Privacy in the Age of Digital Finance: Central Bank Digital Currencies

Jeff Nijsse[1,2*] and Andrea Pinto[2,3†]

[1*]Department of Computer Science and Software Engineering, Auckland University of Technology, Auckland, 1010, New Zealand.
[2]Systems and Computer Engineering Department, Universidad de Los Andes, Bogotá, 111711, Colombia.

*Corresponding author(s). E-mail(s): jeff.nijsse@aut.ac.nz;
Contributing authors: ya.pinto10@uniandes.edu.co;
[†]These authors contributed equally to this work.

Abstract

In an age of financial system digitization and the increasing adoption of digital currencies, Central Bank Digital Currencies (CBDC) have emerged as a focal point for technological innovation. Privacy compliance has become a key factor in the successful design of CBDCs, extending beyond technical requirements to influence legal requirements, user trust, and security considerations. Implementing Privacy-Enhancing Technologies (PET) in CBDCs requires an interdisciplinary approach, however, the lack of a common understanding of privacy and the essential technological characteristics restricts progress. For instance, the technology perspective only addresses techniques requirements without considering the financial system, customer requirements, or regulatory compliance. Thus, this Systematization of Knowledge (SoK) extracted from 67 academic papers, applies the Design Science Research Methodology (DSRM) to understand: (1) how privacy can be defined within the framework of CBDCs and what implications this definition has for CBDCs design, and (2) which techniques, methods, and technologies can be employed to enhance privacy in the CBDCs design. Useful for all stakeholders, from citizens to Central Banks, we propose an innovative definition for privacy and overview the cryptographic landscape to develop guidelines for implementing PETs within the CBDCs context.

Keywords: CBDC, Central Bank Digital Currency, Privacy, DLT, Blockchain, Cryptography, Privacy Enhancing Technology

1 Introduction

In an era characterized by the digitisation of financial systems and the proliferation of digital currencies, Central Bank Digital Currencies (CBDCs) have emerged as a a groundbreaking point for technological innovation. According to data from the Human Rights Foundation (2023), nine Central Banks (CB) have CBDCs available to their citizens[1], and more than 100 CBs are in active phases of research. As nations contemplate the adoption of digital currencies, questions surrounding the safeguarding of data privacy become a central part in the design of CBDCs.

An illustration of public opinion is provided by a 2023 survey conducted by the Bank of Canada (2023), which examined perspectives and preferences regarding a digital Canadian dollar. The survey revealed that when questioned about trust in the government's ability to issue a secure digital dollar, 79% of participants expressed strong disagreement. Furthermore, in ranking the features by importance, over half of the respondents identified personal control over their data as their paramount concern, with one-third emphasising the significance of the capability for anonymous transactions. Similar consultation by the European Central Bank found privacy in payments as the most-important feature in a potential Digital Euro (van Oordt, 2022). A statistical approach comes from a Page-rank analysis of keywords associated with CBDCs finding that privacy is the most searched term with CBDCs (Bhaskar, Hunjra, Bansal, & Pandey, 2022). Considering the established importance of privacy to citizens, this is a topic that has "scarcely been researched" (Tronnier, Harborth, & Hamm, 2022), rather the focus is on payment systems (Jabbar, Geebren, Hussain, Dani, & Ul-Durar, 2023). One systematic literature review found seven themes associated with CBDCs, however, privacy was not one of them, nor was there mention of privacy technology (Hoang, Ngo, & Vu, 2023).

Privacy compliance has assumed a paramount role in the successful conception of CBDCs, extending its influence beyond technical prerequisites to encompass legal mandates, monetary policies, user trust, and security considerations. The incorporation of Privacy-Enhancing Technologies (PETs) into CBDCs necessitates an interdisciplinary approach; nonetheless, the differing views on what constitutes privacy, and its fundamental technological attributes, has impeded progress. To illustrate, the technological perspective has primarily addressed technical requirements in isolation, neglecting the broader context of the financial system, customer requisites, and regulation.

This Systematization of Knowledge (SoK) aims to contribute to the discourse by offering a thorough analysis of the privacy implications linked to the design of CBDCs. Derived from an in-depth examination of 67 academic papers, this SoK employs the Design Science Research Methodology (DSRM) to address two key research questions: (1) how can privacy be defined within the framework of CBDCs, and what implications does this definition has for CBDCs design, and (2) which techniques, methods, and technologies can be employed to enhance privacy in the CBDCs design. We advance an innovative definition of privacy, serving as a foundational cornerstone for a comprehensive perspective. Additionally, we formulate guidelines for the seamless integration of Privacy Enhancing Technologies (PETs) into the context of CBDCs.

[1] Includes the CB of the Eastern Caribbean Currency Union that of Anguilla, Antigua and Barbuda, Dominica, Grenada, Montserrat, Saint Kitts and Nevis, Saint Lucia, and Saint Vincent and the Grenadines.

The contributions of this SoK are (1) a definition of privacy in the context of CBDCs design that is inclusive of three main stakeholder perspecitves: legal and regulatory, technological, and transactional, and (2) an overview of the contemporary landscape in cryptographic techniques for CBDC design and consideration. These contributions are applicable to varied stakeholders outlined in Section 3.2 from policy makers and regulators to researchers and developers.

The rest of the paper is organized as follows. The methodology is introduced with literature review inclusion criteria. A definition of privacy is derived in Section 3 beginning with contemporary ideas of privacy from the literature and considering stakeholders in the design of CBDCs in Section 3.2. Section 4 overviews the Privacy Enhancing Technologies (PET) beginning with general encryption, digital signatures, leading to more advanced cryptography. Other PETs such as mixing and secure hardware are addressed in Section 5, then account strategies and digital identity. Section 6 discusses options for designers and policy makers of CBDCs and conclusion in Section 7.

2 Methodology

To ensure a comprehensive and representative SoK of the concept of privacy in the context of CBDCs, this study adapts the Design Science Research Methodology (Peffers, Tuunanen, Rothenberger, & Chatterjee, 2007). This methodology has six steps: (1) identify problems and motivate, (2) define objectives of the solution, (3) design and development, (4) demonstration, (5) evaluation, and (6) communication. The details of the methodology are presented in Table 1. Following the chosen methodology various combinations of keywords were used when searching in the Scopus, IEEE Xplore, and Science Direct databases. Finally, 67 documents are selected to begin the SoK.

3 Privacy

Privacy in the design of CBDCs plays a pivotal role in upholding users' autonomy over their financial data. It is essential for upholding the principles of autonomy and individual rights in the digital financial landscape. It acts as a safeguard against unauthorized access, surveillance, as well as the potential misuse of sensitive financial information. Preserving privacy within CBDCs is a cornerstone for implementing digital financial systems. Striking a balance between the benefits of CBDCs and implementing robust privacy protection mechanisms is imperative to be aware of at the design stage.

3.1 Current Definitions of Privacy

While the importance of privacy in the design of CBDCs cannot be overstated, the first trend is that a comprehensive understanding of privacy is still a gap within the literature. Studies struggle with the concept of privacy in CBDCs, and a common issue arises—there exists a lack of a clear and well-accepted definition. Nearly half of the analysed documents, 33 of 67 papers, do not elucidate their understanding of privacy in the context of CBDCs. Even when definitions are presented, they often fall short of encompassing the multidimensional nature of privacy within CBDCs. There

Table 1 Design Science Research Methodology as applied to the literature review to develop a definition of privacy in the context of CBDCs.

DSRM Step	Description
Identify problem	Privacy is crucial in CBDCs design, yet there's no consensus on its integration among stakeholders. Privacy is frequently overlooked in new proposals, and references to general "encryption" as a privacy solution lack detail. The complexity of cryptographic privacy technologies adds to the challenge, complicating the real-world implementation of CBDCs.
Define objectives of the solution	The main objective of the research is to perform a SoK to have a structured analysis of the privacy concepts and its application in the design of CDBCs. The SoK begins with literature from the last five years and is supplemented by secondary sourcing. Two research questions are formulated to achieve the objectives: **RQ1**: How can privacy be defined within the framework of CBDCs, and what implications does this definition have for CBDC design? **RQ2**: Which techniques, methods, and technologies can be employed to enhance privacy in design of CBDCs?
Design and development	Filter 1: The following combinations of keywords are used as of August 22, 2023: ("All Metadata": Privacy) AND ("All Metadata": Central Bank) AND ("All Metadata": Digital Currency) OR ("All Metadata": CBDC) Filter 2: Documents from the last five years from 2019–2023 are selected. Filter 3: Peer review documents: article, conference paper, review, or short survey. Filter 4: Documents written in English and available for research purposes. Filter 5: Elimination of repeated documents—a total of 5 documents are duplicates. Filter 6: Abstract analysis for primary filtering of documents. Filter 7: Full-text analysis to select the documents that positively contribute to the SoK. Here, one document is eliminated for not meeting quality standards.
Demonstration	1. A new definition of privacy is developed, and 2. Technological guidelines for enhancing privacy in the design of CBDCs are provided.

are three main perspectives that were found, technological or technical perspective, legal perspective, and transactional perspective. Figure 1.

The second prevailing trend identified is that of privacy from a technical perspective. In this context, privacy is considered a requirement that can be fulfilled based on technological characteristics. For instance, Distributed Ledger Technology (DLT) is a common element in nearly every design proposal from academia - blockchain technology being one of the most popular examples of DLT (J. Han et al., 2021; X. Han, Yuan, & Wang, 2019; Islam & In, 2023; Jabbar et al., 2023; Mazzoni, Corradi, & Nicola, 2022; Portu, 2022; Sanka, Irfan, Huang, & Cheung, 2021; Y.R. Wang, Ma, & Ren, 2022; Yang & Li, 2020; J. Zhang et al., 2021; X. Zhang, 2020; Zhong et al., 2021). Although, depending on the architecture design, DLT may or may not achieve a balance between privacy, transparency, and auditing capacity. Into this perspective, privacy is mainly related to the cryptography capacity of DLT (Lee, Son, Park, Lee, & Jang, 2021; Wüst, Kostiainen, Delius, & Capkun, 2022; yong Liu & Hou, 2020). Cryptography ensures data integrity, confidentiality, and authentication, and can be leveraged for a decentralized network. DLTs provide transparency, giving participants in the network a real-time, tamper-proof ledger of transactions. The trade-off in the

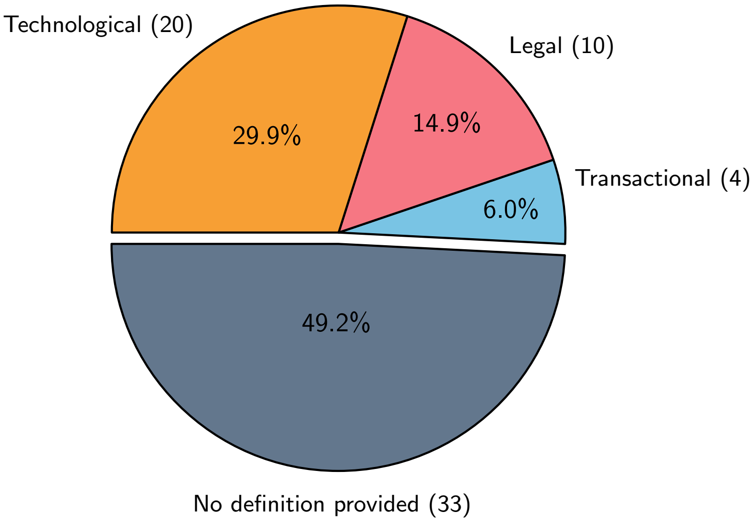


Fig. 1 Analysis of privacy definition in the context of CBDCs identifies four main trends. The strongest trend is an absence of a privacy definition in 33 of 67 papers, followed by a focus on three perspectives: the technological perspective, legal perspective, and transactional perspective.

search for transparency is that privacy concerns arise (Pocher & Veneris, 2021). Users and corporate data are visible to all participants, which may not align with data protection regulations or personal privacy expectations (Wüst et al., 2022; yong Liu & Hou, 2020). Thus, privacy-focused technologies, such as privacy coins and Zero-Knowledge Proofs (ZKP) (Section 4.6), are beginning to address these concerns by providing mechanisms for selective disclosure. These technologies empower users to share specific information based on their need. Nevertheless, the questions of what information is private, needs protection, from whom it should be shielded, and who can have access are ones that developers should not attempt to answer.

The third trend in privacy definitions is focused on addressing legal requirements. This perspective presents an additional challenge, for example, designing a CBDC for implementation in a European Union (EU) country (Portu, 2022; Tronnier et al., 2022) differs from proposing one for development in an Asian nation (Kshetri & Loukoianova, 2022; Ungson & Soorapanth, 2022). Moreover, there are variations in regulatory compliance (Kiayias, Kohlweiss, & Sarencheh, 2022) even among countries within the same region due to their own privacy understanding. In the EU, the General Data Protection Regulation (GDPR) is mandatory as it ensures the protection of users' personal data and privacy rights. However, the approach of the Chinese government may prioritize robust measures for detecting illegal financial activities over personal data protection (F. Allen, Gu, & Jagtiani, 2022). Despite the differences, there is a necessity to align CBDC designs with the legal requirements of various entities, including governments, financial regulatory institutions, and auditing bodies. Surprisingly, defining privacy is still a challenge even for policymakers. Although documents such as GDPR outline specific principles and rules regarding the handling and protection of personal data, it doesn't provide an explicit definition of privacy. However, to bridge the gap between the regulatory landscape and the technical design of CBDCs, a comprehensive definition of privacy that incorporates both legal and technical privacy requirements could serve as a foundational step toward the development of privacy focused CBDCs.

Finally, the least common trend looks at the transactional perspective (Gupta, Pandey, Ammari, & Sahu, 2023; Morales-Resendiz et al., 2021; Opare & Kim, 2020; T. Zhang & Huang, 2022). This perspective is based on protection of data associated with a financial transaction such as: digital identities of senders and recipients, transactional amount and ID, fees, and transactional status. This perspective asks for a high grade of untraceability as part of the characteristics of CBDCs. Current digital transactions offer complete traceability, ensuring the health of financial systems, those seeking privacy or anonymity often turn to cash as their preferred option. Untraceability, while associated with a high level of privacy, must be balanced with the need for legal compliance and the prevention of illegal use of CBDCs. This requires a certain degree of auditing capacity to be integrated into CBDCs systems. There is further limiting data within the transactional perspective. If CBDCs are a key part of the financial system, this must also include ancillary data such as credits reports, tax records, and customer records that needs to be protected by privacy laws.

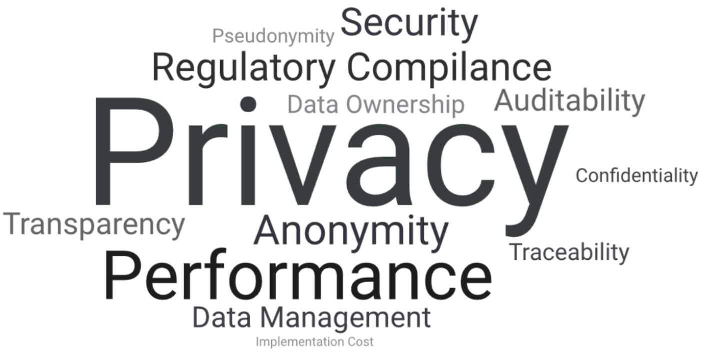


Fig. 2 Privacy related concepts in the context of CBDCs design. The concepts most frequently associated with privacy, listed in descending order, include: performance, regulatory compliance, anonymity, security/cybersecurity, and data management.

Privacy interlaces a multitude of essential concepts; each should contribute to a robust and user-centric financial ecosystem. As is shown in Figure 2. First and foremost, privacy is an ally of security (Agur, Ari, & Dell'Ariccia, 2022; Chand et al., 2023; Islam & In, 2023; Jin & Xia, 2022; Kshetri & Loukoianova, 2022; Lee, Son, Park, et al., 2021; Liu, Ni, & Zulkernine, 2022; Ma et al., 2022; Quamara & Singh, 2022; Scollan & Darling, 2023; Sethaput & Innet, 2021; van Oordt, 2022; H. Wang, 2023; Y.R. Wang et al., 2022; Xu & Jin, 2022), but it should be distinguished from confidentiality—a well-known property of information security that primarily deals with protecting information from unauthorized access. On the other hand, privacy forms a barricade against inappropriate use by authorized entities, ensuring the sanctity of user information. Second, regulatory compliance (Islam & In, 2023; Lee, Son, Park, et al., 2021; Opare & Kim, 2020; Pocher & Veneris, 2021; Sanka et al., 2021; Tronnier, 2021; Ungson & Soorapanth, 2022; H. Wang, 2023; Wilkins, 2022; T. Zhang & Huang, 2022; Zhong et al., 2021), a keystone in the world of finance, relies on the privacy of financial data. Privacy safeguards not only protect the individual but also foster trust in the regulatory bodies, enabling the seamless operation of CBDCs within the confines of the law (Islam & In, 2023; Lee, Son, Jang, et al., 2021; Pocher & Veneris, 2021; Portu, 2022; Wilkins, 2022). Third, transparency and anonymity coexist in the privacy landscape. Transparency assures users that their transactions are legitimate, while anonymity empowers them to transact without fear of undue scrutiny (Alsalmi, Ullah, & Rafique, 2023; Dashkevich, Counsell, & Destefanis, 2020; Gupta et al., 2023; Hsieh & Brennan, 2022; Kiayias et al., 2022; Lee, Son, Park, et al., 2021; Pocher & Veneris, 2021; Quamara & Singh, 2022; Rennie & Steele, 2021; T. Zhang & Huang, 2022). Meanwhile, traceability bridges these two facets by enabling authorized entities to track illicit activities without infringing on the privacy of law-abiding users. Fourth, data ownership and management (X. Zhang, 2020; Zhong et al., 2021) where individuals retain control over their financial data, and the management thereof adheres to stringent privacy principles. In the holistic realm of CBDCs design, privacy acts as the central thread, weaving a narrative of security, regulatory compliance, performance, transparency, anonymity, traceability, data ownership, and data management into a financial ecosystem that empowers users while maintaining the highest standards of integrity and trust.

3.2 Stakeholders in the design of CBDCs

To protect users' privacy in the design of CBDCs is a task that needs a collective effort of diverse stakeholders. The design of CBDCs extends far beyond technology, to the essence of digital society, personal autonomy, and governmental authority. The active participation of several key stakeholders becomes imperative. Through this Sok a set of stakeholders are identified, as is shown in Figure 3: (1) Central Banks Customers, customer engagement is the cornerstone of a secure, customer-centric digital currency that builds trust and catalyses broad adoption (J. Han et al., 2021; Jin & Xia, 2022; T. Zhang & Huang, 2022; X. Zhang, 2020); (2) financial regulators and auditing institutions, with their regulatory standards, guide the development of privacy-compliant CBDCs (Dashkevich et al., 2020; X. Han et al., 2019; Liu et al., 2022); (3) commercial banks and financial institutions, in charge of managing and securing sensitive financial data (Bhaskar et al., 2022; Dupuis, Gleason, & Wang, 2022; Maruo, Yuji, Sugino, & Sei, 2023), (4) government authorities, entrusted with the formulation and enforcement of laws, hold the keys to the legal framework within which CBDCs must operate, ensuring that they protect user privacy while complying with regulations (Ngo, Nguyen, Nguyen, Tram, & Hoang, 2023; Z. Wang, 2023; J. Zhang et al., 2021), and (5) businesses, as a specific type of CBDC user (F. Allen et al., 2022; Kshetri & Loukoianova, 2022; Xu & Jin, 2022), are not only obliged to adhere to privacy regulations but also play a pivotal role in system implementation, their acceptance and trust in the CBDCs are fundamental, as they can pave the way for gaining the trust of citizens. Lastly, malicious actors, which are individuals or organizations with the intent to engage in illegal activities such as network blackmail, fraud, and money laundering inside the CBDC system (Lee, Son, Park, et al., 2021; Wüst et al., 2022; Zhong et al., 2021).

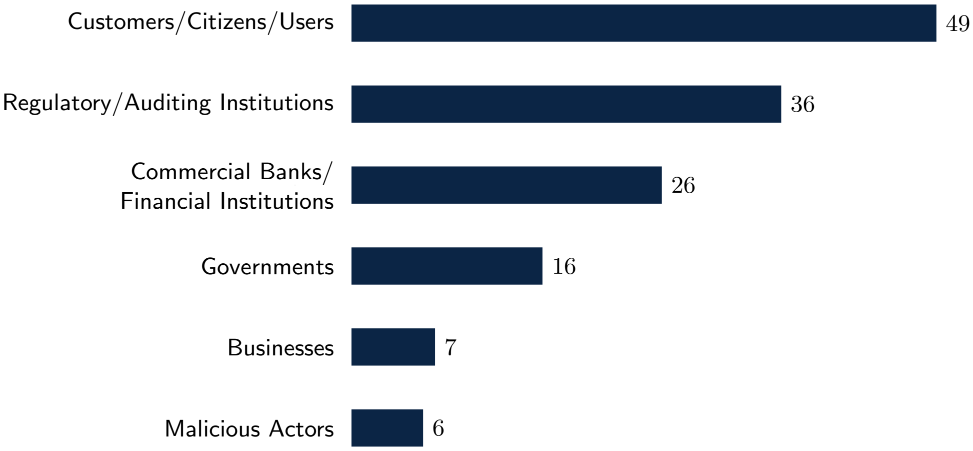
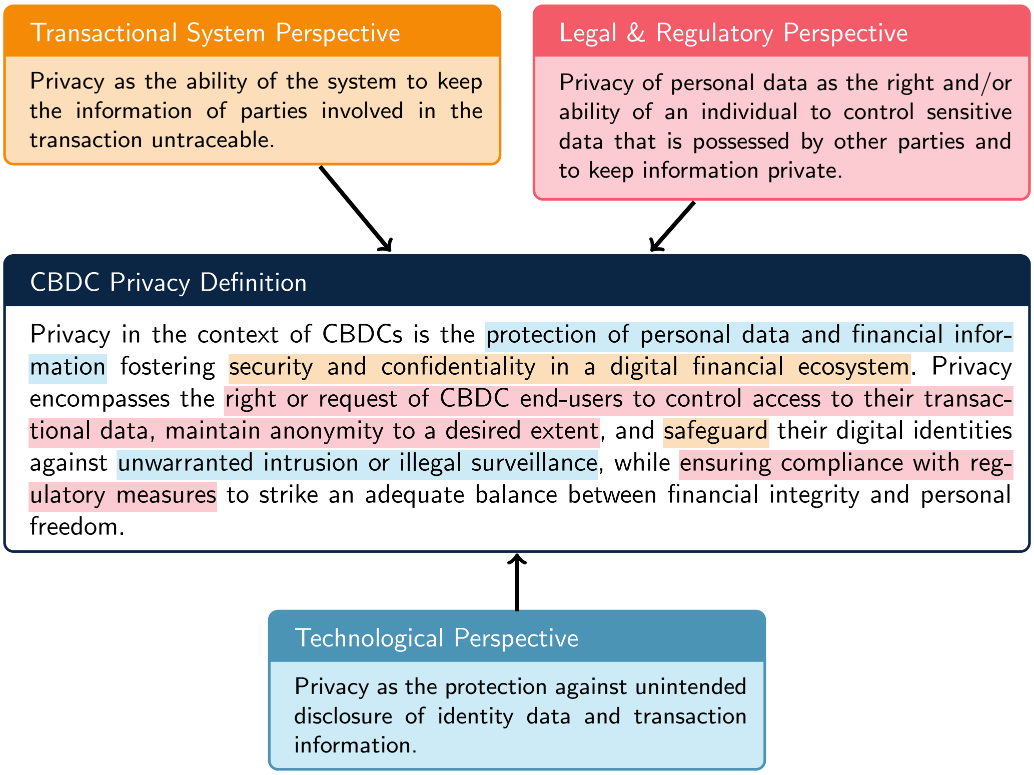


Fig. 3 Stakeholders in CBDC privacy. The most important stakeholders analyzed in the CBDCs design are customers, followed by financial regulations or auditing institutions. The frequencies are not mutually exclusive.

Nonetheless, there are other stakeholders that were not clearly found in the review but should be considered to safeguard privacy. Privacy advocates and civil society organizations acting on behalf of citizens are the guardians of civil liberties monitoring the protection of user privacy rights; technical developers and engineers are architects who can convert privacy principles, developed by governments and regulatory institutions, into operational designs; and academics and researchers enrich the discourse with their ideation and critical evaluation. Together, these stakeholders must work to implement privacy preservation aspects within the CBDCs landscape, under the guidance of the Central Banks that oversee the monetary national policies, shoulder the responsibility of balancing between financial control and individual privacy. Their collective understanding is vital to forging a financial future where privacy is not sacrificed but intricately involve in the functioning of digital currencies, fostering a financial landscape that is both efficient and profoundly respectful of user privacy.

3.3 Proposal definition of privacy in the Context of CBDCs

Authors analyse existing concepts of privacy from different perspectives including legal frameworks, transactional data, and technological vision. There is a need for a unifying and accessible definition of privacy, one that resonates with all the previously mentioned stakeholders. The goal is to propose a definition that seamlessly weaves together the legal, transactional, and technological perspectives, setting a clear and unified path forward in the design of CBDCs. This definition, while precise, shall remain comprehensible to all, providing a foundation upon which a privacy-by-design approach can be built and fostering trust in the digital financial ecosystem. As shown visually in Figure 4,



Transactional System Perspective

Privacy as the ability of the system to keep the information of parties involved in the transaction untraceable.

Legal & Regulatory Perspective

Privacy of personal data as the right and/or ability of an individual to control sensitive data that is possessed by other parties and to keep information private.

CBDC Privacy Definition

Privacy in the context of CBDCs is the protection of personal data and financial information fostering security and confidentiality in a digital financial ecosystem. Privacy encompasses the right or request of CBDC end-users to control access to their transactional data, maintain anonymity to a desired extent, and safeguard their digital identities against unwarranted intrusion or illegal surveillance, while ensuring compliance with regulatory measures to strike an adequate balance between financial integrity and personal freedom.

Technological Perspective

Privacy as the protection against unintended disclosure of identity data and transaction information.

Fig. 4 Proposal definition of privacy. The proposed concept aims to integrate the most important aspects defined through the analyzed papers, in which different perspectives were identified along with the need for a common definition.

Our proposed definition of privacy in the context of CBDCs serves as a broad foundation, acknowledging the multifaceted nature of the subject. It emphasizes the importance of prioritizing privacy in the design of CBDCs, recognizing that achieving this goal goes beyond creating a theoretically perfect technological model. To develop practical and real-world CBDCs proposals, the technological perspective must align not only with legal requirements but also with the complexities of the broader financial system, extending far beyond the realm of central banks. Governments can have varying priorities in CBDCs design, with some emphasizing legal requirements that may limit technological capabilities, while others may be constrained by limited access to high-tech solutions. The question of finding the appropriate balance between these perspectives should be addressed by developers in the initial phases of CBDCs design. However, from an academic viewpoint, each of these perspectives holds equal importance in the creation of a well-designed CBDC.

4 Privacy Enhancing Technology

There is a dominance between blockchain and cryptography as the general tools available to designers, seen in Figure 5, where 58% imply that privacy in CBDC development can be met by the introduction of technical methods. The level of understanding and detail comes in varying degrees. Three sources say nothing more than a general sense that cryptography can be used to assist with privacy (Kesavaraj, Jakhiya, & Bhandari, 2022; Kshetri & Loukoianova, 2022; van Oordt, 2022), while a further six offer no more insight than mentioning 'encryption' (Adams, Boldrin, Ohlhausen, Ralf, & Wagner, 2021; F. Allen et al., 2022; Jin & Xia, 2022; Maruo et al., 2023; Sethaput & Innet, 2021; Tian, Chen, Ding, Zhu, & Zhang, 2019). This leaves a significant void of details to help practitioners.

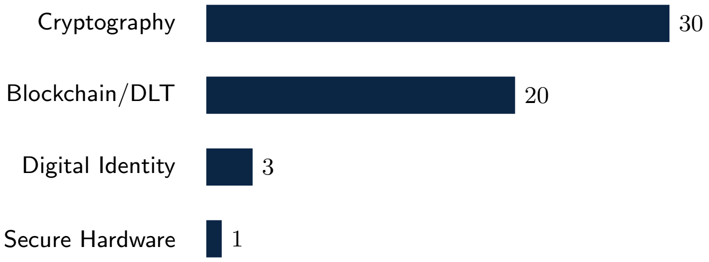


Fig. 5 Privacy-Enhancing Technology (PET) as applied to CBDCs derived from the literature involves traditional cryptographic methods but also a significant amount of blockchain technology and a minority of digital identity and secure hardware. The counts are not mutually exclusive.

The specific cryptographic methods are broken down by count in the literature in Figure 6. ZKPs dominate the discussion in privacy, followed by digital signatures (11 count, in aggregate). The long tail shows singular mentions of specific signature techniques along with coin mixing, and applying verifiable random functions, and secure hardware.

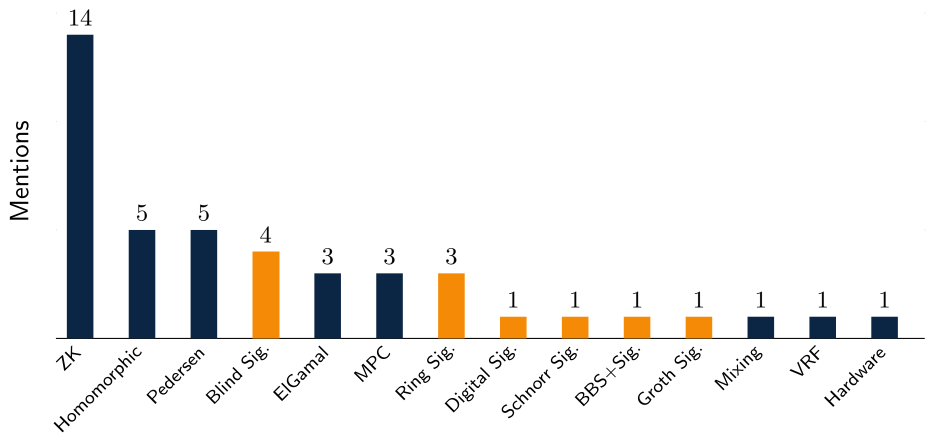


Fig. 6 Cryptographic techniques sorted by occurrence in the privacy literature in the context of CBDCs. Zero-knowledge proofs are the most common with reference in 14 of 67 sources. Digital signature variants are in orange and form in aggregate the next most prominent method with 11 references. The mentions are not mutually exclusive.

Given the definition in Figure 4, privacy can be simplified into layers, each of which that can be achieved using cryptographic methods. Privacy, in the digital environment requires: (A) protection of personal data, (B) protection of financial information, (C) right of users to maintain anonymity, (D) right or request of CBDCs users to control access to their transaction data, (E) ensuring compliance with regulatory measures.

All the cryptographic methods described in Figure 6 are discussed presently and integrated with the privacy definition in a layered stack shown in Figure 7.

4.1 Encryption

The layered approach begins with the protection of data seen as Layer A in Figure 7. In a CBDCs this is transaction data, Know Your Customer (KYC) data, and associated metadata. Regardless of the type of data, standard encryption methods apply. Public-key cryptosystems provide the common method used to secure data, for example, in sending credit card information online[2], or in encrypted email services. Liu et al. (2022) suggest the central bank encrypts user KYC data with the ElGamal cryptosystem, although this is merely standard data encryption.

The ElGamal cryptosystem (1985) is a public key cryptosystem that builds upon the principles of Diffie-Hellman key exchange. Apart from its use as an encryption scheme, ElGamal has been the foundation for various digital signature schemes. The original ElGamal encryption is rarely used in practice for encrypting data (because of its inefficiency and large ciphertexts) but remains influential in the field of cryptography. ElGamal has a probabilistic element from random number inputs that makes

[2] The most well-known is RSA encryption (Rivest, Shamir, & Adleman, 1978) which allows for encryption and digital signatures by the asymmetric key-pair. In practice RSA is used to establish a session key which then is used for data transfer via AES or similar.

it semantically secure, meaning that even if the same plaintext is encrypted multiple times with the same public key, the resulting ciphertexts will appear random and unrelated, making it difficult for an attacker to gain insights into the plaintext based on ciphertext patterns alone. Kiayias et al. (2022) propose a private and regulated CBDC with threshold ElGamal encryption. Their scheme also involves Blind signatures (Section 4.2.4) and ZKPs (Section 4.6). Additionally, Chu et al. (2022) suggest ElGamal can ensure user privacy in offline e-cash.

Standard encryption can digitally protect user data, Layer A, but to protect transaction data, Layer B, additional functionality is required. A transaction is an exchange of information between two parties, which if we reduce to two people, Alice and Bob, can be stated as: Alice sends Bob 1 coin. In this transaction, it doesn't help for Alice to encrypt her coin, as Bob has no assurance that the encrypted object is indeed now his coin. Additionally, were Alice to share her key so Bob can decrypt the object, then Alice has compromised her own security. Both parties need to have access to, or to "see", the transaction to agree on the details. Digital signatures solve this problem.

Layer	**Tools**							
(A) protection of personal data (Alice only)	Standard Encryption: RSA, EC, ElGamal							
(B) protection of transaction data (Alice + Bob)	Standard Digital Signatures: ECDSA, RSA							
(C) right of users to maintain anonymity	Blind	Ring	Schnorr	ZKP	HE	PC	MPC	Mixing
(D) right or request to control access to transaction data				ZKP	HE			
(E) ensuring compliance with regulatory measures	BBS+				HE	PC		PP

Fig. 7 The PET cryptographic stack integrated with layers of the definition in of privacy in Figure 4. Begin at Layer A with standard encryption and add layers to meet the design requirements of the CBDC.

4.2 Digital Signatures

First proposed by Rivest, Shamir, and Adleman (RSA) (1978), Digital signatures prove the authenticity and integrity of a message. A signer uses their private key to sign a message. Anyone with the corresponding public key can verify that the message was signed by the holder of the private key and that the message has not been tampered with. The message data in this case is transaction data, where every transaction requires a signature. For Alice to give Bob 1 coin, she signs the transaction with her private key, which can then be verified by Bob using Alice's public key. (Alice has not had to reveal her private key.) Elliptic Curve Digital Signature Algorithm (ECDSA) is a commonly applied digital signature method seen in Bitcoin and Ethereum, while RSA signatures are common in web browsing.

In the absence of digital signatures, online trust is fundamentally compromised. This is no different for a CBDC. Systems eschewing digital signatures typically resort to analogue counterparts, like signed checks, or verbal tests. In this manner, digital signatures can be a proxy for identity, where a mobile phone can handle transaction signing.

Myriad variations in signatures provide different properties that can add privacy to the components to bolster Layer C in Figure 7: the right of users to maintain anonymity.

4.2.1 Ring Signatures

The key feature of ring signatures is that they allow a signer to create a signature on behalf of a ring of potential signers without revealing exactly who the signer is (Rivest, Shamir, & Tauman, 2001). This ring is a set of public keys, and any holder of the corresponding private key to one of those public keys can create a ring signature. The signer doesn't need to collaborate or obtain permission from the other members of the ring (or the signer's own keys). This provides signer ambiguity. It's like a group signature (Chaum & van Heyst, 1991) but without any centralized group setup[3]. This allows the sender of a transaction to hide in a crowd and is used in Monero transactions. (Lee, Son, Park, et al., 2021; Pocher & Veneris, 2021; Sanka et al., 2021) mention ring signatures in the CBDCs context. These transactions aren't anonymous as the ring is identifiable, however, they provide a layer of privacy to transacting above regular signatures by unlinking the sender.

4.2.2 Schnorr Signatures

Schnorr signatures (Schnorr, 1991) are a simple and efficient elliptic curve signature scheme. Unlike ECDSA, which requires a unique random number for each signature (risking key exposure if repeated), Schnorr signatures inherently avoid this risk and provide a linear structure allowing for multiple signatures. Their linearity makes them particularly attractive for complex cryptographic protocols and reduces the size of multi-sig transactions. Batch verification also improves efficiency. Privacy can be improved by the key combination properties, for example, participants can combine public keys into a single key which appears as such to the verifier. Bitcoin improvement proposal 340 is to introduce Schnorr signatures for Bitcoin[4]. Liu et al. (2022) have an anonymous and traceable CBDC operating in three tiers similar to traditional

[3] In a standard group signature scheme there is a group manager that handles the group public key and oversees revocation in case of malicious activity.

[4] https://github.com/bitcoin/bips/blob/master/bip-0340.mediawiki

banking: CBs, commercial banks, and users. Coin creation by the CB is secured with BBS+ (Section 4.2.3) and Schnorr signatures.

Should a member of a group be malicious, it would be beneficial for the group manager or otherwise to be able to revoke their privileges while maintaining the integrity of the remaining group members.

4.2.3 BBS+ Signatures

BBS+[5] signatures (Boneh, Boyen, & Shacham, 2004) are a type of group signature scheme with the feature of being able to reveal the identity of the signer if necessary (through a designated entity or group manager). This allows for accountability while preserving privacy. BBS+ might be more apt than ring signatures for systems where conditional anonymity is a requirement, such as a central banking authority subject to legal requirements. BBS+ signatures are proposed for the creation of CBDC coins (Liu et al., 2022). Thus, the group manager (CB) can, when required, reveal information. They are especially known for their use in anonymous credential systems to prove membership without revealing identity (Decentralized Identity Foundation, 2023). Layer E in Figure 7 is ensuring compliance with regulatory measures and is applicable to BBS+ methods.

4.2.4 Blind Signatures

To make the transition to digital cash, the link needs to be broken between the issuing authority (the CB) and the user. This function can be accomplished with blind signatures. Blind signatures differ from BBS+ by ensuring the signer's ignorance of transaction content, key for digital cash systems to issue currency while maintaining user privacy and preventing double spending.

Blind signatures (Chaum, 1983) allow a signer to sign a message without viewing its content, ensuring the signer remains ignorant of the message while still vouching for its authenticity. A bank can use blind signatures to sign electronic tokens representing currency units without seeing the actual token's details. When a user spends the digital cash, the bank can't link the withdrawal of the token to its subsequent spending, ensuring user privacy similar to physical cash. They can be used in certain protocols to ensure privacy or in off-chain solutions where transaction details need to be obscured from certain participants. Blind signatures are applicable in the context of CBDCs (Ballaschk & Paulick, 2021; Chu et al., 2022; Kiayias et al., 2022; Lee, Son, Park, et al., 2021), and seem promising, however, the main drawback is that the user can't audit the message they are signing. This drawback can be analogised by signing the outside of a sealed envelope attesting it was in your possession, however, you didn't open and read it.

The scheme in Kiayias et al. (2022) uses blind signatures to protect user privacy. This method preserves anonymity and security. The maintainers know they have signed a valid transaction or account snapshot, but they don't know the specific details of what they signed. The user, on the other hand, ends up with a legitimately signed document without exposing sensitive transaction details to each individual maintainer.

[5] Named after the authors: Boneh, Boyen, and Shacham.

Chu et al. (2022) highlights blind signatures use in offline transaction capability such as with smart cards.

4.2.5 Verifiable Random Function

Lastly, a Verifiable Random Function (VRF) can serve as a proxy for a DS. Both VRFs and digital signatures involve the use of private keys to produce some output (a signature or a random value) and the use of corresponding public keys to verify that output. The VRF produces a random output from a given input in a deterministic manner, where the output can be verified with a proof by anyone holding the corresponding public key. A user with a private key can compute a random value from an input using the VRF. They also produce a proof. Anyone with the public key can then verify, using the proof, that the random value was generated correctly without knowing the private key. A VRF can be seen as a special type of signature scheme where the 'signature' is a random value that is deterministically derived from an input and can be verified with a proof.

Lee, Son, Park, et al. (2021) mentions Groth signatures[6] and VRFs as part of a method to overcome the trusted setup assumption present with SNARKs (Section 4.6) although this is in the context of permissioned blockchain and not CBDCs (Androulaki et al., 2020).

4.3 Multi-Party Computation

Multi-Party Computation (MPC) and commitment schemes such as Pedersen Commitments (PC) (Section 4.4) both deal with hiding information in some form. MPC, based on secure two-party computation (Yao, 1982), is designed to compute functions over secret data without revealing the data. Multiple parties can come together, each bringing their inputs, then MPC can compute a result, and the individual parties are not privy to each other's data. This ensures data privacy, even when collaborating on computations (Layer C in Figure 7). One of the primary applications of MPC in cryptocurrencies is for secure wallet generation and key management. Traditional single-key wallets face risks if the key is lost or stolen. Using MPC, a private key can be split into multiple shares distributed among various parties. To sign a transaction, a threshold number of these shares are required. This approach adds a layer of security, making it harder for attackers to compromise a wallet since they would need to gain access to multiple key shares. A version of this has been implemented in a CBDC construction on Cosmos (J. Han et al., 2021). MPC is similar to Homomorphic Encryption (HE) (Section 4.5) but under different contexts: MPC require multiple parties to interact and be collaborative, whereas HE focusses on calculations of encrypted data. For transfers of digital currency, MPC can be applied to obfuscate details like the transaction amount while still allowing for network validation. Monero calls these confidential transactions. Transaction aggregation is a similar technique that can benefit for MPC, given all parties agree to the aggregation. Lee, Son, Park, et al. (2021) applies MPC to protect privacy during real-time gross settlement between banks.

[6] Groth signatures (Groth, 2010) used as part of ZK proving, provide a way to produce short signatures and are particularly efficient in terms of verification.

4.4 Pedersen Commitments

A different way of aggregation is found in Mimble Wimble which applies PC to combine transactions into a single larger transaction so that an observer cannot determine the link between sender and recipient[7]. Pedersen commitments (Pedersen, 1991) provide a secure mechanism for committing to a message by encapsulating it within a cryptographic envelope. This approach ensures the confidentiality of the original message, safeguarding it from disclosure until the committing party opts to unveil it. The robustness of this technique stems from its binding property, which guarantees that once a message has been committed, any attempt to alter it will be computationally detectable, thereby preserving the integrity of the commitment. Y.R. Wang et al. (2022) apply a Pedersen commitment to allow for auditability of commercial banks by the central bank.

PCs are additively homomorphic meaning that the commitments can be added together without knowing the individual components which is applicable to preserving transaction information. They are also applied in ZKP scenarios to enable transactions that are both private and verifiable. The commitment allows a user to prove that they have knowledge of a value (like a secret key or transaction amount) without revealing the value itself. PCs are used to create transactions where the sender and receiver know the transaction details, but to the rest of the network, these details remain private (Pocher & Veneris, 2021). More broadly they can be used to commit knowledge of a vote, or value of an asset without revealing the vote recipient or amount of value.

Androulaki et al. (2020) propose an auditable anonymous token management system that uses Pedersen commitments to conceal UTXOs in a permissioned blockchain. Project Khokha from the South African Reserve Bank (South Aftrican Reserve Bank, 2018) applies Pedersen commitments and range proofs for transaction privacy in a permissioned instance of Quorum (Opare & Kim, 2020). Both these projects highlight the applicability of Layer E in Figure 7 to ensuring compliance with regulation.

4.5 Homomorphic Encryption

Homomorphic encryption (Gentry, 2009) is a form of encryption that allows computations on ciphertexts, which, when decrypted, matches the result of the operations as if they were performed on the plaintext. Essentially, it lets you work with encrypted data without decrypting it first. The primary allure of HE is in secure data analysis. It allows for private computations in the cloud where the cloud server doesn't know the actual data it's computing on. Applications include encrypted search, privacy-preserving medical research, and secure voting systems. Fully Homomorphic Encryption could enable a system where transaction details are encrypted, yet computations (like verifying the transaction's authenticity or ensuring there are sufficient funds) can be carried out on these encrypted transactions. This means the transaction can be validated without the verifying entity ever seeing the transaction's specifics or the identities of the involved parties (Layer C in Figure 7). Personal privacy can be preserved when central banks or other regulatory entities analyze transaction trends for monetary policy or anti-fraud measures without directly accessing the personal details of the involved

[7] Monero and Zcash also apply Pedersen commitments.

parties. The downside is computational overhead making large volumes of data analysis impractical. Lee, Son, Park, et al. (2021) talk of HE for private calculations such that transaction amounts can be obscured while still adhering to transaction input and output balancing. Similar HE use is seen in Q. Wang, Qin, Hu, and Xiao (2020)'s framework for transaction privacy in Bitcoin.

To enhance user privacy while monitoring for illicit activities, the Australian Transaction Reports and Analysis Centre (AUSTRAC) collaborated with participants from the Fintel Alliance, a public-private initiative it founded, to create advanced data-matching and machine-learning tools aimed at detecting anomalous behaviour. Utilizing HE, these tools can analyse and process machine-learning data while it remains in an encrypted state, thus preserving confidentiality (Rennie & Steele, 2021) and fitting into Layer E in Figure 7.

4.6 Zero-Knowledge Proofs

The mostly widely occuring PET is ZKPs (Kiayias et al., 2022; Lee, Son, Jang, et al., 2021; Lee, Son, Park, et al., 2021; Liu et al., 2022; Opare & Kim, 2020; Pocher & Veneris, 2021; Sanka et al., 2021; Scollan & Darling, 2023; Sethaput & Innet, 2021; Takaragi, Kubota, Wohlgemuth, Umezawa, & Koyanagi, 2023; Tronnier, 2021; Tronnier et al., 2022; Wüst et al., 2022; Zhong et al., 2021). The fundamental idea behind ZKPs is that one party (the prover) can prove to another party (the verifier) that a statement is true, without revealing any specific information about the statement itself (Goldwasser, Micali, & Rackoff, 1989). Zero-knowledge Succinct Non-Interactive ARguments of Knowledge (zk-SNARKS) (Ben-Sasson, Chiesa, Tromer, & Virza, 2003) were developed as a way to create ZK proofs that are both succinct (short in size) and non-interactive (requiring only a single message from the prover to the verifier).

A SNARK by itself achieves a proof of computation but without extra privacy – both parties know what's being proved. By adding in a ZK component, you can have proof of computation without knowledge of what it was to be proved. A classic example involves a sudoku puzzle where the prover shows the verifier a completed puzzle, then the verifier can easily check the solution and both parties are aware of what is being verified (Berentsen, Lenzi, & Nyffenegger, 2023). To add privacy, the verifier can verify the solution without having access to the particular puzzle answer.

They also require a trusted setup which introduces a vulnerability in the derivation of the underlying parameters. The use of SNARKS in cryptocurrencies (Pocher & Veneris, 2021; Sanka et al., 2021) is most well known for being implemented in Zcash. zk-SNARKs enable Zcash to maintain a secure ledger of balances without revealing the amounts or parties involved in transactions. This allows transactions to be verified without revealing any of the transaction details, offering a high level of privacy to its users. Gross, Sedlmeir, Babel, Bechtel, and Schellinger (2022) propose private transactions for a CBDCs within set limits by applying SNARKs, in a similar manner to Zcash. Within the privacy definition zero knowledge sits at Layer C allowing users the technology to maintain anonymity.

Zero-Knowledge Scalable Transparent ARguments of Knowledge (zk-STARKS) (Ben-Sasson, Bentov, Horesh, & Riabzev, 2018), were developed as an alternative to zk-SNARKs, aiming to overcome some of their limitations, especially the need for a trusted setup. They are believed to offer resistance against quantum computer attacks. They are designed to be scalable with the complexity of the statements being proven. The downside is larger size than zk-SNARK proofs, but advancements are continuously made to reduce their size and improve efficiency. No surveys in the literature review mention STARKS, however, Starknet[8] is a layer 2 Ethereum rollup protocol that could act as infrastructure to support development of digital currencies.

5 Privacy-adjacent Techniques

Two techniques come from the blockchain era that are not traditional PETs, but closely related to design and implementation elements that can enhance privacy: the UTXO and account based models, and coin mixing. Subsequently, two remaining topics are related: secure hardware and digital identity.

5.1 UTXO & Account Models

An Unconfirmed Transaction Output (UTXO) model treats a transaction as composed of inputs and outputs. Should the input be 10 coins to purchase services valued at 9 coins, two outputs are created: 9 coins to the merchant and 1 coin change to the payer. This model is advantageous for auditability, scalability, and security, but requires fresh addresses to improve privacy by removing the implicit user-address link. This contrasts with an account model that tracks a balance and a token model that allows for asset transfer in addition to native currency transactions.

Islam and In (2023) design a UTXO model in the context of a permissioned blockchain. To overcome the privacy need for dynamic address use they employ a centralised certificate authority (the CB) to manage IDs and their links to wallet addresses. Repeated use of the same address can lead to de-anonymisation, so Pocher and Veneris (2021) use hierarchical deterministic wallet structures (a different address for each transaction) preventing the easy association of public addresses with individual users. J. Zhang et al. (2021) propose a CBDC via a hybrid scheme to use an account model for basic transactions and a UTXO model for assets other than the native currency. This hybrid model is conceived to improve efficiency when considering a large number of transactions[9] in a permissioned blockchain. Also in a permissioned blockchain, Islam and In (2023) design a UTXO model with dynamic address management through a centralised certificate authority (the CB) to manage the ID–wallet links.

5.2 Mixing

Mixing is related to the idea of privacy pools which hide transactions in a crowd by obfuscating their links in a public ledger. This is susceptible to tainting if a known malicious transaction is in the set. Using zero-knowledge, Buterin, Illum, Nadler, Schär, and Soleimani (2023) suggest an inverse protocol via Privacy Pools (PP), allowing

[8] https://www.starknet.io/

[9] According to data from the China National Network Clearing Corporation, the number of online transactions from January 24 to 30 during the Spring Festival holiday in 2020 is 4.919 billion (J. Zhang et al., 2021).

users to disassociate from a transaction set that has been tainted by publishing a proof that their transaction did not originate from an identified source. Centralised mixing presents a trusted source that has access to the input transaction information, this may be beneficial for auditing purposes (Pocher & Veneris, 2021), while decentralised mixing, such as Tornado Cash, does not allow for straight-forward auditing. Tornado Cash is a non-custodial privacy solution on Ethereum that breaks the on-chain link between source and destination addresses using zk-SNARKs. Samourai, a Bitcoin wallet, has a feature called Whirlpool, that provides transaction mixing via CoinJoin to combine multiple transaction inputs into a single transaction. By doing this, it becomes significantly more difficult to determine which inputs correspond to which outputs.

5.3 Secure Hardware

Secure hardware refers to specially hardened computing infrastructure. Hardening can occur at the processor level in the form of a trusted execution environment (TEE) which is a separate enclave not accessible to other parts of the processor and computing stack, or as a separate module entirely combined of trusted software, firmware, and a chip (S. Allen et al., 2020). The TEE is more common, with smartphones capable of supporting them, for example, Samsung's KNOX. Standalone modules include hardware wallets for cryptocurrency storage, and smart cards that can use NFC and RFID technology, similar to debit cards (Veneris, Park, Long, & Puri, 2021). Both TEEs and modules can be part of a CBDC design.

A TEE can be leveraged by sending and receiving encrypted transaction data to the server, which can then compute expensive cryptographic operations, removing the computation burden on a mobile device. Depending on the cryptographic operations, user privacy can be enhanced (S. Allen et al., 2020).

A secure cash card or NFC based system can allow for offline payments (Lee, Son, Park, et al., 2021) without contacting the bank. The bank originally issues the digital tokens which can be loaded into a secure card or mobile wallet. This yields cash-like privacy for the users and the benefit of transacting in rural areas, or as tourists outside local jurisdictions (Veneris et al., 2021).

5.4 Digital Identity

Digital identity is closely tied to digital methods of financial participation. Cryptocurrencies like bitcoin and ether[10] are pseudonymous meaning that identity can be linked via transaction metadata analysis. De-anonymisation of financial activity leading to someone's past history is irreversible and have downstream social effects. Although this review focuses on CBDCs, there is scope for discussion in the identity space.

Portu (2022) suggest that in order to transact, a payee need only verify their personhood. Once they are identified, the necessary balance requirements can be verified, but that can be done after ID verification. The authors further suggest that NFTs can be the basis for a payee's digital identity. The proposed system is only pseudonymous in nature as publicly readable transactions are at risk of de-anonymization. Takaragi

[10] A style note: coins are lowercase, and networks like Bitcoin and Zcash are capitalised.

et al. (2023) propose a system to apply a delegatable anonymous credential (DAC) via Pedersen commitments and ZK to national ID cards. Their system allows a user to prove they have valid credentials without revealing the private information behind them. Scollan and Darling (2023) suggest decentralised identity (DID) to manage a user's privacy disclosure where and when appropriate as a middle ground between total user anonymity and state surveillance.

6 Discussion

CBDCs may have arrived in the blockchain era, but do not necessarily use a blockchain or require blockchain technology. It's the digital cash nature of cryptocurrency that lends itself to the idea that CBDCs are a blockchain application as shown in Figure 5. Research that mentions blockchain in the context of privacy often presents a tenuous link and ignores regulatory requirements, or suggests strong anonymity via ZKPs, or addresses the pseudonymous nature of public blockchains by introducing a private consortium. There is no clear implementation to meet the requirements of both CBs and citizens. For an overview of blockchain and CBDCs see Dashkevich et al. (2020).

Despite significant research worldwide by CBs, there has been limited success introducing a CBDC to the market. Nigerian's CBDC the eNaira has seen limited uptake as Nigerians have very low trust in their Government monetary system and there is high competition among mobile money operators (Ree, 2023). Other nations have cancelled their plans such as Denmark's e-krone[11], stating that a CBDC would not improve the financial infrastructure and be in competition with their commercial banks. Kenya's central bank has also halted research concluding there is no need to launch a CBDC but will monitor the landscape[12].

Perhaps these offerings suffer from being too early to the market without enough time for public opinion to sway in favour. Either way there are few well-architected solutions for developers to learn from and build upon. Cryptographic methods are recognised as integral to privacy (Figure 5), with myriad options for enhancing user's right to maintain anonymity (Layer C in Figure 7), however, proving difficult to find in practice. The difficulty comes from allowing a balance between privacy and auditability. Contrasting with Layer C, there are few options to assist auditors adhering to compliance in Layer D. For full constructions we find only Platypus (Wüst et al., 2022) that preserves privacy in a centralised manner, and PEReDi (Kiayias et al., 2022), a privacy preserving and regulated construction that is distributed and robust against single points of failure. Liu et al. (2022) propose an anonymous and traceable CBDC, but anonymity is only guaranteed between the CB and the commercial bank. A lone DLT construction is found in Cos-CBDC (J. Han et al., 2021) that is prototyped using the Cosmos-SDK and claims privacy preserving properties. Given the importance of citizen rights and their opinions of financial privacy stated in the introduction, these solutions should be explored further.

[11] https://cbdctracker.org/currency/denmark-e-kroner
[12] https://cbdctracker.org/currency/kenya

7 Conclusion

The SoK provides an overview of the concept of privacy in the context of CBDCs. By combining technological, legal, and transactional perspectives tailored to CBDCs, a novel definition of privacy is introduced. Privacy is defined as the protection of personal data and financial information to foster security and confidence in a digital financial ecosystem; it encompasses the right or request of CBDC end-users to control access to their transactional data, maintain anonymity to a desired extent, and safeguard their digital identities against unwarranted intrusion or illegal surveillance; all while ensuring compliance with regulatory measures to strike an adequate balance between financial integrity and personal freedom.

An overview of the relevant technologies and methods applicable for enhancing privacy in CBDC design is provided that can be leveraged to highlight strengths, such as the variety of options available to help citizens maintain their financial anonymity, and weaknesses, such as the lack of complete implementations to draw from. By examining the cryptographic landscape, this research paves the way for the effective implementation of PETs in CBDCs as researched by academics, tested and built by industry, and legislated by regulators. Contributing to the broader discussion on digital currency, security, privacy standards, and the balance needed between central banks and citizen stakeholders is paramount in the age of digital finance including Central Bank Digital Currencies.

References

Adams, M., Boldrin, L., Ohlhausen, R., Ralf, R.O., Wagner, E. (2021). An integrated approach for electronic identification and central bank digital currencies. *Journal of Payments Strategy & Systems*, *15*, 287-304,

Agur, I., Ari, A., Dell'Ariccia, G. (2022, 1). Designing central bank digital currencies. *Journal of Monetary Economics*, *125*, 62-79, https://doi.org/10.1016/j.jmoneco.2021.05.002

Allen, F., Gu, X., Jagtiani, J. (2022, 6). Fintech, Cryptocurrencies, and CBDC: Financial Structural Transformation in China. *Journal of International Money and Finance*, *124*, , https://doi.org/10.1016/j.jimonfin.2022.102625

Allen, S., Capkun, S., Eyal, I., Fanti, G., Ford, B., Grimmelmann, J., ... Zhang, F. (2020). Design Choices for Central Bank Digital Currency: Policy and Technical Considerations. *Institute of Labor Economics*, *IZA DA No. 13535*, , https://doi.org/10.3386/w27634 Retrieved from www.iza.org

Alsalmi, N., Ullah, S., Rafique, M. (2023, 1). Accounting for digital currencies. *Research in International Business and Finance*, *64*, , https://doi.org/10.1016/j.ribaf.2023.101897

Androulaki, E., Camenisch, J., Caro, A.D., Dubovitskaya, M., Elkhiyaoui, K., Tackmann, B. (2020, 10). Privacy-preserving auditable token payments in a permissioned blockchain system. *In Proceedings of the 2nd ACM Conference on Advances in Financial Technologies*, 255-267, https://doi.org/10.1145/3419614.3423259

Ballaschk, D., & Paulick, J. (2021). The public, the private and the secret: Thoughts on privacy in central bank digital currencies. *Journal of Payments Strategy & Systems*, *15*, ,

Bank of Canada (2023). *Digital Canadian Dollar Public Consultation: Report.* https://www.bankofcanada.ca/wp-content/uploads/2023/11/Forum-Research-Digital-Canadian-Dollar-Consultation-Report.pdf.

Ben-Sasson, E., Bentov, I., Horesh, Y., Riabzev, M. (2018). *Scalable, transparent, and post-quantum secure computational integrity.*

Ben-Sasson, E., Chiesa, A., Tromer, E., Virza, M. (2003). Succinct Non-Interactive Zero Knowledge for a von Neumann Architecture. *In Proceedings of the seventeenth Large Installation Systems Administration Conference (LISA XVII)*, , Retrieved from https://www.usenix.org/conference/usenixsecurity14/technical-sessions/presentation/ben-sasson

Berentsen, A., Lenzi, J., Nyffenegger, R. (2023). An Introduction to Zero-Knowledge Proofs in Blockchains and Economics. *Federal Reserve Bank of St. Louis Review*, *105*(4), 280-294, https://doi.org/10.20955/r.105.280-94

Bhaskar, R., Hunjra, A.I., Bansal, S., Pandey, D.K. (2022, 12). Central Bank Digital Currencies: Agendas for future research. *Research in International Business and Finance*, *62*, , https://doi.org/10.1016/j.ribaf.2022.101737

Boneh, D., Boyen, X., Shacham, H. (2004). Short Group Signatures. *Cryptology eprint archive*, , (http://eprint.iacr.org/2004/174/.)

Buterin, V., Illum, J., Nadler, M., Schär, F., Soleimani, A. (2023). Blockchain Privacy and Regulatory Compliance: Towards a Practical Equilibrium. *SSRN*, , (https://

ssrn.com/abstract=4563364)

Chand, M., Ahmad, V., Kathuria, S., Negi, P., Singh, T., Chhabra, G. (2023). Digital Currency Security with the Intervention of Blockchain. *In Proceedings of the 2nd International Conference on Sustainable Computing and Data Communication Systems*, 1356-1362, https://doi.org/10.1109/ICSCDS56580.2023.10105069

Chaum, D. (1983). *Blind Signatures for Untraceable Payments.*

Chaum, D., & van Heyst, E. (1991). Group Signatures. *Advances in cryptology - eurocrypt '91, workshop on the theory and application of of cryptographic techniques, brighton, uk, april 8-11, 1991, proceedings* (Vol. 547, p. 257-265). Springer.

Chu, Y., Lee, J., Kim, S., Kim, H., Yoon, Y., Chung, H. (2022, 5). Review of Offline Payment Function of CBDC Considering Security Requirements. *Applied Sciences*, *12*, , https://doi.org/10.3390/app12094488

Dashkevich, N., Counsell, S., Destefanis, G. (2020). Blockchain Application for Central Banks: A Systematic Mapping Study. *IEEE Access*, *8*, 139918-139952, https://doi.org/10.1109/ACCESS.2020.3012295

Decentralized Identity Foundation (2023). *The BBS Signature Scheme.* https://identity.foundation/bbs-signature/draft-irtf-cfrg-bbs-signatures.html.

Dupuis, D., Gleason, K., Wang, Z. (2022, 1). Money laundering in a CBDC world: a game of cats and mice. *Journal of Financial Crime*, *29*, 171-184, https://doi.org/10.1108/JFC-02-2021-0035

Elgamal, T. (1985). A Public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms. *IEEE Transactions on Information Theory*, *31*, 469-472, https://doi.org/10.1109/TIT.1985.1057074

Gentry, C. (2009). Fully Homomorphic Encryption Using Ideal Lattices. *In Proceedings of the Annual ACM Symposium on Theory of Computing*, 169-178, https://doi.org/10.1145/1536414.1536440

Goldwasser, S., Micali, S., Rackoff, C. (1989). The Knowledge Complexity of Interactive Proof Systems. *SIAM Journal on Computing*, *18*, 186-208, https://doi.org/10.1137/0218012 (STOC'85)

Gross, J., Sedlmeir, J., Babel, M., Bechtel, A., Schellinger, B. (2022). Designing a Central Bank Digital Currency with Support for Cash-like Privacy. *SSRN*, , (https://ssrn.com/abstract=3891121)

Groth, J. (2010). Short Pairing-Based Non-interactive Zero-Knowledge Arguments. *Advances in Cryptology - ASIACRYPT 2010*, *LNCS 6477*, 321-340, https://doi.org/10.1007/978-3-642-17373-8_19

Gupta, S., Pandey, D.K., Ammari, A.E., Sahu, G.P. (2023, 10). Do perceived risks and benefits impact trust and willingness to adopt CBDCs? *Research in International Business and Finance*, *66*, , https://doi.org/10.1016/j.ribaf.2023.101993

Han, J., Kim, J., Youn, A., Lee, J., Chun, Y., Woo, J., Hong, J.W.-K. (2021). Cos-CBDC: Design and Implementation of CBDC on Cosmos Blockchain. *In Proceedings of the 22nd Asia-Pacific Network Operations and Management Symposium*, 303-308, https://doi.org/10.23919/APNOMS52696.2021.9562672

Han, X., Yuan, Y., Wang, F.-Y. (2019). A Blockchain-based Framework for Central Bank Digital Currency. *IEEE International Conference on Service Operations and Logistics, and Informatics (SOLI)*, 263-268, https://doi.org/10.1109/SOLI48380.2019.8955032

Hoang, Y.H., Ngo, V.M., Vu, N.B. (2023, 1). Central bank digital currency: A systematic literature review using text mining approach. *Research in International Business and Finance*, *64*, , https://doi.org/10.1016/j.ribaf.2023.101889

Hsieh, S.F., & Brennan, G. (2022, 9). Issues, risks, and challenges for auditing crypto asset transactions. *International Journal of Accounting Information Systems*, *46*, , https://doi.org/10.1016/j.accinf.2022.100569

Human Rights Foundation (2023). *CBDC Tracker.* https://cbdctracker.hrf.org/.

Islam, M.M., & In, H.P. (2023, 7). A Privacy-Preserving Transparent Central Bank Digital Currency System Based on Consortium Blockchain and Unspent Transaction Outputs. *IEEE Transactions on Services Computing*, *16*, 2372-2386, https://doi.org/10.1109/TSC.2022.3226120

Jabbar, A., Geebren, A., Hussain, Z., Dani, S., Ul-Durar, S. (2023, 1). Investigating individual privacy within CBDC: A privacy calculus perspective. *Research in*

International Business and Finance, *64*, , https://doi.org/10.1016/j.ribaf.2022.101826

Jin, S.Y., & Xia, Y. (2022). CEV Framework: A Central Bank Digital Currency Evaluation and Verification Framework With a Focus on Consensus Algorithms and Operating Architectures. *IEEE Access*, *10*, 63698-63714, https://doi.org/10.1109/ACCESS.2022.3183092

Kesavaraj, S.V., Jakhiya, C.M., Bhandari, C.N. (2022). A Study on Upcoming Central Bank Digital Currency: Opportunities, Obstacles, and Potential FinTech Solutions using Cryptography in the Indian Scenario. *In Proceedings of the 13th International Conference on Computing Communication and Networking Technologies*, , https://doi.org/10.1109/ICCCNT54827.2022.9984539

Kiayias, A., Kohlweiss, M., Sarencheh, A. (2022, 11). PEReDi: Privacy-Enhanced, Regulated and Distributed Central Bank Digital Currencies. *In Proceedings of the ACM Conference on Computer and Communications Security*, 1739-1752, https://doi.org/10.1145/3548606.3560707

Kshetri, N., & Loukoianova, E. (2022, 3). Data Privacy Considerations for Central Bank Digital Currencies in Asia-Pacific Countries. *Computer*, *55*, 95-100, https://doi.org/10.1109/MC.2022.3141228

Lee, Y., Son, B., Jang, H., Byun, J., Yoon, T., Lee, J. (2021, 11). Atomic cross-chain settlement model for central banks digital currency. *Information Sciences*, *580*, 838-856, https://doi.org/10.1016/j.ins.2021.09.040

Lee, Y., Son, B., Park, S., Lee, J., Jang, H. (2021, 8). A survey on security and privacy in blockchain-based central bank digital currencies. *Journal of Internet Services and Information Security*, *11*, 16-29, https://doi.org/10.22667/JISIS.2021.08.31.016

Liu, Y., Ni, J., Zulkernine, M. (2022). AT-CBDC: Achieving Anonymity and Traceability in Central Bank Digital Currency. *IEEE International Conference on Communications*, *2022-May*, 4402-4407, https://doi.org/10.1109/ICC45855.2022.9839154

Ma, C., Jin, Z., Mei, Z., Zhou, F., She, X., Huang, J., Liu, D. (2022). Internet of Things Background: An Empirical Study on the Payment Intention of Central

Bank Digital Currency Design. *Mobile Information Systems*, *2022*, , https://doi.org/10.1155/2022/4846372

Maruo, Y., Yuji, Y.M., Sugino, S., Sei, S.S. (2023). Balancing privacy and data use: The potential impact of large online platforms and central bank digital currencies. *Journal of Payments Strategy & Systems*, *17*, 142-150,

Mazzoni, M., Corradi, A., Nicola, V.D. (2022, 3). Performance evaluation of permissioned blockchains for financial applications: The ConsenSys Quorum case study. *Blockchain: Research and Applications*, *3*, , https://doi.org/10.1016/j.bcra.2021.100026

Morales-Resendiz, R., Ponce, J., Picardo, P., Velasco, A., Chen, B., Sanz, L., ... Hodge, A. (2021, 3). Implementing a retail CBDC: Lessons learned and key insights. *Latin American Journal of Central Banking*, *2*, , https://doi.org/10.1016/j.latcb.2021.100022

Ngo, V.M., Nguyen, P.V., Nguyen, H.H., Tram, H.X.T., Hoang, L.C. (2023, 1). Governance and monetary policy impacts on public acceptance of CBDC adoption. *Research in International Business and Finance*, *64*, , https://doi.org/10.1016/j.ribaf.2022.101865

Opare, E.A., & Kim, K. (2020). A Compendium of Practices for Central Bank Digital Currencies for Multinational Financial Infrastructures. *IEEE Access*, *8*, 110810-110847, https://doi.org/10.1109/ACCESS.2020.3001970

Pedersen, T.P. (1991). Non-Interactive and Information-Theoretic Secure Verifiable Secret Sharing. *Advances in Cryptology - CRYPT0 '91*, *LNCS 576*, 129-140, https://doi.org/10.1007/3-540-46766-1_9

Peffers, K., Tuunanen, T., Rothenberger, M.A., Chatterjee, S. (2007). A Design Science Research Methodology for Information Systems Research. *Journal of Management Information Systems*, *24*, 45-77, https://doi.org/10.2753/MIS0742-1222240302 Retrieved from https://www.jstor.org/stable/pdf/40398896.pdf

Pocher, N., & Veneris, A. (2021, 5). Privacy and transparency in CBDCs: A regulation-by-design AML/CFT scheme. *IEEE International Conference on Blockchain and Cryptocurrency,*, , https://doi.org/10.1109/ICBC51069.2021.9461090

Portu, T.D. (2022, 12). New trends in retail payments: How technological changes are reshaping the payments system. Introducing a proposal for a new pan-European instant payment system. *Latin American Journal of Central Banking*, *3*, , https://doi.org/10.1016/j.latcb.2022.100075

Quamara, S., & Singh, A.K. (2022, 2). A systematic survey on security concerns in cryptocurrencies: State-of-the-art and perspectives. *Computers and Security*, *113*, , https://doi.org/10.1016/j.cose.2021.102548

Ree, J. (2023). *Nigeria's eNaira, One Year After.* International Monetary Fund. (IMF Working Paper WP/23/104. https://www.imf.org/-/media/Files/Publications/WP/2023/English/wpiea2023104-print-pdf.ashx)

Rennie, E., & Steele, S. (2021). Privacy and Emergency Payments in a Pandemic: How to Think about Privacy and a Central Bank Digital Currency. *LAW, TECHNOLOGY AND HUMANS*, *3*, , https://doi.org/10.5204/thj.1745

Rivest, R.L., Shamir, A., Adleman, L. (1978). Programming Techniques A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. *Communications of the ACM*, *21*, 120-126, https://doi.org/10.1145/359340.359342

Rivest, R.L., Shamir, A., Tauman, Y. (2001). How to Leak a Secret. *ASIACRYPT 2001. Lecture Notes in Computer Science*, *LNCS 2248*, 552-565, https://doi.org/10.1007/3-540-45682-1_32

Sanka, A.I., Irfan, M., Huang, I., Cheung, R.C. (2021, 3). A survey of breakthrough in blockchain technology: Adoptions, applications, challenges and future research. *Computer Communications*, *169*, 179-201, https://doi.org/10.1016/j.comcom.2020.12.028

Schnorr, C.P. (1991). Efficient Signature Generation by Smart Cards. *Journal of Cryptology*, *4*, 161-174, https://doi.org/10.1007/BF00196725

Scollan, B., & Darling, E. (2023). Designing digital currency wallets for broad adoption. *Journal of Payments Strategy & Systems*, *17*, 96-106,

Sethaput, V., & Innet, S. (2021). Blockchain Application for Central Bank Digital Currencies (CBDC). *In Proceedings of the 3rd International Conference on Blockchain Computing and Applications*, 3-10, https://doi.org/10.1109/

BCCA53669.2021.9657012

South Aftrican Reserve Bank (2018). *PROJECT KHOKHA: Exploring the use of distributed ledger technology for interbank payments settlement in South Africa.* https://www.resbank.co.za/content/dam/sarb/publications/media-releases/2022/project-khokha-2/Project%20Khokha%202%20Full%20Report%206%20April%202022.pdf.

Takaragi, K., Kubota, T., Wohlgemuth, S., Umezawa, K., Koyanagi, H. (2023, 3). Secure Revocation Features in eKYC - Privacy Protection in Central Bank Digital Currency. *IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences*, *106 EA*, 325-332, https://doi.org/10.1587/transfun.2022CIP0008

Tian, H., Chen, X., Ding, Y., Zhu, X., Zhang, F. (2019). AFCoin: A framework for digital fiat currency of central banks based on account model. *Information Security and Cryptology. Inscrypt 2018*, *LNCS 11449*, 70-85, https://doi.org/10.1007/978-3-030-14234-6_4

Tronnier, F. (2021). Privacy in Payment in the Age of Central Bank Digital Currency. *IFIP Advances in Information and Communication Technology*, *619 IFIP*, 96-114, https://doi.org/10.1007/978-3-030-72465-8_6

Tronnier, F., Harborth, D., Hamm, P. (2022, 5). Investigating privacy concerns and trust in the digital Euro in Germany. *Electronic Commerce Research and Applications*, *53*, , https://doi.org/10.1016/j.elerap.2022.101158

Ungson, G.R., & Soorapanth, S. (2022, 12). The ASEAN blockchain roadmap. *Asia and the Global Economy*, *2*, 100047, https://doi.org/10.1016/j.aglobe.2022.100047

van Oordt, M.R. (2022, 9). Discussion of "Central bank digital currency: Stability and information". *Journal of Economic Dynamics and Control*, *142*, , https://doi.org/10.1016/j.jedc.2022.104503

Veneris, A., Park, A., Long, F., Puri, P. (2021). Central Bank Digital Loonie: Canadian Cash for a New Global Economy Final Report for the Bank of Canada's Model X Challenge. *SSRN*, , (https://ssrn.com/abstract=3770024)

Wang, H. (2023, 9). How to understand China's approach to central bank digital currency? *Computer Law and Security Review*, *50*, , https://doi.org/10.1016/j.clsr.2022.105788

Wang, Q., Qin, B., Hu, J., Xiao, F. (2020, 6). Preserving transaction privacy in Bitcoin. *Future Generation Computer Systems*, *107*, 793-804, https://doi.org/10.1016/j.future.2017.08.026

Wang, Y.R., Ma, C.Q., Ren, Y.S. (2022, 12). A model for CBDC audits based on blockchain technology: Learning from the DCEP. *Research in International Business and Finance*, *63*, , https://doi.org/10.1016/j.ribaf.2022.101781

Wang, Z. (2023). Money laundering and the privacy design of central bank digital currency. *Review of Economic Dynamics*, , https://doi.org/10.1016/j.red.2023.06.004

Wilkins, C.A. (2022, 1). Discussion of "designing central bank digital currency" by Agur, Ari and Dell'Ariccia. *Journal of Monetary Economics*, *125*, 80-84, https://doi.org/10.1016/j.jmoneco.2021.09.009

Wüst, K., Kostiainen, K., Delius, N., Capkun, S. (2022, 11). Platypus: A Central Bank Digital Currency with Unlinkable Transactions and Privacy-Preserving Regulation. *In Proceedings of the ACM Conference on Computer and Communications Security*, 2947-2960, https://doi.org/10.1145/3548606.3560617

Xu, C., & Jin, B. (2022, 6). Digital currency in China: pilot implementations, legal challenges and prospects. *Juridical Tribune*, *12*, 177-194, https://doi.org/10.24818/TBJ/2022/12/2.02

Yang, J., & Li, Z. (2020). Impact of Bitcoin's Distributed Structure on the Construction of the Central Bank's Digital Currency System. *In Proceedings of the Fourth International Conference on Inventive Systems and Control (ICISC)*, , https://doi.org/10.1109/ICISC47916.2020.9171195

Yao, A.C. (1982). Protocols for Secure Computations. *In Proceedings of the 23rd Annual Symposium on Foundations of Computer Science*, 160-164, https://doi.org/10.1109/SFCS.1982.88

yong Liu, C., & Hou, C.C. (2020). A research on blockchain-based central bank digital currency. *Lecture Notes of the Institute for Computer Sciences, Social-Informatics and Telecommunications Engineering*, *LNICST 317*, 131-139, https://doi.org/10.1007/978-3-030-52988-8_11

Zhang, J., Tian, R., Cao, Y., Yuan, X., Yu, Z., Yan, X., Zhang, X. (2021). A Hybrid Model for Central Bank Digital Currency Based on Blockchain. *IEEE Access*, *9*, 53589-53601, https://doi.org/10.1109/ACCESS.2021.3071033

Zhang, T., & Huang, Z. (2022, 6). Blockchain and central bank digital currency. *ICT Express*, *8*, 264-270, https://doi.org/10.1016/j.icte.2021.09.014

Zhang, X. (2020, 12). Opportunities, challenges and promotion countermeasures of central bank digital currency. *In Proceedings of the 2020 Management Science Informatization and Economic Innovation Development Conference*, 343-346, https://doi.org/10.1109/MSIEID52046.2020.00072

Zhong, P., Wang, B., Wang, A., Zhang, Y., Liu, S., Zhong, Q., Tu, X. (2021). IAP: Instant Auditing Protocol for Anonymous Payments. *In Proceedings of the International Conference on Parallel and Distributed Systems - ICPADS*, *2021-December*, 548-555, https://doi.org/10.1109/ICPADS53394.2021.00074