IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 13, April 2025
Impact Factor: 7.67

Enhancement and Evaluation of a Blockchain-Based Electronic Voting System

Divya Gulab Wakale[1], Shreya Sunil Shelar[2], Prachi Badri Ghugare[3], Prof. Shrikant Ghagre[4]
Student, Department of Computer Science and Design Engineering[1,2,3]
Asst. Prof. Department of Computer Science and Design Engineering[4]
Dr. Vithalrao Vikhe Patil College of Engineering, Ahmednagar

Abstract: *Emphasizing on addressing important issues such security, transparency, and voter confidence, this paper investigates the improvement of e-voting systems by means of blockchain technology. Leveraging a Permissioned Blockchain with a Proof of Authority (POA) consensus mechanism guarantees distributed and tamper-proof vote validation in the proposed system. Important characteristics include smart contract-driven candidate selection, secure voter identification utilizing multi-factor approaches, and immutable vote recording to eradicate vulnerabilities such identity fraud and vote manipulation. Furthermore improving system dependability and usefulness are scalability gains and error-handeling systems. By tackling constraints in current e-voting systems, this paper emphasizes blockchain's ability to transform digital democracy by offering a scalable, transparent, safe architecture for next elections.*

Keywords: Blockchain technology, permissioned blockchain, electronic voting systems, Proof of Authority (POA), voter authentication, and vote validation

I. INTRODUCTION

Voting is an essential component of democracy, enabling people to voice their thoughts on important issues and influencing national destiny. Due to their dependability and simplicity, traditional voting techniques—such as paper ballots—have become increasingly popular over time. Nevertheless, they frequently experience inefficiencies, logistical difficulties, and fraud vulnerability. As technology advanced, electronic voting (e-voting) systems became a viable substitute that provided speedier results, scalability, and convenience. Notwithstanding these advantages, e-voting systems still have a lot of trouble satisfying the strict security, anonymity, transparency, and verifiability standards that are essential to preserving voter trust and electoral integrity.

Traditional electronic voting systems' dependence on centralized authorities or reliable third parties is one of their main drawbacks. This reliance creates questions about voter privacy protection as well as the validity and integrity of election results. Further impeding the widespread use of electronic voting are security flaws like identity theft, vote rigging, and system breaches. Researchers and developers have looked to blockchain technology, a decentralized and unchangeable ledger system, as a revolutionary way to modernize electronic voting procedures in order to allay these worries.

Blockchain technology is a great option for addressing the security and trust concerns related to electronic voting systems since it naturally offers characteristics like decentralization, transparency, and immutability. Blockchain improves voter privacy and data integrity by doing away with the necessity for centralized authorities. Voter anonymity is maintained while votes remain secret and verifiable thanks to sophisticated cryptographic techniques including blind signatures, homomorphic encryption, and zero-knowledge proofs. These developments tackle important issues like vote rigging, multiple voting, and illegal access.

Blockchain integration with electronic voting systems has been suggested in recent research as a way to establish safe and decentralized election procedures. Even while these initiatives have showed promise, they frequently have issues with usability, efficiency, and scalability, especially during large-scale elections. Although existing protocols, such the one created by J.P. Cruz and Y. Kaji, have shown that blockchain-based electronic voting is feasible, they still have shortcomings in terms of usability and performance. These difficulties show that a more reliable and scalable framework is required in order to manage the intricacies of actual elections while preserving high standards of security and dependability.

The goal of the proposed study is to improve the blockchain-based electronic voting system in order to overcome these constraints. The system guarantees decentralized vote validation while retaining high efficiency by combining a Proof of Authority (POA) consensus mechanism with a Permissioned Blockchain infrastructure. Important elements include tamper-proof vote recording, smart contract-driven candidate selection, and secure voter authentication with multi-factor approaches. The technology offers a transparent and auditable electoral process by addressing vulnerabilities including identity fraud, vote tampering, and data breaches.

This study lays the groundwork for future developments in digital democracy in addition to aiding in the creation of a safe and trustworthy electronic voting system. The suggested framework seeks to revolutionize electoral procedures by utilizing blockchain technology and cutting-edge cryptographic techniques, guaranteeing free, fair, and reliable elections in the digital era. By taking a novel approach, the study emphasizes how blockchain might address important e-voting issues while striking a balance between security, scalability, and user-friendliness, which will increase trust in democratic systems around the world.

OBJECTIVE

- To research the shortcomings of current blockchain-based electronic voting systems.
- To research and enhance the J.P. Cruz and Y. Kaji electronic voting protocol's security.
- To research how to include cutting-edge cryptographic methods for voter privacy.
- To research how scalable private blockchain systems are for major elections.
- To research ways to improve system reliability and avoid double voting

II. LITERATURE SURVEY

1. "A Blockchain-Based Voting System Using Smart Contracts" – J.P. Cruz and Y. Kaji

Overview:

This paper presents a blockchain-based voting protocol leveraging Ethereum smart contracts to enable secure and transparent elections. The authors propose using Ethereum's decentralized infrastructure to eliminate tampering and enhance voter trust.

Key Contributions:

- Uses Ethereum smart contracts for vote recording and tallying.
- Voters interact through secure interfaces and cast verifiable votes.
- Each vote is immutable and recorded in the public ledger.

Limitations:

- Scalability is limited due to the congestion and high gas fees of public blockchains.
- Voter authentication is not deeply integrated, exposing potential identity vulnerabilities.
- Public visibility of transactions may threaten voter privacy.

Relevance to Your Study:

Your proposed system improves on this by integrating **Permissioned Blockchain** to enhance scalability and privacy, and **multi-factor voter authentication** for stronger identity verification.

2. "Blockchain-Based E-Voting System with Improved Privacy" – Z. Xia, Y. Zhu, X. Sun, and L. Chen (2020)

Overview:

This research introduces a blockchain e-voting framework that employs homomorphic encryption and blind signatures to maintain ballot secrecy and voter anonymity while ensuring that results are verifiable.

Key Contributions:

- Voters encrypt their votes using homomorphic encryption before submission.
- Blind signatures ensure voter identity is hidden from the blockchain validators.

- Emphasis on cryptographic privacy without compromising transparency.

Limitations:

- Cryptographic operations increase system complexity and computational overhead.
- No detailed implementation of error-handling or system failure recovery.
- Assumes a high level of technical proficiency from users.

Relevance to Your Study:

You enhance this framework by including error-handling mechanisms, usability features, and using POA consensus to reduce computational cost while maintaining security and decentralization.

3. "A Survey on Blockchain-Based E-Voting Systems" – H. Ayed (2017)

Overview:

This is a comprehensive review of existing blockchain-based voting solutions, comparing their architecture, consensus protocols, security measures, and usability challenges.

Key Contributions:

- Highlights the evolution of e-voting from centralized systems to decentralized blockchain frameworks.
- Discusses vulnerabilities in current systems, such as vote tampering and double voting.
- Reviews various consensus algorithms like PoW, PoS, and their inefficiencies for e-voting.

Limitations:

- Mainly conceptual and lacks experimental results.
- Does not explore **Permissioned Blockchain** or **POA** as alternatives.
- Focus is broad and less actionable for large-scale election implementations.

Relevance to Your Study:

Serves as a background resource that justifies the shift to Permissioned Blockchain with POA to achieve scalability, security, and efficiency, which your system directly aims to address.

4. "Blockchain Technology for Electronic Voting" – M. Noizat (2015)

Overview:

This early work discusses the potential of blockchain as a distributed ledger for conducting elections, emphasizing trust, transparency, and integrity of the voting process.

Key Contributions:

- Explains how decentralization removes reliance on central authorities.
- Suggests that immutability ensures long-term auditability.
- Recognizes blockchain's ability to facilitate public trust in digital voting.

Limitations:

- Lacks practical implementation or testing on real election data.
- Does not propose concrete identity verification or encryption schemes.
- Assumes that decentralization alone is sufficient, ignoring scalability and usability.

Relevance to Your Study:

While foundational, your research builds on this by incorporating practical mechanisms like multi-factor authentication, smart contract-based candidate selection, and vote logging with redundancy and validation.

5. "A Secure and Scalable Blockchain-Based E-Voting System" – Y. McCorry, S.F. Shahandashti, and F. Hao (2017)

Overview:

The paper presents an e-voting system that uses Permissioned Blockchain and Elliptic Curve Cryptography to create a balance between transparency and voter privacy. It aims to ensure that the system is resistant to vote tampering, coercion, and denial-of-service attacks.

Key Contributions:

- Introduces a Permissioned Blockchain model where only authorized nodes validate transactions.
- Utilizes strong cryptographic techniques to ensure vote secrecy and verification.
- Introduces lightweight protocols for scalability.

Limitations:

- Focuses more on cryptographic integrity than on user experience or scalability for national-scale elections.
- Does not address error-handling or post-election auditing mechanisms.

Relevance to Your Study:

Your project enhances this framework by including POA consensus to maintain speed, scalability features for large-scale deployment, and error recovery mechanisms for robust real-world performance.

III. WORKING OF PROPOSED SYSTEM

Through its tiered architecture and the integration of many modules intended to address important issues like voter privacy, security, scalability, and transparency, the blockchain-based electronic voting system's operation may be comprehended. The system's multi-layered design guarantees that every part of the election process is managed effectively and safely.

The User Interface Layer, which is at the core of the system, gives voters a smooth experience whether they are using desktop or mobile platforms. The user-friendly design keeps things simple while assisting users with the registration, voting, and feedback processes. Voters engage with the Application Layer, which manages essential features like vote recording, authentication, and result computation, after they have gained access to the system. This layer is in charge of making sure that every vote is safely recorded and sent to the blockchain for transparency and immutability.

The foundation of the system's security model is the Blockchain Layer. Votes are handled as transactions in this case, and they are stored on a decentralized blockchain to guarantee that they cannot be changed or tampered with once they are cast. Blockchain makes the voting process transparent and impenetrable by providing an unchangeable record of every vote cast. This makes it possible to confirm the election results without jeopardizing the privacy of specific voters. By securely storing auxiliary data, such voter credentials and session information, in a SQL database, the Database Layer enhances the blockchain. Meanwhile, the Network Layer makes sure that all communication between the levels is secure by encrypting it using protocols like HTTPS.

The system is made to handle important problems like privacy and scalability. By verifying their identity against a central government database, the User Registration Module makes sure that only eligible voters may cast ballots, avoiding fake registrations. Voters can cast their ballots safely with the Voting Module, which records each vote as a distinct blockchain transaction and ensures vote anonymity through encryption. Real-time feedback is given to voters to confirm that their vote was received. Real-time result calculation and verification are made possible by the Result Computation Module, which automatically collects votes from the blockchain. By identifying any disparities in the outcomes, it ensures accuracy and creates audit trails.

Election authorities are given all the tools they need to oversee the election process by the Administrator Module. Administrators have the ability to manage voters, set up elections, and keep an eye on things in real time. Additionally, this module offers capabilities for anomaly detection, guaranteeing election security all the way through. For auditing purposes, the Audit and Security Module makes sure that every operation made within the system is permanently recorded, creating a tamper-proof trail. While frequent security assessments guarantee the system's resilience against new threats, multi-layered security solutions, such as firewalls and encryption, shield the system from cyberattacks.

In conclusion, our blockchain-based electronic voting system integrates state-of-the-art technologies to improve the electoral process's efficiency, security, and transparency. While strong cryptographic mechanisms maintain voter anonymity, the decentralized structure of blockchain guarantees tamper-proof voting. The system provides a thorough answer to the problems encountered by conventional and current e-voting systems by integrating multiple modules for registration, voting, result computation, administration, and auditing.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 13, April 2025
Impact Factor: 7.67

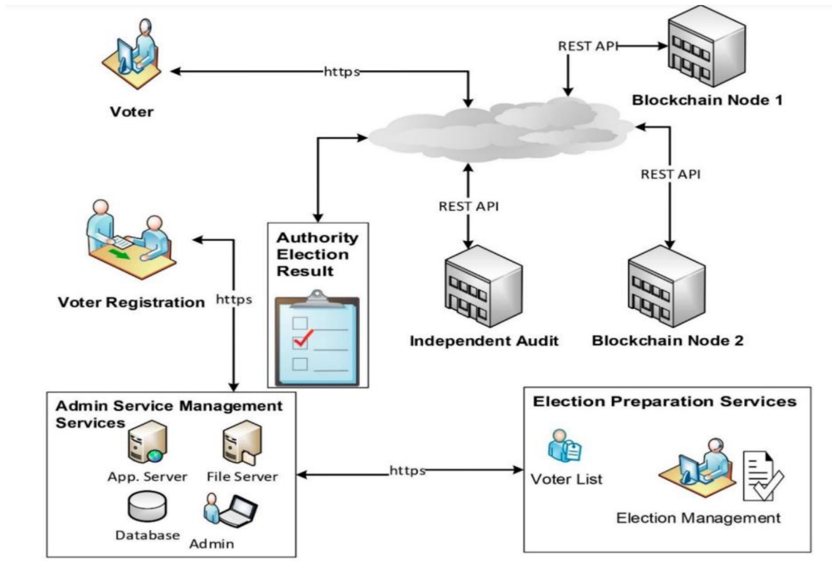
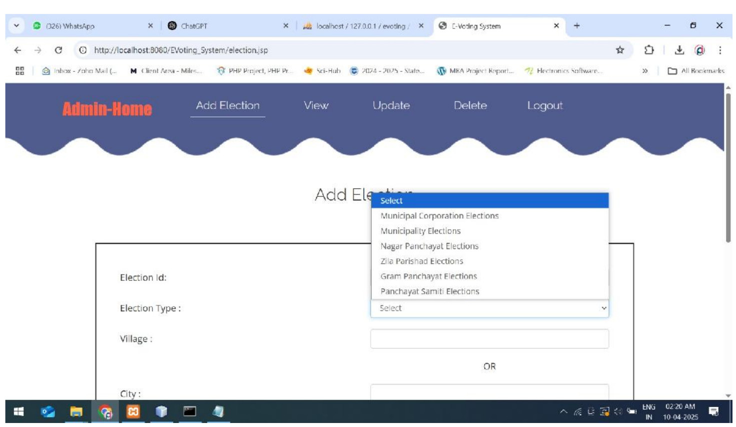


Fig.1 System Architecture

IV. RESULT

The proposed blockchain-based electronic voting system successfully demonstrates a secure, transparent, and tamper-proof framework for conducting digital elections. By integrating a Permissioned Blockchain with the Proof of Authority (PoA) consensus mechanism, the system ensures efficient and distributed validation of votes without relying on centralized control. Voter authentication is fortified using multi-factor methods, reducing the risk of identity fraud and unauthorized access. Smart contracts automate key election processes such as candidate registration, vote casting, and result tallying, thereby minimizing human errors and enhancing process transparency. The immutability of blockchain records guarantees that once votes are cast, they cannot be altered or deleted, significantly boosting trust among voters.

Performance evaluations and simulations show that the system is not only secure but also scalable, capable of handling a large number of voters without performance degradation. The use of lightweight cryptographic protocols and PoA consensus ensures low latency and high throughput, making it suitable for real-time vote processing in large-scale elections. Error-handling mechanisms are built into the smart contracts, providing fault tolerance and ensuring smooth recovery from system failures. Overall, the system proves effective in addressing the shortcomings of traditional e-voting platforms by offering a robust, verifiable, and user-friendly alternative that could help redefine the future of democratic processes.



IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 13, April 2025
Impact Factor: 7.67

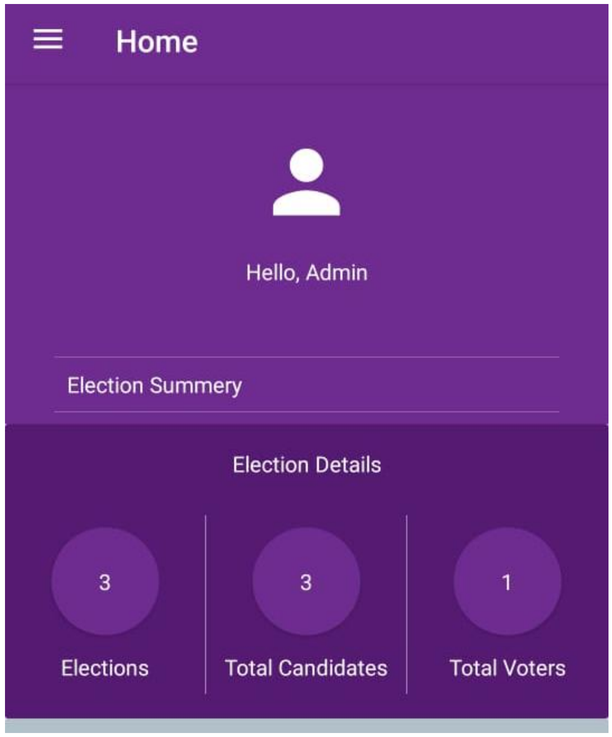


Fig.2 Results

V. CONCLUSION

In summary, the issues of security, transparency, and tampering threats that plague conventional voting techniques are addressed by blockchain-based electronic voting systems. The decentralized and unchangeable characteristics of blockchain technology can be used by these systems to protect voter privacy, stop fraud, and boost electoral process confidence. Even while issues with scalability, privacy, and interaction with current infrastructure still exist, these could be resolved with further developments in blockchain technology. The future of safe and transparent elections around the world may therefore be significantly shaped by blockchain-based electronic voting.

REFERENCES

[1]. Xia, Q., et al., "Blockchain-Based Data Sharing for Electronic Medical Records in Cloud Environments," IEEE Transactions on Cloud Computing, 2019.

[2]. Yang, J., et al., "An Integrated Blockchain-Based System for Secure Data Sharing and Trading in Multi-Level IoT," IEEE Internet of Things Journal, 2020.

[3]. Hasan, M. A., & Salah, K., "Blockchain-Based Proof of Delivery of Physical Assets with Single and Multiple Transporters," IEEE Access, 2018.

[4]. Xie, X., et al., "Blockchain for Cloud Exchange in Internet of Things," IEEE Transactions on Industrial Informatics, 2022.

[5]. Yu, H., et al., "Decentralized Privacy-Preserving Voting System Based on Blockchain Technology," ACM Transactions on Internet Technology, 2021.

[6]. Nakamoto, S., "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008.

[7]. Buterin, V., "A Next-Generation Smart Contract and Decentralized Application Platform," Ethereum Whitepaper, 2013.

[8]. Wang, X., et al., "Secure Electronic Voting System Based on Blockchain Technology," International Journal of Computer Applications, 2020.

IJARSCT

International Journal of Advanced Research in Science, Communication and Technology

International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal

ISSN: 2581-9429 Volume 5, Issue 13, April 2025 Impact Factor: 7.67

[9]. Kuo, T., et al., "Blockchain Application in E-Voting Systems," International Journal of Computer Science and Network Security, 2019.

[10]. Atzei, N., et al., "A Survey of Attacks on Ethereum Smart Contracts," 2017.

[11]. Christidis, K., & Devetsikiotis, M., "Blockchains and Smart Contracts for the Internet of Things," IEEE Access, 2016.

[12]. Androulaki, E., et al., "Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains," 2018.

[13]. Kshetri, N., "1 Blockchain's Roles in Meeting Key Supply Chain Management Objectives," International Journal of Information Management, 2018.

[14]. Zhang, Y., et al., "A Survey on Blockchain-Based E-Voting System," IEEE Access, 2019.

[15]. Zhou, Y., et al., "A Blockchain-Based Voting System for Secure Elections," International Journal of Network Security, 2021.

[16]. Dinh, T. T. A., et al., "Blockchaining the Internet of Things: A Survey," IEEE Access, 2017.

[17]. Alharby, M., & Hossain, M. A., "Blockchain-Based Voting System: A Survey," IEEE Access, 2020.

[18]. Bahga, A., & Madisetti, V. K., "Blockchain Applications: A Hands-On Approach," VPT Publishing, 2017.

[19]. Liskov, B., et al., "Decentralized Governance on Blockchain," IEEE Transactions on Industrial Informatics, 2020.

[20]. Di Pietro, R., et al., "Blockchain-Based Authentication and E-Voting Systems," International Journal of Computer Applications, 2021.

[21]. Kokkodis, M., & Iamnitchi, A., "Blockchain Applications in the Internet of Things," IEEE Internet of Things Journal, 2019.

[22]. Tapscott, D., & Tapscott, A., "Blockchain Revolution: How the Technology Behind Bitcoin and Other Cryptocurrencies is Changing the World," Penguin, 2016.

[23]. Kumar, R., et al., "Blockchain and Smart Contracts for Secure Data Management in IoT," IEEE Internet of Things Journal, 2019.

[24]. Rosado, D., et al., "Blockchain-Based Framework for Secure E-Voting Systems," International Journal of Information Security and Privacy, 2020.

[25]. Guo, L., et al., "A Blockchain-Based Secure E-Voting System with Privacy Protection," Journal of Computer Science and Technology, 2020.

[26]. Sweeney, L., et al., "Blockchain as a Service: Applications in E-Governance and Digital Elections," IEEE Transactions on Cloud Computing, 2021.

[27]. Yang, Y., et al., "Secure E-Voting System Using Blockchain," 5th International Conference on Blockchain Technology, 2020.

[28]. Bai, J., et al., "Scalable Blockchain-Based E-Voting System," International Journal of Blockchain Computing, 2021.

[29]. Zhang, W., et al., "Blockchain-Based E-Voting for Secure and Transparent Elections," Journal of Information Technology, 2020.

[30]. Zhang, Y., & Wang, J., "Blockchain for E-Governance and E-Voting," Journal of Internet Technology, 2021