Archives available at journals.mriindia.com

International Journal on Advanced Electrical and Computer Engineering

ISSN: 2349-9338
Volume 14 Issue 01, 2025

A Blockchain-Based Voting System For Grampanchayat

Jaiswar Nilesh Avadhesh[1], Harsha Dave[2], Gupta Pavan Shravan[3], Gujarti Sahil Zulfikar[4], Mourya Aaditya Akhilesh[5]

[1,3,4,5]Department of Computer Engineering, Shree L.R. Tiwari College of Engineering, Mumbai
[2]Assistant Professor, Department of Computer Engineering, Shree L.R. Tiwari College of Engineering, Mumbai, harsha.dave@slrtce.in
[1]nilesh.a.jaiswar@slrtce.in, [3]pavan.s.gupta@slrtce.in, [4]sahil.z.gujrati@slrtce.in, [5]aaditya.a.mourya@slrtce.in

Peer Review Information

Submission: 18 Jan 2025
Revision: 19 Feb 2025
Acceptance: 22 March 2025

Keywords

Blockchain
Voting System
Decentralization
Smart Contracts
Security
Transparency

Abstract

Electronic voting (e-voting) has gained significant attention in recent years due to its potential to improve efficiency, accessibility, and accuracy in elections. However, many existing e-voting systems suffer from security vulnerabilities such as vote manipulation, hacking attempts, lack of voter privacy, and centralized control, leading to concerns about election integrity. Blockchain technology presents a decentralized, immutable, and transparent solution for secure voting [1][2]. This paper proposes a blockchain-based voting system that ensures the integrity of votes, prevents fraud, and maintains voter anonymity. The proposed system consists of multiple layers, including frontend, backend, database, blockchain, and security layers, each playing a crucial role in election security and efficiency. This paper provides an in-depth analysis of the system architecture, implementation strategies, security measures, challenges, and potential future improvements. It also discusses how blockchain voting can eliminate the need for intermediaries, reduce election costs, and improve trust in democratic processes [3].

Introduction

Background

Voting is the foundation of democracy, allowing citizens to choose their leaders and influence governance. However, traditional voting methods such as paper-based ballots and electronic voting machines (EVMs) face several issues, including:

- Security vulnerabilities: Traditional systems are prone to vote tampering, manipulation, and hacking attempts[5].
- Logistical challenges: Election processes can be slow, costly, and inefficient for large-scale implementations [2].
- Lack of transparency: Centralized control raises concerns about fairness and trust in election results[4].

Although electronic voting was introduced to solve these problems, it remains susceptible to cyberattacks, insider threats, and data manipulation. Many existing e-voting systems lack verifiability, making it difficult for voters to trust the results [1]. Blockchain technology provides a potential solution by offering a decentralized, tamper-proof, and transparent voting system. This technology ensures that no single entity can alter the election outcome, reducing fraud and increasing voter confidence.

Objectives of the Study:

1. To develop a secure, decentralized, and transparent voting system using blockchain [3].

Traditional voting systems rely on centralized databases, making them vulnerable to cyber-

attacks, unauthorized modifications, and data breaches. A blockchain-based voting system ensures that voting data is distributed across multiple nodes, eliminating the risks associated with single-point failures.

The immutable nature of blockchain technology ensures that once a vote is cast and recorded on the blockchain, it cannot be altered or deleted. This prevents election fraud and manipulation by malicious actors.

Transparency is a fundamental feature of blockchain. Every vote transaction is recorded on a public ledger (or a permissioned ledger in private blockchain implementations), allowing stakeholders to verify election results independently without relying on a central authority.

2. *To ensure voter anonymity and integrity of the voting process[7].*

The integrity of the voting process is ensured through cryptographic techniques such as digital signatures, hashing, and end-to-end encryption.

Voter anonymity is achieved through advanced encryption methods. Each voter is assigned a unique cryptographic key that verifies their identity without revealing their personal details. This prevents voter coercion, identity disclosure, and vote tracking.

The use of smart contracts ensures that votes are automatically validated based on predefined election rules, eliminating the possibility of human errors or biased interventions in vote counting. Smart contracts execute election rules without requiring a trusted intermediary, thus further securing the election process.

3. *To reduce electoral fraud and eliminate third-party interference [4].*

One of the major problems with traditional voting systems is the potential for vote duplication, unauthorized access, and manipulation of election results. Blockchain technology ensures that each voter can cast only one vote by implementing a secure authentication mechanism and a consensus protocol that prevents fraudulent voting attempts.

Third-party interference, such as government manipulation, external hacking attempts, or political influences, is minimized as blockchain operates on a decentralized framework. The distributed nature of blockchain ensures that no single entity has control over the election process, making it resistant to tampering and external influence.

The use of blockchain-based identity verification mechanisms ensures that only registered and authorized voters can participate in elections. Unauthorized individuals attempting to access the voting system will be blocked by the system's cryptographic verification layers.

4. *To improve voter accessibility and election efficiency[2]*

By leveraging online and remote voting capabilities, blockchain enables voters to cast their ballots from any location. This significantly benefits individuals who cannot physically visit polling stations due to geographical, health, or time constraints.

The automation of vote counting and result generation reduces the time required to finalize election outcomes. Unlike traditional voting systems, where manual vote counting can take hours or even days, blockchain-based elections can process votes in real time, ensuring faster and more efficient election results.

Logistical barriers, such as ballot printing, distribution, and physical security of polling stations, are significantly reduced with digital voting systems. This makes elections more costeffective while maintaining high levels of security and transparency.

Increased voter turnout is another advantage of online voting. Many eligible voters do not participate in elections due to inconvenient voting processes. Blockchain technology simplifies the voting experience by providing an intuitive, user-friendly, and accessible voting platform that encourages higher participation rates.

LITERATURE REVIEW

Existing Voting Systems

- Paper-based voting systems have been in use for centuries and remain a common method of conducting elections. While they offer a physical proof of votes cast, they are susceptible to various issues, including ballot stuffing, miscounts, loss or destruction of ballots, and long processing times [5].
- The introduction of Electronic Voting Machines (EVMs) aimed to address the inefficiencies of paper ballots by digitizing the voting process. However, EVMs are still prone to security vulnerabilities, such as:
- Tampering and Hacking: EVMs can be manipulated if unauthorized personnel gain access to the software or hardware [3].
- Lack of Transparency: In many cases, voters and election officials have no means of verifying that the machine accurately recorded and counted the votes [1].

- Power Failures & Malfunctions: EVMs depend on electronic components, which can fail or be intentionally manipulated to disrupt elections [5].
- Many governments and organizations have experimented with digital voting systems that allow voters to cast their ballots through web portals or mobile applications.
- However, these systems often rely on centralized databases, which create a single point of failure. If a hacker gains access to the central server, they can alter, delete, or manipulate voting data.

Additionally, lack of voter privacy is another concern in centralized voting systems. Since a single authority maintains the database, there is a risk of personal data exposure or vote tracking, which can lead to voter coercion.

Trust issues arise because voters have no independent way of verifying whether their vote was counted correctly or altered. This lack of transparency diminishes confidence in the electoral process.

Blockchain for Voting [6]

Blockchain technology provides a decentralized, tamperproof voting solution by recording each transaction (vote) in an immutable format.

Each vote is stored in a block, which is cryptographically linked to the previous block, creating an unalterable chain [7]. This ensures that once a vote is recorded, it cannot be changed, deleted, or manipulated by any entity, including election officials [3].

The decentralized ledger eliminates the need for a trusted central authority, reducing risks of fraud or unauthorized access.

Smart contracts are self-executing programs stored on the blockchain that automatically enforce election rules. In a blockchain-based voting system, smart contracts ensure:

- Voter Eligibility Verification: Only registered voters can cast their votes.
- Single Vote Enforcement: A voter can cast only one vote, eliminating duplicate voting.
- Automated Vote Counting: The smart contract instantly counts votes, reducing human errors and manual intervention.

  Since smart contracts operate on decentralized networks, no single authority can interfere with the election process, making results more trustworthy.

  Decentralized Network for Enhanced Security
- Traditional voting systems can be compromised through hacking attempts on a centralized server. Blockchain-based voting, however, distributes data across multiple nodes, making hacking nearly impossible.
- Each vote transaction must be validated by a consensus mechanism (Proof-of-Work, Proof-of-Stake, or other protocols), ensuring that no single entity can alter the voting results.
- The decentralized structure increases fault tolerance, meaning even if some nodes fail or are attacked, the voting process remains unaffected.
- Cryptographic techniques, such as digital signatures and zero-knowledge proofs, further enhance voter privacy while ensuring vote integrity.

SYSTEM ARCHITECTURE

The blockchain-based voting system is structured into five primary layers , each playing a crucial role in ensuring security, decentralization, data integrity, and user accessibility. These layers work in unison to provide a robust, transparent, and efficient electronic voting system [5].

Security Layer

Ensures System Integrity and Privacy:

- All votes and voter data are protected against unauthorized modifications, ensuring that the election process remains tamper-proof [5].
- Voter identity verification mechanisms prevent unauthorized users from accessing the system while preserving voter anonymity. only registered voters can cast their votes.
- One-Vote Policy: Each voter is allowed to cast only one vote, and any attempts to vote multiple times are automatically blocked.
- Automated Vote Counting: The smart contract tallies votes in real time, eliminating the need for manual vote counting and reducing errors.
- Election Finalization: Once the election ends, smart contracts automatically publish the results, ensuring fairness and preventing unauthorized modifications.

Blockchain Layer [1]

- Manages Decentralized Transactions and Stores Votes Immutably:

  Each vote is recorded as a transaction within the blockchain network, ensuring that it is tamper-proof and permanently stored.

  The decentralized nature of blockchain prevents any single authority from manipulating or altering votes, ensuring election transparency.

- Uses Smart Contracts to Automate Election Rules:

Voter Authentication: The smart contract ensures that voters can participate, reducing risks of impersonation or vote duplication.

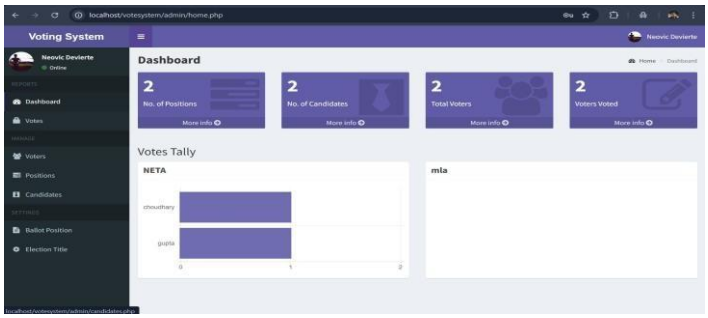

Fig. (1) : Frontend Layer

Database Layer [7]

Stores Encrypted Votes and Voter Details Securely:

- While votes are stored on the blockchain for immutability, sensitive voter information such as identity details are encrypted and stored in a secure off chain database (e.g., MySQL, MongoDB).
- Zero-Knowledge Proofs (ZKP) or similar cryptographic techniques can be used to validate votes without revealing voter identities.
- The database ensures a tamper-proof environment for voter registration and verification, preventing unauthorized modifications to voter credentials.

Backend Layer [3]

Facilitates Authentication, Vote Casting, and Result Processing:

- The frontend ensures a responsive and intuitive voting experience, allowing users to securely log in, verify their eligibility, and cast their votes with minimal effort.
- Security measures such as CAPTCHAs, multifactor authentication (MFA), and SSL encryption ensure that the frontend is protected against phishing attacks and unauthorized access.
- A real-time election progress dashboard can be integrated, displaying vote statistics while maintaining voter anonymity.
- The interface is designed to be accessible on multiple devices, including desktops, mobile phones, and tablets, improving voter participation.

Frontend Layer [4]

Implements Cryptographic Techniques Such as Encryption and Hashing:

- End-to-end encryption secures voter credentials and voting transactions, preventing any third party from intercepting or altering votes.
- Hashing algorithms (SHA-256 or Keccak-256)are used to store votes securely on the blockchain, ensuring that votes cannot be modified once cast.
- Digital signatures and asymmetric cryptography (publicprivate key encryption) ensure that only authorized
- User Authentication: The backend verifies voter identities before allowing them to access the voting interface. Secure login mechanisms such as OTP verification, biometric authentication, or blockchain based identity verification can be integrated.
- Vote Casting Mechanism: Once authenticated, a voter's choice is securely recorded, encrypted, and sent to the blockchain for permanent storage.
- Transaction Processing: The backend manages the conversion of user votes into blockchain transactions, ensuring seamless interaction with smart contracts.
- Result Compilation & Display: After the election ends, the backend retrieves vote counts from the blockchain and securely presents the results to administrators and the public

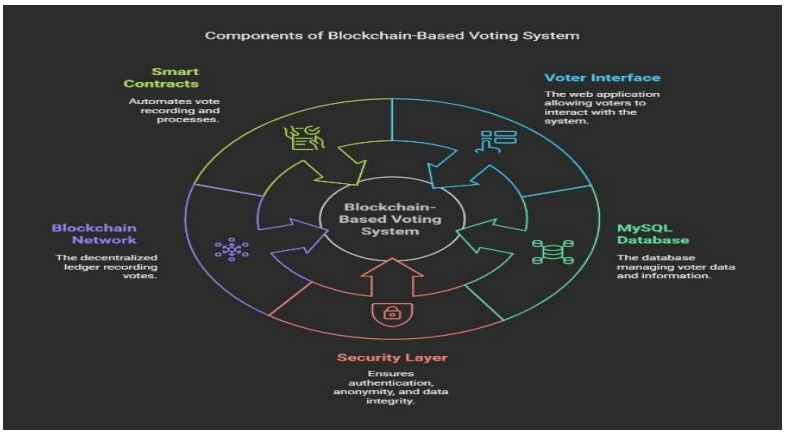

Fig. (2) : Components of Blockchain Based Voting System

IMPLEMENTATION STRATEGY

- Ethereum-Based Smart Contracts for Vote Validation
- Automates voter eligibility checks, vote casting, and counting.
- Ensures one-person-one-vote enforcement.
- Prevents tampering with immutable blockchain storage.
- Publishes final results automatically after election ends.
- SHA-256 Hashing for Security
- Protects vote integrity by converting votes into irreversible hashes.
- Prevents unauthorized alterations of voter credentials.
- Ensures secure voter authentication without exposing personal data.
- Biometric Authentication for Voter Identity Verification
- Uses fingerprint, facial, or iris recognition to prevent voter fraud.
- Provides unique voter identification for secure access.
- Implements multi-factor authentication (MFA) for added security.
- Stores biometric data as encrypted templates, ensuring privacy compliance.

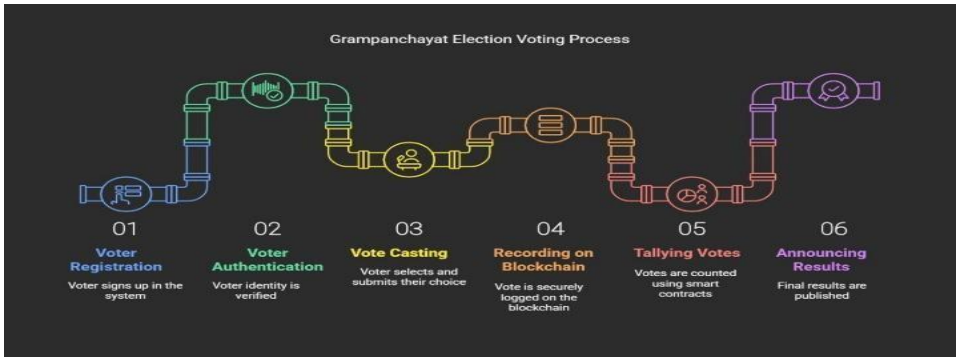

Fig. (3) : Election Voting Process

CHALLENGES AND SOLUTIONS

Scalability

Challenge:

- Blockchain networks experience scalability issues due to high transaction processing times and network congestion, especially during large-scale elections.
- Increased voter participation may lead to slower vote confirmations and higher transaction costs [5].

Solution:

- Implement Layer 2 scaling solutions such as:
- Sidechains: Offload transactions to a secondary blockchain while ensuring security through periodic anchoring to the main blockchain.
- Rollups: Bundle multiple transactions into a single one, reducing on-chain transaction load and improving speed.
- Use blockchain platforms optimized for high throughput, such as Solana or Polygon, instead of traditional Ethereum main net [2].

Privacy concerns

Challenge:

- Blockchain's inherent transparency allows public access to vote transactions, potentially exposing voting patterns or linking votes to individuals.
- Ensuring voter anonymity while maintaining election integrity is a major concern.

Solution:

- Implement Zero-Knowledge Proofs (ZKP) to allow vote verification without revealing voter identities.
- Use Ring Signatures or Homomorphic Encryption to ensure anonymous vote transactions.
- Store only hashed and encrypted vote data on the blockchain to prevent exposure of voting details.

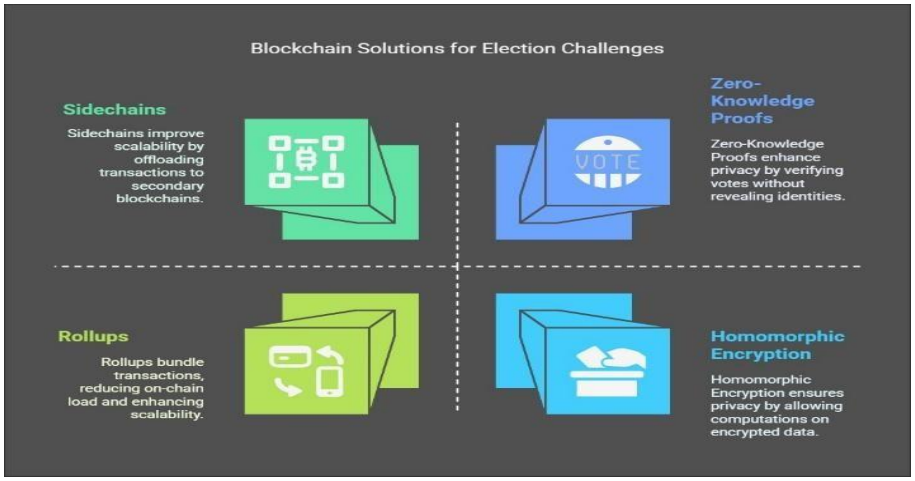

Fig (4). : Blockchain solution for Election Challenges

Voter Education and Adoption

Challenge:

- Many voters may be unfamiliar with blockchain based voting systems, leading to hesitancy in adoption.
- A lack of understanding can result in usability issues, distrust, or misinformation about the security and reliability of the system.

Solution:

- Conduct public awareness campaigns to educate voters on blockchain voting benefits, security, and ease of use.
- Provide step-by-step training programs through online tutorials, workshops, and demo elections.
- Design a user-friendly interface with simple navigation and multilingual support to improve accessibility for all voters.

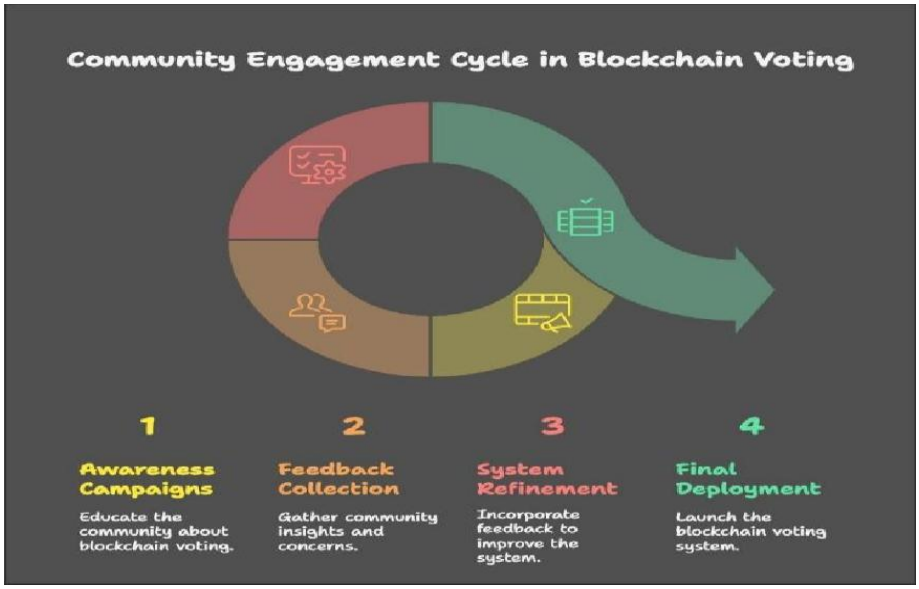

Fig. (5) : Community Engagement Cycle

FUTURE ENHANCEMENTS

- Integration with National ID Systems for Voter Verification [6] – Linking the blockchain voting system with governmentissued national ID databases (such as Aadhaar, Social Security, or Passport systems) can improve voter authentication.
- This ensures that only eligible voters can participate, reducing risks of identity fraud and multiple voting.
- Secure APIs and cryptographic verification techniques can be used to cross-check voter credentials without exposing sensitive personal information.
- AI-Powered Fraud Detection Using Machine Learning [8]
- Implementing machine learning algorithms can help detect anomalies in voting patterns, such as: Multiple voting attempts from the same location.
- Suspicious voting trends that indicate potential hacking attempts.
- Unusual spikes in vote transactions, which could signal bot-driven attacks.
- AI models can analyze historical voting data and flag fraudulent activities in real time, allowing election authorities to take corrective action promptly.

- Mobile App-Based Voting for Better Accessibility
- Developing a secure mobile application for blockchainbased voting will enable voters to cast ballots from anywhere, improving voter turnout.
- The app can include biometric authentication (fingerprint or facial recognition) for added security. User-friendly design and multilingual support will ensure accessibility for people with disabilities and voters in remote areas.
- Offline voting mechanisms with later blockchain synchronization can be explored to ensure accessibility in low-connectivity regions.

CONCLUSION

Blockchain-based voting provides a secure, transparent, and efficient alternative to traditional election systems. By leveraging decentralization, immutability, and cryptographic security, blockchain ensures that votes cannot be tampered with, reducing risks of electoral fraud and manipulation. The transparency of the blockchain ledger enhances voter trust, while cryptographic techniques protect voter privacy and anonymity. Despite the challenges of scalability, privacy concerns, and voter adoption, solutions such as Layer 2 scaling, zero-knowledge proofs, and public awareness initiatives can help overcome these barriers. Additionally, AIpowered fraud detection and mobile-based voting will further improve accessibility and security. As blockchain and AI technologies continue to evolve, future enhancements will make blockchain-based voting more scalable, reliable, and widely adopted. By integrating these innovations, governments and organizations can establish a tamper-proof and trustworthy voting system, strengthening democratic processes worldwide [7].

References

"Blockchain-Based e-Voting System," IEEE Conference Publication. [Online]. Available: https://ieeexplore.ieee.org.

"Blockchain-Based E-Voting Systems: A Technology Review," Electronics Journal, MDPI. [Online]. Available: https://www.mdpi.com.

"Blockchain-Based E-Voting System," ResearchGate. [Online]. Available: https://www.researchgate.net.

"Blockchain-Based E-Voting System: A Decentralized Approach," ResearchGate. [Online]. Available: https://www.researchgate.net.

T. K. Y. Kuo, H. Lu, and M. Xie, "Blockchain-based voting system for electronic democracy," *Proceedings of the 2018 IEEE International Conference on Systems, Man, and Cybernetics (SMC)*, 2018, pp. 2254–2259. Available: https://ieeexplore.ieee.org.

S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," *Bitcoin.org*, 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf. (This is the foundational paper for blockchain technology, often referenced in blockchainbased voting systems).

D. L. McCorry, L. M. L. L. Zhang, and J. R. Y. Zhuang, "Smart contract-based voting system on the blockchain," *Proceedings of the 2017 IEEE International Conference on Blockchain (Blockchain)*, 2017. Available: https://ieeexplore.ieee.org.

N. Christidis and M. Devetsikiotis, "Blockchains and smart contracts for the Internet of Things," *IEEE Access*, vol. 4, pp. 2292-2303, 2016. Available: https://ieeexplore.ieee.org/document/7474206