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 10, April 2025
Impact Factor: 7.67

Design and Implementation of a Blockchain-Based E-Voting System with Enhanced Voter Authentication

Prof. R. C. Dumbre, Dr. Sunil S. Khatal, Sumit Sunil Gawali,
Sambhaji Eknath Avhad, Sanket Vitthal Doke
Department of Computer Engineering
Sharadchandra Pawar College of Engineering, Otur (Dumbarwadi), Junnar, Pune

Abstract: *Focusing on tackling important issues such security, transparency, and voter confidence, this paper investigates the improvement of e-voting systems by means of blockchain technology. Using 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, safe voter identification utilizing multi-factor approaches, and immutable vote recording to eradicate vulnerabilities such identity fraud and vote tampering. Furthermore enhancing system dependability and usefulness are scalability enhancements and error-handling systems. By tackling constraints in current e-voting systems, this paper emphasizes blockchain's ability to transform digital democracy by offering a scalable, transparent, and safe framework for next election procedures*

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

I. INTRODUCTION

One essential component of democracy is voting, which gives people the ability to voice their thoughts on important issues and influence national destiny. Traditional voting procedures, such as using paper ballots, have proven popular over time due to their dependability and simplicity. But they frequently struggle with inefficiencies, logistical issues, and fraud vulnerability. Electronic voting (e-voting) systems became a viable alternative with the development of technology, providing speedier results, scalability, and ease. Notwithstanding these advantages, e-voting systems still have a lot of trouble satisfying the strict security, confidentiality, transparency, and verifiability standards that are essential to preserving political integrity and voter trust.

Reliance on centralized authority or reliable third parties is one of the main drawbacks of traditional electronic voting methods. Concerns about voter privacy protection and the validity and integrity of election results are brought up by this dependence. Security flaws including vote tampering, identity theft, and system breaches have made it more difficult for e-voting to become widely used. Blockchain technology, a decentralized and unchangeable ledger system, has emerged as a game-changing remedy for updating electronic voting procedures in response to these worries.

Decentralization, transparency, and immutability are intrinsic qualities of blockchain technology that make it a prime contender to address the security and trust concerns related to electronic voting systems. By doing away with the necessity for centralized authorities, blockchain improves voter anonymity and data integrity. Modern cryptographic techniques like blind signatures, homomorphic encryption, and zero-knowledge proofs bolster security even more, guaranteeing that votes are verifiable and private without jeopardizing voter privacy. Important issues including vote tampering, multiple voting, and illegal access are addressed by these developments.

In order to provide secure and decentralized electoral procedures, recent research has suggested combining blockchain technology with electronic voting systems. Despite their potential, these initiatives frequently have scalability, efficiency, and usability issues, especially during major elections. Blockchain-based electronic voting has been shown

DOI: 10.48175/568

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 10, April 2025
Impact Factor: 7.67

to be feasible by existing protocols, including the one created by J.P. Cruz and Y. Kaji, however there are still issues with performance and usability. These difficulties demonstrate the need for a more reliable and scalable system that can manage the intricacies of actual elections while upholding high standards of security and dependability.

Through the creation of an enhanced blockchain-based electronic voting system, the proposed study seeks to overcome these constraints. Utilizing a Proof of Authority (POA) consensus mechanism in conjunction with a Permissioned Blockchain infrastructure, the system maintains high efficiency while guaranteeing decentralized vote validity. Secure multi-factor voter authentication, candidate selection powered by smart contracts, and tamper-proof vote recording are essential elements. By addressing vulnerabilities like identity theft, vote tampering, and data breaches, the system offers an electoral process that is transparent and auditable.

In addition to helping to create a safe and trustworthy electronic voting system, this study opens the door for further developments in digital democracy. In order to provide free, fair, and reliable elections in the digital age, the suggested framework intends to revolutionize electoral procedures by utilizing blockchain technology and cutting-edge cryptographic methodologies. The study's creative methodology demonstrates how blockchain technology might address significant e-voting issues while striking a balance between security, scalability, and user-friendliness, ultimately promoting more trust in democratic institutions around the globe.

I. OBJECTIVE

1. To research current blockchain-based electronic voting methods and their drawbacks.
2. To research and enhance the security of the electronic voting protocol developed by J.P. Cruz and Y. Kaji.
3. To research how cutting-edge cryptography methods can be included for voter privacy.
4. To investigate how scalable private blockchain technology is for major elections.
5. Investigating methods to improve system dependability and avoid double voting

II. LITERATURE SURVEY

1. ElectAnon: A Blockchain-Based, Anonymous, Robust and Scalable Ranked-Choice Voting Protocol

Authors: Ceyhun Onur, Arda Yurdakul

Published: March 2022

Overview:

ElectAnon introduces a ranked-choice voting protocol that emphasizes voter anonymity, system robustness, and scalability. It employs zero-knowledge proofs to ensure anonymous vote casting and utilizes timed-state machines to eliminate direct control by authorities during the voting process. The protocol also features a candidate proposal system and modular tallying libraries.

Key Contributions:

- Ensures voter anonymity through zero-knowledge proofs.
- Enhances robustness by removing direct authority control.
- Achieves scalability with up to 89% reduction in gas consumption compared to previous works.

Limitations:

- Implementation complexity due to advanced cryptographic techniques.
- Potential challenges in integrating with existing electoral infrastructures.

2. SBvote: Scalable Self-Tallying Blockchain-Based Voting

Authors: Ivana Stančíková, Ivan Homoliak

Published: June 2022

Overview:

SBvote presents a self-tallying voting protocol designed for scalability and privacy. It leverages smart contracts on platforms like Gnosis and Harmony to facilitate large-scale elections. The system allows voters to independently verify election results without compromising privacy.

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 10, April 2025
Impact Factor: 7.67

Key Contributions:

- Implements a self-tallying mechanism for verifiable results.
- Demonstrates scalability suitable for elections with millions of voters.
- Maintains voter privacy without relying on a central authority.

Limitations:

- Scalability is dependent on the throughput of the underlying blockchain platform.
- Requires voter familiarity with blockchain interactions.

3. Chirotonia: A Scalable and Secure e-Voting Framework based on Blockchains and Linkable Ring Signatures
Authors: Antonio Russo, Antonio Fernández Anta, Maria Isabel González Vasco, Simon Pietro Romano
Published: November 2021
Overview:
Chirotonia proposes an e-voting framework that combines blockchain technology with linkable ring signatures to ensure voter anonymity and prevent double voting. The system uses smart contracts to manage the voting process and is designed to scale for large electorates.
Key Contributions:

- Employs linkable ring signatures for voter anonymity and double-vote prevention.
- Utilizes smart contracts for transparent and tamper-proof vote management.
- Designed to scale efficiently for large-scale elections.

Limitations:

- The complexity of ring signature schemes may pose implementation challenges.
- Requires careful management of cryptographic keys to maintain security.

4. A Privacy-Preserving Blockchain-based E-voting System
Authors: Arnab Mukherjee, Souvik Majumdar, Anup Kumar Kolya, Saborni Nandi
Published: July 2023
Overview:
This paper presents a blockchain-based e-voting system focusing on security and voter privacy. It addresses vulnerabilities in traditional electronic voting machines by integrating cryptographic techniques to ensure vote confidentiality and system integrity.
Key Contributions:

- Enhances voter privacy through cryptographic methods.
- Provides a tamper-proof and auditable voting process.
- Demonstrates a prototype implementation on the Ethereum platform.

Limitations:

- Ethereum's transaction fees and scalability issues may affect practicality.
- The system's reliance on blockchain may pose accessibility challenges for non-technical users.

5. A New Era of Elections: Leveraging Blockchain for Fair and Transparent Voting
Authors: Suniti Chouhan, Gajanand Sharma
Published: February 2025
Overview:
This study introduces a blockchain-based voting system that incorporates advanced voter identity verification methods, including Aadhaar and driving license validation, biometric fingerprint authentication, and a picture rotation pattern. The system aims to enhance election security, transparency, and integrity.

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 10, April 2025
Impact Factor: 7.67

Key Contributions:

- Integrates multi-layered identity verification techniques.
- Utilizes blockchain's immutable ledger for secure vote recording.
- Aims to reduce impersonation risks and unauthorized vote alterations.

Limitations:

- Dependence on national identity databases may raise privacy concerns.
- Implementation complexity due to multiple authentication layers.

III. WORKING OF PROPOSED SYSTEMS

The layered architecture of the blockchain-based electronic voting system and the integration of multiple modules that are intended to handle important issues like voter privacy, security, scalability, and transparency provide insight into how the system operates. Each step of the election process is managed securely and effectively thanks to the system's multi-layered design.

The User Interface Layer, at the center of the system, offers voters a smooth experience on both desktop and mobile platforms. Users are guided through the registration, voting, and feedback processes with ease because to the user-friendly design. Voters engage with the Application Layer after gaining access to the system, which manages essential features including vote recording, authentication, and result computation. For immutability and transparency, this layer is in charge of making sure that every vote is safely recorded and sent to the blockchain.

The foundation of the security concept for the system is the Blockchain Layer. To guarantee that a vote cannot be changed or tampered with after it has been cast, votes are handled here as transactions that are documented on a decentralized blockchain. Blockchain offers transparency and tamper-proofing by providing an unchangeable record of every vote cast. By doing this, the privacy of individual voters is protected while the election results may be confirmed. In order to support the blockchain, the Database Layer handles auxiliary data, such voter credentials and session information, which are safely stored in a SQL database. Meanwhile, the Network Layer makes sure that all communication between the levels is secure by encrypting it using protocols like HTTPS.

The system's architecture takes into account important concerns like privacy and scalability. Through identity verification against a central government database, the User Registration Module prevents fraudulent registrations and guarantees that only registered voters may cast ballots. The Voting Module enables voters to cast their ballots in a secure manner, documenting each vote as a distinct blockchain transaction and guaranteeing vote anonymity through encryption. The confirmation that their vote has been recorded is sent to voters in real time. Votes from the blockchain are automatically compiled by the Result Computation Module, enabling real-time result computation and verification. It creates audit trails and checks for inconsistencies in the outcomes to guarantee accuracy.

Election authorities have access to extensive tools for overseeing the election process through the Administrator Module. Election setup, voter administration, and real-time activity monitoring are all within the administrator's purview. In order to guarantee election security throughout the procedure, this module additionally offers methods for identifying irregularities. In order to provide a tamper-proof trail for auditing purposes, the Audit and Security Module makes sure that every operation made within the system is permanently recorded. The system is protected from cyberattacks by multi-layered security measures including firewalls and encryption, and its resilience against new threats is guaranteed by frequent security audits.

All things considered, this blockchain-based electronic voting system integrates state-of-the-art technologies to improve the electoral process's efficiency, security, and transparency. Blockchain's decentralized structure guarantees tamper-proof voting, and strong cryptographic methods protect voter anonymity. By combining multiple modules for registration, voting, result calculation, administration, and auditing, the system provides a complete answer to the problems that conventional and current e-voting systems confront.

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 10, April 2025
Impact Factor: 7.67

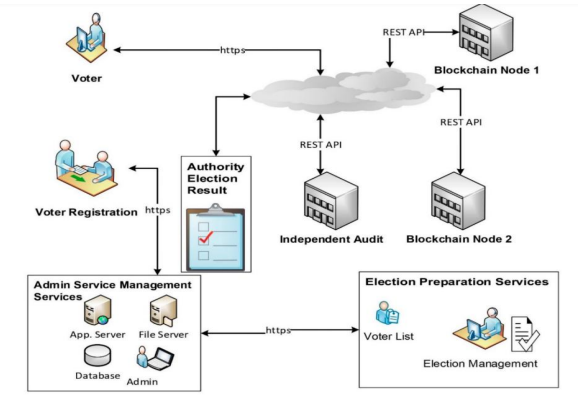
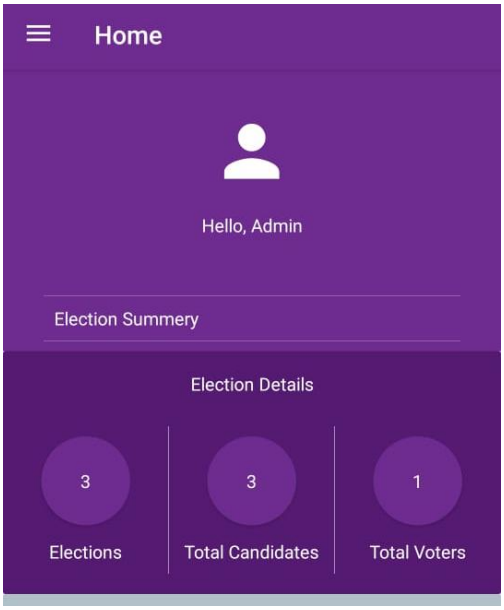


Fig.1 System Architecture

IV. RESULTS

For conducting digital elections, the suggested blockchain-based electronic voting system effectively illustrates a safe, open, and impenetrable architecture. The Proof of Authority (PoA) consensus mechanism and a Permissioned Blockchain are integrated in the system to guarantee distributed and effective vote validation without depending on centralized control. Multi-factor authentication of voters lowers the possibility of identity theft and illegal access. Key election procedures including voter registration, vote casting, and result counting are automated by smart contracts, which reduces human error and increases process transparency. The immutability of blockchain records ensures that votes cannot be changed or removed once they are cast, thereby increasing voter trust.

The system is scalable and secure, able to accommodate a high number of voters without experiencing any performance issues, according to simulations and performance evaluations. It is appropriate for real-time vote processing in large-scale elections because it uses PoA consensus and lightweight cryptographic protocols, which guarantee low latency and high throughput. The smart contracts provide error-handling features that supply fault tolerance and facilitate a seamless recovery from system malfunctions. In general, the system works well to overcome the drawbacks of conventional electronic voting platforms by providing a strong, verifiable, and easy-to-use substitute that may contribute to redefining democratic procedures in the future.



DOI: 10.48175/568

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 10, April 2025
Impact Factor: 7.67

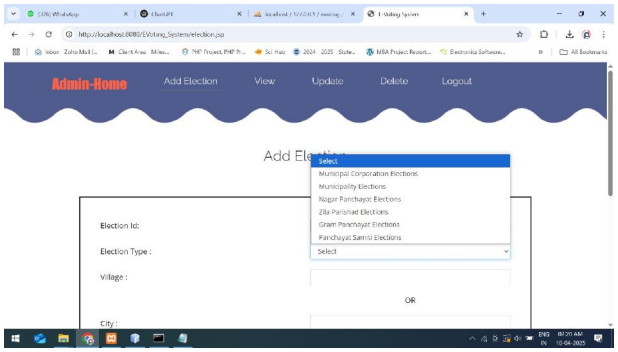


Fig.2 Results

V. CONCLUSION

In conclusion, the issues of security, transparency, and manipulation threats that traditional voting techniques have can be resolved with blockchain-based electronic voting systems. By utilizing the decentralized and unchangeable characteristics of blockchain technology, these systems can protect voter privacy, stop fraud, and boost confidence in the voting process. Even while scalability, privacy, and interaction with current infrastructure remain obstacles, these could be resolved with further developments in blockchain technology. Therefore, the development of safe and transparent elections around the world may be greatly influenced 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.
[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.

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 10, April 2025
Impact Factor: 7.67

[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