DECENTRALIZED AND TAMPER-PROOF VOTING USING BLOCKCHAIN TECHNOLOGY

Prof. Minal Solanki
Assistant Professor, Computer Application, K. D. K College of Engineering, Nagpur, Maharashtra, India
minalsolanki@kdkce.edu.in

Aditya Shete
MCA, Computer Application, K. D. K College of Engineering, Nagpur, Maharashtra, India
adityashete.mca23@kdkce.edu.in

Pallavi Lanjewar
MCA, Computer Application, K. D. K College of Engineering, Nagpur, Maharashtra, India
pallavilanjewar.mca23@kdkce.edu.in

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 cryptographic techniques. The system leverages SHA-256 for secure vote integrity, IPFS for decentralized storage of election data, and Zero-Knowledge Proofs (ZKP) to ensure voter eligibility without revealing identities. 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 vote validation and tallying, reducing human intervention and the risk of manipulation. The system ensures end-to-end verifiability, allowing voters to independently verify their votes without compromising secrecy. Scalability and performance optimizations are considered to handle large-scale elections efficiently. This research outlines the architecture, implementation, and security analysis of the system, demonstrating its potential to revolutionize digital voting.

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

I. Introduction

The integrity of electoral processes is fundamental to democratic governance. Traditional paper-based voting systems, while reliable, are often slow, costly, and susceptible to human error. Existing electronic voting systems attempt to address these issues but introduce new challenges, such as security vulnerabilities, lack of transparency, and dependence on centralized authorities.

Blockchain technology offers a decentralized solution that enhances security, transparency, and verifiability. By leveraging blockchain, cryptographic hashing, and privacy-preserving techniques, e-voting systems can achieve a higher level of trust and security. In this paper, we propose a blockchain-based e-voting system incorporating SHA-256 for data integrity, IPFS for decentralized storage, and Zero-Knowledge Proofs for voter authentication without compromising privacy.

This paper discusses the limitations of existing voting systems, the proposed solution's architecture, implementation, and security aspects. Furthermore, we analyze its performance, potential real-world applications, and future improvements to establish a secure, transparent, and efficient voting mechanism for modern democracies. The integration of smart contracts further automates the vote tallying process, ensuring tamper-proof and real-time results. Additionally, the proposed system is designed to be scalable, making it suitable for national and global elections.

II. Literature Survey

Prof. Anita A. Lahane, Junaid Patel, Talif Pathan, Prathmesh Potdar (2020) Blockchain Technology-Based E-Voting System, ITM Web of Conferences, Vol. 32, ICACC 2020, Mumbai, Maharashtra.

This paper explores the feasibility of blockchain technology in electronic voting systems, focusing on security, transparency, and reducing electoral fraud.

Kashif Mehboob Khan, Junaid Arshad, Muhammad Mubashir Khan (2019) Secure Digital Voting System Based on Blockchain Technology, International Journal of Computer Science and Network Security (IJCSNS), Vol. 19, No. 12, 2019, NED University of Engineering and Technology, Pakistan.

The authors propose a secure digital voting system leveraging blockchain for enhanced authentication, vote integrity, and decentralized vote storage.

Abhishek Subhash Yadav, Ashish Uttamrao Thombare, Yash Vandesh Urade, Abhijeet Anil Patil (2020) E-Voting Using Blockchain

Technology, International Journal of Engineering Research & Technology (IJERT), Vol. 9, Issue 07, July 2020, MIT College of Engineering, Pune.

This study presents a blockchain-based voting framework aimed at eliminating traditional voting system drawbacks, such as tampering and lack of transparency.

Pooja Kumari, Bhagia Sheri, Isma Farah Siddiqui, Khubaib Khatri (2020) Conventional vs. Blockchain-Based E-Vote System, The 15th Asia Pacific International Conference on Information Science and Technology (APIC-IST), 2020, Mehran University of Engineering and Technology, Pakistan.

A comparative analysis of conventional electronic voting systems versus blockchain-based solutions, evaluating security, efficiency, and reliability.

Uzma Jafar, Mohd Juzaiddin Ab Aziz, Zarina Shukur, Hafiz Adnan Hussain (2022) A Systematic Literature Review and Meta-Analysis on Scalable Blockchain-Based Electronic Voting Systems, Springer Nature - Journal of Supercomputing, 2022, analyzing authentication, data privacy, transparency, and verifiability challenges in blockchain-based voting.

This paper reviews scalability challenges in blockchain-based e-voting systems, focusing on authentication, data privacy, transparency, and verifiability.

III. Proposed Methodology

To establish a secure, transparent, and decentralized e-voting system, we propose a blockchain-based voting mechanism that integrates SHA-256 hashing, IPFS for decentralized storage, and Zero-Knowledge Proofs (ZKP) for voter privacy. The proposed system ensures voter authentication, secure vote casting, and tamper-proof vote storage while maintaining anonymity and transparency.

1. System Architecture

The system architecture of the blockchain-based e-voting system consists of multiple interconnected components that ensure secure, transparent, and tamper-proof voting. The process begins with the voter, who must first authenticate themselves. Authentication is performed using registered data stored in a secure database to verify the voter's eligibility. Once authenticated, the voter can cast their vote, which is then processed by a smart contract deployed on the blockchain.

The smart contract serves as the core logic of the voting system, enforcing rules such as checking if the candidate is valid, recording votes, incrementing vote counts, and computing the final result. The smart contract executes functions like isValidCandidate(c), vote(v, c), voteIncrement(c), voteCount(c), and result(), ensuring that votes are recorded accurately without any possibility of tampering.

Once a vote is cast, it is validated and added to the blockchain as a new block. The system uses a consensus mechanism, such as Proof of Work (PoW), Proof of Authority (PoA), or Proof of Stake (PoS), to validate and secure each block. Each block in the blockchain contains crucial information, including a hash, a reference to the previous block's hash, and details of the votes cast for candidates. This ensures data integrity and prevents any unauthorized modifications.

The blockchain structure ensures that all votes remain immutable, transparent, and decentralized, eliminating the risks of vote manipulation or fraud. The architecture ensures that once a vote is recorded in a block, it is permanently stored and linked to the previous blocks, maintaining a continuous and verifiable voting record.

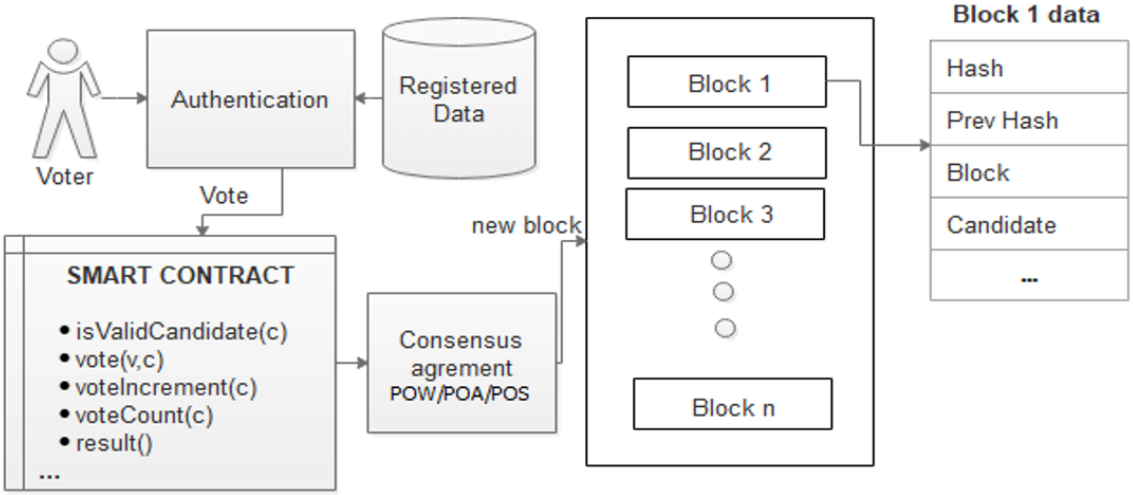

Fig. System Architecture

2. Cryptographic Security Techniques

The blockchain-based e-voting system employs various cryptographic security techniques to ensure data integrity, confidentiality, and authenticity. SHA-256 cryptographic hashing is used to secure votes and voter identities, ensuring that no unauthorized alterations can occur. Each vote is hashed before being stored in the blockchain, making it nearly impossible to tamper with past records. Additionally, Zero-Knowledge Proofs (ZKP) are implemented to verify voter eligibility without revealing their identities, ensuring privacy while preventing duplicate voting. Public-Key Cryptography (PKC) is used to enable secure authentication and digital signatures, ensuring that only authorized voters can participate. Furthermore, the system integrates InterPlanetary File System (IPFS) for decentralized storage, eliminating single points of failure and ensuring the availability of election data. These cryptographic techniques collectively enhance the security, transparency, and reliability of the e-voting system.

- **Role of SHA-256 in Blockchain-based E-Voting:** SHA-256 plays a crucial role in blockchain-based e-voting by ensuring data integrity, security, and transparency. It converts voter information and votes into a fixed-length hash, making tampering easily detectable. Even a small change in input results in a completely different hash, preventing unauthorized modifications. Additionally, SHA-256 helps maintain voter anonymity by hashing sensitive details before storing them on the blockchain. It also links blocks securely, ensuring immutability and preventing fraud, such as double voting. By enabling secure and efficient vote verification, SHA-256 strengthens the reliability of blockchain-based e-voting systems.

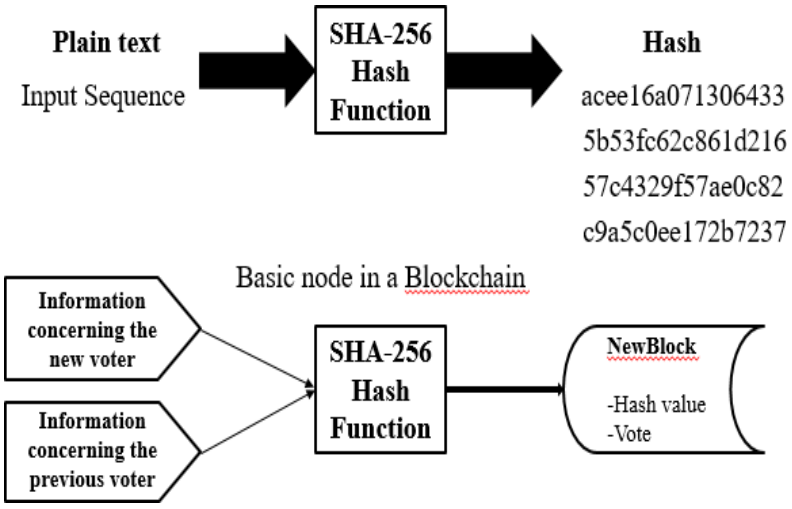

Fig. Role of SHA-256 in Blockchain-based E-Voting

3. Voting Process

The blockchain-based e-voting process ensures security, transparency, and voter anonymity. It starts with voter authentication, where cryptographic techniques verify eligibility while maintaining privacy. After authentication, the voter selects a candidate, and the vote is encrypted before submission. The vote data is then hashed using SHA-256, converting it into a fixed-length hash to prevent tampering. A new block is created, containing the hashed vote, the previous block's hash, and a timestamp. This block is linked to the blockchain, ensuring immutability. The network validates the block through a consensus mechanism, preventing fraud and double voting. Once verified, the vote is permanently stored, making it transparent and secure while ensuring election integrity.

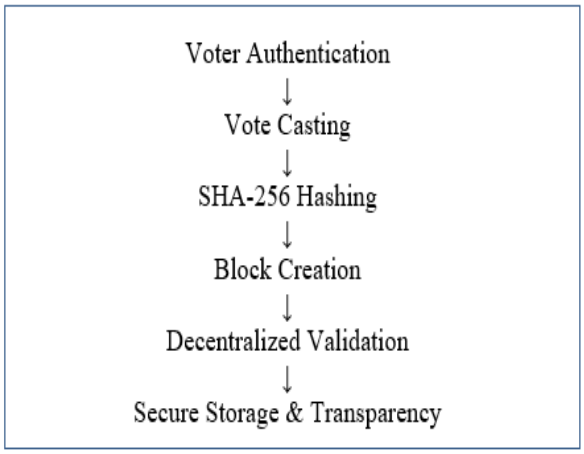

Fig. Voting Process

4. Security Features

- **SHA-256 Hashing:** Every vote is processed through the SHA-256 cryptographic hash function, converting it into a fixed-length hash. This ensures that even the slightest modification to a vote will produce an entirely different hash, making tampering easily detectable.
- **Cryptographic Encryption:** Votes are encrypted before being transmitted and stored on the blockchain. This prevents unauthorized access and ensures that only verified nodes can process vote data while keeping voter identities anonymous.
- **Blockchain Immutability:** Once a vote is recorded in a block and added to the blockchain, it cannot be altered or deleted. This prevents vote manipulation and ensures election integrity, as any attempt to change previous votes would require modifying all subsequent blocks, which is computationally infeasible.
- **Decentralized Validation:** The voting system relies on consensus mechanisms like Proof of Work (PoW) or Proof of Stake (PoS) to validate transactions. This eliminates a central authority, reducing the risk of fraud, hacking, or unauthorized alterations.
- **Zero-Knowledge Proofs (ZKP):** This cryptographic method allows the system to verify voter eligibility without revealing personal details. Voters can prove their right to vote without exposing their identity, enhancing privacy and security.
- **Transparency and Auditability:** Blockchain's distributed ledger allows public verification of recorded votes without revealing voter identities. Election authorities and independent auditors can validate the voting process without compromising security.

IV. Future Scope

1. Reducing Voter Fraud: Blockchain could be used to significantly reduce voter fraud by ensuring that only eligible voters participate and that each voter only casts one vote. Research could explore additional ways of combining biometric verification (fingerprints, facial recognition) with blockchain to create tamper-proof, secure systems for voter eligibility.

2. User Experience and Accessibility

- **User-Centric Interfaces**: Making the voting process simple and accessible is key. Research could explore the design of intuitive blockchain-based voting interfaces for a broad range of voters, including those unfamiliar with blockchain technology or lacking advanced tech skills.
- **Multilingual Support**: Ensuring that voting systems are accessible to non-native speakers and people from diverse linguistic backgrounds is another area where blockchain could be integrated into a multilingual voting framework.

3. Interoperability: In a world with multiple blockchain networks, ensuring interoperability between different blockchain systems for cross-border or national elections is crucial. Future research might focus on protocols that allow blockchain-based voting systems to interact with other election systems (both digital and traditional).

V. Conclusion

The proposed blockchain-based e-voting system addresses the fundamental challenges of traditional and electronic voting systems by leveraging decentralization, cryptographic security, and privacy-preserving techniques. By integrating SHA-256 for data integrity, IPFS for decentralized storage, and Zero-Knowledge Proofs (ZKP) for voter authentication, the system ensures transparency, security, and anonymity. Additionally, the use of smart contracts automates vote tallying, reducing human intervention and eliminating potential manipulation. Through its decentralized architecture, the system mitigates risks such as vote tampering, centralized control, and cyber threats, making it a robust alternative to conventional voting mechanisms. The real-time verifiability of votes enhances voter confidence, while the scalability of the system makes it suitable for elections of various scales, from local to national levels. Despite its advantages, the implementation of blockchain-based e-voting faces challenges such as network scalability, regulatory compliance, and user adoption. In conclusion, this research demonstrates that blockchain technology has the potential to revolutionize the electoral process, ensuring a secure, transparent, and tamper-proof voting mechanism that upholds the integrity of democratic governance

VI. Acknowledgment

We express our sincere gratitude to our project guide, **Prof. Minal Solanki**, for her continuous guidance, valuable insights, and support throughout this research. Her expertise and encouragement have been instrumental in shaping this work. We would also like to thank the respected **Dr. Anup Bhange, Head of the Master of Computer Applications (MCA) Department**, as well as other faculty members for their helpful advice and guidance. Their support and encouragement have

played a crucial role in the successful completion of this research. Furthermore, we extend our appreciation to our peers and mentors for their constructive feedback and discussions, which have helped refine our ideas. Lastly, we acknowledge the contributions of various researchers and authors whose work has served as a foundation for our study.

References

1. Albin Benny, Aparna Ashok Kumar, Abdul Basit, Betina Cherian, and Amol Kharat (2020). Blockchain-Based E-Voting System. Department of Computer Engineering, PCE, Navi Mumbai, India. SSRN. DOI: https://ssrn.com/abstract=3648870.
2. Uzma Jafar, Mohd Juzaiddin Ab Aziz, Zarina Shukur, and Hafiz Adnan Hussain (2022). A Systematic Literature Review and Meta-Analysis on Scalable Blockchain-Based Electronic Voting Systems. Sensors, Vol. 22, 7585. DOI: https://doi.org/10.3390/s22197585.
3. Prof. Anita A. Lahane, Junaid Patel, Talif Pathan, and Prathmesh Potdar (2020). Blockchain Technology-Based E-Voting System. ITM Web of Conferences, Vol. 32, ICACC 2020, Mumbai, Maharashtra. DOI: https://doi.org/10.1051/itmconf/20203203001.
4. Abhishek Subhash Yadav, Ashish Uttamrao Thombare, Yash Vandesh Urade, and Abhijeet Anil Patil (2020). E-Voting Using Blockchain Technology. International Journal of Engineering Research & Technology (IJERT), Vol. 9, Issue 07, July 2020. DOI: https://www.ijert.org.
5. Pooja Kumari, Bhagia Sheri, Isma Farah Siddiqui, and Khubaib Khatri (2020). Conventional vs. Blockchain-Based E-Vote System. The 15th Asia Pacific International Conference on Information Science and Technology (APIC-IST), Mehran University of Engineering and Technology, Pakistan. DOI: https://www.researchgate.net/publication/343017419.
6. Kashif Mehboob Khan, Junaid Arshad, and Muhammad Mubashir Khan (2019). Secure Digital Voting System Based on Blockchain Technology. International Journal of Computer Science and Network Security (IJCSNS), Vol. 19, No. 12, NED University of Engineering and Technology, Pakistan. DOI: https://core.ac.uk/display/155779036.
7. Kavya Ramesh Naidu, Ankush Dinesh Ingale, Pratiksha Sukhadeo Gaikwad, Hitesh Rajendra Thakare, Sujal Sunil Chavan, and Prof. Yogeshk Sharma (2023). Online Voting System. International Research Journal of Modernization in Engineering, Technology and Science (IRJMETS), Vol. 5, Issue 5. DOI: https://www.doi.org/10.56726/IRJMETS38984.
8. David Khoury, Elie F. Kfoury, Ali Kassem, and Hamza Harb (2018). Decentralized Voting Platform Based on Ethereum Blockchain. Department of Computer Science, American University of Science and Technology.
9. Vaibhav Anasune, Pradeep Choudhari, Madhura Kelapure, Pranali Shirke, and Prasad Halgaonkar (2019). Online Voting: Voting System Using Blockchain. Literature Survey, Project Report on Blockchain-Based Voting System
10. Krish Depani. (Year). Decentralized Voting System. GitHub Repository. Available at: https://github.com/Krish-Depani/Decentralized-Voting-System.