A Survey on Security and Privacy in Blockchain-based Central Bank Digital Currencies

Yunyoung Lee[1], Bumho Son[1], Seongwan Park[1], Jaewook Lee[1], and Huisu Jang[2*]
[1]Seoul National University, Seoul, Republic of Korea
{tommja, andymogul, sucre87, jaewook}@snu.ac.kr
[2]Soongsil University, Seoul, Republic of Korea
yej523@ssu.ac.kr

Received: June 12, 2021; Accepted: August 6, 2021; Published: August 31, 2021

Abstract

The increasing interest in Central Bank Digital Currencies has heightened the need for the suitable security technologies for preserving the privacy of users of the CBDC. Although the CBDC system architecture is deeply related to the legacy payment system and the public blockchain system, security and privacy issues of the CBDC are completely different from those of the existing systems as the purpose of the CBDC is to achieve auditable privacy. We demonstrate the taxonomy of the security and privacy issues in CBDC system according to the following areas: identity, transaction, consensus and auditability. We also emphasize the research gaps in the fields stem from the CBDC's unique characteristics including the authorized audit risk problem and the cross-border payments problem. This study contributes to the current understanding of the security and privacy concerns of CBDCs and addresses the remaining gaps in this field of research.

Keywords: central bank digital currencies, middle-ground blockchain, privacy, security

1 Introduction

Central Bank Digital Currencies (CBDCs) refer to fiat currencies issued in digital form by a central bank, which is distinct from physical money or the reserve/settlement accounts. However, the technical definition of CBDCs could differ depending on the purpose of the issuing entity [18]. [34] defines CBDCs having a separate operating structure distinct from the central bank to provide functions for retail transactions and interest payment based on a wider access range than that of bank reserves. [49] expands the discussion of CBDCs to digital currencies based on high-level techniques beyond the simple digitization of a fiat currency and refers to the relationship between CBDCs and cryptocurrencies such as Bitcoin or Ethereum , which are based on distributed ledger technologies. [11] divides CBDCs into "token-based" and "account based" according to the configuration rules. Account-based CBDCs would lower transaction costs under the control of the central bank and token-based CBDCs would use to utilize distributed ledger system, like Bitcoin or Ethereum. [8] aims to identify the role of CBDC in each scenario in which CBDCs are used as a complement to cash or deposits, bank reserves or accounting units.

The technical definition of CBDCs differ because the governments that are considering issuing CBDCs have different purposes. In general, the main purposes for issuing CBDCs are financial stability, monetary policy implementation, financial inclusion, payment efficiency (domestic, cross-border), and

Journal of Internet Services and Information Security (JISIS), volume: 11, number: 3 (August 2021), pp. 16-29
DOI:*10.22667/JISIS.2021.08.31.016*
*Corresponding author: School of Finance, Soongsil University, Seoul, Republic of Korea, 06978, Tel: +82-(0)2-828-7389

payment safety/robustness. However, the situations of each issuing country (dramatic decrease in cash flow, highly volatile fiat currency value, etc.) and the purpose of the CBDC issued (small settlements, large settlements), so the importance of each major purpose will change [9]. The issuance of CBDCs can lead to changes in the long-established financial system, such as the emergence of new payment methods, dis-intermediation of commercial banks, and difficulties managing policy management are often cited as problems that CBDCs still need to solve [6]. In particular, security and privacy in CBDCs emerged as one of the most important discussions because, CBDC can cause structural changes in the financial system itself. The security and privacy issues of CBDC have characteristics that distinguish them from centralized financial systems or public blockchains. Most CBDCs do not aim to make all transaction details public, like Bitcoin, or private, like Zcash. The CBDC issuer is likely to prefer to provide personal information protection to users of the CBDC system under normal circumstances with the ability to reveal transaction information in special situations such as for antim money laundering (AML) proisions or law enforcement. In this study, we aim to deal with major issues related to the privacy and security of CBDCs upon implementation from a middle-ground position. Section 2 describes the privacy and security issues related to the implementation of CBDCs, and Section 3 addresses important issues that still lack sufficient research and require more discussion. Finally, Section 4 discusses the summary and significance of the study.

2 Security and Privacy issues in CBDCs

There are different kinds of CBDC design models, and each has its own level of privacy and security. For example, in a permissioned blockchain where a small number of entities can see and verify all transactions, the whole transaction log including the identities of the participants, is open to those entities, but the transactions are completely hidden from the public. However, the entity nodes should be highly trusted. If they get attacked or hacked, all the transaction data might be leaked, so this entails a huge security risk. Otherwise, single points of failure are less likely to happen in a public blockchain, like Bitcoin and Ethereum. If all transactions are unencrypted on the public blockchain, then we need not trust any third party and can have relative security from specific node attacks. However, the transactions are open to everyone participating in the blockchain, thus providing a low level of privacy. As shown in [38], although users take pseudonyms that seem to be anonymous, they are linked with outside information and it is easy to uncover the identities of real users.

From the perspective of the middle ground in designing CBDCs, it is necessary to provide a sufficient level of privacy and security to users, while ensuring compliance with regulations such as AML. There are several cryptographic and systematic approaches that can be applied to the blockchain to enhance security and privacy at the cost of complexity, which we discuss in the following sections.

2.1 Identity Privacy

Identity Privacy is the ability to hide the identities of the users participating in the system. Identity privacy might vary considerably between systems, differing in its openness and transaction verifying process. [21] summarizes the privacy level of many different platforms including Bitcoin, the credit card system, and cash.

User identities might be leaked in three different situations. First, as mentioned above, blockchain systems that only use pseudonyms for privacy are vulnerable to de-anonymization. The transaction patterns of each user might be exposed, such that it is possible to predict his or her future behavior. In a worse case, the transaction itself would be combined with outside information and the transaction participants might be linked with their real identities. Figure 1 shows that blockchain users can be

easily de-anonymized when transactions are open to all and outside information is obtainable. Second, at a network level, a light node might ask the full node about the existence of transactions, and those queries as well as network data(e.g., IP address) might be good hints at a user's identity, as discussed in [2]. Third, CBDCs are likely to comply with know your customer(KYC) provisions to easily deal with AML, and law enforcement. Middle-ground CBDCs, unlike public blockchain systems, might require some special nodes to store personal data with proper classification. These special entities are highly likely to be exposed to a single point of failure, which can result in the indirect leakage of personal data, including user identities.

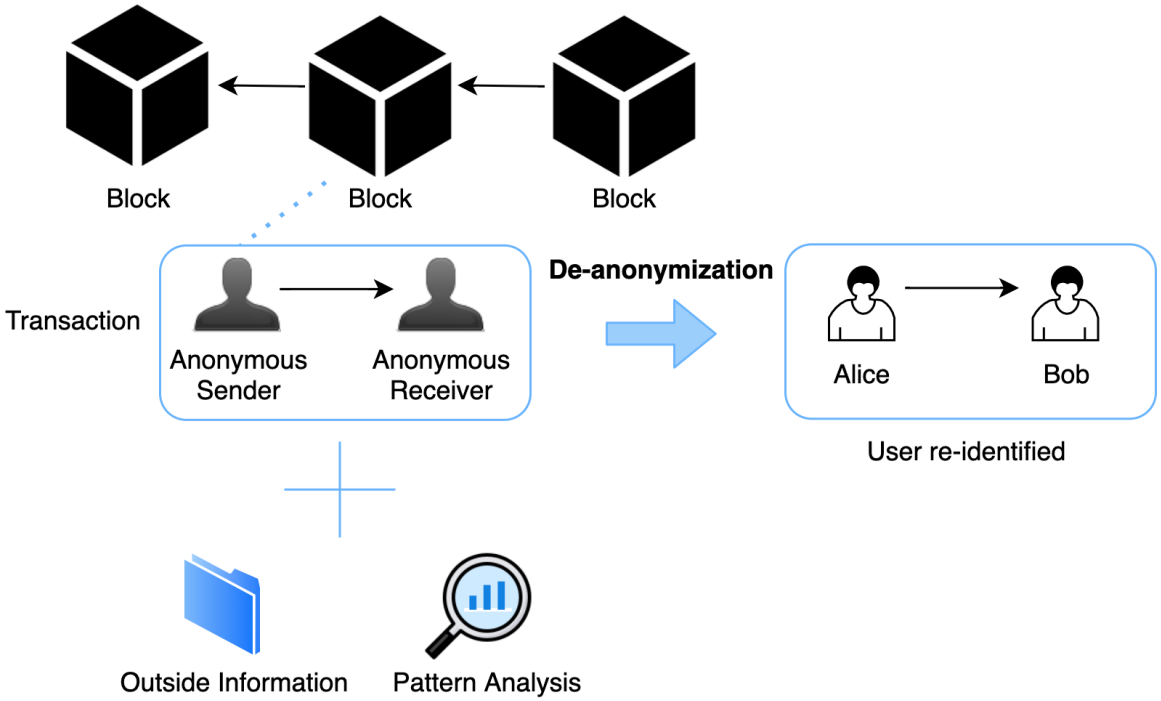


Figure 1: De-anonymization of users by combining the transaction pattern with auxiliary user information

2.1.1 De-anonymization

Many public blockchain systems, such as Bitcoin and Ethereum, have transaction structures that show the sender and receiver addresses explicitly. Because of this property of openness, a large proportion of the users can be re-identified by different ways. [23] lists several attacks for de-anonymizing users' real identities: network analysis, address clustering, and transaction fingerprinting. These attacks make use of IP addresses, clustered addresses, and transaction analysis and combine them with any outside information to identify users. Several cryptographic approaches can make this re-identification process intractable and ensure that the transactions are encrypted. Some studies apply them to propose new blockchain-based CBDC designs.

Secure Multi Party Computations (MPC) One way to prevent de-anonymization is to implement MPC, which enables jointly computing a function with participants' inputs while keeping each input pri-

vate. This idea can be applied to Real-time Gross Settlement (RTGS) systems, where several commercial banks make high-value fund transfers to each other. [5] proposes a MPC based solution to perform the liquidity optimization for decentralized RTGS system, keeping their transactions confidential. They show three versions, one of which keeps the source and destination private, as well as the transaction amount.

Zero Knowledge Proof (ZKP) ZKP is also being used as a building block for private identities. Zerocash [43], known as Zcash is widely known for using zerok-knowledge succinct noninteractive argument of knowledge proofs (zk-SNARKs) to prove the validity of transactions without revealing the participants or the amount. However, as shown in [31], Zcash users are identifiable using heuristics based on patterns of usage. [19] attempts to protect the anonymity of commercial banks in an indirect CBDC model by proposing a supervised anonymous issuance (SAI) scheme, using zk-SNARKs and a multi-receiver signature encryption scheme. The scheme ensures that the issuer's identity remain hidden while allowing other commercial banks to verify whether the issuance is allowable and the issuer is qualified. [27] proposes a CBDC system design that allow fully private transfers between users while still complying with AML regulations by imposing limits on private transfers, using zk-SNARKs.

Ring Signatures Ring signatures are another option to obscure identities in a transaction. First introduced by [42], ring signatures make it possible to specify a set of possible signers without revealing which member actually produced the signature. Monero uses Ring Confidential Trasnaction (RingCT) [40] to hide the sender's identity by combining it with a set of fake senders and amount of the transaction. However, [37] shows that this mixing strategy is still vulnerable to re-identification. There are few studies on CBDC designs attempting to take advantage of ring signatures. [26] proposes a CBDC system based on a permissioned blockchain, with non-custodial wallets for privacy-preserving purposes. The proposed model suggests ring signatures, ZKP, and stealth address as building blocks of non-custodial wallets, which offer retail users cash-like anonymity.

Systematic Approaches There are some proposed systematic approaches for hiding transactions, including the identities of the participants. [12] proposes Corda, which creates a private permissioned environment where, all transaction data are shared only between the counterparties of transaction, so outsiders cannot even know that the transaction is happening in the first place. The transaction is validated by those counterparties, and a notary pool attests the uniqueness of each transaction, ensuring the security of the transactions.

2.1.2 Network-level attack

De-anonymization of identities is not the only risk in CBDC designs. There might be risks inherent to the network or node communication. For example, nodes that have more permissions compared to other nodes are likely to receive more privacy-sensitive requests. Retail users, especially when using their mobile phones, are not likely to hold the full set of block data. They might ask the validator node or full node, which stores the whole blockchain, if a specific transaction they are interested in is contained in the block or not. In that situation, the validator node itself, which takes the light client's requests, might know which transaction this client is interested in. In p2p networks, another malicious peer node might see this request unless it is encrypted.

The Bitcoin network has a similar privacy issue. To solve this issue, SPV nodes in Bitcoin use a bloom filter to ask for transactions of interest. They do not specify the exact transaction, and they can handle the level of privacy by controlling the parameters of bloom filters.

From the perspective of the middle-ground, network-level attacks might be more severe since those requests are more likely to contain more privacy-sensitive data to enable the compliance with AML/

Combating the Financing of Terrorism (CFT) regulations. The Skipchain [32] structure enables validation of blocks without the need for privacy-preserving queries. CBDC designs can adopt this structure for a robust approach.

2.2 Transaction privacy

Public blockchain networks make every participating nodes able to save the blockchain which holds the transaction history. It strengthens the transparency and privacy of the blockchain network because everyone can see the change in the blockchain when a malicious attacker tries to manipulate previously issued and recorded transactions on the blockchain. However, compared to the current securities settlement system or bank account system, opening transaction details to the public is an apparent threat to privacy.

As discussed above, privacy issues on the blockchain exist because transaction details are recorded in the blockchain. Therefore, we classify potential privacy threats according to the content of the transaction to be protected. The first category is data privacy, which implies the protection of the identities of the sender and receiver, or protecting the token amount of the transaction. The second is program privacy. Blockchain transactions can contain any type of programming code (i.e., a smart contract). Even when smart contract issuers intend to use them for commercial purposes, smart contract code becomes open-source intentionally. Finally, program privacy explains how to protect program code on blockchain.

2.2.1 Data Privacy

Data privacy includes protecting the participant identities and transactions amount in a transaction. It is hard problem to solve because the key property to maintain is the recording of the transaction on the blockchain. Therefore, schemes hiding transaction details using encryption techniques are proposed.

Secure MPCs The goal of MPC [48] is to ensure that make multiple parties can compute a function that requires inputs from parties jointly while not revealing their own private inputs to each other. After [48] proposed a two-party MPC protocol, [25] proposed a general framework for multi-party MPCs.

Rethinking the purpose of recording transactions on a public blockchain in a block, blockchain systems must be able to check the transaction availability by computing the sum of the sending transaction amount and receiving transaction amount. If we think of the computing procedure as the objective function of an MPC, the MPC can be used to protect transaction data details by encrypting transactions by setting participating receivers and senders as parties of the MPC.

[5] proposed a secure MPC-based solution to manage the RTGS system in decentralized settings. The proposed system ensures the privacy of the entities in an MPC, by hiding the amounts, the source addresses of each transaction, or the destinations. Corda, the protocol proposed by [12] uses similar scheme as MPC. It makes participants of a transaction share data only with each other and ensures that the private input of any party is not revealed to the public. It is different from MPCs in which other parties participating in transactions can find other participants' private inputs, but MPCs are still applicable to Corda.

Homomorphic Encryption [41] introduced homomorphic encryption, which is a scheme that enables computation on ciphertext resulting in the same result as computation on plaintext. In the same sense as MPCs, homomorphic encryption enables the system to encrypt transaction amounts while the blockchain system can verify the transaction. For an application of homomorphic encryption in a blockchain system, [47] proposed an improved system of Zerocoin [36], a Bitcoin-based transaction system that can hide the amounts of the transaction. The proposed scheme encrypts the transaction amounts with a homomorphic property. In terms of functionality, the proposed scheme can arbitrarily encrypt amounts in frequent

transactions and use them for homomorphic computations, while Zerocoin supports only certain divided values besides other arbitrary values in real transactions.

ZKPs ZKPs are one of the most widely used privacy-preserving schemes. ZKP schemes enable entities to prove a claim without revealing their own private inputs. When a ZKP scheme is applied in blockchain system, transaction participants can prove their positive balance without revealing the actual transaction amount. [29] proposed a shielded payment scheme Zcash using zk-SNARKs to hide the addresses of the transaction sender and receiver.

2.2.2 Program Privacy

Writing smart contract requires the code writer to understand cryptographic technologies and consensus algorithms of a distributed ledger. Furthermore, one of the biggest problems in executing smart contracts on a blockchain is the privacy limitation. The privacy of smart contracts means both privacy for the programming code and privacy for the input data of the smart contract.

[33] protected the input of smart contracts by executing the smart contract off-chain. It restricts the role of the on-chain blockchain system to verify the result of the executions using ZKP. [1] and [30] proposed similar ideas around executing smart contracts somewhere away from the main blockchain. Even though the proposed schemes protect privacy for most entities, potential threats remain because centralized nodes such as a manager or client are responsible for executing the smart contract. Protean, proposed by [3], provides special functional units to avoid having all nodes keep smart contracts and computations. The functional units consist of a randomness unit, state unit, execution unit, and private storage unit to run secure specialized modules that cannot be implemented securely by a smart contract.

For a specific application of secure smart contracts, [39] used secure device-to-device communication mechanism in a trading system to protect the deposit data of sellers and buyers. [45] implemented a privacy-preserving smart contract on the Ethereum platform with their proposed smart contract structure. Table 1 summarizes the classification of various privacy-preserving techniques implemented in past research that aim to maintain identity and transaction privacy.

	Identity Privacy		**Transaction Privacy**	
	De-anoymization	Network-level attack	Data Privacy	Program Privacy
Secure Multiparty Computation	[5]	-	[5], [12]	-
Zero Knowledge Proof	[43] , [31] , [19] , [27]	-	[29]	-
Ring Signature	[42] , [37] , [26]	-	-	-
Homomorphic Encryption	-	-	[47]	-
Others	[12]	[32]	-	[33] , [1], [30] , [3] , [39] , [45]

Table 1: Classification of the privacy-preserving techniques used in CBDC models

2.3 Consensus and Auditability

Blockchain-based models for CBDCs differ from the existing public cryptocurrencies as most CBDCs aim to take the advantage of blockchain technology while maintaining control over monetary issuance

and supply. While blockchain technology can bring about innovation in the current financial market structure as it enables value transfer between two entities without a trusted third-party, it also possesses some problems in terms of scalability and resource allocation due to its distributed setting. To solve such problems, many researchers proposed blockchain-based middle-ground CBDC architectures with different layers where the participating entities of each layer are given different permissions and roles. In this section, we discuss the security issues to consider when designing these middle-ground models.

2.3.1 Consensus

The traditional blockchain consensus mechanisms such as Proof-of-Work(PoW) cannot be implemented directly in middle-ground models as these consensus mechanisms require all nodes to be "full" nodes. In other words, typical PoW mechanisms require that all nodes have the ability to mine a new valid block and store the full blockchain in their own storage system. However, as CBDCs aim to become a versatile currency throughout a nation, it is very impractical for all users to participate in the consensus protocol. Thus, several variations in which only the designated nodes participate in the consensus process were proposed for CBDCs. These specific security properties should be considered in these CBDC models.
No Double-Spending: Double-spending is the act of transferring cash that has already been used previously. Different from a physical currency, CBDC transactions should be verified to check whether the currency was used only once by one user at a time. This is the most basic security property that blockchain-based CBDCs should meet.
Non-Repudiation: Non-repudiation requires that all the participants' actions in the payment process are recorded correctly, so they cannot deny any of the actions that they processed in the past.
Unforgeability: Similar to preventing counterfeiting of physical cash, CBDCs should not be issued by institutions or individuals besides the central bank.

[20] proposed the first hybrid blockchain-based CBDC framework, namely RSCoin, which can provide the centralization of a monetary authority to a certain entity (eg. central banks) and keep the blockchain's transparency. RSCoin introduces mintettes as their system intermediaries, which are responsible for maintaining the transaction ledger. These mintettes can be represented as the full node in the traditional blockchain, but the difference is that they produce a lower-level block, which should be sent to the central bank for higher-level block production. These higher blocks form a chain, which is then exposed to the other external users. [50] argued the limitations of traditional PoW, Proof-of-Stake(PoS), Practical Byzantine Fault Tolerance(PBFT) and Delegated Proof-of-Stake(DPOS) mechanisms in their hybrid model, and proposed a new consensus mechanism called POA-PBFT which showed improvements over the DPOS-BFT algorithm. POA-PBFT changes the election process of bookkeeping nodes from voting by all the participants to direct modifications by the central bank. Additionally, the block producers in the original DPOS algorithm have freedom to increase the block number as they wish, but in the POA-PBFT setting, a designated node specified by the central bank has the authority to produce a fixed block-number block. This can effectively reduce the probability of forked chains, as the chain cannot grow freely if the specified node does not proceed in block production.

2.3.2 Auditability

As we mentioned in the previous section, blockchain-based CBDC systems with a middle ground approach differ from the traditional blockchain mechanisms as they permit different levels of authority for different nodes. Consequently, most CBDC architectures divide the participating nodes into different layers, and the main difference between these CBDC schemes and decentralized cryptocurrencies is in the regulatory layer nodes. The nodes in the regulatory layer are responsible for monitoring the whole CBDC cycle including verifying transactions, issuing the CBDC, and monitoring the system, such that

the CBDC system can provide a safe asset transfer environment for the lower-level users.

Regulatory compliance is one of the key areas with which CBDC must comply. Most governments or related institutions, potential operators of CBDCs, aim to protect the economy against malicious economic activities such as money laundering or tax evasion. CBDC systems should have auditability as a function; however this conflicts with the fundamental characteristics of a public blockchain. The fundamental characteristics of a blockchain include that the owner of the asset has full authority to decide when, how much, and to whom a transaction is issued and whether or not to disclose the details. In contrast, the auditability of a CBDC must prevent transactions that do not comply with regulations, regardless of the intent or preference of the asset owner, while maintaining the privacy and security of legitimate transactions. CBDCs are inevitably distinct from public blockchains or the existing centralized structure, and have no choice but to have a middle-ground form. Recent research efforts explored how to implement an auditable distributed ledger system. How to implement auditability in CBDC systems is an open research area. There are various technological building blocks for such designs already. We provide a taxonomy of auditability technologies based on system configuration considerations including which ledger is introduced to the CBDC system, the extent that it covers privacy, and the cryptographic techniques leveraged. A CBDC ledger could be "permissioned" or "permissionless" depending on whether authorization is required to read, maintain, or especially, write, the ledger. Most CBDC designs prefer a "permissioned" ledger because most of them force predetermined auditors audit assigned transactions. However, a few studies implement auditability in ledgers such as a public blockchain. We also cover how auditability functions are implemented differently for the two types of ledgers: "ledger-based" and "token-based" also known as the untransacted transaction output(UTXO) model. We investigate the extent to which each implemented audit function guarantees the privacy range discussed in Sections 2.1 and 2.2. In accordance with the extent to which privacy is guaranteed, we use the following notations: S(sender identities), R(receiver identities), and T(transactions).

[13] do not mention that they propose permissioned ledgers, but discuss auditability under the assumption that there are authorized users who can manage the database. The authors implement auditability by limiting the total amount of tradable transactions for a certain period instead of verifying the transaction contents in a zero-knowledge-based manner. In this system, only the sender remains anonymous, regardless of the recipient and transaction amount. Only when the transaction amount limit is reached, can the public key of the sender can be estimated through the signatures of the auditor and the recipient, though it is also possible to track the transaction history with the public key.

In the context of permissioned ledgers, [4] presents a privacy-preserving token management system for permissioned blockchains that also supports fine-grained auditing. The authors leverage advanced cryptographic techniques such as verifiable random function (VRF), Elgamel encryption, Groth signatures, Pedersen commitments, Pointchevavl-Sanders signatures to overcome the strong trusted setup assumption, which is a common and well-known disadvantage of zk-SNARK. Authorized auditors audit transactions without disclosing the contents of the transactions within their framework. [24] propose implementing auditability based on strong privacy protection using zkSNARKs under the permissioned and UTXO-based CBDC structure. They propose a modified Zcash model that includes predetermined administrators who proceed with additional signatures when the transaction amount exceeds the upper limit. The disadvantage of this method is that it requires strong trust setup assumptions as mentioned above. [10] is similar to [24], but, adopts an account-based ledger system. They introduce the KYC process before participating to the transaction network and implements dedicated agencies to manage transaction details post-event.

[15] suggests a similar technique, called the blind signature [14], for implementing a CBDC system that preserves transaction privacy and fulfill regulatory requirements. Their asymmetric approach can conceal the identity of senders, but not that of receivers. [44] provides a similar privacy function with the technology of [15] through zkSNARKs. [46] propose a CBDC framework that does not expose transac-

tion details, but keeps the identity of the sender private. They also adopt a hardware-based solution to provide private execution of transactions, even when users are offline. Table 2 summarizes the taxonomy of the auditability techniques in CBDCs.

Auditability system	Ledger structure	Assumptions	UTXO or Account-based	Cryptographic shemes	Privacy
[13]	-	Total limit	UTXO	ZKP	S
[4]	Permissioned	Authorized auditors	UTXO	VRF Groth sig.	S,R,T
[24]	Permissioned	Authorized auditors	UTXO	zkSNARKs	S,R,T
[10]	Permissioned	Authorized auditors	Account -based	zkSNARKs	S,R,T
[15]	Permissioned	Authorized auditors	UTXO	blind-sig.	S
[44]	Permissioned	Authorized auditors	UTXO	zkSNARKs	S
[46]	Permissioned	Authorized auditors	Account -based	temper-proof hardware	S

Table 2: Taxonomy of the auditability techniques of the CBDC

3 Research Challenges

From the consumer needs that CBDCs could address, [6] derives the main design choices of CBDCs: architecture, central bank infrastructure, access technologies, and retail or wholesale interlinkages. The architecture of CBDCs constitutes whether the CBDC will be a direct claim on the central bank or an indirect claim through intermediaries and the operational roles of the participants in the CBDC system including the central bank or other intermediaries. The CBDC infrastructure decides whether the ledger database would be a decentralized ledger system or conventional central ledger system. Access technology addresses the privacy and accessibility issues for users. Most academic studies on cryptography with a focus on privacy-oriented digital payment systems contribute to the enhancement of access technology. Retail or wholesale interlinkages, which is the last design component of CBDCs, relate to specific tehcniques for implementing corss-border payments. Components besides access technology based on privacy-enhancing needs are relatively less discussed in academic and industrial fields. We present the research gaps in these sectors from a privacy and security perspectives in this section.

Authorized Auditor Risk All design elements of the CBDC system mentioned above should be closely connected and operated to implement a safe CBDC system that satisfies the needs of users. In relation to the architecture and infrastructure elements, the distribution of the roles of each system participant and the discussion of the ledger database structure relates directly to the consensus on the transaction details between users, which means the extent of the security of the entire ledger system. In particular, CBDC systems often suffer from high computational costs when applying privacy-enhancing technologies based on cryptography such as ZKP because a promising CBDC system, unlike public blockchains, aim to provide an additional auditability function. In addition, linking CBDC account with the identity of the real user when necessary is inevitable for AML/CFT control.

Therefore, many researchers inevitably adopt a scheme where the authorized participants who manage the transaction details or user identities are introduced to protect user privacy and achieve regulatory compliance simultaneously [13, 4, 24, 10, 15, 44, 46]. It is necessary to specify the authority and limits of system members with authority besides the central bank; however, such discussions are relatively scarce. In addition, most studies assume that users with additional privileges are all honest and have no incentive to act maliciously in the system, which is in stark contrast to the general public blockchain. The field seems to need a wide discussion on how to keep malicious behavior between users with different privileges in check to claim enhanced privacy and security through the distribution of privileged users in a CBDC system beyond the centralized form. Currently, research on how the participation of malicious users affects the consensus and security of the entire network in general public blockchains such as Bitcoin and Ethereum is conducted from the game theory, economics, cryptographic, and computer network perspectives. Studies considering malicious authorized players in a CBDC system would bridge the gap between the security analysis of public blockchain consensus and that of the "middle-ground" CBDC system consensus.

Cross-border Payments with CBDCs Most CBDC projects aim to cover both the domestic payment process and, payments that occur across geographical distances, or cross-border payments. Many researchers believe in the potential of CBDC technology to reduce the current inefficiency in cross-border payments. To incorporate cross-border payments in CBDC system, blockchain-based CBDCs should consider cross-chain swap methods, as cross-border payments typically must transfer multiple currencies on different ledgers. [7] argues that the benefits of CBDC technology would be difficult to achieve in cross-border environments, unless the government or central banks consider the cross-border aspects from the ground when designing their own CBDC systems. However, most of the current research on security or privacy in CBDCs are not focused on multi-chain environments, but rather on a single-chain payment system. Thus, cross-border payments on CBDCs introduces new challenges. Although it is common to assume that the central banks responsible for individual CBDC chains are trustworthy, the trustworthiness of foreign central banks cannot be guaranteed. Accordingly, the privacy model and the security model of cross-border CBDC payments requires fresh consideration.

Privacy-preserving techniques with multiple chains, should guarantee that the participating nodes have access to only the transactions they are related to. Therefore typical homomorphic encryption schemes cannot be used because the secret key holders should not be able to utilize a common secret key to decrypt the other chain's transaction data. Thus, some variants of the fully homomorphic encryption schemes can be used to solve such problems. [35] proposed an on-the-fly multiparty computation model based on a multikey homomorphic scheme, which is capable of computing inputs encrypted with multiple secret keys. Additionally, [16] designed a multikey-homomorphic encryption using TFHE [17] (homomorphic encryption scheme based on ring learning with errors), which enables the secure computation of multiple ciphertexts encrypted with different keys followed by bootstrapping. Future researchers might refer to these multikey homomorphic encryption schemes to design CBDC payment systems that can successfully execute transactions with other CBDC chains that use different secret keys.

In terms of consensus mechanisms, cross-chain payment systems should also meet the security requirements mentioned in Section 2.3.1. As ledger updates in different chains occur asynchronously, new transaction execution protocols are needed to account for the atomicity of transactions between the nodes on distinct blockchains. [28] proposed a method to safely transfer numerous assets between multiple blockchains that incorporates a hashed timelock contract (HTLC) in the transactions. HTLC is a technology that uses pre-defined time boundaries (timelock) and secret hash values (hashlock) for executing the transactions. Some ongoing CBDC projects such as [22] considered cross-border payments with on-ledger escrow using HTLC or conditionial payment channels with HTLC. However, there is still

room for improvement as the proposed protocol guarantees the safety of payments only with several preconditions. In addition, HTLC possesses its own failure-to-deliver scenarios that require analysis.

4 Conclusion

With the central banks' growing interests in CBDCs, the practical issues of CBDCs including privacy and security, are also widely discussed in various fields of research. Researchers proposed several promising blockchain-based CBDC models with a middle-ground approach for practical applications. This survey has provided a broad taxonomy of the different existing privacy and security preserving solutions. For identity and transaction privacy, secure MPCs, ZKPs, ring signatures and some other smart contract-based methodologies were implemented to successfully compute transactions without revealing any sensitive information. Additionally, this paper presents secure protocols for middle-ground blockchain consensus and auditability. While there is extensive research on these issues, some challenges and limitations remain to be thoroughly discussed. We hope that our survey can inspire future CBDC researchers to solve these problems with diverse approaches.

This work was supported by the National Research Foundation of Korea Grant through the Korean Government (MEST) under NRF-2019R1F1A1058061.

References

[1] M. Al-Bassam, A. Sonnino, S. Bano, D. Hrycyszyn, and G. Danezis. Chainspace: A sharded smart contracts platform. *arXiv preprint arXiv:1708.03778*, August 2017.

[2] S. Allen, S. Čapkun, I. Eyal, G. Fanti, B. A. Ford, J. Grimmelmann, A. Juels, K. Kostiainen, S. Meiklejohn, A. Miller, et al. Design choices for central bank digital currency: Policy and technical considerations. Technical report, National Bureau of Economic Research, August 2020.

[3] E. C. Alp, E. Kokoris-Kogias, G. Fragkouli, and B. Ford. Rethinking general-purpose decentralized computing. In *Proc. of the Workshop on Hot Topics in Operating Systems (HotOS'19), Bertinoro, Italy*, pages 105–112. ACM, May 2019.

[4] E. Androulaki, J. Camenisch, A. D. Caro, M. Dubovitskaya, K. Elkhiyaoui, and B. Tackmann. Privacy-preserving auditable token payments in a permissioned blockchain system. In *Proc. of the 2nd ACM Conference on Advances in Financial Technologies (AFT'20), New York, New York, USA*, pages 255–267. ACM, October 2020.

[5] S. Atapoor, N. P. Smart, and Y. T. Alaoui. Private liquidity matching using mpc. `https://eprint.iacr.org/2021/475` [Online; accessed on August 15, 2021], April 2021.

[6] R. Auer and R. Böhme. The technology of retail central bank digital currency. Technical report, Bank for International Settlements, March 2020.

[7] R. Auer, P. Haene, and H. Holden. Multi-cbdc arrangements and the future of cross-border payments. Technical Report 115, Bank for International Settlements, March 2021.

[8] O. Bjerg. Designing new money-the policy trilemma of central bank digital currency. Technical report, Cophenhagen Business School, June 2017.

[9] C. Boar, H. Holden, and A. Wadsworth. Impending arrival–a sequel to the survey on central bank digital currency. Technical Report 107, Bank for International Settlements, February 2020.

[10] T. Bontekoe. Balancing privacy and accountability in digital payment methods using zk-snarks. Master's thesis, University of Twente, 2020.

[11] M. D. Bordo and A. T. Levin. Central bank digital currency and the future of monetary policy. Technical report, National Bureau of Economic Research, August 2017.

[12] G. Calle and D. Eidan. Central bank digital currency: an innovation in payments. Technical report, R3, April 2020.

[13] J. Camenisch, S. Hohenberger, and A. Lysyanskaya. Balancing accountability and privacy using e-cash. In *Proc. of the 5th International Conference on Security and Cryptography for Networks (SCN'06), Maiori, Italy*, volume 4116 of *Lecture Notes in Computer Science*, pages 141–155. Springer, Berlin, Heidelberg, September 2006.

[14] D. Chaum. Blind signatures for untraceable payments. In *Proc. of the 2nd Annual International Cryptology Conference (Crypto'82), Santa Barbara, California, USA*, pages 199–203. Springer, Boston, MA, 1983.

[15] D. Chaum, C. Grothoff, and T. Moser. How to issue a central bank digital currency. *arXiv preprint arXiv:2103.00254*, February 2021.

[16] H. Chen, I. Chillotti, and Y. Song. Multi-key homomorphic encryption from tfhe. In *International Conference on the Theory and Application of Cryptology and Information Security*, pages 446–472. Springer, November 2019.

[17] I. Chillotti, N. Gama, M. Georgieva, and M. Izabachene. Faster fully homomorphic encryption: Bootstrapping in less than 0.1 seconds. In *Proc. of the 22nd International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT'16), Hanoi, Vietnam*, volume 10031 of *Lecture Notes in Computer Science*, pages 3–33. Springer, Berlin, Heidelberg, December 2016.

[18] C. . M. Committee et al. Central bank digital currencies. Technical report, Bank for International Settlements, March 2018.

[19] W. Dai, X. Gu, and Y. Teng. A supervised anonymous issuance scheme of central bank digital currency based on blockchain. In *Proc. of the 20th International Conference on Algorithms and Architectures for Parallel Processing (ICA3PP'20), New York, New York, USA*, volume 12454 of *Lecture Notes in Computer Science*, pages 475–493. Springer, Cham, October 2020.

[20] G. Danezis and S. Meiklejohn. Centrally banked cryptocurrencies. In *Proc. of the Network and Distributed System Security Symposium 2016 (NDSS'16), San Diego, California, USA*. Internet Society, February 2016.

[21] S. Darbha and R. Arora. Privacy in cbdc technology. Technical report, Bank of Canada, June 2020.

[22] European Central Bank, Bank of Japan. Synchronised cross-border payments - stella project report phase 3. `https://www.ecb.europa.eu/paym/intro/publications/pdf/ecb.miptopical190604.en.pdf` [Online; accessed on August 15, 2021], June 2019.

[23] Q. Feng, D. He, S. Zeadally, M. K. Khan, and N. Kumar. A survey on privacy protection in blockchain system. *Journal of Network and Computer Applications*, 126:45–58, Januray 2019.

[24] C. Garman, M. Green, and I. Miers. Accountable privacy for decentralized anonymous payments. In *Proc. of the 20th International Conference on Financial Cryptography and Data Security (FC'16), Christ Church, Barbados*, volume 9603 of *Lecture Notes in Computer Science*, pages 81–98. Springer, Berlin, Heidelberg, February 2016.

[25] O. Goldreich, S. Micali, and A. Wigderson. How to play any mental game, or a completeness theorem for protocols with honest majority. In *Providing Sound Foundations for Cryptography: On the Work of Shafi Goldwasser and Silvio Micali*, pages 307–328. ACM, October 2019.

[26] G. Goodell, H. D. Al-Nakib, and P. Tasca. A digital currency architecture for privacy and owner-custodianship. *Future Internet*, 13(5):130, May 2021.

[27] J. Gross, J. Sedlmeir, M. Babel, A. Bechtel, and B. Schellinger. Designing a central bank digital currency with support for cash-like privacy. `http://dx.doi.org/10.2139/ssrn.3891121` [Online; accessed on August 15, 2021], July 2021.

[28] M. Herlihy. Atomic cross-chain swaps. In *Proc. of the 2018 ACM symposium on principles of distributed computing (PODC'18), Egham, UK*, pages 245–254. ACM, July 2018.

[29] D. Hopwood, S. Bowe, T. Hornby, and N. Wilcox. Zcash protocol specification. `https://github.com/zcash/zips/blob/master/protocol/protocol.pdf` [Online; accessed on August 15, 2021], October 2016.

[30] H. Kalodner, S. Goldfeder, X. Chen, S. M. Weinberg, and E. W. Felten. Arbitrum: Scalable, private smart contracts. In *Proc. of the 27th USENIX Security Symposium (SEC'18), Baltimore, Maryland, USA*, pages 1353–1370. USENIX Association, August 2018.

[31] G. Kappos, H. Yousaf, M. Maller, and S. Meiklejohn. An empirical analysis of anonymity in zcash. In *Proc. of the 27th USENIX Conference on Security Symposium (SEC'18), Baltimore, Maryland, USA*, pages

463–477. USENIX Association, August 2018.

[32] E. Kokoris Kogias. Secure, confidential blockchains providing high throughput and low latency. Technical report, EPFL, 2019.

[33] A. Kosba, A. Miller, E. Shi, Z. Wen, and C. Papamanthou. Hawk: The blockchain model of cryptography and privacy-preserving smart contracts. In *Proc. of the 2016 IEEE symposium on security and privacy (S&P'16), San Jose, California, USA*, pages 839–858. IEEE, May 2016.

[34] M. Kumhof and C. Noone. Central bank digital currencies-design principles and balance sheet implications. Technical Report 725, Bank of England, May 2018.

[35] A. López-Alt, E. Tromer, and V. Vaikuntanathan. On-the-fly multiparty computation on the cloud via multikey fully homomorphic encryption. In *Proc. of the 44th Annual ACM symposium on Theory of computing (STOC'12), New York, New York, USA*, pages 1219–1234. ACM, May 2012.

[36] I. Miers, C. Garman, M. Green, and A. D. Rubin. Zerocoin: Anonymous distributed e-cash from bitcoin. In *Proc. of the 2013 IEEE Symposium on Security and Privacy (S&P'13), Berkeley, California, USA*, pages 397–411. IEEE, May 2013.

[37] M. Möser, K. Soskaz, E. Heilman, K. Lee, H. Heffan, S. Srivastava, K. Hogan, H. Jason, A. Miller, A. Narayanan, and N. Christin. An empirical analysis of linkability in the monero blockchain. *arXiv preprint arXiv:1704.04299*, April 2018.

[38] J. D. Nick. Data-driven de-anonymization in bitcoin. Master's thesis, ETH-Zürich, 2015.

[39] S. R. Niya, F. Shüpfer, T. Bocek, and B. Stiller. Setting up flexible and light weight trading with enhanced user privacy using smart contracts. In *Proc. of the 2018 IEEE/IFIP Network Operations and Management Symposium (NOMS'18), Taipei, Taiwan*, pages 1–2. IEEE, April 2018.

[40] S. Noether. Ring signature confidential transactions for monero. `https://eprint.iacr.org/2015/1098` [Online; accessed on August 15, 2021], December 2015.

[41] R. L. Rivest, L. Adleman, M. L. Dertouzos, et al. On data banks and privacy homomorphisms. *Foundations of secure computation*, 4(11):169–180, 1978.

[42] R. L. Rivest, A. Shamir, and Y. Tauman. How to leak a secret. In *Proc. of the 7th International Conference on the Theory and Application of Cryptology and Information Security (ASIACRYPT'01), Gold Coast, Australia*, volume 2248 of *Lecture Notes in Computer Science*, pages 552–565. Springer, Berlin, Heidelberg, December 2001.

[43] E. B. Sasson, A. Chiesa, C. Garman, M. Green, I. Miers, E. Tromer, and M. Virza. Zerocash: Decentralized anonymous payments from bitcoin. In *Proc. of the 2014 IEEE Symposium on Security and Privacy (S&P'14), Berkeley, California, USA*, pages 459–474. IEEE, November 2014.

[44] K. Tinn and C. Dubach. Central bank digital currency with asymmetric privacy. `http://dx.doi.org/10.2139/ssrn.3787088` [Online; accessed on August 15, 2021], February 2021.

[45] A. Unterweger, F. Knirsch, C. Leixnering, and D. Engel. Lessons learned from implementing a privacy-preserving smart contract in ethereum. In *Proc. of the 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS'18), Paris, France*, pages 1–5. IEEE, February 2018.

[46] A. Veneris, A. Park, F. Long, and P. Puri. Central bank digital loonie: Canadian cash for a new global economy. `http://dx.doi.org/10.2139/ssrn.3770024` [Online; accessed on August 15, 2021], February 2021.

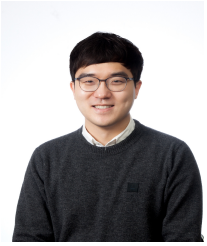
[47] Q. Wang, B. Qin, J. Hu, and F. Xiao. Preserving transaction privacy in bitcoin. *Future Generation Computer Systems*, 107:793–804, June 2020.

[48] A. C. Yao. Protocols for secure computations. In *Proc. of the 23rd Annual Symposium on Foundations of Computer Science (SFCS'82), Chicago, Illinois, USA*, pages 160–164. IEEE, July 1982.

[49] Q. Yao. Technical aspects of cbdc in a two-tiered system. `https://www.itu.int/en/ITU-T/Workshops-and-Seminars/20180718/Documents/Yao%20Qian.pdf` [Online; accessed on August 15, 2021], 2018.

[50] J. Zhang, R. Tian, Y. Cao, X. Yuan, Z. Yu, X. Yan, and X. Zhang. A hybrid model for central bank digital currency based on blockchain. *IEEE Access*, 9:53589–53601, April 2021.

Author Biography



Yunyoung Lee received B.S., M.S. degrees in industrial engineering from Seoul National University, South korea in 2018 and 2020. He is currently pursuing the Ph.D. degree in the Department of Industrial Engineering. His research interests include deep learning, central bank digital currencies, and time series analysis.

Bumho Son received B.S. degree in industrial engineering from Seoul National University, South korea in 2017, where he is currently pursuing the Ph.D. degree with the Department of Industrial Engineering. His research interests include deep learning, asset pricing, and blockchain economics.

Seongwan Park received B.S. degree in industrial engineering from Seoul National University, South Korea in 2021, where he is currently pursuing the Ph.D. degree with the Department of Industrial Engineering. His research interests include blockchain and deep learning.

Jaewook Lee is a professor in the Department of Industrial Engineering at Seoul National University, Seoul, Korea. He received the B.S. degree in mathematics from Seoul National University, and the Ph.D. degree in applied mathematics from Cornell University in 1993 and 1999, respectively. His research interests include central bank digital currencies, machine learning, neural networks, global optimization, and their applications to data mining and financial engineering.

Huisu Jang is an assistant professor for finance at the Soongsil University. She received the B.S., M.S., and Ph.D. degrees in industrial engineering from Seoul National University, South Korea, in 2013, 2015, and 2018, respectively. Her research interests include statistical machine learning, time series analysis, blockchain, and computational finance.