A Review of Privacy-Preserving Blockchain Architectures for Central Bank Digital Currency Systems

Shubhangi Santosh Kekate[1], Dr. Syed Sumera Ali[2], A. T. Jadhav[3], Dr. D. L. Bhuyar[4], Dr. G. B. Dongre[5]
[1]*MTech Student at Dept. of Electronics & Communication (Advanced Communication Technology), CSMSS Chh. Shahu College of Engineering, Chhatrapati Sambhajinagar (Aurangabad), MH, India*
[2]*Associate Professor & Head, Dept. of Electronics & Communication (Advanced Communication Technology), CSMSS Chh. Shahu College of Engineering, Chhatrapati Sambhajinagar (Aurangabad), MH, India*
[3]*Assistant Professor, Dept. of Electronics & Communication (Advanced Communication Technology), CSMSS Chh. Shahu College of Engineering, Chhatrapati Sambhajinagar (Aurangabad), MH, India*
[4]*Professor & Head, Dept. of Electronics & Computer Engineering, CSMSS Chh. Shahu College of Engineering, Chhatrapati Sambhajinagar (Aurangabad), MH, India*
[5]*Principal of CSMSS Chh. Shahu College of Engineering, Chhatrapati Sambhajinagar (Aurangabad), MH, India*

***Abstract*—The rapid growth of digital financial systems and the emergence of Central Bank Digital Currencies (CBDCs) have introduced critical challenges related to user privacy, transaction security, and regulatory compliance. While blockchain technology offers transparency and decentralization, it often conflicts with the privacy requirements of financial systems. This paper presents a comprehensive review of privacy-preserving blockchain architectures applicable to CBDC systems, focusing on techniques such as zero-knowledge proofs, secure multi-party computation, and advanced consensus mechanisms.**

***The study analyzes existing research works to evaluate their effectiveness in balancing privacy, scalability, and performance within centralized monetary frameworks. Key findings highlight that although several architectures improve transactional privacy, they often introduce trade-offs in terms of computational complexity, latency, and system scalability. Furthermore, current solutions lack standardization and struggle to meet regulatory requirements such as auditability and traceability.**

***This review identifies significant research gaps, including the need for efficient consensus protocols, interoperability among CBDC platforms, and practical deployment frameworks. To address these challenges, the paper proposes a conceptual approach based on a Proof-by-Approval consensus mechanism, extending Proof-of-Reputation to enhance decentralization and security while acknowledging its limitations in performance and implementation complexity.**

Finally, the paper outlines future research directions toward developing scalable, energy-efficient, and regulation-compliant privacy-preserving blockchain systems for next-generation digital currencies.

***Index Terms*—Privacy-Preserving, Decentralized Platform, Banking Transactions, Blockchain Technology, Unspent Transaction Outputs (UTXOs), Data Security, Cryptographic Techniques, Financial Institutions, Transaction Transparency, Digital Banking Solutions, etc.**

I. INTRODUCTION

The objective of this paper is to review existing blockchain mechanisms, consensus protocols, and privacy-preserving approaches applicable to *Central Bank Digital Currency* systems. Digital banking has significantly transformed the global financial ecosystem, however a general perspective as well. In Private Blockchain network the participants are known and trusted and there is a level of confidentiality. For example, in a conglomerate, many of the mechanisms aren't needed or they are replaced with legal binding contracts making everyone whoever has signed the contract to abide to these rules. It rapidly changes the technical decisions used to build the solution. Blockchain unlike traditional systems is dynamic enough to become a leader in implementation

in a mercurial market scenario. In a blockchain the supreme advantage it ensures is that each party has a record which is maintained in a ledger available to each one. It is a ledger widely passed between different users thereby creating a shared database which is replicated to these users and who can access it only after they have the access right for it. Consensus, provenance, immutability, finality are the various aspects into which it works, making sure that all these facets work together into a reasonable amalgamation.

II. NEED OF BLOCKCHAIN FOR BANKING SECURITY

The major question that arises is to why use blockchain when already the market has flourishing plethora of other databases. What substantial importance it holds against the competing products. For this let's understand the problem with the existing systems.

They could be summed up as follows:

- Difficult to monitor and evaluate asset ownership and its transfer in a trusted business network.
- Inefficient, expensive, vulnerable: All these factors extremely hinder the performance and there by destroying the progress.

The following issues are commonly observed in banking data security systems and transaction approach which defined here

- To migrate the centralization of banking transaction into the decentralized approach.
- To create a single platform where user can access all bank accounts using transactional authentication.
- To eliminate all physical things dependency which is must require for banking transaction.
- To implement such approach on global environment using secure and time-efficient manner.
- We notice that the decentralized architecture provides the automatic data recovery from different attacks.

III. LITERATURE REVIEW

- Zhang et al. (2023)

Presents a secure and efficient framework for implementing Central Bank Digital Currency (CBDC) using consortium blockchain technology. The authors focus on maintaining a balance between transparency and user privacy by adopting the Unspent Transaction Output (UTXO) model, which enhances transaction traceability while protecting sensitive user information. The system ensures that transactions are verifiable and tamper-proof without revealing personal identities, thus improving trust and security in digital currency systems. Additionally, the use of consortium blockchain allows controlled access to authorized participants such as banks and regulatory bodies, making the system more scalable and practical for real-world financial applications.

- Cohen et al. (2024)

Focused on cryptanalysis of optical layer security using advanced techniques such as phase masking and coherent detection. Although not directly blockchain-based, the study provides strong insights into secure communication systems, which are relevant for financial infrastructures. The research highlights vulnerabilities in physical-layer security and proposes improvements, contributing indirectly to strengthening secure data transmission in blockchain-based banking systems.

- Kumar et al. (2024)

Presented a comprehensive review of smart contract security with a focus on decentralized finance (DeFi). The study identifies key vulnerabilities such as reentrancy attacks, overflow issues, and improper validations. It also discusses mitigation strategies and formal verification methods. This work is highly relevant to CBDC systems, as secure smart contracts are essential for implementing automated and trustless financial transactions.

- Nujumudeen et al. (2026)

Introduced a hybrid chaos-based cryptographic framework designed for lightweight IoT security. The proposed method enhances encryption efficiency while reducing computational complexity, making it suitable for low-power devices. Although focused on IoT, the approach offers valuable insights into lightweight privacy-preserving techniques that can be adapted for scalable blockchain architectures in CBDC systems.

- G et al. (2024)

Proposed a novel blockchain-enabled methodology for secure banking transactions using cybersecurity principles. The study integrates blockchain with authentication and encryption techniques to improve transaction security and data integrity. The findings demonstrate enhanced protection against fraud and cyberattacks, though challenges related to implementation complexity and system performance remain.

- Muthu & Kartheeban (2024)

Presented a comprehensive survey of blockchain technology as "Trust as a Service." The paper discusses how blockchain can replace traditional trust mechanisms in financial systems through decentralization and immutability. It evaluates different consensus mechanisms and highlights limitations such as scalability and energy consumption, which are critical concerns for CBDC adoption.

- Paul & Kulkarni (2024)

Explored the integration of blockchain technology with machine learning for secure online banking systems. The study demonstrates how machine learning models can detect fraudulent activities while blockchain ensures secure data storage. This hybrid approach improves system intelligence and security, making it highly relevant for advanced CBDC frameworks.

- Shen et al. (2019)

Proposed a blockchain-based approach for privacy-preserving image retrieval in medical IoT systems. The framework ensures secure data sharing while maintaining user privacy through encryption and decentralized storage. Although applied in healthcare, the techniques are applicable to financial systems where sensitive transaction data must be protected.

- Shinde et al. (2023)

Provided a comprehensive survey on the integration of blockchain with artificial intelligence, machine learning, and IoT. The study highlights how these technologies can enhance automation, security, and decision-making in various domains. It identifies challenges such as interoperability and data privacy, which are also key concerns in CBDC systems.

- Pothavarjula & Sirisha (2022)

Investigated decentralized ledger applications using Ethereum in blockchain networks. The study explains how Ethereum enables smart contract execution and decentralized applications for secure transactions. While the platform offers flexibility and transparency, issues such as gas fees, scalability, and performance limitations are identified, which impact its suitability for large-scale CBDC deployment.

From the above studies, it is clear that combining blockchain technology with advanced authentication methods can improve fraud detection systems. Therefore, this review focuses on developing a secure and reliable banking system using blockchain along with a dual keypad and two-step verification process to enhance user authentication and prevent fraud in multi-participant transactions.

Table-1: Comparison table

Author	Year	Technique	Advantage	Limitation
Zhang et al.	2023	Privacy-Preserving Blockchain Framework	Enhanced transaction security and privacy	High computational overhead
Cohen et al.	2024	Optical Layer Security (Cryptanalysis)	Strong secure communication insights	Not directly applicable to blockchain
Kumar et al.	2024	Smart Contract Security Review	Identifies major DeFi vulnerabilities	Lacks implementation framework
Nujumudeen et al.	2026	Chaos-based Cryptography	Lightweight and efficient encryption	Limited applicability to banking systems
G et al.	2024	Blockchain-based Secure Banking	Improved fraud prevention and data integrity	Complex implementation

Muthu & Kartheeban	2024	Blockchain Trust-as-a-Service	Decentralization and trust enhancement	Scalability and energy issues
Paul & Kulkarni	2024	Blockchain + Machine Learning	Intelligent fraud detection	High system complexity
Shen et al.	2019	Blockchain for Privacy in IoT	Strong data privacy and secure sharing	Limited to specific domain (healthcare)
Shinde et al.	2023	Blockchain + AI + IoT Survey	Comprehensive integration study	Interoperability challenges
Pothavarjula & Sirisha	2022	Ethereum-based Blockchain	Supports smart contracts and DApps	Gas fees and scalability issues

IV. PROBLEM DEFINITION

The review aims to address the growing concerns surrounding the security and privacy of banking transactions in an increasingly digital landscape. Traditional banking systems often struggle with vulnerabilities, including data breaches and unauthorized access to sensitive information.

This review proposes a privacy-preserving, transparent decentralized platform that leverages a custom blockchain and utilizes Unspent Transaction Outputs (UTXOs) to enhance the security of banking transactions. By combining these technologies, the platform seeks to provide users with greater control over their financial data while ensuring transparency and trust in transaction processes, ultimately aiming to mitigate risks associated with conventional banking methods.

V. PROPOSED REVIEW FRAMEWORK

The proposed review framework is a conceptual model synthesized from existing blockchain-based banking and CBDC research and is intended to identify future research directions rather than represent an implemented system. The proposed system introduces a multi-perspective fraud detection mechanism using a custom blockchain framework for multi-participant banking transactions. It focuses on creating a secure, transparent, and tamper-proof ledger where all transactions are recorded in blocks linked cryptographically to maintain integrity. Each transaction initiated by a user undergoes validation by multiple network participants (banks, nodes, or authorized entities), ensuring that fraudulent or unauthorized actions are identified before final approval. The blockchain structure allows for distributed verification, making it impossible for any single party to alter or manipulate transaction data without consensus from others. This ensures accountability and auditability across all participants in the banking system.

The blockchain architecture consists of a few fundamental concepts like decentralization, digital signature, mining and data integrity.

- Decentralization:

Rather than one central authority overpowering others in the ecosystem, blockchain explicitly distributes control amongst all peers in the transaction chain.

- Digital signature:

Blockchain enables an exchange of transactional value using public keys by the mechanism of a unique digital sign i.e., code for decryption known to everyone on the network and private keys known only to the owner to create ownership.

- Mining:

In a distributed system every user mine and digs deep into the data which is then evaluated according to the cryptographic rules and it also acknowledges miners for confirmation and verification of the transactions.

- Data integrity:

Complex algorithms and agreement among users ensure that transaction data, once agreed upon, cannot be tampered with and thus remains unaffected. Data stored on blockchain acts as a single version of truth for all parties involved hence reducing the risk of fraud.

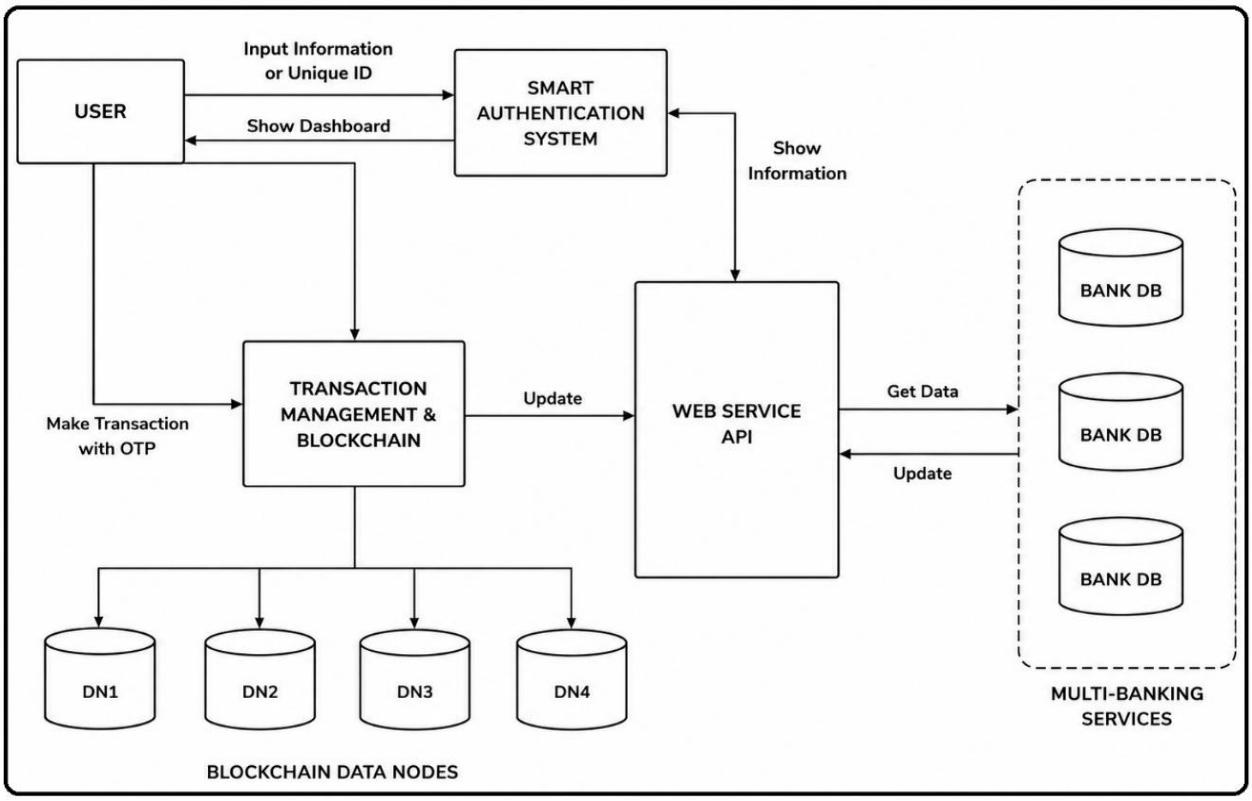

Fig. 1: Proposed System Architecture

The system architecture consists of several key modules — User Module, Bank Module, and Blockchain Security Module. The user module handles login, registration, and transaction initiation using enhanced authentication features such as visual dual keypad and two-step verification. The bank module manages transaction validation, digital signatures, and consensus generation. The blockchain module stores the validated transactions, performs hashing operations, and ensures the immutability of each block. Every transaction is digitally signed, timestamped, and stored permanently in the ledger, providing a clear and traceable audit trail. Fraud detection is achieved by continuously monitoring transaction patterns, identifying unusual behaviors, and raising alerts for suspicious activities.

Moreover, the system integrates with a Java-based web application for user interaction and real-time monitoring. It employs secure communication protocols and cryptographic hashing algorithms (such as SHA-256) to protect sensitive financial data. The incorporation of blockchain with AI-based fraud analysis ensures that every transaction is verified from multiple perspectives — user, bank, and network — before being executed. This layered approach strengthens the overall resilience of the banking network, providing a secure and scalable framework for future financial systems.

VI. COMPARATIVE ANALYSIS OF EXISTING BLOCKCHAIN BANKING SYSTEMS

- *CBDC Models*

Central Bank Digital Currency (CBDC) is a digital form of money issued by the government. It works like physical cash but in electronic form, making transactions faster and more secure. CBDC can be used by the public (retail) or by banks (wholesale). It ensures better control and transparency in financial systems. In this project, CBDC helps create a reliable and government-backed digital payment system.

- *Hyperledger*

Hyperledger is a private blockchain platform designed for business and banking applications. It allows only authorized users to access the system, ensuring high security and privacy. Transactions are faster because it does not require mining like public blockchains. It is

widely used in industries where data protection is important. For this project, it represents a secure and controlled blockchain model.

- *Ethereum*

Ethereum is a public blockchain that supports smart contracts, which automatically execute agreements. It allows developers to build decentralized applications (DApps). Anyone can access and view transactions, making it transparent but less private. It also has transaction fees and scalability issues. Despite this, it is useful for flexible and programmable blockchain systems.

- *Bitcoin UTXO Model*

Bitcoin uses the UTXO (Unspent Transaction Output) model to manage transactions. In this system, each transaction uses previous outputs as inputs, ensuring strong security and traceability. It is highly reliable and transparent. However, it is not suitable for complex banking applications due to limited flexibility. It mainly focuses on simple peer-to-peer transactions.

- *Permissioned Blockchain*

A permissioned blockchain restricts access to only authorized users. It is commonly used in banking and enterprise systems where privacy is required. This type of blockchain offers faster transactions and better control compared to public blockchains. It also allows role-based access and data protection.

- *Consensus Comparison*

Consensus mechanisms are used to validate transactions in a blockchain network. Different methods include Proof of Work (PoW), Proof of Stake (PoS), PBFT, and PoA. PoW is secure but slow, while PoS is more energy-efficient. PBFT and PoA are faster and suitable for private systems. For this project, PBFT or PoA is preferred due to high speed and efficiency.

VII. CBDC ARCHITECTURES

Central Bank Digital Currency (CBDC) is a digital form of money issued and regulated by a country's central bank. Unlike cryptocurrencies, CBDCs are backed by the government and are designed to provide secure, reliable, and efficient digital payment systems. Different CBDC architectures have been proposed by researchers and financial institutions to meet various requirements related to security, privacy, scalability, and regulatory compliance [11]-[14]. The major CBDC architectures include Retail CBDC, Wholesale CBDC, Token-Based CBDC, and Account-Based CBDC.

A. Retail CBDC

Retail CBDC is intended for use by the general public, including individuals, businesses, and merchants. It works as a digital alternative to physical cash and can be used for day-to-day financial transactions such as payments, fund transfers, and online purchases. Retail CBDC can improve financial inclusion by providing easy access to digital payment services, especially in regions with limited banking facilities. It also helps in reducing dependency on physical cash while offering faster and more transparent transactions [12], [13]. However, issues related to privacy protection and large-scale transaction management remain important challenges.

B. Wholesale CBDC

Wholesale CBDC is designed for use by financial institutions such as commercial banks and other authorized organizations. It is mainly used for inter-bank settlements and large-value transactions. This model improves the efficiency of financial operations by reducing settlement time and operational costs. Since only authorized participants can access the system, Wholesale CBDC offers better control and security [11], [12]. It is considered suitable for improving existing banking infrastructure and supporting real-time financial settlements.

C. Token-Based CBDC

In a Token-Based CBDC system, ownership is verified through possession of a digital token. Transactions are validated by checking the authenticity of the token rather than verifying the identity of the user. This approach is similar to the use of physical cash, where ownership is determined by possession [11], [13]. Token-Based CBDCs provide better privacy and can support secure peer-to-peer transactions. However, challenges such as token management, prevention of double spending, and

regulatory monitoring must be addressed to ensure secure implementation.

D. Account-Based CBDC

Account-Based CBDC relies on user identity verification and account ownership for transaction processing. In this model, users maintain accounts with the central bank or authorized financial institutions. Every transaction is linked to a verified account, making it easier to monitor and audit financial activities. Account-Based CBDCs support regulatory requirements such as Know Your Customer (KYC) and Anti-Money Laundering (AML) policies [13], [14]. Although this model provides better control and transparency, it may raise concerns regarding user privacy and data protection.

VIII. CONCLUSION

This review presents a secure and efficient blockchain-based approach for modern banking systems, with a strong focus on Central Bank Digital Currency (CBDC). By integrating blockchain technology into banking transactions, the system ensures a decentralized structure where no single authority has complete control, thus improving trust and reliability. The use of cryptographic techniques and secure algorithms enhances data privacy, ensuring that sensitive financial information remains protected from unauthorized access.

The proposed system improves transparency in financial transactions, as all records are stored in an immutable and traceable manner on the blockchain. This transparency helps in reducing fraud, increasing accountability, and building confidence among users and financial institutions. Additionally, the incorporation of privacy-preserving mechanisms ensures that while transactions are transparent, user identities and sensitive details are well protected.

Furthermore, the adoption of a permissioned blockchain model makes the system more efficient and suitable for real-world banking applications, offering faster transaction processing and controlled access. The integration of CBDC within this framework provides a digital alternative to traditional currency, supporting secure, fast, and low-cost transactions.

ACKNOWLEDGMENT

The authors would like to thank the reviewers, faculty members, and institutional authorities for their valuable guidance and support during the preparation of this manuscript.

REFERENCES

[1] M. M. Islam and H. P. IN, “A privacy-preserving transparent central bank digital currency system based on consortium blockchain and unspent transaction outputs,” *IEEE Transactions on Services Computing*, vol. 16, no. 4, pp. 2372–2386, Jul.–Aug. 2023, doi: 10.1109/TSC.2022.3226120.

[2] R. Cohen et al., “Cryptanalysis of practical optical layer security based on phase masking of mode-locked lasers and multi-homodyne coherent detection,” Journal of Lightwave Technology, vol. 42, no. 19, pp. 6712–6730, Oct. 2024, doi: 10.1109/JLT.2024.3410646.

[3] A. Kumar, N. Sharma, S. Malhotra, S. Devliyal, and B. V. Kumar, “Smart contract security: A review with a focus on decentralized finance,” in Proc. 3rd Int. Conf. Innovation in Technology (INOCON), Bangalore, India, 2024, pp. 1–5, doi: 10.1109/INOCON60754.2024.10511387.

[4] F. Nujumudeen, M. N. Mubarak, Y. K. Sharma, et al., “A hybrid chaos-based cryptographic framework for lightweight IoT security: Enhancing efficiency and security in low-power devices,” Peer-to-Peer Networking and Applications, vol. 19, p. 53, 2026, doi: 10.1007/s12083-025-02188-1.

[5] G. D, M. R. Kantha, D. S. Mani, R. K. J, Y. Nandurkar, and A. A. A. Samhan, “A novel blockchain enabled methodology to perform secure banking transactions using cybersecurity principles,” in Proc. Int. Conf. Innovative Computing, Intelligent Communication and Smart Electrical Systems (ICSES), Chennai, India, 2024, pp. 1–6, doi: 10.1109/ICSES63760.2024.10910706.

[6] S. E. Muthu and K. Kartheeban, “A comprehensive survey of blockchain technology—Trust as a service,” in Proc. 3rd Int. Conf. Sentiment Analysis and Deep Learning

(ICSADL), Bhimdatta, Nepal, 2024, pp. 544–552, doi: 10.1109/ICSADL61749.2024.00095.

[7] V. Paul and P. Kulkarni, "Integration of blockchain technology and machine learning in online secure banking system," in Proc. 8th Int. Conf. Computational System and Information Technology for Sustainable Solutions (CSITSS), Bengaluru, India, 2024, pp. 1–4, doi: 10.1109/CSITSS64042.2024.10816977.

[8] M. Shen, Y. Deng, L. Zhu, X. Du, and N. Guizani, "Privacy-preserving image retrieval for medical IoT systems: A blockchain-based approach," IEEE Network, vol. 33, no. 5, pp. 27–33, Sept.–Oct. 2019, doi: 10.1109/MNET.001.1800503.

[9] N. K. Shinde, A. Seth, and P. Kadam, "Exploring the synergies: A comprehensive survey of blockchain integration with artificial intelligence, machine learning, and IoT for diverse applications," in Machine Learning and Optimization for Engineering Design, A. S. Shastri, K. Shaw, and M. Singh, Eds. Singapore: Springer, 2023, doi: 10.1007/978-981-99-7456-6_7.

[10] P. P. Pothavarjula and B. Sirisha, "An investigation of decentralized ledger applications using Ethereum in a blockchain network," in Proc. 9th Int. Conf. Computing for Sustainable Global Development (INDIACom), New Delhi, India, 2022, pp. 524–529, doi: 10.23919/INDIACom54597.2022.9763219.

[11] M. L. Bech and R. Garratt, "Central bank cryptocurrencies," BIS Quarterly Review, Bank for International Settlements, Basel, Switzerland, pp. 55–70, Sep. 2017.

[12] R. Auer, G. Cornelli, and J. Frost, "Rise of the central bank digital currencies: Drivers, approaches and technologies," BIS Working Papers, no. 880, Bank for International Settlements, Basel, Switzerland, Aug. 2020.

[13] J. Kiff, J. Alwazir, S. Davidovic, S. Farias, A. Khan, T. Khiaonarong, M. N. Moreno-Sanchez, H. Tourpe, and P. Zhou, "A survey of research on retail central bank digital currency," IMF Working Paper WP/20/104, International Monetary Fund, Washington, DC, USA, Jun. 2020.

[14] European Central Bank, "Report on a digital euro," European Central Bank, Frankfurt am Main, Germany, Oct. 2020.