International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 09 Issue: 04 | April - 2025 SJIF Rating: 8.586 ISSN: 2582-3930

The Decentralized Voting System Using Blockchain

Vinit Todi, Ashutosh Sharma, Jill Prajapati, Gaurav Kulkarni

ITM (SLS) Baroda University
ITM (SLS) Baroda University
ITM (SLS) Baroda University
ITM (SLS) Baroda University

Abstract - This research paper presents a decentralized voting system leveraging blockchain technology to ensure security, transparency, and voter anonymity. By utilizing Ethereum smart contracts, IPFS for secure media storage, and role-based access control, this system mitigates risks associated with traditional voting mechanisms such as central authority control and fraud. Inspired by previous studies, including Khan et al. (2018), Li et al. (2020), and Sharma & Kumar (2021), our approach eliminates intermediaries, ensuring a tamper-proof and verifiable election process. This paper explores the problem statement, methodology, tools, challenges, and expected outcomes of the project.

Key Words: Blockchain, decentralized voting, Ethereum, smart contracts, IPFS, security, transparency.

1. INTRODUCTION

Voting is an essential component of decision-making in organizations and institutions. However, traditional voting systems, including paper-based and electronic solutions, face challenges related to security vulnerabilities, lack of transparency, and susceptibility to fraud. Blockchain technology has been widely proposed as a solution to these issues due to its decentralized and immutable nature. Studies such as those by Khan et al. (2018) and Berenjestanaki et al. (2024) emphasize how blockchain enhances electoral processes by providing a tamper-proof and transparent system. This paper proposes a blockchainbased voting system designed to ensure fair and verifiable elections within institutions and organizations.

2. PROBLEM STATEMENT

Current electronic and manual voting systems rely on centralized authorities, making them prone to manipulation and security threats. Many blockchain-based voting systems still depend on external authentication providers, limiting decentralization. Our system aims to address these challenges by:

- Eliminating centralized control through blockchain-based smart contracts.
- Ensuring voter anonymity and authentication without third-party verification.
- Providing an immutable, transparent voting process accessible to all participants.

3. OBJECTIVE

- Develop a fully decentralized voting platform using Ethereum smart contracts.
- Implement role-based access control for election administrators and voters.
- Integrate IPFS for secure storage of voter-related data and election records.
- Design a scalable and user-friendly UI to improve accessibility and engagement.
- Strengthen security using encryption protocols to prevent tampering.

4. Literature Review

Blockchain Technology and Its Application in Voting

Blockchain technology offers several crucial features like decentralization, cryptographic security, and transparency that make it an attractive candidate for re-engineering electronic voting systems. At its core, blockchain eliminates the requirement of central authority by distributing trust across a network of nodes. In a voting context, this means:

• **Security and Integrity:** Each vote is recorded as a transaction on a distributed ledger, making unauthorized alterations extremely difficult.
• **Transparency and Auditability**: Public ledgers allow stakeholders to verify the tally without compromising voter anonymity.
• **Smart Contracts**: Automated protocols can enforce voting rules and ensure that votes are counted accurately.

These attributes have driven a diverse body of research exploring how blockchain can be integrated into secure and transparent voting systems.

Review of Selected Research Papers

1. Kashif Mehboob Khan, Junaid Arshad, and Muhammad Mubashir Khan – Secure Digital Voting System based on Blockchain Technology

They explored the application of blockchain technology to enhance the security, transparency, and verifiability of electronic voting (e-voting) systems. Also, the authors proposed a blockchain-based e-voting system that leverages the cryptographic foundations of blockchain to address key challenges in e-voting, such as voter anonymity, vote integrity, and end-to-end verifiability. Key contributions include:

- **Blockchain Integration**: Proposed a blockchain-based e-voting system which took benefits of blockchain's cryptographic and decentralized features.
- **Double Voting Prevention**: Uses biometric authentication to ensure one-person, one- vote.
- **Receipt Freeness**: Stops voters from showing their voting choices to others.
- **Limitations:** The authors note that further research is required on "double voting" in e-voting system.

2. Berenjestanaki et al. (2024) – Blockchain- Based E-Voting Systems

The research by Berenjestanaki et al. (2024) highlights various important advantages of blockchain-based e- voting systems, which are commonly discussed in existing literature, such as:

- **Security**: Blockchain's immutability ensures that once a vote is recorded, it cannot be altered, giving a tamper-proof platform for voting. The study highlights that 88.89% of the reviewed papers emphasize security as a essential advantage.
- **Decentralization**: By distributing authority across a network, blockchain reduces the risk of centralized control and potential corruption.
- **Efficiency**: Blockchain can reduce the cost and time associated with traditional voting systems.

Although there are some limitations which are discussed in the paper, such as:

- **Security Threats**: Blockchain systems are vulnerable to various attacks, such as hash-based attacks, smart contract vulnerabilities, and private key leakage.
- **Scalability**: As the number of participants and transactions increases, blockchain systems face scalability issues.

3. Li et al. (2020) – Blockchain-based Electronic Voting System: A Survey

In this survey, Li and co-authors review various blockchain-based voting proposals. The paper categorizes existing systems based on their blockchain architectures and cryptographic methods. Key insights from the survey include:

- **Comparative Analysis**: The paper outlines the strengths and weaknesses of different approaches, providing a valuable reference for subsequent research.
- **Identification of Challenges**: Issues such as scalability, user adoption, and regulatory acceptance are highlighted as major hurdles.
- **Future Research Directions**: Developing more efficient algorithms and layer-2 scaling solutions is critical for handling large scale elections. Moreover, designing user friendly interfaces and ensuring accessibility for all voters is essential aspects.

4. Khan et al. (2018) – Secure Digital Voting System based on Blockchain Technology

The author proposed a paper on "secure digital voting system" which leverages the cryptographic foundation of blockchain in order to achieve end to end verifiability and vote integrity. Their work includes:

- **E-Voting Requirements:** The paper signifies variety of requirements in order to fulfil the basic demands like privacy, eligibility criteria, and receipt freeness.
- **Related Works**: The paper reviews many existing e-voting systems and protocols, highlighting their strengths and limitations such as Self-Tallying Voting Systems (by Kiayias and Yung (2002)), Two Round Protocols (by Hao et al. (2010)) and many more.

The author also references other significant e-voting systems, including Helios (Adida, 2008), Bingo Voting (Bohli et al., 2007), and Star-Vote (Bell et al., 2013), which have played a role in advancing secure and verifiable e-voting systems.

5. Sharma & Kumar (2021) – Enhancing Electronic Voting with Blockchain: Challenges and Opportunities

Focusing on practical implementation, Sharma and Kumar explore both the technical and regulatory challenges of deploying blockchain-based voting systems. Their analysis includes:

- **Trade-Off Analysis**: A discussion on balancing transparency with voter privacy, including the inherent trade-offs.
- **Scalability and Performance**: Checking how different blockchain platforms perform under high transaction volumes typical in national elections.
- **Policy and Regulatory Issues**: Addressing the legal and institutional challenges that must be overcome before such systems can be widely adopted.

Their work is particularly useful for policymakers and technologists seeking to understand the broader implications of blockchain in electoral contexts.

5. Proposed Solution/Methodology

The proposed decentralized voting system consists of the following components:

1. **Frontend:** React.js and Next.js for an intuitive voting interface.
2. **Blockchain Backend:** Ethereum-based smart contracts for secure vote recording.
3. **IPFS Storage:** Secure, decentralized storage for voter registration records and election data.
4. **Role-Based Access Control:** Security features to prevent unauthorized actions in the election process.

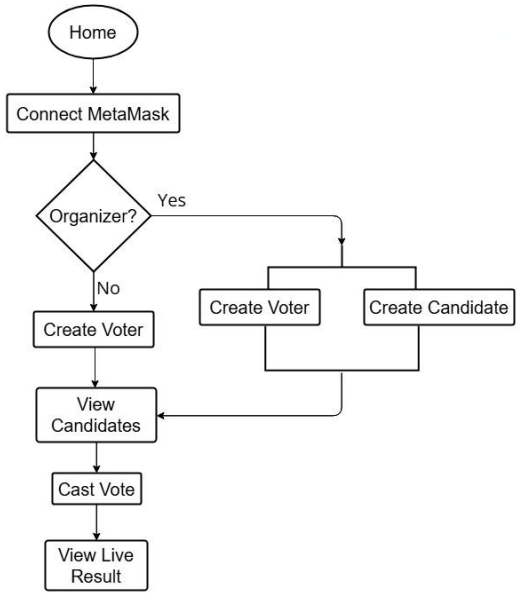
Tools and Technologies:

- **Frontend:** React.js, Next.js
- **Backend:** Ethereum Smart Contracts (Solidity), Web3.js
- **Storage:** IPFS for decentralized and tamper-proof election records.
- **Security:** Wallet-based authentication, Smart contract access control, Role-based permissions (Admin, Voter), IPFS content addressing for data integrity.
- **Testing and Deployment:** Hardhat

System Architecture:

1. Voters register via the decentralized application (DApp), ensuring privacy and authentication through smart contracts.
2. Election administrators set up voting events using blockchain-based rules.
3. Votes are cast and stored immutably on the Ethereum blockchain.
4. Results are automatically tallied and publicly verifiable through blockchain explorers.

Flowchart:



6. Security and Privacy Measures

To enhance security and maintain voter privacy, the system implements:

- **Immutable Voting Records:** All votes are permanently stored on the blockchain and cannot be altered.
- **Decentralized Authentication:** Eliminating reliance on third-party verification mechanisms.
- **End-to-End Encryption:** Ensuring that voter identities and choices remain confidential throughout the election process.

7. Challenges and Expected Outcomes

Challenges:

- Ensuring **scalability** for elections with a high number of participants.

- Reducing **gas fees** associated with Ethereum-based smart contract transactions.
- Balancing **transparency and voter privacy** while maintaining security.

Expected Outcomes:

- A fully functional, decentralized voting system offering transparent election processes.
- Reduction in administrative overhead and dependency on central authorities.
- A scalable and user-friendly platform suitable for institutional elections.

8. Conclusions and Future Work

This research presents a blockchain-based voting system designed to improve security, transparency, and accessibility in institutional elections. By leveraging Ethereum smart contracts and IPFS storage, our approach eliminates central control, enhances voter privacy, and ensures election integrity. Future improvements may include:

- **Scalability enhancements**, such as integrating layer-2 solutions to reduce Ethereum transaction fees.
- **Biometric authentication integration** to further enhance voter verification.
- Enhance IPFS integration for faster document retrieval

REFERENCES

[1] Kashif Mehboob Khan, Junaid Arshad, and Muhammad Mubashir Khan. A Secure Digital Voting System based on Blockchain Technology.
[2] Berenjestanaki et al. (2024). A Blockchain-Based E-Voting Systems.
[3] Li, Y., Chen, G., & Li, X. (2020). Blockchain-based Electronic Voting System: A Survey.
[4] Khan et al. (2018). A Secure Digital Voting System based on Blockchain Technology.
[5] Sharma, K., & Kumar, S. (2021). Enhancing Electronic Voting with Blockchain: Challenges and Opportunities. IEEE Transactions on Engineering Management.