iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 13 **Issue:** VII **Month of publication:** July 2025

DOI: https://doi.org/10.22214/ijraset.2025.73177

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue VII July 2025- Available at www.ijraset.com

Voting System Based on Blockchain

Prof. Nitin Thakre[1], Mr. Shubham Jha[2], Mr. Pushpak Khobragade[3], Mr. Amit Prasad[4]
[1]*Assistant Professor,* [2, 3, 4]*Student, Department of Computer Science Engineering, Govindrao Wanjari College of Engineering and Technology, Nagpur, Maharashtra, India*

Abstract: ***The traditional voting process, whether paper-based or electronic, is often criticized for its lack of transparency, susceptibility to fraud, and dependence on centralized authorities. Blockchain technology, particularly in the Web3 ecosystem, provides a decentralized, secure, and tamper-proof solution for digital voting. This paper explores how blockchain can enhance election integrity by leveraging decentralized applications (DApps), smart contracts, and cryptographic security. The proposed system employs Ethereum-based smart contracts to automate vote casting and tallying while ensuring voter privacy through zero-knowledge proofs. Decentralized Identity (DID) is integrated for secure authentication, preventing double voting and identity fraud. The paper discusses system architecture, security considerations, scalability challenges, and real-world applications of blockchain voting, highlighting how Web3 can transform democratic elections.***
Keywords: Blockchain, Smart Contracts, Web3, Voting System, Cryptographic Security.

I. INTRODUCTION

Elections are a cornerstone of democracy, allowing citizens to express their will and participate in governance. However, traditional voting systems—whether paper-based or electronic—have long faced challenges related to security, transparency, and efficiency. Paper ballots are prone to human error, manipulation, and logistical inefficiencies, while electronic voting systems rely heavily on centralized authorities, making them vulnerable to cyberattacks, hacking, and data breaches. Additionally, concerns regarding voter authentication, vote tampering, and delayed vote counting further undermine public trust in elections. These challenges highlight the urgent need for a more secure and transparent voting mechanism that ensures integrity and fairness.Blockchain technology, introduced by Satoshi Nakamoto in 2008, has emerged as a promising solution to these problems. Blockchain operates as a decentralized, immutable ledger that records transactions transparently and securely. By leveraging cryptographic techniques, blockchain ensures that once data (such as a vote) is recorded, it cannot be altered or deleted.

Despite its advantages, blockchain voting faces challenges in regulatory acceptance, privacy concerns, and user accessibility.

II. LITERATURE REVIEW

The integration of blockchain technology in voting systems has been explored extensively in academic research, focusing on its potential to enhance security, transparency, and efficiency. Traditional electronic voting (e-voting) systems face multiple challenges, such as susceptibility to cyberattacks, lack of voter anonymity, and centralization issues, which blockchain can address through its decentralized and immutable ledger. This section reviews key studies that have contributed to the development of blockchain-based voting systems and highlights the existing gaps that need to be addressed.

Foundations of Blockchain and Its Application in Voting

Blockchain was introduced by Nakamoto (2008) as a decentralized and immutable ledger, later proposed for voting to enhance security and transparency. Swan (2015) highlighted blockchain's potential in governance, while Ayed (2017) emphasized its ability to eliminate central authorities, ensuring verifiable and tamper-proof elections.

Decentralized Identity and Secure Authentication

Voter authentication is crucial for secure elections. Zyskind et al. (2015) proposed decentralized identity (DID) for self-sovereign authentication. Kari et al. (2018) explored smart contract-based verification to prevent fraud, and Serrano et al. (2020) demonstrated how Zero-Knowledge Proofs (ZKPs) could verify voter eligibility while preserving privacy.

Smart Contracts for Secure and Transparent Elections Smart contracts automate vote registration and tallying, reducing manipulation risks. Zhang et al. (2019) showcased Ethereum-based smart contract voting for tamper-proof results. Zhou et al. (2021) studied security measures like multi-signature authentication. Aleo et al. (2021) warned of vulnerabilities in smart contracts, stressing the need for audits to prevent exploits.

Scalability and Performance Challenges in Blockchain Voting

©IJRASET: All Rights are Reserved

Blockchain voting faces transaction speed and scalability issues. Buterin (2018) proposed Layer-2 solutions like sharding and zk-Rollups to optimize performance. Dinh et al. (2020) suggested hybrid public-private blockchains for efficiency. Liu et al. (2022) recommended sidechains to handle high voter turnout without compromising decentralization.

DApp, and the vote is immutably recorded on the ledger. Smart contracts automatically count and publish results in real-time, eliminating the risk of manipulation. To address scalability, Layer-2 solutions such as zk-Rollups or sidechains optimize transaction efficiency, ensuring the

III. PROPOSED WORK

The proposed blockchain-based voting system aims to eliminate centralized control, prevent fraud, and enhance transparency in elections. By leveraging smart contracts, the system ensures that votes are recorded immutably and counted automatically without human intervention. Decentralized Identity (DID) authentication allows voters to verify their eligibility securely, preventing double voting and identity fraud while maintaining privacy through Zero-Knowledge Proofs (ZKPs). Unlike traditional voting systems that rely on central authorities, this model operates on a public blockchain, ensuring that election results are verifiable by all participants

To address scalability and performance challenges, the system integrates Layer-2 solutions such as zk-Rollups or sidechains to optimize transaction efficiency while reducing gas fees. Additionally, a user-friendly Web3-based front-end (ReactJS DApp) provides seamless access for voters, ensuring ease of use. The smart contract logic governs the entire process, from voter registration to final result declaration, eliminating risks of tampering or manipulation.

This approach not only ensures security and efficiency but also makes voting more accessible and transparent for large-scale elections, corporate governance, and decentralized autonomous organizations (DAOs). Future improvements will focus on regulatory compliance, integration of quantum-resistant cryptography, and broader adoption across various democratic systems.

IV. METHODOLOGY

The proposed blockchain-based voting system leverages Ethereum smart contracts, decentralized identity (DID) verification, and cryptographic security to ensure a transparent and tamper-proof election process. The system architecture consists of a Web3-based front-end (ReactJS DApp) for user interaction, smart contracts for vote validation and tallying, and decentralized storage (IPFS) for securely managing voter credentials. Voter authentication is achieved using self-sovereign identity (SSI) and zero-knowledge proofs (ZKPs) to verify eligibility without exposing personal data. The voting process follows a structured workflow: voters register using a decentralized identity system, authenticate via cryptographic keys, cast their vote through the blockchain system can handle large-scale elections. By combining

decentralization, automation, and cryptographic security, this methodology ensures a reliable, fraud-resistant, and accessible voting process.blockchain technology and regulatory changes may affect the applicability of the conclusions over time.

V. APPLICATIONS

A. National and Local Elections

Blockchain voting ensures transparent, tamper-proof elections by preventing fraud, double voting, and manipulation. It allows for secure remote voting, increasing accessibility while maintaining voter anonymity and trust.

B. Corporate Governance and Shareholder Voting

Companies can implement blockchain voting for board meetings and shareholder decisions, ensuring fairness and security. The immutable ledger eliminates disputes, and smart contracts automate result verification without intermediaries.

C. University and Institutional Elections

Educational institutions can conduct student body elections, faculty votes, and policy decisions using blockchain. The system ensures accurate, verifiable results while preventing vote tampering and increasing participation.

D. Decentralized Autonomous Organizations (DAOs)

DAOs rely on blockchain voting to enable community-driven decision-making in a fully decentralized manner. Smart contracts ensure that voting results are publicly verifiable and instantly executed without external influence.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |

VI. ADVANTAGES

1) Enhanced Security and Fraud Prevention: Blockchain's cryptographic security ensures votes cannot be altered, deleted, or manipulated once recorded. This eliminates risks like double voting, voter impersonation, and ballot tampering.
2) Transparency and Trust: Every vote is publicly verifiable on the blockchain while maintaining voter anonymity. This builds public trust in elections by preventing hidden interference or vote rigging
3) Decentralization and Elimination of Middlemen: Unlike traditional systems controlled by central authorities, blockchain voting is distributed across multiple nodes, making it resistant to hacks, corruption, and centralized control..
4) Privacy and Anonymity: Technologies like Zero-Knowledge Proofs (ZKPs) ensure that votes are recorded without revealing voter identities, maintaining confidentiality and compliance with privacy laws..
5) Accessibility and Remote Voting: Blockchain allows secure online voting from anywhere, increasing participation, especially for disabled individuals, overseas voters, and those in remote areas.
6) Real-Time and Automated Vote Counting: Smart contracts automatically count and verify votes, reducing delays and human errors. Election results are available instantly, eliminating manual vote tallying inefficiencies.

VII. CONCLUSION AND FUTURE WORK

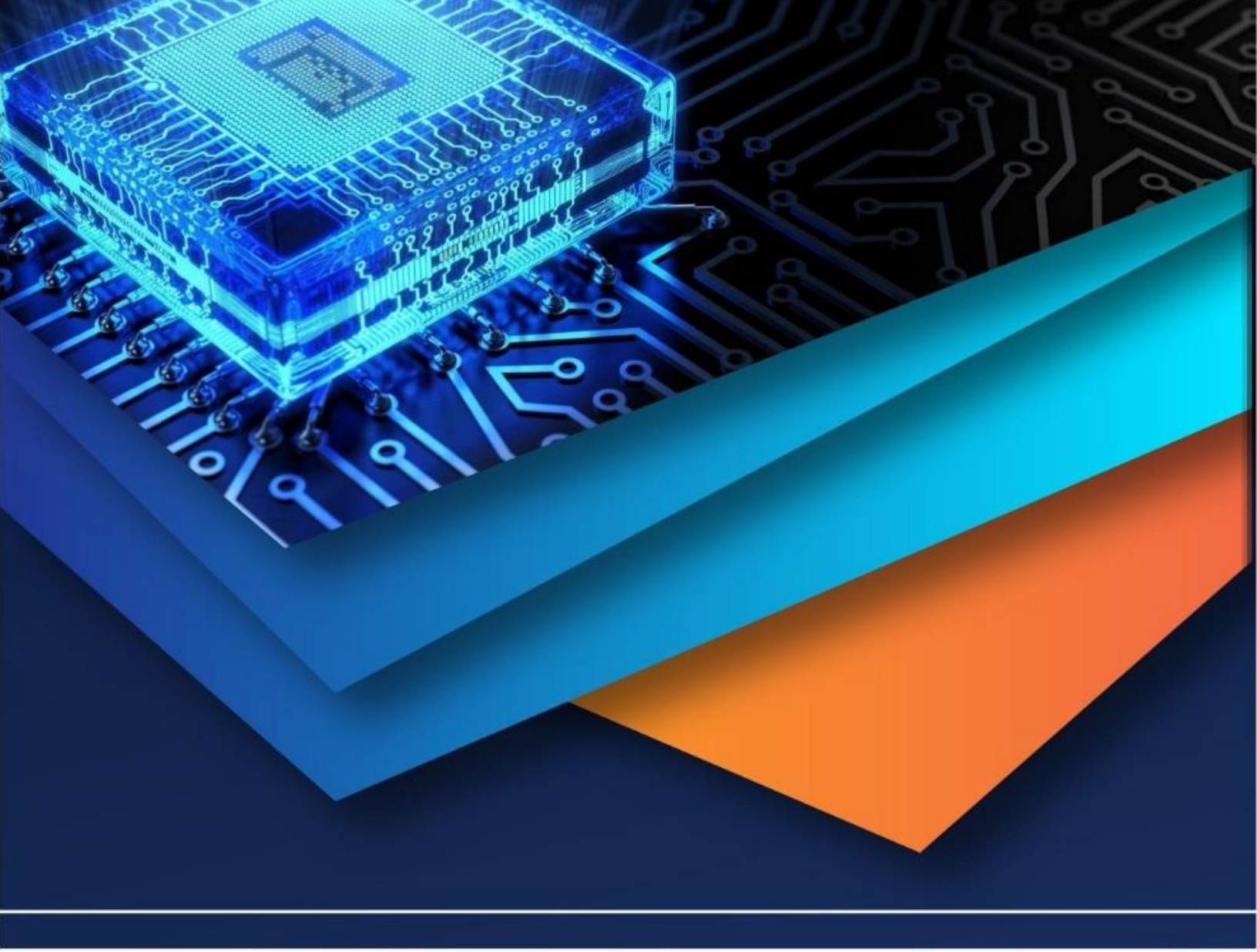
Blockchain-based voting presents a secure, transparent, and decentralized alternative to traditional election systems. By leveraging smart contracts, decentralized identity (DID), and cryptographic security, it ensures tamper-proof vote recording, automated counting, and enhanced voter privacy. This system eliminates fraud, central authority control, and manual errors, making elections more trustworthy and efficient. Despite its advantages, challenges like scalability, regulatory acceptance, and accessibility need further refinement.

Future improvements should focus on enhancing scalability through Layer-2 solutions and optimizing blockchain protocols to support large-scale elections. Additionally, legal and regulatory frameworks must be developed for widespread adoption. Integration of quantum-resistant cryptography and AI-driven fraud detection can further strengthen security. Lastly, improving the user-friendliness of blockchain voting platforms will encourage greater public participation and acceptance.

REFERENCES

[1] Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. Retrieved from https://bitcoin.org/bitcoin.pdf
[2] Swan, M. (2015). Blockchain: Blueprint for a New Economy. O'Reilly Media.
[3] Ayed, A. B. (2017). A Conceptual Secure Blockchain-Based Electronic Voting System. International Journal of Network Security & Its Applications, 9(3), 1-9.
[4] Zyskind, G., Nathan, O., & Pentland, A. (2015). Decentralizing Privacy: Using Blockchain to Protect Personal Data. In 2015 IEEE Security and Privacy Workshops (pp. 180-184).
[5] Kari, M., Danil, F., & Smirnov, A. (2018). Smart Contract-Based Voting System on Ethereum Blockchain. Journal of Information Security and Applications, 43, 1-8.
[6] Yavuz, E. A., Koç, Z., Çabuk, U. C., & Dalkılıç, G. (2018). Towards Secure E-Voting Using Ethereum Blockchain. In 2018 6th International Symposium on Digital Forensic and Security (ISDFS) (pp. 1-7). IEEE.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)