ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26apr870

Secure Central Bank Digital Currency Using Distributed Ledger Technology

Dr. D. A. Vidhate[1]; Prajesh Gaikwad[2]; Aditya Gadge[3]; Abhijay Jadhav[4]; Sai Yewale[5]

[1]Prof., Department of Information Technology, Dr. Vithalrao Vikhe Patil College of Engineering, Ahilyanagar, Savitribai Phule Pune University, Pune, Maharashtra, India
[2,3,4,5]Students, Department of Information Technology, Dr. Vithalrao Vikhe Patil College of Engineering, Ahilyanagar, Savitribai Phule Pune University, Pune, Maharashtra, India

Publication Date: 2026/04/18

Abstract: The growth of financial technology has introduced Central Bank Digital Currency (CBDC), which is basically a digital version of money issued by central banks. In this work, a blockchain-based system is proposed that uses QR codes and UID numbers to make transactions easier and more secure. Blockchain helps keep a proper record of transactions so they cannot be easily changed or tampered with. Using QR codes makes payments quick and simple, especially for everyday use. The system also uses smart contracts to handle processes automatically. Since everything runs on a decentralized network, it reduces dependency on a single authority and lowers the chances of fraud. At the same time, user privacy is maintained by storing only encrypted verification data instead of actual personal details.

Keywords: *Blockchain Technology, QR, SCM, SHA256, Mining, blockchainn, Java, Government/ Admin Module, Secure and Transparent Transactions.*

How to Cite: Dr. D. A. Vidhate; Prajesh Gaikwad; Aditya Gadge; Abhijay Jadhav; Sai Yewale (2026) Secure Central Bank Digital Currency Using Distributed Ledger Technology. *International Journal of Innovative Science and Research Technology*, 11(4), 1078-1083. https://doi.org/10.38124/ijisrt/26apr870

I. INTRODUCTION

Today, People can do almost everything online (banking, shopping, storing and sharing personal information). To access these services in the most secured manner is very critical. Many authentication methods are available such as username and password, barcode, finger print and face detection. But these methods have some advantages as well as disadvantages. Username and password are not providing security; fingerprints and face identity are the methods which are very costly and not affordable by common users. To overcome all the drawbacks the Blockchain technology is introduced for online banking transactions. Blockchain based online banking are used in banking transactions for security; it provides more security than barcode and other techniques. Banks provide a way to economically develop people and countries. They make it easy, safe and convenient for financial trading. Banks are involved in welfare activities and contribute to individual social causes as well. In India, most banks provide passbooks, Automated Teller Machines (ATM), e-banking, mobile banking and telephone banking for financial relationships. E-banking and mobile banking will be more convenient for busy individuals among these financial deals. Blockchain is essentially the technique that provides for various transactional systems to store decentralized approach data. Basically, during data transactions, it is implemented to achieve the highest data security and eliminate different network and data attacks from malicious requests. They are the process which is followed by entire system.

- User entry as user identification number for email id and password.
- Once system validate the authenticating the current request it will show the dashboard where all user's account information.
- User can select specific account and login with own credentials and system send the OTP and two step verification.
- Once OTP and QR Code validate by system it will shows home page where user can do any transaction like check balance, transfer amount etc.
- When any transaction has completed system store entire information into the blockchain.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26apr870

II. PROBLEM STATEMENT

Existing digital banking networks have many problems - by using a single location for data, those systems are open to risks. There are gaps in security which allow for theft. As information is not visible to users, individuals cannot see how the system operates. Due to the factors, attackers can enter the network without permission. To fix those flaws, a framework for digital money that functions across many nodes is necessary.

With a system based on block chain, the Central Bank issues digital currency. It uses programs that execute themselves automatically to handle agreements. On this network computers use specific rules to reach a consensus on data. If a user makes a transaction, the record is visible to everyone. Because the data is difficult for anyone to change, the ledger remains accurate. For every entry the system provides a way to verify the history. When a person logs in, the platform confirms their identity through strict steps. It keeps the information in its original state through encryption. In this environment, the financial structure stays functional even during attacks. Accountability is present because the system tracks every action. Trust grows among participants because the technology ensures the rules are followed.

III. LITERATURE REVIEW

- [1] Kumar and Jeelan propose a blockchain-based system designed to assist state governments in managing land plots and the distribution of government funds. The system integrates multiple departments into a unified platform, enabling secure application submission, approval workflows, and fund allocation. By utilizing cryptographic encryption, consensus algorithms, and the immutable nature of blockchain, the system prevents unauthorized access and ensures tamper-proof records. This approach offers enhanced transparency and operational efficiency across government schemes.
- [2] Krishna et al. develop a blockchain model for tracking government fund transactions in a sequential and verifiable manner. The system maintains an immutable record of each project's progress using hashed data structures, making it impossible to alter or delete transaction history. It further introduces controlled access, ensuring that sensitive information is only shared on a need-to-know basis. This method ensures data security and integrity and promotes accountability in public financial management.
- [3] Raluca Veronica et al. explore the concept of digital identity within e-governance through the adoption of self-sovereign identity (SSI) models based on blockchain. The paper provides a detailed overview of the system's technical architecture, highlighting how individuals can retain control over their digital identities without reliance on central authorities. Blockchain's decentralized nature and cryptographic tools ensure privacy, authenticity, and data consistency, paving the way for secure identity management frameworks
- [4] Fernandes and Shamitha present a blockchain solution focused on the Public Works Department (PWD), addressing issues related to fund allocation and tender tracking. The paper identifies low-level corruption and lack of transparency as major challenges in public works. The proposed system logs every transaction—ranging from project initiation to employee payments—on an immutable blockchain ledger. This ensures traceability and reduces opportunities for manipulation or financial mismanagement.
- [5] Peng et al. propose a peer-to-peer file storage and sharing platform based on a consortium blockchain. The system facilitates secure data retrieval and authorization across multiple government and private organizations. The blockchain integrates identity authentication protocols and permission control mechanisms, guaranteeing that only authorized entities can access data. The study discusses the potential of such a system to support data integrity and inter-organizational collaboration.
- [6] Careja and Tapus suggest a blockchain-based digital identity verification framework using cryptographic signatures issued by trusted entities. These signatures act as digital equivalents of physical identity proofs, securely stored on the blockchain and used by public authorities for identity validation. The system not only ensures secure storage and access to personal data but also builds trust and interoperability across institutions involved in public services.
- [7] De Salve et al. propose a multi-layer trust framework designed to strengthen selfsovereign identity (SSI) systems on blockchain networks. The model incorporates verifiable credentials, decentralized identifiers (DIDs), and smart contracts, deployed on both private and public blockchains. The paper demonstrates how this framework improves data reliability, combats misinformation, and enhances the scalability and trustworthiness of digital identity solutions
- [8] Xu et al. introduce a fog-enabled, private blockchain-based identity authentication system tailored for smart home environments. The system registers all fog nodes and smart devices on a localized blockchain, where authentication is managed using smart contracts and off-chain mechanisms. The proposed approach ensures robust performance and privacy protection, making it a secure solution for identity verification in IoT-based environments.
- [9] Elisa et al. design a blockchain-enabled e-government framework that incorporates an artificial immune system to enhance security and threat detection. The system leverages blockchain's immutable structure along with encryption and validation tools to protect government data from internal and external attacks. Evaluated using simulation tools and real datasets, the framework demonstrates resilience, data integrity, and suitability for secure public sector applications.
- [10] Gawade et al. present a blockchain-based system for fund allocation and tracking within state government operations. Their model tackles low-level corruption by logging every transaction with cryptographic hashes and timestamps. The system guarantees transparency and authenticity of transactions, providing proof at each stage of fund disbursement and utilization, which can be audited and verified at any time.

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26apr870

IV. SYSTEM METHODOLOGY

The proposed blockchain-based online banking system is designed around three core components — the User Group, Bank Group, and the Blockchain Network — which collaboratively ensure secure, transparent, and tamper-resistant financial transactions.

A. Steps:

➢ *User Group:*

This group represents the end-users who perform various online banking activities such as balance inquiries, fund transfers, and account updates. Each transaction request generated by a user is securely transmitted to the banking system for validation and processing.

➢ *Bank Group:*

The bank acts as an intermediary between the user and the blockchain network. Upon receiving a transaction request, the banking server retrieves relevant details from the bank database, processes the transaction, and forwards it to the blockchain module for additional verification and recordkeeping.

➢ *Blockchain Processing Module:*

This module ensures secure transaction recording and data immutability through blockchain mechanisms. It follows a structured process:

- Transaction Formation: The user's transaction request is created and preliminarily verified.
- Hash Generation: A unique cryptographic hash (e.g., SHA-256) is generated to maintain data integrity.
- Mining: The transaction undergoes a mining process to validate and include it in a new block.
- Consensus Mechanism: Agreement among all network nodes is achieved before adding the validated block to the chain.

➢ *Peer-to-Peer (P2P) Blockchain Network:*

After successful verification, the newly created block is added to the decentralized P2P blockchain network, where every participating node maintains an updated copy of the ledger. This distributed structure guarantees transparency, security, and immutability, ensuring that all online banking transactions are permanently recorded and resistant to tampering or unauthorized modification.

V. SYSTEM METHODOLOGY

The proposed banking structure is a system which contains combination of three parts which include a user group. There is also a bank group. And there is a blockchain network - those parts interact to ensure that transactions are open for inspection. When a person starts a banking activity, they might choose to look at their current balance. It is also possible for them to send money to another account - those requests travel to the banking system in a way that protects against interception. To handle those requests, the bank functions as a middle entity. By collecting data, the bank prepares the request. The bank confirms that a transaction is legitimate. The bank sends the data to the blockchain module. On this module the system checks each transaction - by using records that cannot be changed, the system stores the data. As a transaction is verified, the system adds it as a block to a network - this network connects computers directly to one another. There is a ledger that every computer on the network shares. Because of this design, the records are visible to everyone. With this method the system protects against attacks. If someone tries to change a record without permission, the structure stops them.

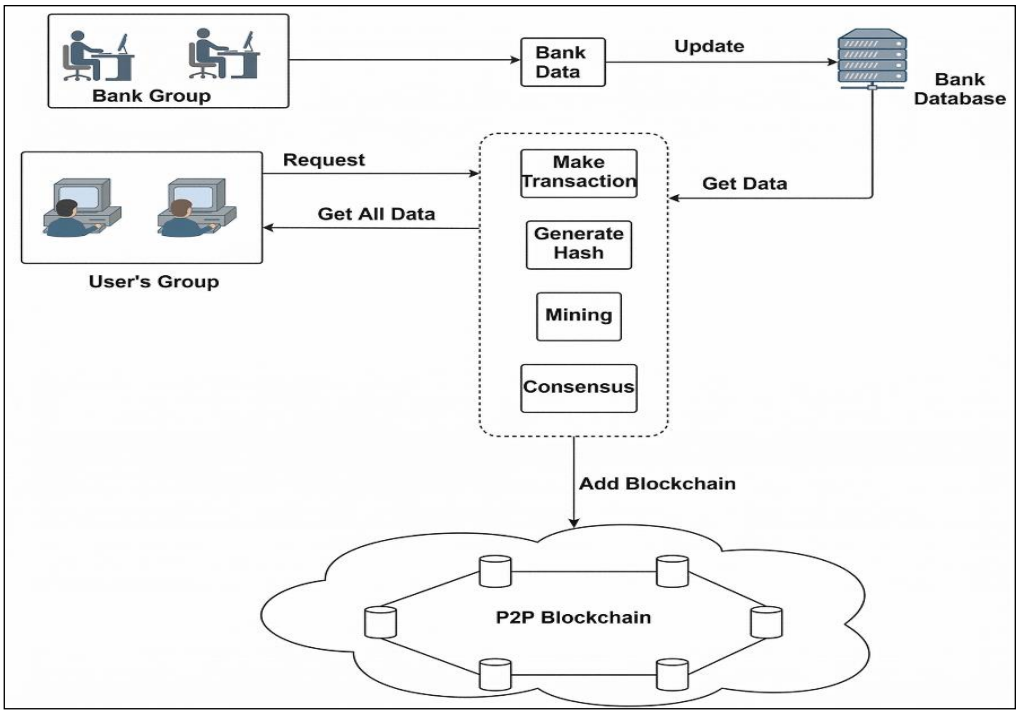

Fig.1: System Architecture Design

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26apr870

VI. RESULT AND ANALYSIS

The results and discussion section presents an evaluation of the proposed blockchain-based online banking system in terms of performance, efficiency, and security. The system demonstrates reliable transaction processing through decentralized validation, ensuring transparency and resistance to tampering. Cryptographic techniques and consensus mechanisms play a key role in maintaining data integrity while enabling secure transaction recording. Performance metrics such as transaction validation time, block generation time, and computational efficiency are analyzed under different network conditions. The use of smart contracts further enhances automation and reduces processing delays. Overall, the findings highlight the effectiveness of the system in handling transactions efficiently while maintaining strong security standards. These results are further supported by graphical and tabular analyses illustrating system behavior under varying parameters and difficulty levels.

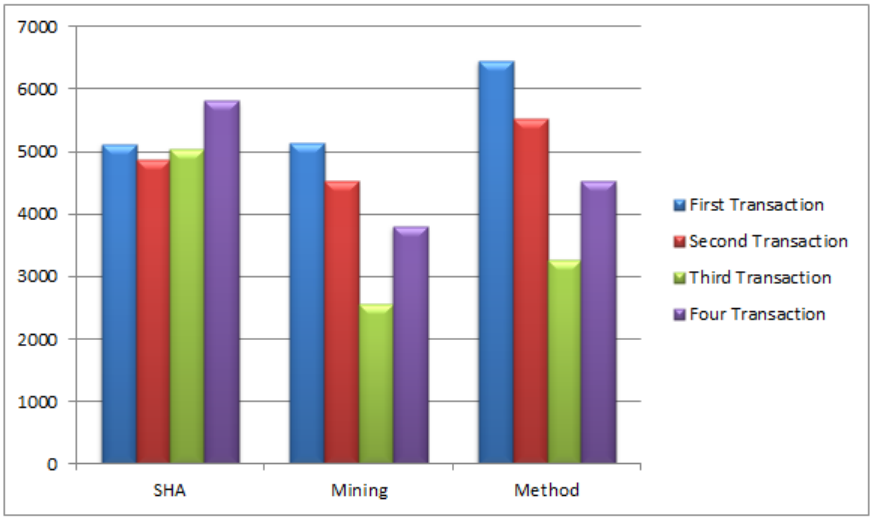

Fig 2: The Time Required (in Milliseconds) for a Complete Transaction with Different Records in the Blockchain Using 4 Data Nodes in the P2P Network is Being Calculated.

Hassard defined mining difficulty levels based on the required number of leading zeros in a hash:

- Level 1 (Two Leading Zeros "00"): Miners must generate a hash starting with at least two zeros.
- Level 2 (Three Leading Zeros "000"): The difficulty increases as hashes must now begin with a minimum of three zeros.
- Level 3 (Four Leading Zeros "0000"): Hashes must start with four zeros, making the mining process more challenging.
- Level 4 (Five Leading Zeros "00000"): At the highest difficulty, hashes require five leading zeros, significantly increasing computational effort.

Table 1: Block Generation Time Using PoW Using Various Difficulty Levels (sec)

Records (Blocks)	Difficulty L-1	Difficulty L-2	Difficulty L-3	Difficulty L-4
5	10	16	40	60
10	22	26	60	80
15	38	46	114	120
20	70	123	138	180
25	97	142	178	248

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26apr870

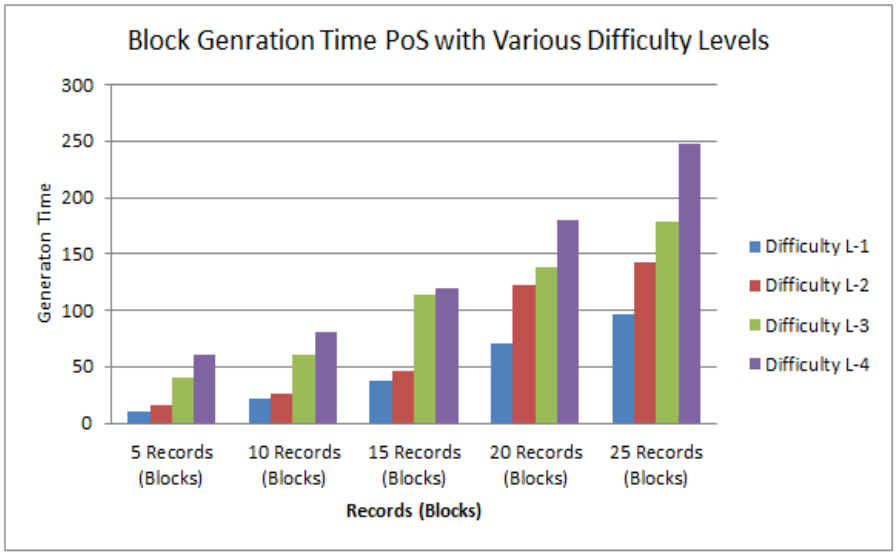

Fig 3: Block Generation Time in Seconds Using Pos with Various Difficulty Levels

Figure 3 illustrates the trend across all four difficulty levels, showing that as difficulty increases, the time required grows not linearly but with an exponential tendency. This indicates that higher difficulty levels substantially increase the computational challenges for validators, potentially necessitating higher stakes or more advanced processing. Overall, the comparison demonstrates how PoS Maxstake behaves under varying difficulty conditions.

VII. CONCLUSION

The proposed blockchain-based online banking system creates a safer and more transparent way for people to carry out financial transactions online. It uses smart contracts and cryptographic hashing to keep data secure and make sure no one can change records without authorization. Compared to traditional systems, it reduces reliance on a central authority, which helps lower the chances of fraud or system breakdowns. Users can also trust the system more since every transaction is recorded and can be verified when needed. The inclusion of automation speeds up processes and reduces manual work for banks. Overall, this approach shows how blockchain can make online banking more reliable, efficient, and trustworthy in everyday use

REFERENCES

[1]. Kumar, Anil, And Syed Jeelan. ”Blockchain-Based State Government Fund Allocation And Track- ing System.” International Journal Of Mechanical Engineering Research And Technology 16.9 (2024): 120-129.

[2]. Krishna, Chinnam Prudhvi, Gadeajay Reddy, And T. Venket Babu. ”Government Fund Allocation And Tracking System Using Blockchain Technology.” , IEEE 2024.

[3]. Raluca Veronica, Et Al. ”A Proposal Of Digital Identity Management Using Blockchain.” Revue Roumaine Des Sciences Techniques—S´erie ´Electrotechnique Et ´Energ´etique 69.1 (2024): 85-90.

[4]. Fernandes, Devakrishnan A. Joshwa, And Erica Fernandes Shamitha. “Public Work Department Fund Allocation And Tender Tracking System Using Blockchain.” (2023).

[5]. Peng, Shaoliang, Et Al. “A Peer-To-Peer File Storage And Sharing System Based On Consortium Blockchain.” Future Generation Computer Systems 141 (2023): 197-204.

[6]. Careja, Alexandru-Cristian, And Nicolae Tapus. “Digital Identity Using Blockchain Technology.” Procedia Computer Science 221 (2023): 1074-1082.

[7]. De Salve, Andrea, Et Al. “A Multi-Layer Trust Framework For Self Sovereign Identity On Blockchain.” Online Social Networks And Media 37 (2023): 100265.

[8]. Xu, Xianbin, Yajun Guo, And Yimin Guo. “Fog-Enabled Private Blockchain-Based Identity Au- thentication Scheme For Smart Home.” Computer Communications 205 (2023): 58-68.

[9]. Elisa, Noe, Et Al. “A Secure And Privacy-Preserving E-Government Framework Using Blockchain And Artificial Immunity.” IEEE Access 11 (2023): 8773-8789.

[10]. Gawade, Rishita, Et Al. “Government Fund Allocation And Tracking System Using Blockchain.” International Journal Of Multidisciplinary Innovative Research 2.2 (2022)

[11]. C. -H. Lin, S. -P. Li, Y. -C. Lin and C. -H. Tsai, “Blockchain-based Secure Storage System for Medical Image Data,” 2023 IEEE 3rd International Conference on Electronic Communica- tions, Internet of Things and Big Data (ICEIB), Taichung, Taiwan, 2023, pp. 158-163, doi: 10.1109/ICEIB57887.2023.10170051.

[12]. A. K. Hebballi, B. J, A. Agarwal and M. Challa, “Securing Medical Data Records using Blockchain in a Cloud Computing Environment,” 2023 Third International Conference on Advances in Electri- cal, Computing, Communication and Sustainable Technologies (ICAECT), Bhilai, India, 2023, pp. 1-5, doi: 10.1109/ICAECT57570.2023.10118338. Secure

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/26apr870

CBDC(Central Bank Digital Currency) Using Distributed Ledger Technology 35

[13]. J. Liu et al., "Conditional Anonymous Remote Healthcare Data Sharing Over Blockchain," in IEEE Journal of Biomedical and Health Informatics, vol. 27, no. 5, pp. 2231- 2242, May 2023, doi: 10.1109/JBHI.2022.3183397.

[14]. G. Xu et al., "A Privacy-Preserving Medical Data Sharing Scheme Based on Blockchain," in IEEE Journal of Biomedical and Health Informatics, vol. 27, no. 2, pp. 698- 709, Feb. 2023, doi: 10.1109/JBHI.2022.3203577.

[15]. X. Jian, R. Parthasarathy and B. W. Huang, "An Exploratory Study on the Design of Emergency First Aid Privacy Protection Computing System Based on Blockchain," 2023 8th International Con- ference on Business and Industrial Research (ICBIR), Bangkok, Thailand, 2023, pp. 447-451, doi: 10.1109/ICBIR57571.2023.10147687.

[16]. B. Bhandari, P. R. Vairagade, H. Trivedi, H. Thakre, G. Indurkar and A. Yadav, "Decentralized Medical Healthcare Record Management System Using Blockchain," 2023 11th International Con- ference on Emerging Trends in Engineering & Technology - Signal and Information Processing (ICETET - SIP), Nagpur, India, 2023, pp. 1-5, doi: 10.1109/ICETET-SIP58143.2023.10151658.

[17]. T. Devi., S. B. Kamatchi and N. Deepa, "Enhancing the Security for Healthcare Data using Blockchain Technology," 2023 International Conference on Computer Communication and Infor- matics (ICCCI), Coimbatore, India, 2023, pp. 1-7, doi: 10.1109/ICCCI56745.2023.10128545.

[18]. H. Ryu, H. Kim, S. Agarwal, D. K. Sharma, B. Kapito and P. Ali, "Data Sovereignty Provi- sion Blockchain for Remote Healthcare Service," 2023 6th International Conference on Informa- tion Systems and Computer Networks (ISCON), Mathura, India, 2023, pp. 1-4, doi: 10.1109/IS- CON57294.2023.10112016.

[19]. P. Marry, K. Yenumula, A. Katakam, A. Bollepally and A. Athaluri, "Blockchain based Smart Healthcare System," 2023 International Conference on Sustainable Computing and Smart Systems (ICSCSS), Coimbatore, India, 2023, pp. 1480-1484, doi: 10.1109/ICSCSS57650.2023.10169704.

[20]. A. Agarwal, R. Joshi, H. Arora and R. Kaushik, "Privacy and Security of Healthcare Data in Cloud based on the Blockchain Technology," 2023 7th International Conference on Computing Methodologies and Communication (ICCMC), Erode, India, 2023, pp. 87-92, doi: 10.1109/IC- CMC56507.2023.10083822