IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 5, May 2026

DOI: 10.17148/IJARCCE.2026.15546

Blockchain-Based Secure Voting System

Palak S Sachar[1], Sania Shaikh[2], Muktha Reddy[3], Dr. Muhibur Rehman T.R[4]

6th Sem B.E(CS&E), Ballari institute of technology and management (BITM), Ballari, Karnataka-583104[1-3]

Associate Professor, Department of computer science and Engineering,

Ballari institute of technology and management (BITM), Ballari, Karnataka-583104[4]

Abstract: The process of voting plays a crucial role in maintaining a fair and democratic system, yet existing methods often face issues related to trust, transparency, and security. Traditional paper-based voting can be slow and prone to manual errors, while electronic voting systems, though faster, still depend on centralized control, making them vulnerable to tampering and cyber threats. These challenges highlight the need for a more reliable and secure approach to conducting elections.

To address these concerns, this study proposes a blockchain-based voting system that ensures data integrity and transparency. By using a decentralized ledger, each vote is securely recorded and cannot be altered once it is added to the system. The use of encryption techniques helps maintain voter privacy, while the transparent nature of blockchain allows verification without exposing sensitive information. This approach minimizes the risk of fraud and increases confidence in the voting process.

The proposed system aims to create a balance between security, transparency, and usability. It provides a structured framework where voters can cast their votes securely and verify them if needed, without compromising anonymity. Overall, the system demonstrates how blockchain technology can be effectively applied to modernize voting systems and improve trust in digital elections.

Keywords: Blockchain, E-Voting, Security, Transparency, Smart Contracts, Decentralization

I. INTRODUCTION

Voting is a fundamental component of democratic systems, enabling citizens to express their opinions and select their representatives. However, conventional voting methods often suffer from several limitations including lack of transparency, susceptibility to tampering, and logistical challenges. Electronic voting systems were introduced to address some of these issues, but they still rely heavily on centralized infrastructures, making them vulnerable to cyberattacks and data manipulation.

Blockchain technology has emerged as a promising solution to overcome these limitations. It is a distributed and decentralized system where data is stored across multiple nodes, making it highly resistant to tampering. Each transaction is recorded in a block and linked to previous blocks, forming a secure chain of records.

The proposed blockchain-based voting system aims to provide a secure, transparent, and efficient voting mechanism. By eliminating the need for a central authority, the system ensures that votes cannot be altered once recorded. Additionally, it allows voters to verify their votes without compromising anonymity, thereby increasing trust in the electoral process.

In addition to security concerns, another major challenge in existing voting systems is the lack of transparency and voter confidence. Many voters are often unsure whether their vote has been recorded correctly or counted fairly. This uncertainty can reduce participation and weaken trust in the overall electoral process. A system that allows verification without compromising voter identity can significantly improve confidence and encourage wider participation in elections.

Blockchain technology offers a promising solution by providing a decentralized and tamper-resistant platform for recording votes. Each transaction in the blockchain is securely linked to the previous one, making it nearly impossible to alter any recorded data without detection. By integrating such technology into voting systems, it becomes possible to ensure both transparency and privacy at the same time. This approach not only strengthens the integrity of elections but also aligns with the growing need for secure and efficient digital solutions in modern governance.

IJARCCE ISSN (O) 2278-1021, ISSN (P) 2319-5940

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 5, May 2026

DOI: 10.17148/IJARCCE.2026.15546

II. LITERATURE REVIEW

[1] Early electronic voting systems were developed to make elections faster and reduce manual effort compared to traditional paper-based methods, but these systems still depended on centralized control which created concerns regarding data security, manipulation, and lack of transparency in the overall process.
[2] To improve protection, several approaches introduced cryptographic techniques to secure voting data during transmission, which helped reduce data leaks but did not fully eliminate the risk of tampering once the data was stored in centralized systems.
[3] Many online voting platforms focused on strengthening voter authentication mechanisms to prevent unauthorized access, yet issues such as duplicate voting and misuse of login credentials were still observed in several implementations.
[4] Some systems introduced verification features that allowed voters to confirm whether their vote was recorded correctly, which improved trust but often made the system slightly complex and less user-friendly for general users.
[5] With the advancement of blockchain technology, decentralized voting systems started gaining attention as they ensure that once a vote is recorded it cannot be modified, thereby improving reliability and increasing confidence in the system.
[6] Smart contract-based approaches were explored to automate vote counting and result generation, which reduced human involvement and helped minimize errors during the counting process.
[7] Distributed network models removed the need for a central authority by storing data across multiple nodes, which reduced the chances of system failure and protected the system from targeted cyberattacks.
[8] Some systems combined encryption techniques with blockchain technology to maintain both security and voter privacy, ensuring that voter identity remains protected while keeping the process transparent and verifiable.
[9] One major challenge identified in blockchain-based voting systems is scalability, especially when handling a large number of voters and transactions at the same time in real-world scenarios.
[10] Biometric authentication methods were introduced in certain systems to improve voter verification and prevent fraud, but they raised concerns regarding the storage and protection of sensitive personal data.
[11] Hybrid approaches that combine traditional voting methods with blockchain technology were suggested to balance usability and security, making such systems more practical for real-world adoption.
[12] Overall, most existing systems focus on specific aspects such as security, transparency, or authentication, but there is still a need for a complete solution that integrates all these features into one efficient and reliable voting platform.

III. PROPOSED SYSTEM

The proposed system is designed to provide a secure and transparent voting platform using blockchain technology. It consists of several key modules including voter registration, authentication, vote casting, and result verification.

During registration, voters provide their details, which are securely stored. Authentication is performed using unique credentials to ensure that only eligible voters can participate.

Once authenticated, voters can cast their votes through a user-friendly interface. Each vote is encrypted and recorded as a transaction on the blockchain. The decentralized nature of the system ensures that no single entity has control over the data

The system also includes a verification feature that allows voters to confirm that their vote has been successfully recorded without revealing their identity. This enhances transparency while maintaining privacy.

It includes voter authentication, encrypted vote casting, and decentralized storage to ensure that no unauthorized changes can be made. This approach improves trust, prevents fraud, and allows voters to verify their participation without revealing their identity.

IV. METHODOLOGY

The proposed system works by using blockchain technology to securely record and manage voting data in a decentralized manner. The process begins with voter registration, where user details are collected and verified through a secure authentication mechanism to ensure that only eligible voters can access the system. Once verified, each voter is provided with unique credentials that allow them to participate in the voting process.

After authentication, the voter can cast their vote through a simple and user-friendly interface. Each vote is encrypted before being submitted to the blockchain network, where it is treated as a transaction. The network nodes validate the

DOI: 10.17148/IJARCCE.2026.15546

transaction using a consensus mechanism, ensuring that only legitimate votes are recorded. Once validated, the vote is added to a block and linked to the existing chain, making it permanent and tamper-proof.

The system also ensures voter privacy by separating identity information from the actual vote data. Cryptographic techniques are used so that votes can be verified without revealing the voter's identity. Additionally, the decentralized structure eliminates the need for a central authority, reducing the risk of manipulation or system failure. This continuous process of authentication, encryption, validation, and storage ensures that the voting system remains secure, transparent, and reliable.

V. IMPLEMENTATION

The system is implemented using web-based technologies to ensure accessibility and ease of use. The frontend is developed using HTML, CSS, and JavaScript, providing a simple interface where users can register, log in, and cast their votes without difficulty.

The backend handles user authentication, vote processing, and interaction with the blockchain network. It ensures that only valid users can access the system and that each vote is securely processed before being recorded.

A lightweight blockchain framework is used to store votes as encrypted transactions. Each transaction is validated and added to a block, which is then linked to the existing chain, ensuring data integrity and preventing any modification.

The system follows a modular design where components such as authentication, vote casting, and blockchain storage operate independently but are well integrated. This structure makes the system easier to maintain, scalable, and adaptable for future improvements.

VI. RESULTS AND DISCUSSION

The system was tested under different conditions to evluate its performance and reliability. During normal operation, the voting process worked smoothly, and all votes were recorded correctly on the blockchain without any data loss or delay.

When multiple users accessed the system simultaneously, it was able to handle the transactions efficiently, though slight delays were observed due to validation processes. This shows that the system is reliable but may require optimization for large-scale use.

The security features performed effectively, as each vote remained encrypted and tamper-proof after being added to the blockchain. Any attempt to alter stored data was unsuccessful, proving the strength of the decentralized structure.

Overall, the system demonstrated improved transparency, as users could verify that their vote was recorded without revealing their identity. This builds trust and shows that blockchain-based voting can be a practical and secure solution for modern elections.

VII. CONCLUSION

This paper presented a blockchain-based secure voting system aimed at improving the reliability and transparency of elections. By leveraging decentralized technology, the system ensures that votes are securely recorded and cannot be altered.

The proposed solution enhances trust in the voting process and provides a practical approach to modernizing electoral systems. Future work may focus on improving scalability, integrating advanced authentication methods, and optimizing system performance.

REFERENCES

[1] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008.
[2] B. Adida, "Helios: Web-based Open-Audit Voting," in Proceedings of the USENIX Security Symposium, 2008, pp. 335–348.
[3] J. Benaloh, "Verifiable Secret-Ballot Elections," Ph.d. dissertation, Yale University, 2011

International Journal of Advanced Research in Computer and Communication Engineering

Impact Factor 8.471 ⁜ Peer-reviewed & Refereed journal ⁜ Vol. 15, Issue 5, May 2026

DOI: 10.17148/IJARCCE.2026.15546

[4] G. Zyskind, O. Nathan, and A. Pentland, "Decentralizing Privacy: Using Blockchain to Protect Personal Data," in Proceedings of the IEEE Security and Privacy Workshops, 2015, pp. 180–184.
[5] M. Swan, Blockchain: Blueprint for a New Economy, O'Reilly Media, 2015.
[6] K. Christidis and M. Devetsikiotis, "Blockchains and Smart Contracts for the Internet of Things," IEEE Access, vol. 4, pp. 2292–2303, 2016.
[7] P. McCorry, S. F. Shahandashti, and F. Hao, "A Smart Contract for Boardroom Voting with Maximum Voter Privacy," in Proceedings of the International Conference on Financial Cryptography, 2017, pp. 357–375.
[8] A. B. Ayed, "A Conceptual Secure Blockchain-Based Electronic Voting System," International Journal of Network Security & Its Applications, vol. 9, no. 3, pp. 01–09, 2017.
[9] F. S. Hardwick, A. Gioulis, R. N. Akram, and K. Markantonakis, "E-Voting with Blockchain: An E-Voting Protocol with Decentralisation and Voter Privacy," in Proceedings of the IEEE International Conference on Internet Technology and Secured Transactions, 2018, pp. 156–161.
[10] N. Kshetri and J. Voas, "Blockchain in Developing Countries," IT Professional, vol. 20, no. 2, pp. 11–14, 2018.
[11] K. M. Khan, J. Arshad, and M. M. Khan, "Secure Digital Voting System Based on Blockchain Technology," International Journal of Electronic Government Research, vol. 16, no. 2, pp. 1–15, 2020.
[12] A. Singh and P. Sharma, "Blockchain-Based Secure E-Voting System: Challenges and Opportunities," Journal of Information Security and Applications, vol. 55, pp. 102–110, 2021.

