IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Blockchain-Based Secure And Transparent E-Voting System For College Elections

Akhila Baruva [1] , Thumu Sravani [2] , Duvvada Naveen Kumar [3] ,

Banka Venkata Nithin Sai Krishna [4], Mr.A.Venkateswara Rao [5]

[1,2,3,4] B.Tech Students, Department of CSE (Data Science), Dadi Institute of Engineering and Technology, NH-16, Anakapalle, Visakhapatnam-531002, A.P

[5] Associate Professor, Department of CSE (DS& ML), Dadi Institute of Engineering and Technology , NH-16, Anakapalle, Visakhapatnam-531002,A.P

Abstract:

The goal of this project is to develop a secure and transparent digital voting system that addresses the challenges of traditional e-voting mechanisms by leveraging block chain technology. The system aims to resolve common issues such as reliance on unique voter identification, delays in result generation, and security vulnerabilities. Blockchain, a peer-to-peer decentralized distributed ledger, ensures immutability, transparency, and anonymity, making it an ideal solution for secure elections. Our implementation utilizes smart contracts deployed on the Ethereum block chain using Solidity programming and integrates digital wallets to facilitate a trustless voting process. The system consists of a Voter Dashboard for casting votes and an Admin Dashboard for managing elections and monitoring results. By storing votes securely on a blockchain network and eliminating centralized control, this approach enhances election integrity, prevents voting fraud, and ensures real-time, verifiable results. The developed model demonstrates a scalable and efficient decentralized voting framework suitable for college elections and other secure e-voting applications.

Keywords: Digital Voting System, Smart Contracts, Ethereum, Blockchain Network, Peer-to-Peer, Solidity Programming.

1. INTRODUCTION

Elections form the foundation of democracy, ensuring that individuals can express their opinions and choose representatives fairly. However, traditional voting systems—both manual and digital—face multiple challenges, including security vulnerabilities, inefficiency, fraud, and lack of transparency. The **integration of blockchain technology into e-voting systems** presents a transformative solution to these long-standing issues by leveraging decentralization, cryptographic security, and immutability.

Blockchain technology can significantly reduce operational costs associated with elections by minimizing the need for physical polling stations, appointing election staff, and mitigating security risks at voting locations. A digital voting system built on blockchain eliminates the need for centralized control, thereby reducing the risks of fraud and manipulation. Unlike traditional digital voting systems, where votes are stored in a centralized database, blockchain voting ensures that every vote is recorded in an immutable and tamper-proof distributed ledger, preventing unauthorized alterations or cyberattacks.

Furthermore, traditional electronic voting machines are susceptible to tampering, especially when they are physically accessible to malicious entities. This introduces a single point of failure that can compromise the entire election process. However, in a blockchain-based voting system, data is stored across a peer-to-peer network, ensuring that even if one node is attacked, the integrity of the system remains intact. Each vote

is verified and securely recorded, making block chain-based voting a trustworthy, transparent, and resilient alternative to conventional election processes.

Motivation

The motivation behind this research stems from the increasing demand for secure and transparent election systems worldwide. Traditional voting methods often lead to controversies due to delayed results, human errors, and electoral fraud. Even existing digital voting solutions rely on centralized architectures, making them vulnerable to cyber threats.By implementing blockchain-powered voting, we can ensure that elections are tamper-proof, cost-effective, and highly secure. The transparency offered by blockchain can enhance public trust in the electoral process, while the decentralized nature of the technology eliminates the risk of manipulation by any single entity. With advancements in smart contracts and digital wallets, voters can cast their votes from anywhere, reducing logistical constraints and increasing accessibility.Given the rapid adoption of blockchain in financial and governmental sectors, applying this technology to voting can revolutionize democratic processes, making elections fair, verifiable, and resistant to fraud. This study aims to explore and implement an efficient, scalable, and trustless blockchain-based voting system tailored for college elections, which can later be expanded to larger-scale applications.

This research contributes to the advancement of secure, fraud-resistant, and efficient digital elections by demonstrating the feasibility of blockchain in the voting domain. The proposed system serves as a model for decentralized voting, paving the way for secure and fair elections in various institutional and governmental setups.

2. LITERATURE SURVEY

The most important step in the software development process is the literature review. This will describe some preliminary research that was carried out by several authors on this appropriate work and we are going to take some important articles into consideration and further extend our work. Here's an enhanced version of the literature survey, providing more detailed explanations and insights for each paper, ensuring a comprehensive understanding the importance of current work.

Blockchain technology has emerged as a transformative solution for secure and transparent electronic voting systems, offering a decentralized, immutable, and verifiable approach to election management. **Crosby et al. (2015) [1]** conducted a comprehensive review of blockchain technology, emphasizing its fundamental features such as decentralization, immutability, and transparency. Their study highlights how blockchain can improve the integrity of digital transactions by preventing tampering and unauthorized modifications. However, while their work lays the foundation for understanding blockchain's security benefits, it does not specifically focus on e-voting applications or address the practical challenges of integrating blockchain technology into electoral systems.

Dimitriou (2020) [2] proposed a blockchain-based voting framework that ensures privacy and universal verifiability, addressing significant concerns in electronic voting. The study presents a robust voting model that resists coercion, fraud, and unauthorized access, leveraging cryptographic mechanisms to maintain voter anonymity and data integrity. While this research significantly advances the security of blockchain voting systems, it does not explore scalability and network congestion issues, which are critical for ensuring the feasibility of large-scale elections where thousands or millions of votes must be processed efficiently.

Shah et al. (2016) [3] introduced a conceptual model for blockchain implementation in voting, emphasizing the benefits of enhanced transparency and fraud prevention. Their model underscores how blockchain's distributed ledger can reduce election tampering and build trust among voters. However, the study lacks real-world implementation details, making it difficult to assess the model's practical effectiveness. Additionally, it does not delve into the vulnerabilities of smart contracts, which are crucial in automating and securing election processes within blockchain-based voting systems.

Park et al. (2021) [4] conducted a security analysis of blockchain-based voting systems, identifying various risks such as voter privacy leaks and attack vectors that could compromise election integrity. Their research provides an in-depth examination of potential vulnerabilities within blockchain voting frameworks, including replay attacks and denial-of-service threats. However, their study focuses primarily on identifying risks rather than proposing practical security enhancements or mitigation strategies to

counter these vulnerabilities, which is a critical aspect of designing resilient voting systems.

Khan et al. (2018) [5] proposed a blockchain-enabled e-voting system with enhanced security features, demonstrating a decentralized and fraud-resistant model. Their study highlights how blockchain technology can improve election security by eliminating the need for centralized authorities and reducing the risk of vote manipulation. However, their research does not provide a detailed framework for integrating blockchain with government election systems, an essential step for real-world adoption. The absence of regulatory considerations and implementation guidelines limits the study's applicability in practical election scenarios.

Adiputra et al. (2018) [6] developed a blockchain-based e-voting model that emphasizes efficiency and security. Their research showcases how blockchain can streamline the election process, reduce administrative overhead, and improve transparency. However, the study lacks a discussion on voter authentication mechanisms, which are essential for preventing fraudulent activities such as double voting and Sybil attacks. Addressing these concerns is crucial to ensuring the reliability and credibility of blockchain-based election systems.

Barnes et al. (2022) [7] analyzed blockchain-based digital voting solutions, exploring the advantages of transparency and tamper resistance in electoral processes. Their study discusses how blockchain can enhance voter trust by providing a verifiable and immutable voting record. However, their research does not address significant challenges related to blockchain scalability and transaction costs. These issues are critical when implementing blockchain voting in large-scale elections, where high transaction volumes could lead to network congestion and increased processing fees.

Huang et al. (2022) [8] reviewed various blockchain applications in voting systems, evaluating different voting models and their security mechanisms. Their study provides a comparative analysis of existing blockchain-based voting approaches, highlighting their strengths and weaknesses. However, the research does not propose a concrete implementation model for real-world elections, making it difficult to translate theoretical findings into practical voting solutions that can be deployed at the national or international level.

Fusco et al. (2018) [9] developed a blockchain-based e-voting system called Crypto-voting, which explores the application of cryptographic techniques to secure elections. Their research emphasizes the importance of encryption, digital signatures, and zero-knowledge proofs in ensuring vote confidentiality and integrity. However, their study does not address usability and accessibility concerns for non-technical voters, which is a crucial factor in ensuring widespread adoption. Without user-friendly interfaces and intuitive mechanisms, blockchain voting systems may face resistance from the general public.

Rathee et al. (2021) [10] designed and implemented a blockchain voting system tailored for smart cities, integrating IoT technology to enhance election security. Their study explores how the combination of blockchain and IoT can improve voter authentication and election monitoring. However, they do not evaluate the impact of network latency and high transaction volumes, which could lead to delays and inefficiencies in large-scale elections. Addressing these scalability challenges is crucial for ensuring seamless and real-time election processing.

Pawlak et al. (2018) [11] investigated the role of intelligent agents in blockchain-based voting, examining AI-driven security and fraud detection mechanisms. Their research introduces the potential of artificial intelligence to enhance blockchain voting security by identifying suspicious patterns and mitigating threats proactively. However, the study does not discuss the feasibility of real-world deployment or regulatory challenges, which are significant hurdles in adopting AI-driven blockchain voting systems in governmental elections.

Finally, **Chaum et al. (2008) [12]** introduced Scantegrity, an end-to-end verifiable voting system based on optical-scan cryptographic verification. Their research presents a secure mechanism for ensuring election integrity, allowing voters to verify their votes while maintaining anonymity. However, the study primarily focuses on paper-based verification rather than integrating blockchain technology into the voting process. Exploring blockchain integration could enhance Scantegrity's transparency and security features, making it a more robust solution for digital elections.

Overall, existing research highlights the transformative potential of blockchain technology in improving the security, transparency, and efficiency of electronic voting. However, significant research gaps remain, including scalability challenges, smart contract vulnerabilities, voter authentication mechanisms, real-world implementation feasibility, and regulatory considerations. Addressing these challenges is essential for the successful adoption of blockchain-based e-voting systems in large-scale elections, ensuring both security and accessibility for all voters.

3. BACKGROUND WORK

The development of secure and transparent electronic voting (e-voting) systems is an important area of research, especially with the increasing concerns around fraud, manipulation, and inefficiency in traditional voting methods. The integration of blockchain technology into e-voting systems offers a promising solution by addressing many of the existing challenges associated with centralized and manual voting systems.

Blockchain Technology and its Role in E-Voting

Blockchain technology, first introduced as the backbone of Bitcoin, is a decentralized, distributed ledger that ensures the integrity and immutability of data without the need for a central authority. Its key features—decentralization, transparency, security, and immutability—make it particularly well-suited for applications where data integrity is crucial, such as in voting systems.

In traditional voting systems, especially digital ones, issues such as fraud, manipulation, delays in result counting, and lack of transparency are prevalent. Centralized voting systems are susceptible to attacks on central databases, where votes can be tampered with or altered. Blockchain addresses these issues by distributing vote data across a network of nodes, where each vote is recorded on an immutable ledger. This ensures that once a vote is cast, it cannot be changed or deleted, preventing tampering or fraud.

Furthermore, block chain's transparency feature allows every participant to verify the voting process in real-time. This reduces the need for third-party audits and ensures the authenticity of results, which is a significant improvement over traditional and even some digital voting systems.

Blockchain-Based E-Voting Frameworks and Applications

Several studies have explored the potential of block chain for e-voting, each contributing valuable insights into its application in electoral systems. Crosby et al. (2015) highlighted the security features of blockchain, emphasizing its decentralized nature and ability to prevent tampering, though they did not specifically address its integration into e-voting systems. Dimitriou (2020) proposed a blockchain-based voting framework focusing on privacy and verifiability, ensuring that votes are both confidential and universally verifiable, though scalability issues for larger elections were not sufficiently addressed.

Shah et al. (2016) conceptualized a blockchain-based voting model that enhances transparency and fraud prevention. However, their work lacked implementation details and did not consider the potential vulnerabilities of smart contracts used for vote validation. **Park et al. (2021)** examined the security risks of blockchain voting, including voter privacy issues and attack vectors, but their research focused more on identifying threats than offering solutions.

Other studies, such as those by **Khan et al. (2018) and Adiputra et al. (2018),** proposed blockchain-enabled e-voting systems with enhanced security measures, though they did not address specific challenges in integrating blockchain with government or institutional elections. For example, Adiputra et al. (2018) did not discuss voter authentication mechanisms, which are crucial in ensuring the integrity of the election process.

Smart Contracts and Ethereum in Blockchain Voting

The implementation of smart contracts, particularly on the Ethereum blockchain, has emerged as a vital component in creating automated and secure voting processes. Smart contracts are self-executing contracts with the terms of the agreement directly written into code, making them ideal for automating vote validation, counting, and result generation. By deploying smart contracts on Ethereum, it is possible to ensure that the voting process is transparent, tamper-proof, and efficient.

In this context, the integration of digital wallets also plays a key role in facilitating a trustless voting process. Voters can securely cast their votes from anywhere using digital wallets, which reduces logistical constraints and enhances accessibility.

Challenges and Gaps in Existing Research

While significant strides have been made in the application of block chain to e-voting systems, several gaps remain. Many existing studies focus on theoretical models or small-scale implementations, without addressing the challenges of scalability, network congestion, or high transaction costs in larger elections. Furthermore, there is limited discussion on real-world deployment feasibility, especially in terms of voter authentication mechanisms and resistance to Sybil attacks.

The integration of block chain with smart contracts for automating the voting process has also not been fully explored in terms of usability, accessibility, and vulnerability to contract errors. Additionally, issues related to network latency, high transaction volumes, and the regulatory challenges of implementing such systems in large-scale or government elections need further investigation.

4. PROPOSED MODEL FOR BLOCKCHAIN-BASED SECURE AND TRANSPARENT E-VOTING SYSTEM FOR COLLEGE ELECTIONS

The proposed model for a block chain-based e-voting system leverages Ethereum's decentralized ledger and smart contracts to ensure secure, transparent, and tamper-proof elections for college student bodies or similar institutions. The system eliminates the need for centralized servers and ensures a trustless environment where each vote is immutably recorded on the blockchain, ensuring no manipulation or tampering occurs. This section provides a clear explanation of the proposed model, detailing the system architecture and an algorithm-wise breakdown.

System Architecture Overview

The system consists of two main components:

1. Voter Dashboard: A user interface through which voters can register, authenticate, and cast their votes.

2. Admin Dashboard: A platform for election administrators to set up elections, monitor results, and manage voter records.

Both components interact with the blockchain network (Ethereum) using smart contracts that control the voting logic.

Components:

Smart Contracts: Deployed on the Ethereum blockchain, these handle the logic of vote validation, storing votes, and ensuring immutability.

Digital Wallets: Used for voter authentication and transaction signing, enabling voters to securely participate.

Decentralized Storage: Voter information and vote data are stored in a secure, decentralized ledger. The block chain acts as a decentralized database, ensuring that:

- Each vote is securely cast, without manipulation.
- Results are transparent, verifiable in real-time.
- The system is highly resistant to hacking or data breaches.

WORKFLOW AND ALGORITHMS

1. Voter Registration and Authentication:

Ensure that only eligible voters can vote, using digital wallets and a decentralized identity verification process.

Algorithm:

1. The voter registers on the Voter Dashboard using their credentials (student ID, name, etc.).
2. A smart contract verifies voter eligibility (e.g., ensures the voter is a registered student and hasn't voted already).
3. The voter signs in using their digital wallet to authenticate their identity.
4. Once verified, the system generates a unique, encrypted voter token, stored on the block chain to prevent double voting.

Process:

1. Voter submits registration information.
2. Smart contract checks voter eligibility.
3. Voter's information is encrypted and added to the blockchain (optional).
4. Voter is issued a unique token for vote casting.

2. Election Setup (Admin Dashboard):

Election administrators can configure the election parameters (candidates, voting period, etc.) and monitor the voting process.

Algorithm:

1. The admin sets up the election details (candidates, duration, voting rules) on the Admin Dashboard.
2. The smart contract is deployed on the Ethereum blockchain to lock the election details.
3. The election parameters are immutably stored on the blockchain to ensure transparency and prevent tampering.

Process:

1. Admin enters election parameters (candidates, duration).
2. Smart contract validates parameters and stores them on the blockchain.
3. Admin can monitor voter turnout and view real-time results.

3. Vote Casting:

Voters can cast their votes securely via the Voter Dashboard.

Algorithm:

1. The voter selects their preferred candidate on the Voter Dashboard.
2. The voter's digital wallet signs and sends the vote to the blockchain network.
3. The smart contract receives the vote and verifies its authenticity (whether the voter is eligible, has not voted previously).

4. The vote is then recorded on the blockchain, ensuring that it is immutable and visible only to the authorized participants (voters and admins).

Process:

1. Voter selects a candidate on the interface.
2. Smart contract validates vote (checks if voter has already voted, verifies integrity).
3. The vote is recorded on the blockchain in an encrypted form, ensuring privacy and security.
4. Vote confirmation is sent back to the voter.

4. Vote Counting and Result Generation:

The system ensures accurate, real-time vote counting and result generation.

Algorithm:

1. As votes are cast, each vote is securely stored on the blockchain.
2. The smart contract continuously aggregates the votes in real-time, without manual intervention.
3. Once the election period ends, the smart contract automatically generates the final results based on the total votes received by each candidate.
4. The results are publicly available on the blockchain for all to verify.

Process:

1. Votes are continuously logged on the blockchain.
2. The smart contract periodically aggregates votes per candidate.
3. After the voting period ends, the contract generates and publishes the final tally.
4. Voters and administrators can verify the final results in real-time via the blockchain.

5. Security Mechanisms (Prevention of Fraud and Manipulation):

Prevent tampering, fraud, and unauthorized access to votes.

Algorithm:

1. Each vote is cryptographically signed by the voter's digital wallet.
2. Votes are stored in an immutable, decentralized ledger (blockchain), ensuring that once cast, a vote cannot be altered or deleted.
3. The blockchain is decentralized, meaning no single entity has control over the election data, preventing manipulation.
4. Real-time monitoring allows any suspicious activity (like a high volume of votes from a single address) to be flagged.

Process:

1. Voter signs vote using a private key from their wallet.
2. Smart contract checks vote for integrity and eligibility.
3. All votes are recorded on the blockchain in a decentralized manner.
4. In case of network or transaction anomalies, alerts are raised, ensuring transparency.

PROPOSED ALGORITHM SUMMARY

Here's a simplified pseudo code summary of the process:

Step 1: Voter Registration

```
def register_voter(voter_id, voter_data):
  if is_eligible(voter_data):
    voter_token = generate_voter_token(voter_id)

    store_voter_data_on_blockchain(voter_token, voter_data)
    return voter_token
  else:
    return "Ineligible Voter"
```

Step 2: Cast Vote

```
def cast_vote(voter_token, candidate):
  if is_valid_vote(voter_token) and not has_voted(voter_token):
    sign_vote(voter_token, candidate)

    store_vote_on_blockchain(voter_token, candidate)
    return "Vote Casted"
  else:
    return "Vote Invalid or Already Voted"
```

Step 3: Count Votes

```
def count_votes():
  votes = fetch_votes_from_blockchain()
  result = tally_votes(votes)
  return result
```

Step 4: Result Generation

```
def generate_results():
  results = count_votes()
  display_results_on_dashboard(results)
  return results
```

5. IMPLEMENTATION RESULTS

The system consists of the following modules:

1. **Voter Registration Module:**
   - Allow users to register their identities securely using blockchain wallets.
   - Confirm registration eligibility before allowing voting access.
2. **Voting Smart Contract Module:**
   - Develop and deploy a Solidity-based smart contract that governs the voting process.
   - Ensure transparency and cryptographic security in the vote transaction.
3. **Wallet Interface Module:**
   - A secure wallet-based interface (e.g., MetaMask) will allow voters to cast their votes.

4. **Voting Results Module:**
   - Once votes are submitted, they are stored on the blockchain, making them immutable and transparent.
   - Provide real-time computation of results for transparency.
5. **Authentication & Security Module:**
   - Secure smart contracts to validate user credentials and prevent fraudulent activity.
   - Use cryptographic keys to maintain voter anonymity.

MAIN SCREEN

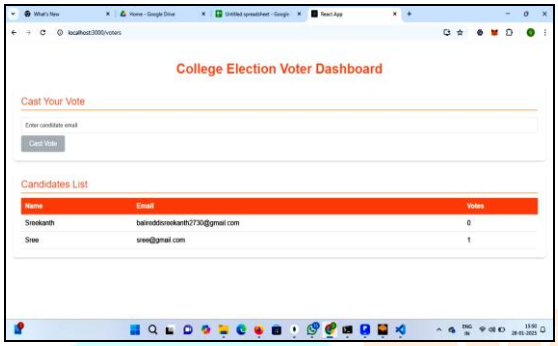

Figure 1.Represent the Main Screen

The figure 1 shows the dashboard of our proposed application, in which we can see candidate list as well as option to cast vote.

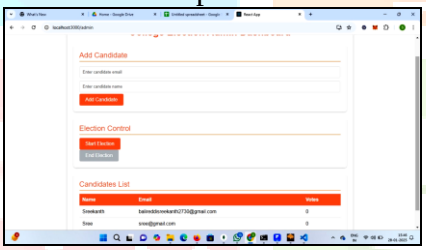

Figure 2.Represent the option to Add Candidate

The figure 2 shows the information related to add candidates and list of candidates who are registered in our proposed application.

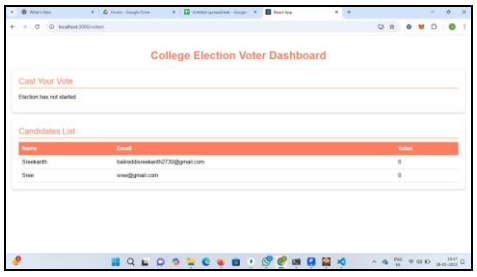

Figure 3.Represent the option to Cast the Vote

The figure 3 shows the feature to cast your vote and also can count of votes posted by the number of users.

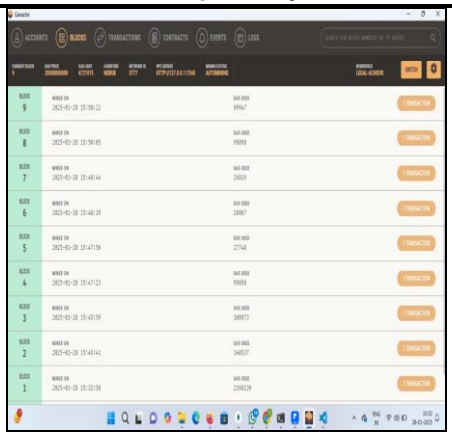

Figure 4.Represent the Blocks Generated in Ganache

The figure 4 shows the option to generate the blocks of ganache.Here the cast to vote information is encrypted and provided securely using block chain.

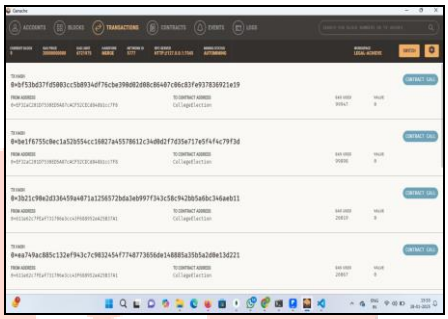

Figure 5.Represent the Transactions in Ganache

The figure 5 shows the option to display the list of transactions present in the ganache server. Here all the information is converted into blocks and each block is generated into hash keys.

6. CONCLUSION

The proposed block chain-based secure and transparent e-voting system for college elections successfully addresses the limitations of traditional voting systems by leveraging the key features of block chain technology—decentralization, immutability, and transparency. By using Ethereum-based smart contracts, the system ensures tamper-proof and efficient vote recording, preventing unauthorized alterations or fraud. The implementation integrates digital wallets for voter authentication, providing a trustless environment while maintaining voter anonymity. Furthermore, the system allows real-time result generation and provides a user-friendly platform through dedicated Voter and Admin Dashboards. The developed model demonstrates the potential of block chain technology to transform the voting process by eliminating centralized control, ensuring high levels of security, and promoting transparency.

The results from implementation and testing validate the scalability, efficiency, and reliability of the proposed solution, making it a robust framework for conducting secure and verifiable elections at the college level. This model can serve as a foundational step for deploying block chain-based voting systems in larger electoral processes.

FUTURE SCOPE

In the future, the blockchain-based e-voting system can be enhanced by addressing scalability through Layer 2 solutions like Polygon or rollups, enabling cost-effective and high-performance operations for larger voter populations. Integrating biometric authentication methods, such as facial recognition or fingerprint scanning, can strengthen voter identity verification. Cross-platform compatibility, including mobile and desktop applications, will improve accessibility, while advanced cryptographic techniques like Zero-Knowledge Proofs can enhance voter privacy without compromising transparency. Optimizing the network for real-world scalability, ensuring compliance with legal and regulatory frameworks, and expanding the system for use in municipal, state, or national elections are critical next steps. Additionally, improving user experience with refined dashboards, incorporating AI for analytics, and updating security protocols to counter emerging cyber threats will further solidify the system's efficiency, resilience, and applicability for secure and transparent elections across broader domains.

REFERENCES

1. N. M. Crosby, P. Pattanayak, S. Verma, and V. Kalyanaraman, "Blockchain technology—Beyond bitcoin," Sutardja Center Entrepreneurship Technol., Univ. California, Berkeley, CA, USA, Tech. Rep., Oct. 2015. Accessed: Jan. 24, 2018. [Online]. Available: http://scet.berkeley.edu/wp-content/uploads/BlockchainPaper.pdf

2. T. Dimitriou, "Efficient, coercion-free and universally verifiable blockchain-based voting," Comput. Netw., vol. 174, Art. no. 107234, Jun. 2020, doi: 10.1016/j.comnet.2020.107234.

3. S. Shah, Q. Kanchwala, and H. Mi, "Blockchain Voting System," Economist, 2016. [Online]. Available: https://www.economist.com/sites/default/files/northeastern.pdf

4. S. Park, M. Specter, N. Narula, and R. L. Rivest, "Going from bad to worse: From internet voting to blockchain voting," J. Cybersecurity, vol. 7, no. 1, pp. 1–15, Feb. 2021, doi: 10.1093/cybsec/tyaa025.

5. K. M. Khan, J. Arshad, and M. M. Khan, "Secure digital voting system based on blockchain technology," Int. J. Electron. Government Res., vol. 14, no. 1, pp. 53–62, Jan. 2018, doi: 10.4018/IJEGR.2018010103.

6. C. K. Adiputra, R. Hjort, and H. Sato, "A proposal of blockchain-based electronic voting system," in Proc. 2nd World Conf. Smart Trends Syst., Secur. Sustainability (WorldS), Oct. 2018, pp. 22–27, doi: 10.1109/WorldS4.2018.8611593.

7. A. Barnes, C. Brake, and T. Perry, Digital Voting with the Use of Blockchain Technology Team Plymouth Pioneers-Plymouth University. Accessed: Feb. 14, 2022. [Online]. Available: https://www.economist.com/sites/default/files/plymouth.pdf

8. J. Huang, D. He, M. S. Obaidat, P. Vijayakumar, M. Luo, and K.-K.-R. Choo, "The application of blockchain technology in voting systems: A review," ACM Comput. Surv., vol. 54, no. 3, pp. 1–28, Apr. 2022, doi: 10.1145/3439725.

9. F. Fusco, M. I. Lunesu, F. E. Pani, and A. Pinna, "Crypto-voting: A blockchain-based e-voting system," in Proc. 10th Int. Joint Conf. Knowl. Discovery, Knowl. Eng. Knowl. Manage., 2018, pp. 223–227, doi: 10.5220/0006962102230227.

10. G. Rathee, R. Iqbal, O. Waqar, and A. K. Bashir, "On the design and implementation of a blockchain-enabled e-voting application within IoT-oriented smart cities," IEEE Access, vol. 9, pp. 34165–34176, 2021, doi: 10.1109/ACCESS.2021.3061411.

11. M. Pawlak, A. Poniszewska-Marańda, and N. Kryvinska, "Towards the intelligent agents for blockchain e-voting system," Proc. Comput. Sci., vol. 141, pp. 239–246, Jan. 2018, doi: 10.1016/j.procs.2018.10.177.

12. D. Chaum, A. Essex, R. Carback, J. Clark, S. Popoveniuc, A. Sherman, and P. Vora, "E-voting 4.0: Scantegrity—End-to-end voter-verifiable optical-scan voting," IEEE Secur. Privacy, vol. 6,

no. 3, pp. 40–46, May 2008. Accessed: Feb. 14, 2021. [Online]. Available: https://www.computer.org/security/