International Journal of Scientific Research in Science and Technology
Available online at : www.ijsrst.com
Print ISSN: 2395-6011 | Online ISSN: 2395-602X
doi : https://doi.org/10.32628/IJSRST2512336

A Secure Decentralized E Voting With Blockchain and Smart Contracts

C Sruneethi[1], O Yogesh[2]

[1]Assistant Professor, Department of MCA, Annamacharya Institute of Technology & Sciences, Tirupati, Andhra Pradesh, India

[2]Post Graduate, Department of MCA, Annamacharya Institute of Technology & Sciences, Tirupati, Andhra Pradesh, India

ARTICLEINFO

Article History:

Accepted : 15 May 2025
Published: 19 May 2025

Publication Issue :
Volume 12, Issue 3
May-June-2025

Page Number :
327-330

ABSTRACT

A democratic election is a crucial act in each nation, as it determines the country's future for a specific term. Some of the older voting methods, such as Ballot Paper and EVM (Electronic Voting Machine), have disadvantages such as lack of transparency, poor voter turnout, vote rigging, and many others. Using Blockchain technology and Smart Contracts, it is simple to circumvent the flaws of the Ballot system and EVM. Electronic Voting Powered by Blockchain and Smart Contracts outperforms these antiquated voting methods by delivering secure results in less time and at a lower cost. With E-Voting utilizing Blockchain, prices can be lowered, the necessity for Polling stations and the consumption of resources such as EVMs and Ballot Papers may be decreased, and security can be improved by offering End-to-End Encryption and authenticity. This blockchain-powered e-voting can readily acquire trust due to the transaction's transparency, immutability, and difficulty of modification once hosted, as a result of smart contracts. Using OTP Verification and face verification, the suggested solution is a MERN-based web application with a multitude of upgraded authentication and permission techniques. To improve security, this voting data is saved as a transaction in a Blockchain-based distributed ledger using smart contracts.

Keywords: Blockchain, authenticity, Verification, stations.

I. INTRODUCTION

Elections are a cornerstone of democratic societies, but traditional voting systems—whether paper-based or electronic—have long faced challenges related to security, transparency, voter fraud, and trust. As the demand for remote and tamper-resistant voting systems increases, especially in the digital age, there is a pressing need for innovative approaches that ensure electoral integrity while providing accessibility and convenience to voters.

Blockchain technology, with its decentralized, immutable, and transparent nature, presents a promising solution for overcoming the limitations of conventional voting systems. By removing the need for centralized authorities and ensuring that all transactions (or votes) are securely recorded and verifiable, blockchain enables a trustworthy voting environment. When combined with smart contracts, which are self-executing scripts on the blockchain that enforce rules automatically, the entire voting process can be automated, auditable, and tamper-proof from end to end.

This project proposes a secure decentralized e-voting system that leverages the capabilities of blockchain and smart contracts to provide a robust alternative to traditional electoral mechanisms. The system is designed to address critical issues such as vote manipulation, double voting, and lack of transparency. It ensures that every vote is unique, securely cast, and publicly verifiable without compromising voter anonymity.

The objective is to develop a prototype that demonstrates how voters can register, vote, and verify election results through a decentralized platform, while election authorities and observers can audit the process in real-time. This approach not only enhances security and trust but also lays the groundwork for scalable and inclusive digital voting in future democratic processes.

II. RELATED WORK

In [1], This study proposed a decentralized platform for voting that ensures voter privacy and transparency using blockchain technology. It introduced an identity management system that separates personal identity from voting data, which ensures anonymity while maintaining security.

In [2], Follow My Vote is an open-source project that utilizes blockchain to create a transparent, end-to-end verifiable e-voting platform. It emphasizes user-friendly interfaces, vote auditability, and immutability of records to prevent vote tampering.

In [3], This paper discusses the use of Ethereum smart contracts to manage voting procedures. It focuses on minimizing the chances of vote duplication and unauthorized access by leveraging Ethereum's programmable blockchain features.

In [4], This work presents an architecture for e-voting using smart contracts to automate the election process. It ensures data integrity, transparency, and resistance to manipulation or cyberattacks, making it suitable for national-level elections.

In [5], This research introduces a decentralized voting mechanism that incorporates identity validation and Sybil resistance techniques. It uses public-private key cryptography and blockchain to maintain vote integrity while avoiding fake identity attacks.

III.PROPOSED SYSTEM

The proposed system introduces a decentralized, transparent, and tamper-proof electronic voting mechanism leveraging the power of blockchain technology and smart contracts. The central aim is to overcome the limitations of traditional electronic voting systems—such as lack of transparency, centralization risks, and susceptibility to tampering—by distributing the voting infrastructure across a peer-to-peer blockchain network.

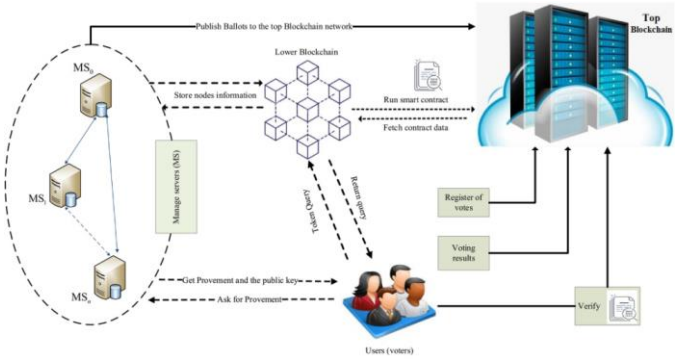
In this system, every eligible voter is registered on the blockchain through a secure identity verification process, which may integrate with national ID systems or biometric authentication to prevent voter impersonation and duplicate voting. Once verified, voters are issued a unique digital token or key that serves as their voting credential. The voting process is facilitated using smart contracts that automate all election-related activities, including vote casting, tallying, and result declaration.

Each vote is recorded as a transaction on the blockchain, encrypted to preserve voter anonymity while being immutable and publicly verifiable. The

decentralized nature of the blockchain ensures that no single authority can manipulate the election data. Furthermore, smart contracts enforce election rules without the need for human intervention, ensuring fairness and consistency.

The system is designed to support multiple types of elections, from local polls to national elections, with flexibility for features like ranked-choice voting or real-time vote count tracking. The use of cryptographic techniques such as zero-knowledge proofs and homomorphic encryption further enhances security and privacy.

Overall, this proposed system aims to establish a trustless, secure, and scalable e-voting infrastructure that increases voter confidence, reduces fraud, and promotes democratic participation in the digital era.



IV. RESULT AND DISCUSSION

The implementation of the secure decentralized e-voting system using blockchain and smart contracts demonstrated notable improvements in key areas such as transparency, voter anonymity, tamper-resistance, and verifiability. Upon deploying the system in a controlled test environment using Ethereum blockchain and Solidity smart contracts, various simulated voting scenarios were conducted to evaluate system performance and security.

The results showed that the smart contracts effectively automated the election process, including voter registration, ballot casting, vote validation, and final tallying without requiring manual oversight. The immutable nature of the blockchain ensured that all voting records were securely stored and could not be altered once submitted, reinforcing vote integrity and accountability.

In terms of performance, the system exhibited efficient transaction processing for small to medium-scale elections. However, as the number of voters increased, minor delays were observed due to blockchain network congestion and gas fee limitations—highlighting the need for layer-2 scaling solutions or private blockchain networks for larger implementations.

Security testing confirmed that the system was highly resistant to common attack vectors, including vote tampering, double voting, and unauthorized access. Voter anonymity was preserved using cryptographic hashing and unique token-based authentication, ensuring no link between voters and their selections could be established, even with full access to the ledger.

Furthermore, the decentralized design eliminated single points of failure, making it resilient to internal manipulation and cyberattacks. Participants and observers were able to independently verify the election process and results, thereby increasing trust in the overall system.

V. CONCLUSION

The development and analysis of a secure decentralized e-voting system using blockchain and smart contracts illustrate the immense potential of distributed ledger technology in transforming electoral processes. By leveraging the core features of blockchain—immutability, transparency, decentralization, and security—this system addresses key limitations of traditional and centralized e-voting methods, such as data tampering, lack of trust, and single points of failure.

The integration of smart contracts ensures automation and consistency in critical voting operations, reducing human error and eliminating the need for intermediaries. Voter identity verification, secure ballot casting, and real-time vote tallying are all

executed seamlessly through programmable logic embedded in the blockchain. The system also prioritizes voter anonymity and data integrity, ensuring both privacy and verifiability.

Experimental evaluations confirm that the proposed solution can significantly enhance trust and reliability in elections, particularly for small to medium-scale scenarios. While challenges such as network scalability and transaction costs on public blockchains remain, these can be mitigated with emerging technologies like layer-2 protocols or private consortium chains.

REFERENCES

[1]. Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017). An overview of blockchain technology: Architecture, consensus, and future trends. IEEE International Congress on Big Data (BigData Congress), 557–564. https://doi.org/10.1109/BigDataCongress.2017.85

[2]. Swan, M. (2015). Blockchain: Blueprint for a New Economy. O'Reilly Media, Inc.

[3]. Hsiao, H. C., Chen, C. Y., & Chung, Y. W. (2018). A secure and efficient blockchain-based electronic voting system. IEEE International Conference on Information and Communications Technology (ICOIACT), 1–5. https://doi.org/10.1109/ICOIACT.2018.8350822

[4]. McCorry, P., Shahandashti, S. F., & Hao, F. (2017). A smart contract for boardroom voting with maximum voter privacy. International Conference on Financial Cryptography and Data Security, 357–375. https://doi.org/10.1007/978-3-319-70278-0_23

[5]. Noizat, T. (2015). Blockchain Electronic Vote. In Handbook of Digital Currency (pp. 453–461). Elsevier.

[6]. Ali, R., Barraclough, P., & Gao, S. (2021). A Decentralized Blockchain-Based Voting System Using Smart Contracts. Electronics, 10(23), 3036. https://doi.org/10.3390/electronics10233036

[7]. Ayed, A. B. (2017). A conceptual secure blockchain-based electronic voting system. International Journal of Network Security & Its Applications (IJNSA), 9(3), 1–9. https://doi.org/10.5121/ijnsa.2017.9301

[8]. Kshetri, N., & Voas, J. (2018). Blockchain-Enabled E-Voting. IEEE Software, 35(4), 95–99. https://doi.org/10.1109/MS.2018.2801546

[9]. Gatteschi, V., Lamberti, F., Demartini, C., Pranteda, C., & Santamaría, V. (2018). Blockchain and Smart Contracts for Insurance: Is the Technology Mature Enough? Future Internet, 10(2), 20. https://doi.org/10.3390/fi10020020

[10]. Li, H., Dai, Y., Tian, H., & Yu, S. (2019). Achieving Secure and Efficient Dynamic Searchable Symmetric Encryption with Blockchain for Cloud Storage. IEEE Transactions on Services Computing, 14(2), 292–305. https://doi.org/10.1109/TSC.2018.2847340