IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 11, April 2025
Impact Factor: 7.67

Tamper-Proof Digital Voting Using Smart Contracts and Blockchain Technology

Prof. Minal Solanki[1], Aditya Shete[2], Pallavi Lanjewar[3]
Assistant Professor, Computer Application[1]
MCA, Computer Application[2,3]
, K. D. K College of Engineering, Nagpur, Maharashtra, India
minalsolanki@kdkce.edu.in[1], adityashete.mca23@kdkce.edu.in[2], pallavilanjewar.mca23@kdkce.edu.in[3]

Abstract: *Electronic voting (e-voting) systems are crucial for modern democracy, yet they often suffer from security vulnerabilities, lack of transparency, and centralized control, leading to potential election fraud. This paper proposes a blockchain-based e-voting system that enhances security, transparency, and voter privacy using advanced cryptographic techniques. The system leverages SHA-256 hashing for secure vote integrity, for decentralized and resilient storage of election data, and Zero-Knowledge Proofs (ZKP) to ensure voter eligibility without revealing personal identities, preserving the confidentiality of the electoral process. By utilizing blockchain's decentralized and tamper-resistant nature, the proposed system aims to eliminate single points of failure, prevent vote manipulation, and maintain voter anonymity.*

Furthermore, smart contracts automate critical processes such as vote validation, ballot recording, and result tallying, significantly reducing human intervention and minimizing the risk of manipulation or errors. The system ensures end-to-end verifiability, allowing voters to independently audit and verify that their votes were counted accurately without compromising the secrecy of their selections. Scalability and performance optimizations, including off-chain data handling and efficient consensus mechanisms, are incorporated to manage the demands of large-scale national or regional elections without degrading system performance. This research outlines the system's comprehensive architecture, detailed implementation strategies, and rigorous security analysis, addressing potential threats such as double voting, voter coercion, and denial-of-service attacks. Through simulation and case studies, the paper demonstrates the system's feasibility, efficiency, and resilience under various adversarial scenarios. By offering a transparent, secure, and user-friendly voting experience, the proposed blockchain-based e-voting solution has the potential to revolutionize digital elections and restore public trust in democratic processes worldwide.

Keywords: Blockchain, E-voting, Ganache, SHA-256, Zero-Knowledge Proofs, Smart Contracts, Immutable Ledger, Election Security

DOI: 10.48175/IJARSCT-25865