Decentralized Voting

Athilakshmi S[1], Praveen Kumar G[2], Koushikan S[3], Perumal V[4], Jeeva J[5]
[1,2] Assistant professor, Dept. of CSE, Kamaraj College of Engg & Tech.., Virudhunagar, Tamil Nadu, India
[3,4,5] UG Student, Dept. of CSE, Kamaraj College of Engg & Tech.., Virudhunagar, Tamil Nadu, India

Abstract: **Democratic voting is a critical component of governance in any nation. Existing methods, such as paper ballots and electronic voting machines (EVMs), face several challenges, including lack of transparency, voter fraud, vote tampering, low voter turnout, and security vulnerabilities. The transition to a fully digital voting system has been hindered primarily by concerns over security and trustworthiness. Blockchain technology presents a promising solution to these issues by leveraging its decentralized, transparent, and immutable characteristics. This paper explores the potential of blockchain technology in designing a secure and transparent e-voting system. By utilizing smart contracts on the Ethereum blockchain, we demonstrate the development and testing of a prototype e-voting application. The system integrates features like limited token allocation to prevent duplicate voting, real-time verification, and a transparent tallying process. Additionally, the paper discusses the benefits and limitations of employing blockchain technology in e-voting while showcasing a practical web-based implementation. The findings highlight blockchain's ability to enhance security, transparency, and trust in electoral processes, paving the way for future advancements in this domain.**

Keywords: **E-voting, Smart-contracts, Blockchain, Ethereum**

1. INTRODUCTION

Blockchain technology has emerged as a revolutionary concept, gaining prominence with the introduction of Bitcoin, the first widely recognized cryptocurrency. Its decentralized architecture and ability to ensure transparency and security have made it a topic of significant interest across various domains. Initially developed to support cryptocurrency transactions, blockchain technology has evolved to offer applications far beyond financial systems. Its potential to securely store and manage sensitive information—such as personal assets, medical records, and government data—has opened new avenues for innovation.

One of the most promising applications of blockchain is in the realm of electronic voting (e-voting). As voting is a fundamental process in democratic systems, ensuring its integrity, transparency, and accessibility is paramount. Traditional voting methods, whether paper-based or electronic, face challenges such as vote tampering, lack of transparency, and logistical inefficiencies. Blockchain, with its inherent characteristics of decentralization, immutability, and cryptographic security, provides an opportunity to address these concerns.

This paper investigates the implementation of a blockchain-based e-voting system using Ethereum's smart contract framework. By leveraging blockchain, the proposed system aims to enhance trust and transparency in elections while mitigating vulnerabilities associated with traditional voting methods. Furthermore, this study highlights the practical considerations of integrating blockchain into voting processes and explores its limitations, providing a foundation for future advancements in secure and efficient e-voting systems.

2. OBJECTIVES

The following are the objectives of our work.

- Enhanced Data Capacity: Achieve a significant improvement in data storage density compared to traditional methods by utilizing colour encoding techniques.
- Versatile Shape Flexibility: Design adaptable systems capable of functioning effectively across varying shapes and dimensions to meet diverse application requirements.
- Expanded Application Scope: Explore and expand the potential applications of blockchain-based e-voting systems beyond traditional use cases, addressing areas like security and accessibility.

- Enhanced Security: Integrate advanced cryptographic features to safeguard the voting process, ensuring voter anonymity and data protection.
- Improved Transparency: Leverage blockchain's decentralized nature to guarantee transparency and eliminate risks of tampering or manipulation.
- User-Friendly Design: Create intuitive interfaces and tools that simplify the voting process for users, promoting wider adoption and participation.

3. METHODOLOGY

The methodology of our work is as discussed below:

3.1. System Architecture Design

The system was built using the MVC architecture:

Model: Managed user and vote data with MySQL.

View: Provided a web-based user interface.

Controller: Handled authentication and voting logic.

Blockchain ensured decentralization, transparency, and immutability.

3.2. Voter Registration and Authentication

Voters registered with unique credentials stored securely in a database.

Two-factor authentication (login and OTP) enhanced security.

3.3. Blockchain Integration

Smart contracts on Ethereum secured vote recording and prevented duplication.

Gas fees ensured transaction validity and incentivized miners.

3.4. Voting Process

Voters cast encrypted votes via the web app.

Blockchain's decentralized ledger ensured transparency and tamper resistance.

3.5. Result Compilation and Verification

Votes were tallied on-chain, with real-time results displayed.

Voters verified their votes using public keys.

3.6. Testing and Validation

The system was tested for security, transparency, and scalability. Scalability challenges for large elections were noted for future improvements.

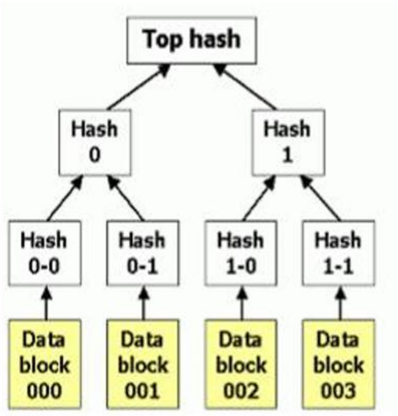

Figure I: The hash table

4. SYSTEM DESIGN

A flowchart is a visual representation of a process or algorithm, using standardized symbols to illustrate the sequence of steps and decisions involved. This diagram is a high-level view of a system. The below depicted diagram we have showcased the working principle of our work.

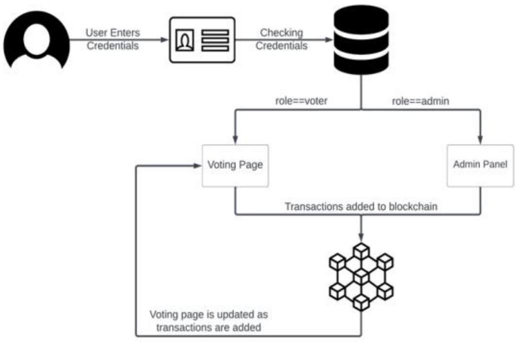

Figure II: A Flow Diagram of our decentralized voting system project

5. MODULES

5.1. Registration

This handles voter registration by collecting and securely storing unique voter details, such as name, roll number, and mobile number. The information is stored in a secure database for verification and authentication purposes.

5.2. Authentication

To ensure secure access, this module implements a two-factor authentication process. Users log in with their credentials and verify their identity using a one-time password (OTP) sent to their registered mobile number.

5.3. Blockchain Integration

It is utilizes the Ethereum blockchain and smart contracts to securely record votes. It prevents duplicate voting by validating each transaction and ensures immutability and transparency of the voting process. Gas fees are used to process transactions.

5.4. Voting

This enables voters to cast their votes via a user-friendly web application. It encrypts votes using public-private key encryption, ensuring confidentiality and secure data transfer to the blockchain.

5.5. Results

This module tallies the votes directly from the blockchain, providing real-time results displayed on the web application. It also allows voters to verify their votes using their unique public keys, ensuring transparency and trust.

5.6. Administration

Designed for election administrators, this module facilitates system monitoring and management. Administrators can oversee registration, authenticate users, manage smart contracts, and ensure the overall integrity of the voting process.

5.7. Testing and Validation

This module focuses on evaluating the system’s performance, including its security, transparency, and scalability. It ensures the application meets the requirements for small-scale and potential large-scale elections.

6. EXPERIMENTAL ANALYSIS

The robustness of our work is as discussed below.

6.1. System Setup:

- The Ethereum blockchain was used to host the smart contracts, with the application deployed on a web-based platform.
- A local test environment, including wallets and accounts generated using tools like Ganache and MetaMask, simulated the voting process.

6.2. Voting Simulation:

- Voters were required to register and authenticate using their credentials and OTPs.
- Once authenticated, votes were cast and recorded securely on the blockchain.
- Gas fees ensured each vote was processed uniquely, preventing duplication.

6.3. Result Compilation:

- Votes were tallied directly on the blockchain, and real-time results were displayed on the web application.
- Voters were able to verify their votes using public keys, confirming transparency and accuracy.

6.4. Performance Evaluation:

- The system demonstrated robust performance in terms of vote security and integrity.
- Transparency was ensured through the public nature of the blockchain ledger, allowing verifiability without compromising voter anonymity.

7. FUTURE WORK

This project is a proof-of- the implemented blockchain-based e-voting system successfully demonstrated enhanced security and transparency, there are several areas for further exploration and improvement:

7.1. Scalability:

- Future efforts should focus on optimizing the system for large-scale elections, ensuring it can handle millions of transactions efficiently without compromising performance or increasing costs.
- Exploring alternative blockchain networks or Layer 2 solutions could improve transaction speed and reduce gas fees.

7.2. Voter Anonymity:

- Enhancing voter privacy without compromising the transparency of the overall system is a critical challenge. Advanced cryptographic techniques, such as zero-knowledge proofs, could be integrated to address this issue.

7.3. Authentication Enhancements:

- Incorporating biometric authentication methods, such as fingerprint or facial recognition, could strengthen voter identity verification and eliminate reliance on mobile OTPs.

7.4. Accessibility and Usability:

- Developing user-friendly interfaces and support for multiple devices (e.g., mobile phones and tablets) can increase accessibility and encourage higher voter participation.

7.5. Security Advancements:

- Further research into protecting the system against cyberattacks, such as Distributed Denial of Service (DDoS) or phishing attempts, is essential for robust deployment in critical elections.

7.6. Integration with Existing Systems:

- Exploring ways to integrate blockchain-based e-voting with traditional voting infrastructure could provide a hybrid solution during the transition phase to fully digital elections.

7.7. Global Deployment Feasibility:

- Researching the legal, technical, and logistical challenges of deploying blockchain-based e-voting systems globally, including in countries with limited internet infrastructure, will be critical for widespread adoption.

8. RESULTS AND DISCUSSION

The results and discussion of our work are discussed below.

8.1. Results:

The blockchain-based e-voting system successfully demonstrated enhanced security, transparency, and reliability in small-scale simulations. Votes were securely recorded on the Ethereum blockchain, ensuring immutability and preventing tampering. The system's two-factor authentication and public-private key encryption provided robust voter authentication and data confidentiality. Real-time vote tallying and voter verifiability enhanced trust and transparency. However, challenges such as scalability, transaction costs, and limited voter anonymity were identified, highlighting the need for further optimization to make the system viable for large-scale or national elections..

8.2. Discussion:

The results demonstrate that blockchain technology can significantly improve the security and transparency of e-voting systems. However, practical challenges such as scalability, cost-efficiency, and voter anonymity need to be addressed for broader adoption. Future enhancements, including the use of alternative blockchain platforms and advanced cryptographic techniques, are essential to overcome these limitations. While the current implementation is well-suited for small-scale elections, extensive research is required to make blockchain-based voting systems viable for national or global elections.

9. CONCLUSION

The blockchain-based e-voting system demonstrated secure, transparent, and tamper-proof vote recording using Ethereum smart contracts. It effectively addressed issues like duplicate voting and ensured voter authentication. However, challenges such as scalability, transaction costs, and limited voter anonymity were noted. While suitable for small-scale elections, further research is needed to optimize the system for large-scale implementations, enhancing privacy and scalability for broader adoption.

10. REFERENCES

[1] Madise, Ü. Madise and T. Martens, “E-voting in Estonia 2005. The first practice of country-wide binding Internet voting in the world.”,Electronic voting, 2nd International Workshop, Bregenz, Austria,(2006) August 2-4.

[2] J. Gerlach and U. Grasser, “Three Case Studies from Switzerland: E-voting”, Berkman Center Research Publication, (2009).

[3] S. G. Stenerud and C. Bull, “When reality comes knocking Norwegian experiences with verifiable electronic voting”, Electronic Voting. Vol. 205. (2012), pp. 21-33.

[4] C. Meter and A. Schneider and M. Mauve, “Tor is not enough: Coercion in Remote Electronic Voting Systems. arXiv preprint. (2017).

[5] D. L. Chaum, “Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms”, Communication of the ACM. Vol. 24(2). (1981), pp. 84-90.

[6] T. ElGamal, “A public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms”, IEEE Trans. Info. Theory. Vol. 31. (1985), pp. 469-472.

[7] S. Ibrahim and M. Kamat and M. Salleh and S. R. A. Aziz, “Secure E-Voting with Blind Signature”, Proceeding of the 4th National Conference of Communication Technology, Johor, Malaysia, (2003) January 14-15.

[8] J. Jan and Y. Chen and Y. Lin, "The Design of Protocol for e-Voting on the Internet", Proceedings IEEE 35th Annual 2001 International Carnahan Conference on Security Technology, London, England, (2001) October 16-19.

[9] D. L. Dill and A.D. Rubin, "E-Voting Security", Security and Privacy Magazine, Vol. 2(1). (2004), pp. 22-23.

[10] D. Evans and N. Paul, "Election Security: Perception and Reality". IEEE Privacy Magazine, vol. 2(1). (2004), pp. 2-9. 8 International Journal of Network Security & Its Applications (IJNSA) Vol.9, No.3, May 2017

[11] Trueb Baltic, "Estonian Electronic ID – Card Application Specification Prerequisites to the Smart Card Differentiation to previous Version of EstEID Card Application." http://www.id.ee/public/TBSPEC-EstEID-Chip-App-v3_5-20140327.pdf

[12] Cybernetica. "Internet Voting Solution." https://cyber.ee/uploads/2013/03/cyber_ivoting_NEW2_A4 _web.pdf.

[13] D. Springall, T. Finkenauer, Z. Durumeric, J. Kitcat, H. Hursti, M. MacAlpine, and J. A. Halderman, "Security Analysis of the Estonian Internet Voting System." Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security. (2014), pp. 703-715.

[14] Ministry of Local Government and Modernisation. "Internet Voting Pilot to be Discontinued." https://www.regjeringen.no/en/aktuelt/Internet-voting-pilot-to-be-discontinued/id764300/

[15] J. A. Halderman, and V. Teague, "The New South Wales iVote System: Security Failures and Verifications Flaws in a Live Online Election." International Conference on E-Voting and Identity. (2015), pp. 35-53.

[16] S. Wolchok, E. Wustrow, D. Isabel, J. A. Halderman, "Attacking the Washington, DC Internet Voting System." International Conference on Financial Cryptography and Data Security (2012), pp. 114-128.

[17] National Institute of Standards and Technology, "Federal Information Processing Standards Publication", (2012).

[18] S. Nakamoto, "A Peer-to-Peer Electronic Cash System", (2008).

[19] F. Reid and M. Harrigan, "An Analysis of Anonymity in the Bitcoin System", Security and Privacy in Social Networks. (2013), pp. 1-27.

[20] S. Raval, "Decentralized Applications: Harnessing Bitcoin's Blockchain Technology." O'Reilly Media, Inc. Sebastopol, California (2016).

[21] J. R. Douceur, "The Sybil Attack", International Workshop on Peer-to-Peer Systems, (2002).