

Interest in Central Bank Digital Currency (CBDC) is growing in many countries due to the weakening status of paper fiat currencies, the popularisation of digital assets and technological advances in blockchain [1]. Bank for International Settlements (BIS) defined CBDC as a digital means of payment for which the central bank is directly responsible and that is represented by a unit of national account [2]. For example, in the case of stablecoins [3], it cannot be CBDC because it is not issued directly by the central bank. Similarly, if there is a digital dollar issued by the Bank of Korea, it cannot be called CBDC because the currency that Korea can take responsible for is only Korean Won (KRW). Summarizing these, CBDC is a means of payment that can be issued and held accountable directly by the national central bank.

Currently, 80% of the world's central banks are considering introducing CBDC, and they are interested in CBDC for several reasons [1, 4, 5]:

- **Financial inclusion** : It is necessary to overcome the instability of cash and design a completely secure financial system.
- **Resilience** : When the payment and settlement systems operated by the private sector is abruptly terminated, there should be a payment system with complete resilience like cash to prevent non-payable situation.
- **Cross-border payment** : During cross-border payment process, CBDC can reduce extra costs, trade efficiently and increase transparency.
- **Public privacy** : CBDC can help prevent crime while ensuring privacy through traceable anonymity.

In addition, CBDC is continuously attracting attention due to fiscal transfer, preparation of standards for electronic payment and so on.

In this paper, we design a retail CBDC architecture with consideration on technical issues for implementation. It covers the roles and requirements of each participant in the hierarchical structure of the central bank, commercial banks and customers, and presents technical elements for safe and reliable CBDC distribution and trading processes. In particular, we construct a system with the distributed ledger based on a blockchain, because it is cryptographically secure and can be prevented from single point of failure.

However, most existing blockchain platforms have clear performance limitations to be used for CBDC. For example, Bitcoin [6] is typically capable of processing 7 transactions per second (TPS), which is significantly less than Visa networks processing 1,700 TPS in the USA [7]. Another problem is that interoperability between blockchains is not guaranteed. For example, cross-border payment is difficult between countries that developed Bitcoin-based CBDC and countries that developed Ethereum-based CBDC.

In this paper, we propose *Cos-CBDC*, a CBDC system based on Cosmos blockchain [9]. The transaction capacity of *Cos-CBDC* can be up to 15,000 TPS depending on the block size and the number of validators in the BFT-based consensus algorithm. It also supports an inter-chain protocol to connect and communicate with different blockchains. In addition, we propose a key management system to manage various CBDC users, and make transactions safe and privacy-preserving possible.

The main contributions of this paper are :

- We design and implement *Cos-CBDC* as a digital currency operated by a central bank. We explain why Cosmos blockchain is suitable for a CBDC platform.
- We propose a key management system of *Cos-CBDC*. We make it possible to hierarchically manage a large number of keys in *Cos-CBDC* and differentiate privileges according to users.

The rest of the paper is organized as follows. In Section II, we introduce the background and related work about blockchain for CBDC and key management. Then, in Section III, we design and implement *Cos-CBDC*. We also describe a key management system for *Cos-CBDC*. In Section IV, we analyze *Cos-CBDC* in terms of reliability and scalability. In Section V, we conclude this paper and suggest possible future works.

## II. Background and Related Work

### A. Blockchain for CBDC

Determining which blockchain platform to use is an important issue for the development of blockchain-based CBDC. The core ledger of the blockchain determines the order of transactions among users and stores transaction information in blocks that cannot be falsified. It should also ensure that transactions are confirmed within a low latency that supports simultaneous transactions of multiple users. Although [10] chooses R3 Corda and [11] chooses Hyperledger Fabric as the blockchain platforms for CBDC, these platforms are not suitable for implementing cross-border payments. As there is no standardized blockchain platforms for CBDC systems, most of CBDCs are being independently developed with different platforms by countries. To address this issue, [12] emphasizes the importance of the interoperability protocol, which supports connections between heterogeneous blockchains.

Various scaling methods for blockchain performance have been proposed as with interoperability. [8, 13] present an overall roadmap for blockchain design to increase scalability in terms of network, consensus, storage and data structure. [14] proposes a multiple blockchains architecture that the inter-chain transaction between heterogeneous blockchains is possible. They explain that there is the three commit phase for confirming transaction message in inter-chain transaction, so the average throughput of inter-chain transaction is lower than that of intra-chain transaction. Several approaches have been proposed to apply a multiple blockchains architecture to CBDC [15, 16]. However, they have conducted experiments in their own sandbox and do not use a public blockchain platform.

We have decided to use Cosmos [9] that easily supports inter-chain transactions and vertical scaling among existing blockchain platforms. Cosmos is an inter-chain that allows multiple blockchains to interoperate while security properties are guaranteed. To this end, Cosmos created two types of blockchain structures: Hubs and Zones. Zones are separate blockchains and hubs are blockchains specifically designed to connect Hubs together. The hubs and zones of the Cosmos network communicate with each other through Inter-Blockchain Communication (IBC) protocol. Tokens and transaction messages can be transferred safely and quickly from one zone to another through the hub without interzone exchange. The Cosmos hub tracks the total amount of tokens held by each zone, and anyone can connect a new zone to Cosmos hub, making it compatible with the new blockchain. Cosmos makes blockchain easy to develop with Tendermint Core and Cosmos SDK [17]. The IBC protocol and peg zones [18] allow different types of blockchains to trade tokens and data with each other. In addition, Cosmos allows blockchain applications to scale to millions of users through horizontal and vertical scalability solutions.

### B. Key Management

[19] proposes a method of signing the transaction using the private key of CBDC owner through the blockchain. The validator verifies the validity using the public key of transaction. If the private key is exposed to outside, a malicious user can create a valid signature and cause financial damage to CBDC owner. Therefore, the safe storage and management of private keys is one of the important requirements in designing CBDC systems.

In general, digital wallets manage private keys, and various key management systems based on Public Key Infrastructure (PKI) [20] are presented. There is a possibility that private keys may be leaked due to man-in-the-middle attacks [21] or wallet thefts [22]. Therefore, when signing a transaction, there have been studies on ways in which signing is possible only with the consent of multiple users. For example, there are signing methods such as Multi signature (Multisig) [23] and Multi-party Computation (MPC) [24]. Multisig is a technology that enhances security by requiring more than one signature for a transaction. Unlike this, MPC is a method for participating parties to jointly compute a function without knowing other's input. MPC is also called privacy-preserving computation. In this paper, we propose a method for Group Key Management system [25] to generate a Group Key with MPC.

## III. Design and Implementation

### A. Requirements

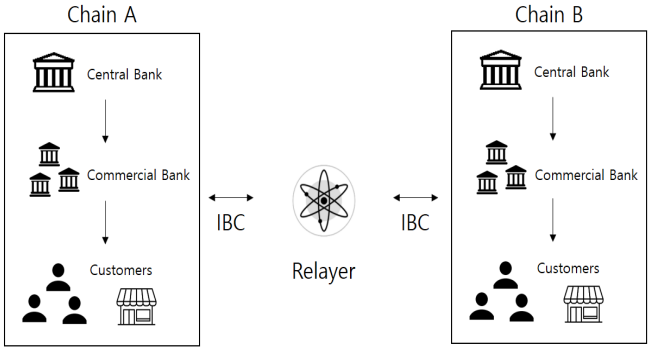



Fig. 1: Inter-Blockchain Transactions in Cosmos

As blockchain technology advances, the consensus algorithm or network structure has been upgraded, which greatly improved the performance of blockchain systems [26, 27]. However, since there is no international standard for CBDC, and there is no guarantee that a certain blockchain can be selected as a standard CBDC platform even if its performance is satisfactory. In addition to the performance aspect, considering compatibility with the existing banking system is an important factor in designing a CBDC. BIS reported that cross-border payment benefits users greatly in adopting CBDC [28]. Therefore, it is important that CBDC blockchain platforms be interoperable. We propose that Cosmos, which enables communication between heterogeneous blockchains with the IBC protocol, is the most suitable for CBDC among existing blockchain platforms. Cosmos connects to other blockchains through an off-chain channel called *relayer*. As shown in Fig. 1, the *relayer* acts as a router that forwards transaction packets to the appropriate blockchain using the chain ID.

### B. User Layer

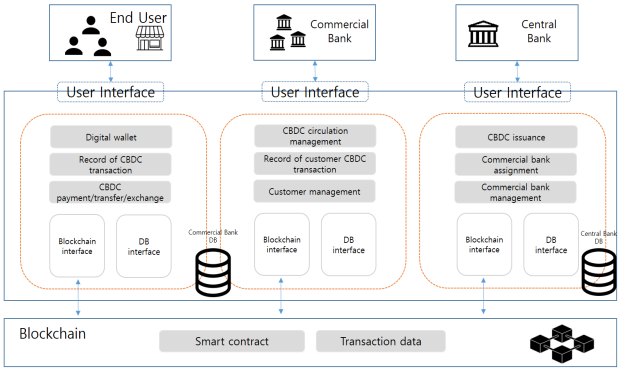



Fig. 2: CBDC High-level system design

CBDC users will be divided into three main types: the central bank, commercial banks, and customers, as illustrated in Fig 2. The central bank has the privilege to issue and allocate CBDC. Its key role is to manage CBDC safely and effectively. That is why it has the highest privilege in CBDC system. Commercial banks are responsible for distributing CBDC smoothly, managing CBDC for customers and conducting inter-bank wholesale transactions. They need to build an efficient system to ensure that there is no inconvenience caused by latency or throughput because they interact directly with a number of users. Customers are main CBDC users with retail transactions. They can be divided into KYC (Know-Your-Customer) [29] users and non-KYC users. KYC is the process of identifying a customer at a bank. KYC process is essential for transactions through banks. On the other hand, off-chain transactions like cash can be traded without KYC process. In this paper, CBDC system is designed exclusively for KYC users.

### C. Blockchain Layer

**Bottleneck.** All CBDC transactions are stored on the blockchain. If a client sends a request message, remote procedure call (RPC), to the blockchain, it can easily look up transaction records. However, sending numerous RPCs for simple tasks such as checking transaction history may cause bottlenecks to nodes. This reduces transaction processing speed and results in latency, which have a significant impact on smooth CBDC usage. To prevent this, it is possible to increase throughput by dividing transactions into the requests that need to be recorded in blockchain and the other requests that do not. Regardless of TPS of the blockchain, this is about whether individual clients of the bank can handle requests from millions to tens of millions of users. It is possible to create multiple clients to distribute the workload, but in that case, there is a burden of running a number of full nodes that stores all transaction data. Therefore, it is possible to use an independent database that synchronizes with CBDC blockchain in real time in terms of data accessibility and ease of management. For example, banks can use relational database for higher capacity of reading and writing data compared to blockchain [30]. As shown in Fig. 3, the specific process is as follows:

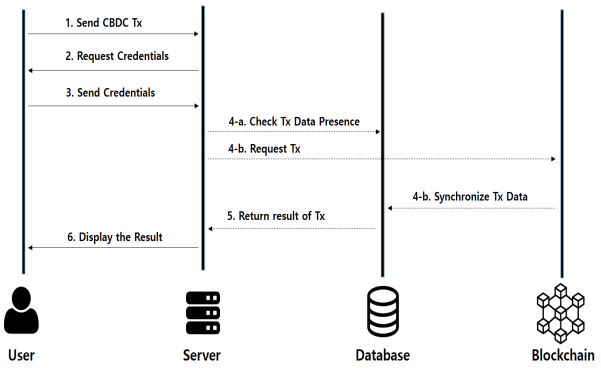



Fig. 3: CBDC Transaction Workflow with Middleware Database

1) A CBDC user asks transactions such as transfers, exchanges, and payments.
2) The bank requests a user credential.
3) The user provides his credential and the bank confirms it.
4) a) The bank verifies that there is data in the bank database to process transactions, and if so, proceed to the next step. If there is no data, it works like 4-b.
   b) The bank sends transactions on blockchain to handle user requests. In blockchain, the transaction is checked to make sure that there is nothing wrong with the transactions, and if not, the transactions are carried out successfully. The bank database synchronizes information on the blockchain in real time.
5) The result of transaction requests is delivered to the bank.
6) The transaction results are sent to the user.

The database is not associated with the execution of transactions and is synchronized with the data stored on the blockchain, serving only as a middleware to reduce response

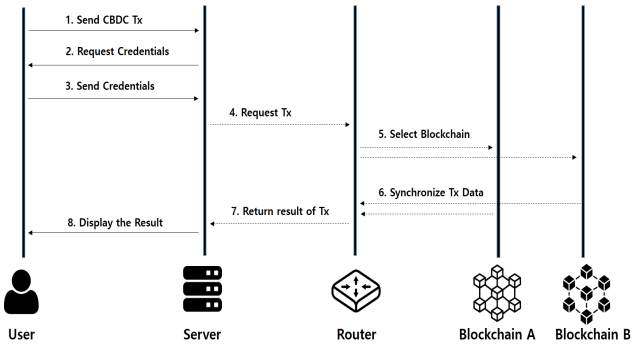



Fig. 4: CBDC Transaction Workflow with Router

latency. This allows banks to design their own specialized database schemas for easy management, and minimizes long-latency RPC requests to increase data accessibility. In other words, this is an example of how to overcome the bottleneck of blockchain clients. However, this method is not a fundamental solution because databases are likely to be falsified more easily than blockchain ledger and there are additional costs for synchronization.

**Blockchain Routing.** We propose a blockchain routing system with inter-chain transactions between heterogeneous blockchains. Each independent blockchain can act as a side-chain and the performance of *Cos-CBDC* can be improved horizontally. Unlike a single ledger blockchain such as Bitcoin and Ethereum, *Cos-CBDC* is easy to create a side-chain with Cosmos software development kit (Cosmos-SDK). Therefore, it must be determined which blockchain should be selected when executing transactions. This requires a *router* to analyze transaction requests and select the appropriate blockchain. As shown in Fig. 4, the specific process is as follows:

1) A CBDC user asks transactions such as transfers, exchanges, and payments.
2) The bank requests the user credential.
3) The user delivers his or her credential and the bank confirms it.
4) The bank sends the transactions on the blockchain to handle the user's requests.
5) The router determines which blockchain will execute the transaction through the sender's wallet address. If the receiver exists on another blockchain, it executes inter-chain transaction.
6) The router synchronizes information on blockchain in real time.
7) The result of the transaction request is delivered to the bank.
8) Transaction results are sent to user.

Through such horizontal scaling, the bottleneck can be solved by preventing excessive RPC requests to a single node. Since each node does not store all CBDC transactions, it is efficient for banks to operate nodes in terms of TPS and latency.

### *D. Key Management Layer*

It is important for *Cos-CBDC* to know and manage in which blockchain a specific user exists. To this end, we propose a Group Key Management (GKM) for efficient key management. GKM is a suitable method for key management with a hierarchical structure. In CBDC transactions, users need to have different privileges to create transactions. For example, only central bank should have the highest level of privilege for issuing and managing CBDC. Commercial banks should have more privileges than customers for CBDC distribution and customer management. Otherwise, indiscriminate key generation or signing is possible, making the KYC process difficult, and CBDC may be used for crime. Therefore, a multi-layered architecture is needed for key management in CBDC transactions. As shown in Fig. 5, in CBDC architecture, GKM system can be composed of the central bank, commercial banks, and customers.

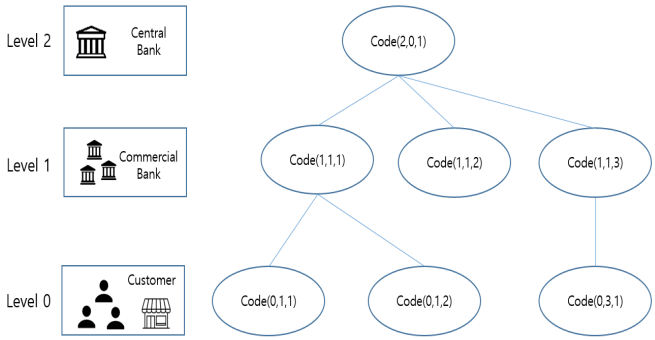



Fig. 5: Group Key Management for Cos-CBDC

In multi-layered architecture, it is assumed that the nodes in the upper layer have more privileges than the nodes in the lower layer. The number written on the node is a code to identify the group, and is represented by a Code(i, j, k). i denotes the level of the node, j denotes the position of parent node in upper layer and k denotes the position in current layer. A Group Key (GK), $GK_{i,j,k}$, is used in the blockchains which have a Code(i,j,k) to generate messages. Banks can use the GK in deciding whether to approve any transactions in the same group. To do this, it is necessary to make GK not a key dependent on a specific blockchain. $GK_{i,j,k}$ is computed in the following way where $c_1, c_2, c_3$ denote the child groups and $f(\cdot)$ denotes a one way function with equal length of input and output values.

$$GK_{i,j,k} = f(GK_{i-1,k,c_1}, GK_{i-1,k,c_2}, ..., GK_{i-1,k,c_l})$$

Our goal is to differentiate privileges based on the user level and enable efficient management. In this way, the group key of the upper layer is updated. When the GK of the parent group is updated, it is assigned to the child groups. This allows the group key of the upper layer to have more privileges and enables a hierarchical structure. We also propose to use the MPC method for function $f(\cdot)$. This makes it possible that child groups do not share

key information while updating parent's GK. Then, we can achieve privacy-preserving of child groups and secure key generation.

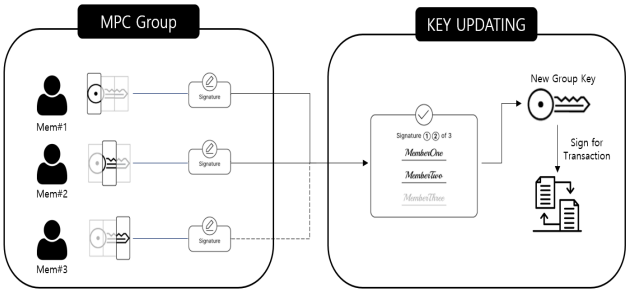


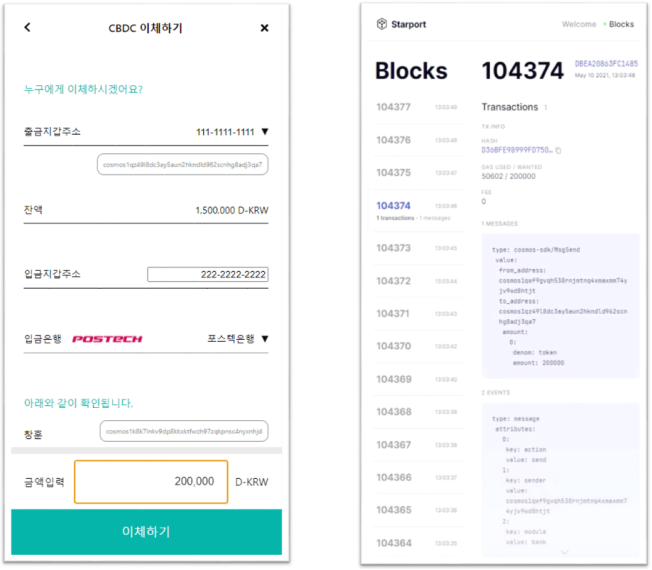

Fig. 6: GKM system with MPC

Fig. 6 shows how MPC works in a GKM system. When n of m signatures are created, where n denotes MPC threshold and m denotes the number of members in the blockchain, the group key update proceeds. The member's key used for key update is independent of the blockchain. When the group key is updated successfully, the bank that manages the group key can use it to create special-purpose transactions such as issuing or distributing CBDC.

### *E. Demo*

*Cos-CBDC* operates collaboratively on a web, a mobile, and a server. An overall operation flow of *Cos-CBDC* is as follows. First, the central bank will be responsible for issuing CBDC. The central bank selects the type of CBDC, types the amount of CBDC to be issued. There are three types of CBDC in *Cos-CBDC* : regular CBDC, time limited CBDC, time reducing CBDC. Regular CBDC is a CBDC that can be used like existing cash. It is free of payment and remittance and can be easily exchanged for fiat cash. In the case of time limited CBDC, if it is not used within a set deadline, the funds will disappear and can no longer be used. Time reducing CBDC is funds that reduce CBDC reserves by a certain percentage to induce the use of CBDC issued for specific purposes, such as disaster assistance. Therefore, time limited and time reducing CBDC are designed to be usable within a certain period of time in limited places.

When CBDC is normally allocated to individual customers, they can use banking services according to their intended use and purpose. Fig. 7 shows the scenario of transferring CBDC to another user. Fig. 7-(a) is a User Interface (UI) for the customer, and the customer can enter the amount to be remitted and the account number of the recipient. When user enters the account number, CBDC wallet address mapped one-on-one with the number will automatically appear. This is to replace the complex Cosmos wallet address. When the transfer is completed normally, the transfer record is stored on the Cosmos blockchain as illustrated in Fig. 7-(b). Since the cash exchange and store payment scenarios are also fundamentally the same as CBDC transfer process, we have developed a demo in a similar way. We also have implemented a scenario where store customers




(a) Transfer UI (b) Cosmos Blockchain UI

Fig. 7: Screenshots of *Cos-CBDC*

convert CBDC to cash. The Korean version of the full demo video can be viewed on YouTube[1].

## IV. Discussion

**Reliability.** Cosmos is powered by Byzantine Fault Tolerance (BFT) consensus algorithms like Tendermint [31]. Therefore, *Cos-CBDC* cannot have more than 1/3 malicious nodes. If there are n nodes in the blockchain network and $P_1$ is the probability of error in a single node, the probability of failure in the intra-chain transaction is:

$$\sum_{i=\lfloor \frac{n}{3}+1 \rfloor}^{n} \binom{n}{i} P_1^i (1-P_1)^{n-i}$$

If each blockchains has n nodes equally and $P_2$ is the probability of success in transaction transmission, the probability of success in the inter-chain transaction is :

$$\left(1 - \sum_{i=\lfloor \frac{n}{3}+1 \rfloor}^{n} \binom{n}{i} P_1^i (1-P_1)^{n-i}\right)^2 P_2$$

Then, the probability of success for m transactions is :

$$\left(1 - \sum_{i=\lfloor \frac{n}{3}+1 \rfloor}^{n} \binom{n}{i} P_1^i (1-P_1)^{n-i}\right)^{2m} P_2^m$$

As the number of nodes increases, the success rate of inter-chain transaction increases.

**Scalability.** *Cos-CBDC* is theoretically possible to connect heterogeneous blockchains or create side-chains. Therefore, *Cos-CBDC* can be effectively applied in cross-border payment and wholesale. It is possible for each bank and country

[1]https://www.youtube.com/watch?v=DqvWH7rcHTU

to use the most specialized blockchain for their own business, so it is highly scalable in terms of compatibility. However, as the number of blockchains of *Cos-CBDC* increases, a central system that continuously tracks where users belong is needed. In addition, inter-chain transactions show lower performance in terms of network traffic and latency than intra-chain transactions. Indiscriminately connecting side chains or heterogeneous blockchains to CBDC network is likely to lower the overall system performance. That is why CBDC systems should be designed with the trade-offs between scalability and compatibility taken into account.

## V. Conclusion

We have proposed *Cos-CBDC*, a blockchain system for CBDC while taking benefits from horizontal scaling and inter-chain transactions. We implemented *Cos-CBDC* based on Cosmos blockchain, and our experiments show that the performance of *Cos-CBDC* improves with the number of blockchains. It shows that inter-chain transactions do not significantly affect TPS although the latency of confirmation is longer. Also, we propose GKM system with MPC for efficient key management in *Cos-CBDC*.

In this paper, we have implemented *Cos-CBDC* in the same network not to consider the network latency. However, in inter-chain transactions, network latency is an important factor affecting TPS because it is related to the timeout of the transaction. In addition, a key update is required whenever CBDC users are added and removed. It is necessary to study the overhead required for key update. We leave them as a future work.

## ACKNOWLEDGMENT

This work was supported by the Institute of Information & Communications Technology Planning & Evaluation (IITP) grant funded by the Korean government (MSIT) (2018-0-00749, Development of Virtual Network Management Technology based on Artificial Intelligence) and the ITRC (Information Technology Research Center) support program (IITP-2021-2017-0-01633).

## References

[1] Auer, R. A., Cornelli, G., & Frost, J., "Rise of the central bank digital currencies: drivers, approaches and technologies," CESifo Working Paper, no. 8655, 2020.

[2] Boar, C., Holden, H., & Wadsworth, A., "Impending arrival a sequel to the survey on central bank digital currency," BIS paper, no. 107, p. 19, 2020.

[3] Mita, M., Ito, K., Ohsawa, S., & Tanaka, H., "What is stablecoin?: A survey on price stabilization mechanisms for decentralized payment systems," 2019 8th International Congress on Advanced Applied Informatics (IIAI-AAI), pp. 60-66, 2019.

[4] Danezis, G., & Meiklejohn, S. Centrally banked cryptocurrencies. arXiv preprint arXiv:1505.06895, 2015.

[5] Ali, R., Barrdear, J., Clews, R., & Southgate, J. The economics of digital currencies. Bank of England Quarterly Bulletin, Q3, 2014.

[6] Nakamoto, S. Bitcoin: A peer-to-peer electronic cash system. Manubot, 2019

[7] "Small business retail" [Online]. Available at https://usa.visa.com/run-your-business/small-business-tools/retail.html

[8] Croman, K., Decker, C., Eyal, I., Gencer, A. E., Juels, A., Kosba, A., ... & Wattenhofer, R. On scaling decentralized blockchains. In International conference on financial cryptography and data security, pp. 106-125, 2016.

[9] "Cosmos" [Online]. Available at https://cosmos.network/docs/resources/whitepaper.html

[10] Calle, G., & Eidan, D., "Central Bank Digital Currency: an innovation in payments," R3 White Paper, 2020.

[11] Maharjan, S., Ko, K., Kang, C., Woo, J., & Hong, J. W., "A Study of CBDC Model Applicable for the Current Banking Environment", KNOM Conference 2020, pp. 56-60, 2020.

[12] Qasse, I. A., Abu Talib, M., & Nasir, Q. "Inter blockchain communication: A survey," ArabWIC 6th Annual International Conference Research Track, pp. 1-6, 2019.

[13] Allen, S., Čapkun, S., Eyal, I., Fanti, G., Ford, B. A., Grimmelmann, J., ... & Zhang, F. Design Choices for Central Bank Digital Currency: Policy and Technical Considerations (No. w27634). National Bureau of Economic Research, 2020.

[14] Kan, L., Wei, Y., Muhammad, A. H., Siyuan, W., Linchao, G., & Kai, H. A multiple blockchains architecture on inter-blockchain communication. In 2018 IEEE International Conference on Software Quality, Reliability and Security Companion (QRS-C), IEEE, pp. 139-145, 2018.

[15] Sun, H., Mao, H., Bai, X., Chen, Z., Hu, K., & Yu, W. Multi-blockchain model for central bank digital currency. In 2017 18th International Conference on Parallel and Distributed Computing, Applications and Technologies (PDCAT), IEEE, pp. 360-367, 2017.

[16] Tsai, W. T., Zhao, Z., Zhang, C., Yu, L., & Deng, E. A multi-chain model for CBDC. In 2018 5th International Conference on Dependable Systems and Their Applications (DSA), IEEE, pp. 25-34, 2018.

[17] Kwon, J., Tendermint: Consensus without mining. Draft v. 0.6, fall, 1(11), 2014.

[18] "Peggy", [Online]. Available at https://github.com/cosmos/gravity-bridge

[19] Han, X., Yuan, Y., & Wang, F. Y., "A blockchain-based framework for central bank digital currency," IEEE International Conference on Service Operations and Logistics, and Informatics (SOLI), pp. 263-268, 2019.

[20] Pal, O., Alam, B., Thakur, V., & Singh, S., "Key management for blockchain technology," ICT Express, 2019.

[21] Ekparinya, P., Gramoli, V., & Jourjon, G. Impact of man-in-the-middle attacks on ethereum. In 2018 IEEE 37th Symposium on Reliable Distributed Systems (SRDS), IEEE, pp. 11-20, 2018.

[22] Saad, M., Spaulding, J., Njilla, L., Kamhoua, C., Shetty, S., Nyang, D., & Mohaisen, A. Exploring the attack surface of blockchain: A systematic overview. arXiv preprint arXiv:1904.03487, 2019.

[23] Ohta, K., & Okamoto, T., "Multi-signature schemes secure against active insider attacks," IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 82(1), pp. 21-31, 1999

[24] Yao, A. C., "Protocols for secure computations," In 23rd Annual Symposium on Foundations of Computer Science, pp. 160-164. 1982.

[25] Pal, O., Alam, B., Thakur, V., & Singh, S., "Key management for blockchain technology," ICT Express, 2019.

[26] "Solana", [Online]. Available at https://solana.com/solana-whitepaper.pdf

[27] "Hedera Hashgraph", [Online]. Available at https://hedera.com/papers

[28] Auer, R., Haene, P., & Holden, H. Multi-CBDC arrangements and the future of cross-border payments, 2021.

[29] Kapsoulis, N., et al., "Know Your Customer (KYC) Im-plementation with Smart Contracts on a Privacy-Oriented Decentralized Architecture," Future Internet, 12(2), 41, 2020.

[30] Chen, S., Zhang, J., Shi, R., Yan, J., & Ke, Q. A comparative testing on performance of blockchain and relational database: Foundation for applying smart technology into current business systems. In International Conference on Distributed, Ambient, and Pervasive Interactions , Springer, pp. 21-34, 2018.

[31] Buchman, E. Tendermint: Byzantine fault tolerance in the age of blockchains (Doctoral dissertation), 2016.