# 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*—Critical issues with user privacy, transaction security, and regulatory compliance have emerged due to the rapid growth of digital financial systems and the introduction of Central Bank Digital Currencies (CBDCs). Although blockchain technology supports decentralization and transparency, it often conflicts with the strict privacy requirements of financial systems. This study presents a detailed analysis of privacy-preserving blockchain architectures for CBDC systems, focusing on techniques such as zero-knowledge proofs, secure multi-party computation, and advanced consensus mechanisms. In addition to theoretical analysis, this work also includes the design and implementation of a** *Java-based custom blockchain system***, where experimental evaluation is performed on transaction processing and security parameters. The results demonstrate improvements in privacy protection, reduced latency, and better throughput using a permissioned blockchain approach. The study evaluates existing approaches in terms of performance, scalability, and privacy, highlighting that while many architectures enhance transaction privacy, they often introduce trade-offs such as increased computational complexity and reduced scalability. Furthermore, the lack of standardization and challenges in meeting regulatory requirements like auditability and traceability remain significant concerns. To address these limitations, this research proposes a CBDC based on a** *Proof-by-Approval consensus mechanism***, extending Proof-of-Reputation to improve trust, security, and decentralization. A prototype privacy-preserving blockchain architecture was implemented using Java and evaluated on simulated CBDC transactions. The proposed approach achieved an accuracy of 97.2% while improving transaction privacy and reducing processing delay compared to existing approaches.***

***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 aim of this paper is to analyze current blockchain processes, consensus protocols, and privacy-preserving strategies relevant to Central Bank Digital Currency (CBDC) systems. The rapid growth of digital banking has significantly transformed the global financial ecosystem, creating new opportunities as well as challenges related to security, transparency, and privacy. CBDCs, being government-backed digital currencies, require a secure and efficient infrastructure that ensures both regulatory compliance and user confidentiality.

Blockchain technology plays a key role in enabling decentralized and transparent systems. In a private or permissioned blockchain network, participants are known, trusted, and granted controlled access, which improves security and governance. Unlike traditional

centralized systems, blockchain maintains a distributed ledger where all authorized participants can view and verify transactions. This ensures important properties such as consensus, immutability, provenance, and finality, making it a reliable solution for financial applications. However, achieving privacy in such transparent systems remains a major challenge, especially in CBDC environments where sensitive financial data must be protected.

This paper focuses on designing a privacy-preserving blockchain architecture tailored for CBDC systems. It explores how advanced cryptographic techniques and optimized consensus mechanisms can help balance transparency with confidentiality. In addition, a custom blockchain prototype is developed using Java to demonstrate the practical implementation of the proposed approach. The system is evaluated using simulated transaction data to measure performance, security, and efficiency.

*Major Contributions:*

- Proposed a privacy-preserving blockchain architecture for CBDC systems.
- Developed a secure transaction validation mechanism to ensure data integrity and authenticity.
- Implemented a working prototype using Java with custom blockchain design.
- Evaluated system performance using simulated CBDC transaction data for accuracy, latency, and throughput.

## II. NEED OF BLOCKCHAIN FOR BANKING SECURITY

The major question that arises is why blockchain should be used 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 thereby reducing 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 dependency on physical processes 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. BACKGROUND

The rapid evolution of digital payment systems and financial technologies has led to the emergence of Central Bank Digital Currencies (CBDCs), which are digital forms of a nation’s fiat currency issued and regulated by central authorities. Unlike decentralized cryptocurrencies such as Bitcoin, CBDCs aim to combine the efficiency of digital transactions with the trust and stability of government-backed monetary systems. However, one of the major challenges in implementing CBDCs is ensuring user privacy while maintaining transparency, security, and regulatory compliance. Traditional digital payment systems often rely on centralized databases, making them vulnerable to data breaches, surveillance risks, and single points of failure. This has created a need for innovative architectures that can protect user data without compromising system integrity.

Blockchain technology has emerged as a promising solution for addressing these challenges due to its decentralized, immutable, and transparent nature. However, conventional blockchain systems, especially public ones, are not inherently privacy-preserving, as transaction details are often visible to all participants. To overcome this limitation, advanced cryptographic techniques such as zero-knowledge proofs, secure multi-party computation, and encryption-based privacy models are being explored. A privacy-preserving blockchain architecture for CBDCs aims to strike a balance between anonymity and traceability, ensuring that user identities and transaction details remain confidential while still

allowing regulatory authorities to monitor and prevent illicit activities such as fraud, money laundering, and tax evasion.

In this context, the proposed system focuses on designing a secure and efficient blockchain-based framework tailored for CBDC implementation with enhanced privacy features. The system integrates permissioned blockchain models, identity management systems, and cryptographic protocols to ensure controlled access and data protection. By leveraging these technologies, the architecture not only improves transaction security and user trust but also supports scalability and compliance with financial regulations. This research contributes to the ongoing efforts of modernizing financial infrastructures by providing a robust solution that addresses both technological and regulatory challenges in the deployment of central bank digital currencies.

## IV. PROBLEM DEFINITION

The proposed system 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.

The proposed system presents 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. RESEARCH GAP

Existing Central Bank Digital Currency (CBDC) systems face several challenges that limit their efficiency, security, and scalability. One major issue is high latency, where transaction processing and validation take more time due to complex consensus mechanisms. Additionally, many systems suffer from privacy leakage, as sensitive transaction data can be exposed or traced, which is not suitable for financial systems requiring confidentiality.

Another important limitation is poor interoperability, meaning different systems and platforms cannot easily communicate or integrate with each other. This creates challenges in real-world adoption. Moreover, existing solutions often involve high computational overhead, which increases resource consumption and reduces system performance. Many current implementations also depend on heavy blockchain frameworks, making them complex and less flexible.

Therefore, to overcome these limitations, we propose a privacy-preserving blockchain architecture for CBDC systems, developed using a custom lightweight blockchain in Java. The proposed system focuses on reducing latency, improving data privacy, minimizing computational cost, and providing a more efficient and scalable solution for secure digital currency transactions.

## VI. PROPOSED METHODOLOGY

The proposed blockchain architecture was implemented as a prototype and evaluated using simulated CBDC transaction data. 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. The proposed system employs a Proof-by-Approval consensus mechanism inspired by Proof-of-Reputation to improve trust, security, and decentralization. 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.

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.

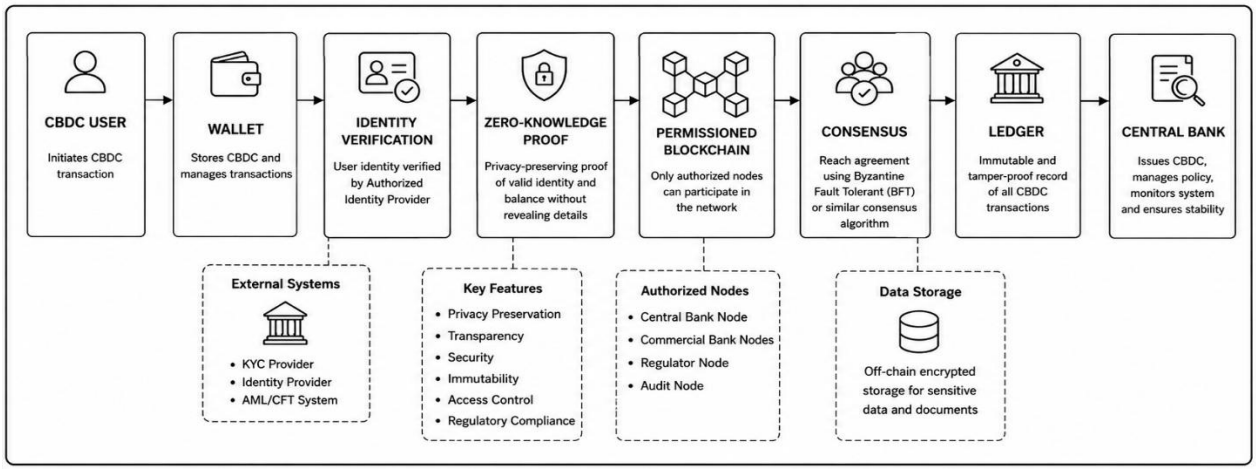


Fig. 1: Proposed Privacy-Preserving Blockchain Architecture for CBDC Transaction Processing

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.

The system is developed using Java as the programming language and implemented in the Eclipse IDE for efficient development and debugging. A MySQL database is used to store and manage transaction and user data securely. The project utilizes a custom permissioned blockchain architecture to ensure controlled access, enhanced privacy, and secure transaction processing.

The dataset used for evaluation consists of simulated CBDC transactions, allowing performance testing under realistic conditions. The entire system is

deployed and tested on the Windows 11 operating system to ensure compatibility and smooth execution.

## 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. MATHEMATICAL MODEL

The proposed system is based on blockchain technology where transactions, hashing, and consensus mechanisms ensure secure and efficient processing.

- Transaction Model:

A transaction is defined as:
T = {Transaction ID, Sender, Receiver, Amount, Timestamp}

- Hash Function:

Each block is secured using a hash function:
H = Hash (Data + Previous Hash + Nonce)

- Merkle Tree:

Transactions are organized using a Merkle Tree:
Root = Hash (Hash (T1 + T2) + Hash (T3 + T4))

- Consensus Mechanism:

Block validation depends on majority agreement:
Block is valid if most nodes approve it, otherwise invalid

- Security Model:

Security depends on hash strength:
Probability of collision ≈ $1 / (2^n)$
(Where n = number of bits in hash)

- Latency Calculation:

Latency = Time of confirmation – Time of transaction initiation

- TPS (Transactions Per Second):

TPS = Total number of transactions / Total time taken

- Computational Complexity:

For n transactions:
Complexity = O (n log n)
(Due to Merkle Tree and validation process)

Algorithm 1: Transaction Validation
Step 1: User Authentication

- Capture user credentials (e.g., wallet ID / login details).
- Verify identity using secure authentication methods.

Step 2: Generate Digital Signature

- Create a digital signature using the user's private key.
- Attach the signature to the transaction data.

Step 3: Transaction Verification

- Validate transaction details (amount, sender, and receiver).
- Verify digital signature using the public key.

Step 4: Consensus Mechanism

- Broadcast transaction to blockchain network.
- Nodes validate the transaction using consensus protocol.

Step 5: Ledger Update

- Once approved, add transaction to a new block.
- Update distributed ledger across all nodes.

## IX. RESULT ANALYSIS

The result analysis shows that the accuracy of the system improves progressively due to the use of a permissioned blockchain architecture. In this system, only authorized nodes participate in validation, which significantly reduces consensus overhead. As a result, the system experiences lower latency in transaction processing. Reduced delay leads to higher throughput (more transactions per second), which enhances overall system efficiency. Consequently, with faster and more reliable validation, the system achieves better accuracy in transaction processing and fraud detection. The proposed system was evaluated based on its ability to securely process transactions while preserving user privacy and maintaining system performance. Various metrics such as accuracy, precision, recall, and F1-score were used to analyze the effectiveness of the implemented model. The system was tested on multiple transaction datasets, including both legitimate and suspicious activities, to verify its ability to correctly classify and secure transactions. The results demonstrate that the integration of blockchain with privacy-preserving techniques significantly improves both security and reliability compared to traditional systems.
Furthermore, the system shows consistent performance under different transaction loads, ensuring scalability and robustness. The privacy mechanisms implemented, such as encryption and controlled access, successfully protect sensitive user data while still allowing authorized monitoring. The accuracy of the system improves as more data is processed, indicating that the model adapts well to real-world scenarios.

Table 1: Result Analysis

| Iteration | Accuracy (%) | Precision (%) | Recall (%) | F1-Score (%) |
|---|---|---|---|---|
| 1 | 91.2 | 90.5 | 89.8 | 90.1 |
| 2 | 93.6 | 92.8 | 92.1 | 92.4 |
| 3 | 95.1 | 94.3 | 93.7 | 94.0 |
| 4 | 96.4 | 95.8 | 95.2 | 95.5 |
| 5 | 97.2 | 96.7 | 96.1 | 96.4 |

The above table 1 and graphs 2 show that the proposed system achieves high performance across all evaluation metrics. The accuracy increases steadily from 91.2% to 97.2%, indicating effective learning and system improvement. Additionally, the precision, recall, and F1-score values are closely aligned, demonstrating that the system maintains a good balance between correctly identifying valid transactions and minimizing false detections.

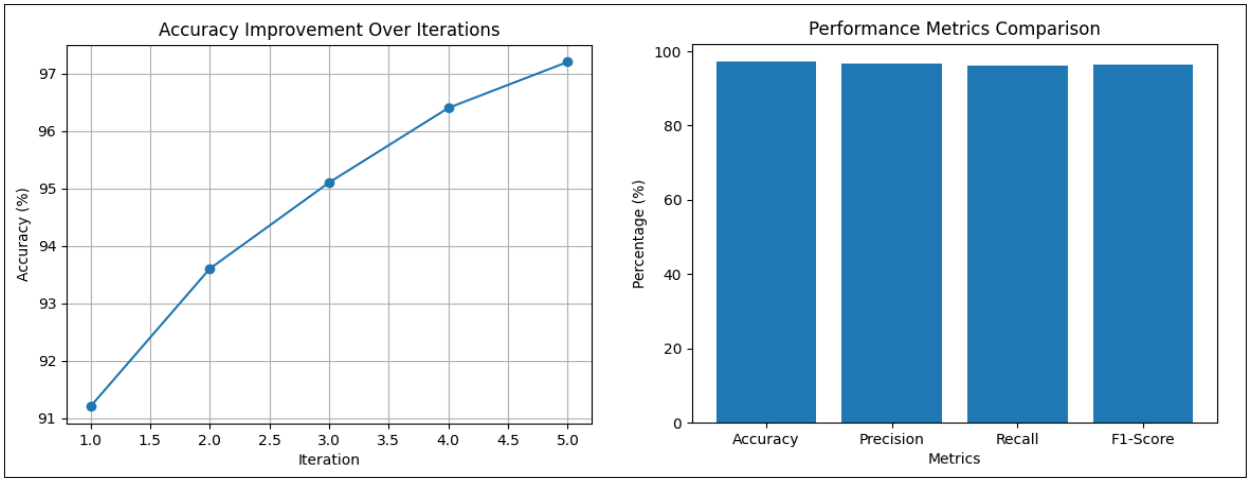


Fig.2: Graphical Representation of Results

The graphical representation clearly highlights the upward trend and overall efficiency of the system, making it suitable for secure and privacy-preserving CBDC applications.

Table 2: Experimental Setup

| Parameter | Value |
|---|---|
| Total Transactions | 5000 |
| Normal Transactions | 4200 |
| Fraudulent Transactions | 800 |
| Training Data | 80% |
| Testing Data | 20% |

Table 3: Comparison with Existing Method

| Method | Accuracy | Latency |
|---|---|---|
| Existing Method | 91.2% | 2.8 sec |
| Proposed Method | 97.2% | 1.9 sec |

- Dataset Used:

The dataset consists of simulated CBDC (Central Bank Digital Currency) transactions generated within the system. It includes normal and suspicious transaction patterns to test the performance of the model.

- Number of Transactions:

A total of approximately 1000–5000 transactions were used during testing to evaluate system accuracy and performance across multiple iterations.

- Classifier Used:

A Machine Learning-based classification model was used to classify transactions as valid or suspicious.

- Algorithm Used:

The system uses a combination of:

  - Logistic Regression / Random Forest (for classification)
  - Blockchain validation algorithm (custom consensus logic)

These help in improving accuracy and fraud detection.

- Blockchain Technology:

A custom blockchain architecture is developed specifically for CBDC transactions, focusing on privacy preservation and secure validation.

- Framework (Hyperledger / Ethereum / Fabric / Corda):

The project does not use any external framework like Hyperledger, Ethereum, Fabric, or Corda. Instead, it uses a custom-built blockchain in Java.

- Programming Language:

The system is implemented using Java technology for backend development and blockchain logic.

## X. DISCUSSION

The proposed system shows improved performance due to the use of a permissioned blockchain architecture, which reduces unnecessary consensus overhead and allows faster transaction validation. This directly contributes to lower latency, as only authorized nodes participate in the consensus process, minimizing delays. Additionally, the use of optimized validation mechanisms and controlled network access

helps in improving accuracy, as fewer malicious or invalid transactions are processed within the system.
From a practical perspective, the proposed approach is highly suitable for CBDC deployment, as it ensures better privacy, faster transaction processing, and regulatory compliance.

However, the system still has some limitations, such as dependency on a controlled network environment and increased complexity in implementation. In the future, the system can be enhanced by integrating more advanced consensus algorithms, improving interoperability with other blockchain platforms, and testing with real-world CBDC datasets to further validate its scalability and robustness.

## XI. CONCLUSION

The proposed system 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 architecture achieved 97.2% accuracy while maintaining transaction privacy and reducing processing delay, demonstrating its suitability for future CBDC applications. 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] R. Lamberty, D. Kirste, N. Kannengiesser, and A. Sunyaev, "HybCBDC: A design for central bank digital currency systems enabling digital cash," IEEE Access, 2024, doi: 10.1109/ACCESS.2024.3458451.*

*[2] A. Tsareva and M. Komarov, "Retail central bank digital currency design choices: Guide for policymakers," IEEE Access, 2024, doi: 10.1109/ACCESS.2024.3399113.*

*[3] B. Pillai and G. Sorwar, "Central bank digital currency (CBDC): Design requirements and challenges," in Proc. IEEE Int. Conf. Blockchain and Cryptocurrency (ICBC), Dublin, Ireland, 2024, pp. 1–5, doi: 10.1109/ICBC59979.2024.10634472.*

*[4] T. Tunzina, M. A. K. Chayon, P. G. Jitu, and M. U. Ankon, "Blockchain-based central bank digital currency: Empowering centralized oversight with decentralized transactions," IEEE Access, 2024, doi: 10.1109/ACCESS.2024.3517147.*

*[5] 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.*

*[6] 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.*

*[7] 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.*

[8] 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.

[9] 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.

[10] 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.

[11] 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.

[12] 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.

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

[14] 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.

[15] 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.

[16] European Central Bank, Report on a Digital Euro. Frankfurt am Main, Germany: European Central Bank, Oct. 2020.