IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

BLOCKCHAIN-BASED SECURE E-VOTING SYSTEM WITH VOTER PRIVACY

[1]Yogesh J, [2]Dr. V. Rajasekar
[1]Student, [2]Associate Professor
Department of Computer Science and Engineering,
SRM Institute of Science and Technology, Vadapalani Campus, Chennai, India

Abstract: The requirement for safe and transparent election systems has significantly increased with the development of digital technologies. Although electronic voting provides ease and speed in the generation of election results, existing voting systems struggle with issues such as central control, vote tampering, lack of transparency, and privacy violations. This paper presents a Blockchain-Based Secure E-Voting System with Voter Privacy. The proposed system utilizes blockchain technology to create a decentralized environment for safe vote recording and verification. Smart contracts perform various election-related activities such as voter validation, vote submission, detection of duplicate votes, and result declaration. The system ensures voter privacy through cryptographic methods including public and private key encryption. Experimental evaluation using simulated election data demonstrates accuracy in authentication, vote validation, duplicate vote detection, and result verification. The proposed framework is highly effective in academic institutions and organizations.

Index Terms: Blockchain, E-Voting, Voter Privacy, Smart Contract, Cryptography, Secure Election, Decentralized Voting.

I. INTRODUCTION

Voting is one of the most important activities in the democratic process. The process provides citizens with a platform to participate in decision-making and leadership selection. Traditionally, voting systems such as ballot papers and electronic voting machines have been widely used in various countries. Although these systems are functional and widely used, they struggle with issues such as manual errors, delays in generating results, lack of transparency, and vote tampering.

Electronic voting systems were introduced to improve efficiency and minimize labor costs. However, many voting systems are based on centralized architecture, posing problems of trust and security. If the central server is compromised, the entire election process may be compromised as well. Ensuring voter privacy remains one of the most significant requirements in the voting process; an efficient e-voting system should record and count votes correctly without compromising the identity or selection of the voter.

Blockchain technology can resolve these problems in an efficient and effective manner. It is a digital ledger that stores data in a secure and unalterable way, replicated over all nodes in the system. Once data is added to the blockchain, it is practically impossible to alter or delete it. These characteristics make blockchain an ideal solution for the voting process, where trust, transparency, and integrity are of utmost importance.

This paper proposes a secure e-voting system based on blockchain technology that is transparent and ensures voter privacy.

II. PROBLEM STATEMENT

The voting systems currently in place have various issues including: centralized control, vote tampering, voter impersonation, duplicate voting, lack of privacy protection, and lack of transparent verification.

A secure digital voting system should: only allow authorized voters to vote, allow each voter to vote only once, protect the privacy of voters, and be able to verify results without any possibility of manipulation. The proposed project addresses these issues through blockchain technology and its inherent security features.

III. LITERATURE SURVEY

Several researchers have studied and implemented blockchain-based voting systems to improve security and transparency in the voting process.

Satoshi Nakamoto first implemented blockchain technology with the development of Bitcoin [1]. Though it was developed for digital currency, the concept of the immutable ledger is highly useful in the context of voting systems.

Ayed developed a conceptual framework for a blockchain-based electronic voting system and proved that blockchain technology can be used to prevent fraud and increase transparency. However, the system failed to place sufficient emphasis on privacy protection features [12].

McCorry et al. implemented a smart contract-based voting system on the Ethereum platform and proved that blockchain technology can be used for vote validation and counting. However, the cost overhead was identified as a limitation [6].

Zyskind et al. focused on the privacy of voting systems and proved that identity and transaction data can be decoupled within blockchain technology. These studies collectively demonstrate that blockchain can be used for secure voting, while the proposed system addresses the remaining limitations in usability, anonymity, and scalability.

IV. PROPOSED SYSTEM

The proposed system is a blockchain-based secure electronic voting system enabling eligible users to register, authenticate, cast encrypted votes, and verify election results. The system is designed with three major aspects: Security, Transparency, and Voter Privacy.

The system comprises several modules working in harmony: Voter Registration, Authentication, Candidate Management, Vote Casting, Smart Contract Validation, Blockchain Storage, and Result Generation. The system guarantees the security of all votes, eliminates double voting, and preserves voter anonymity throughout the election.

V. SYSTEM ARCHITECTURE

The proposed system architecture comprises four major entities: Election Authority (Admin), Voter, Smart Contract Layer, and Blockchain Ledger.

The admin is responsible for creating elections and maintaining candidate information. The voter authenticates with valid credentials, selects a candidate, and casts a ballot. The vote is encrypted and sent to the smart contract for validation before being stored in the blockchain. Once all votes are cast, election results are generated. Figure 1 illustrates the overall workflow of the proposed system.

VI. MODULE DESCRIPTION

6.1 Voter Registration Module

This module is responsible for registering eligible voters in the system. Each voter is assigned a unique voter ID along with a cryptographic identity.

6.2 Authentication Module

This module authenticates the voter before allowing access to the voting portal. Authentication may involve login credentials, OTP, or key-based authentication.

6.3 Candidate Management Module

This module allows the administrator to create elections and manage candidate information.

6.4 Vote Casting Module

The voter selects a candidate and casts the ballot in encrypted form.

6.5 Smart Contract Module

This module checks the voter's eligibility, prevents duplication of votes, and validates the ballot before blockchain submission.

6.6 Blockchain Storage Module

Votes are recorded in blockchain blocks, where each block contains transaction information and hash links.

6.7 Result Generation Module

When the election ends, the system automatically counts all valid votes and produces a verified result.

VII. DATASET DESCRIPTION

A simulated election dataset was used to test the proposed system. Since real election information is sensitive and unavailable for public use, a realistic artificially generated dataset was employed. The dataset includes registered voter information, candidate details, encrypted vote transactions, vote validation logs, timestamps, and blockchain block records. Each voter was assigned a unique voter ID and credentials.

VIII. METHODOLOGY

The working methodology of the proposed e-voting system proceeds as follows: the election authority initiates the election; voters are registered and issued credentials; the voter logs in and undergoes authentication; the voter selects a candidate and casts the ballot; the ballot is encrypted and submitted to the smart contract; the smart contract validates the ballot and checks for duplicate votes; valid ballots are stored in the blockchain; finally, votes are tallied and results are published.

IX. ALGORITHM

Algorithm: Secure Blockchain Voting Process

Input: Registered voters, candidate list

Output: Verified election result

1. Start election
2. Register eligible voters
3. Generate cryptographic credentials
4. Authenticate voter
5. Check if voter has already voted
   a. If valid: accept vote → encrypt vote → validate via smart contract → store in blockchain
   b. Else: reject vote
6. Count all valid votes after election closes
7. Publish result and End

X. EXPERIMENTAL RESULTS

The proposed system was tested using simulated election data to evaluate its efficiency and security. The system performed well across voter authentication, encrypted ballot submission, vote validation, blockchain storage, and result generation. Out of 500 registered voters, 472 valid votes were recorded. The remaining 28 votes were rejected during validation due to duplicate submissions or authentication failures, demonstrating the effectiveness of the proposed framework.

XI. GRAPH ANALYSIS

11.1 Performance Graph

Figure 2 shows the performance of the proposed system in terms of key parameters of an efficient e-voting system, including authentication rate, validation accuracy, and blockchain throughput.

11.2 Vote Distribution Graph

Figure 3 shows the distribution of valid votes across five candidates in the proposed system, illustrating fair and transparent result generation.

11.3 Validation Outcome Graph

Figure 4 categorizes votes into valid votes, duplicate votes, and invalid authentication attempts. These graphical representations help in understanding the effectiveness and practical behavior of the system more clearly.

XII. SECURITY FEATURES

12.1 Cryptographic Hashing

Each block in the blockchain is linked through secure hashes, ensuring data integrity and tamper-resistance across the chain.

12.2 Public-Key Encryption

Votes are encrypted before storage using asymmetric encryption, ensuring that only authorized parties can access vote data.

12.3 Digital Signatures

Digital signatures verify that votes are cast by legitimate, authenticated voters and have not been altered in transit.

12.4 Immutable Ledger

Once stored in the blockchain, a vote is immutable and cannot be modified or deleted by any entity.

12.5 Duplicate Vote Prevention

The smart contract ensures that only a single vote is accepted per eligible voter, eliminating the possibility of duplicate voting.

XIII. VOTER PRIVACY MECHANISM

The protection of voter privacy is a key goal of the proposed system, achieved through: anonymous voter identifiers, encrypted vote payloads, separation of voter identity from vote content, and secure verification without revealing individual vote selections. The proposed system thus maintains transparency of the election outcome while preserving the privacy of individual votes.

XIV. ADVANTAGES OF THE PROPOSED SYSTEM

The proposed system provides several advantages: secure storage of votes, improved voter privacy, transparency in vote verification, prevention of duplicate votes, efficient vote counting, and reduced reliance on centralized authorities.

XV. APPLICATIONS

The proposed system can be applied in: elections in colleges and universities, student council voting, shareholder voting in companies, board member selection, private organization polling, and pilot-level digital governance applications.

XVI. LIMITATIONS

The system also has some limitations: blockchain transaction overhead, the requirement for internet connectivity, scalability issues in large-scale voting scenarios, and the need for greater user awareness and acceptance. These limitations may be addressed in future implementations.

XVII. FUTURE ENHANCEMENTS

Possible improvements to the system include: biometric authentication integration, enhanced privacy through zero-knowledge proofs, mobile voting support, AI-powered fraud monitoring, and large-scale real-world deployment.

XVIII. CONCLUSION

This paper proposes a Blockchain-Based Secure E-Voting System with Voter Privacy that improves the security, transparency, and confidentiality of the voting process. The proposed system ensures votes are stored securely and rendered unalterable after submission. It can authenticate voters, enforce one-time voting, provide privacy, and verify results in a transparent manner. Experimental analysis demonstrates the potential of this framework to improve voting security across educational, organizational, and real-world scenarios.

REFERENCES

[1] Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. https://bitcoin.org/bitcoin.pdf

[2] Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2018). An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends. IEEE Congress on Big Data, 557-564.

[3] Crosby, M., Pattanayak, P., Verma, S., & Kalyanaraman, V. (2016). Blockchain Technology: Beyond Bitcoin. Applied Innovation Review, 2, 6-10.

[4] Christin, N. (2020). The Future of Secure Voting: Blockchain and Beyond. Communications of the ACM, 63(4), 28-30.

[5] Sharma, T., & Agarwal, R. (2019). Blockchain Technology in E-Governance and Voting. International Journal of Computer Applications, 178(7), 1-4.

[6] Yavuz, E., Koc, A. K., Cabuk, U. C., & Dalkilic, G. (2018). Towards Secure E-Voting Using Ethereum Blockchain. ISDFS Proceedings.

[7] Kshetri, N. (2017). Can Blockchain Strengthen the Internet of Things? IT Professional, 19(4), 68-72.
[8] Szabo, N. (1997). The Idea of Smart Contracts. Retrieved from https://szabo.best.vwh.net/smart.contracts.html
[9] Rikken, O., & Zwitter, A. (2020). Trust in Blockchain-Based Voting Systems: The Role of Public Perception. Technology in Society, 63, 101395.
[10] Ali, R., Clarke, N., & Furnell, S. (2020). An Evaluation of the Usability and Security of E-Voting Systems. Computers & Security, 88, 101640.
[11] Ayed, A. B. (2017). A Conceptual Secure Blockchain-Based Electronic Voting System. IJNSA, 9(3), 1-9.
[12] Atzori, M. (2017). Blockchain Technology and Decentralized Governance. Journal of Governance and Regulation, 6(1), 45-62.
[13] Khurana, M., & Baral, R. (2021). A Secure E-Voting System Using Blockchain and Fingerprint Authentication. Procedia Computer Science, 185, 318-326.
[14] Kim, H. M., & Laskowski, M. (2018). Ontology-Driven Blockchain Design for Provenance. ISAFM, 25(1), 18-27.
[15] JavaFX Documentation. Oracle. https://openjfx.io