Content is available at: CRDEEP Journals
Journal homepage: http://www.crdeepjournal.org/category/journals/global-journal-of-current-reseach-gjcr/

Global Journal of Current Research
(ISSN: 2320-2920) (Scientific Journal Impact Factor: 6.122)

UGC Approved-A Peer Reviewed Quarterly Journal

Research Paper

The Use of Blockchain in Electronic Voting Machines to Enhance Security

Mayur Parmar[1]
Assistant Professor, Department of Business Management, Saurashtra University, Rajkot, India.

ARTICLE DETAILS

Corresponding Author:
Mayur Parmar

Key words:
Blockchain, Electronic Voting Machines (EVMs), Security, Decentralization, Immutability, Cryptographic Digital Elections, E-Voting Framework.

ABSTRACT

Electronic voting machines (EVMs) have revolutionized elections by improving efficiency and accuracy, yet they face significant security concerns, including hacking, vote tampering, and lack of transparency. These vulnerabilities raise doubts about electoral integrity, leading to demands for a more secure and verifiable voting system. Blockchain technology, with its decentralized, immutable, and cryptographically secure nature, presents a promising solution to enhance EVM security and trustworthiness. A blockchain based e-voting system ensures that once a vote is recorded, it cannot be altered, thereby preventing manipulation. Decentralization eliminates single points of failure, reducing the risk of cyberattacks. Cryptographic encryption safeguards voter privacy while enabling public verification of election results. Smart contracts automate vote tallying, minimizing human intervention and potential fraud. Despite these advantages, challenges such as scalability, regulatory barriers, and accessibility must be addressed before widespread implementation. This paper explores the theoretical integration of blockchain with EVMs, analyzing its benefits and limitations. It proposes a secure e-voting framework incorporating authentication mechanisms, encrypted vote storage, and consensus-based verification. By reviewing existing blockchain voting models and pilot projects, this study highlights key considerations for future research and policy development, aiming to advance secure, transparent, and efficient digital elections worldwide.

1. Introduction

1.1 Background

EVMs have revolutionized the electoral process by improving efficiency, reducing manual errors, and enabling faster results. However, concerns regarding their security persist, with risks such as vote manipulation, hacking, and lack of voter trust.

1.2 Problem Statement

The integrity of elections is critical for democratic governance, and any potential breach in EVM security undermines voter confidence. Traditional EVMs operate in a centralized manner, making them susceptible to cyber threats. Blockchain technology, known for its decentralized and tamper-proof properties, offers a novel approach to mitigating these security concerns.

1.3 Research Objectives

This paper aims to:

- Analyze the security vulnerabilities in current EVMs.
- Examine blockchain's potential to improve EVM security.
- Propose a theoretical framework for blockchain-based electronic voting.

Discuss challenges and future directions.

[1] *Author can be contacted at: Assistant Professor, Department of Business Management, Saurashtra University, Rajkot, India*

Received: 15-01-2025; Sent for Review on: 18-01-2025; Draft sent to Author for corrections: 30-01-2025; Accepted on: 10-02-2025; Online Available from 14-02-2025
DOI: [10.13140/RG.2.2.15902.04168](10.13140/RG.2.2.15902.04168)

2. Literature Review

J. Padma, A. Devayani, K. R. Devi, L. Akhil in their paper *Secure Digital Voting System* (ijerst, Jan 2025) proposes an online e-voting system utilizing blockchain to address traditional voting security challenges. It discusses decentralized validation, cryptographic security, and transparency in blockchain-based voting.

S. Pandya in his paper *Advanced Blockchain-Based Framework for Enhancing Security, Transparency, and Integrity in Decentralized Voting Systems*discusses a blockchain-based electronic voting system that enhances election security by reducing risks of vote tampering and cyber threats.

J. I. Janjua, U. Aslam, T. Abbas, A. Ihsan in their paper *Implementing Blockchain Technology for Enhanced Security in Voting Systems(IJPSSR)*presents a novel voting system design using blockchain for security and privacy. It explores the advantages of decentralization in ensuring fair elections.

M. M. R. Chowdhury, M. Leary in their paper *How Blockchain Technologies Would Be Impactful for Ensuring Free, Fair, and Trustful Elections in Developing Countries*examines how blockchain technology can ensure election transparency in developing countries, mitigating voter fraud and electoral manipulation.

H. Mutaher, R. S. Hameed in their paper *An Enhanced Blockchain-Based E-Voting System with Authentic Key Agreement*Proposes a blockchain-based e-voting system with key authentication mechanisms to prevent unauthorized access and ensure election integrity.

N. Indrason, W. Khongbuh, K. Baital in their paper *MBCSD-IoT: A Multi-Level Blockchain-Assisted SDN-Based IoT Architecture for Secured E-Voting System*Discusses a multi-layered blockchain framework integrated with IoT and SDN for improving e-voting security.

A. A. Duvey, P. Rahi, S. S. Basa, M. Sachdeva in their paper *Optimizing the EVM with Internet and Blockchain Technology*presents asystematic review of how blockchain can enhance electronic voting machines (EVMs) with end-to-end encryption and smart contracts.

3. Proposed Blockchain-Based EVM Framework

3.1 System Architecture

The proposed blockchain-based electronic voting machine (EVM) is designed to address security vulnerabilities in traditional voting systems by leveraging blockchain's key features—decentralization, immutability, cryptographic security, and transparency. This system ensures that votes remain tamper-proof while maintaining voter anonymity and enabling real-time verifiability. The architecture consists of five key components:

3.1.1. Voter Authentication Layer

To prevent unauthorized voting and impersonation, the system implements a **robust voter authentication process**. This involves:

- *Biometric Verification:* Voters authenticate their identity using biometric data such as fingerprint, iris scan, or facial recognition. This ensures that each vote is cast by a legitimate voter and prevents multiple voting attempts.
- *Digital Identity on Blockchain:* Each registered voter is assigned a unique digital identity (DID) stored on a secure, permissioned blockchain. This decentralized identity management system ensures that only verified individuals can participate in the election while protecting voter privacy.

3.1.2. Voting Process

Once authentication is complete, the voter proceeds to cast their vote through a secure interface. The voting process includes the following steps:

- *Vote Encryption:* After the voter selects a candidate, the vote is encrypted using advanced cryptographic algorithms such as homomorphic encryption or Elliptic Curve Cryptography (ECC). This prevents vote exposure even to network participants.
- *Recording on a Private Blockchain:* Instead of storing votes on a centralized server, each vote is recorded on a private blockchain ledger that is accessible only to authorized election officials and auditors.
- *Cryptographic Hash Assignment:* Each vote is assigned a unique cryptographic hash, ensuring that any modification attempt would be detected instantly. The hash functions as a fingerprint for each vote, maintaining data integrity.

3.1.3. Consensus Mechanism

A major concern in digital voting is ensuring that only valid votes are counted. To achieve this, the system employs a blockchain consensus mechanism to validate votes. A suitable consensus algorithm for voting applications is:

- *Proof of Authority (PoA):* Unlike Proof of Work (PoW), which consumes high computational power, PoA relies on a limited number of trusted validators (e.g., election authorities) to validate votes before they are added to the blockchain. This ensures a balance between security, efficiency, and scalability.

Other possible mechanisms include Byzantine Fault Tolerance (BFT) and Delegated Proof of Stake (DPoS), which further enhance security while optimizing resource usage.

3.1.4. Immutable Ledger

Once votes are recorded and validated, they are stored on a **distributed, immutable blockchain ledger**. This ensures:

- *Tamper Resistance:* Since blockchain data is append-only, no entity—including administrators—can alter or delete votes. Any attempt to modify data would create an inconsistency in the blockchain, making fraud immediately detectable.
- *Decentralized Storage:* The ledger is maintained across multiple nodes rather than a single central server, preventing cyberattacks, unauthorized alterations, or system failures.

3.1.5. Real-Time Auditing & Transparency

One of the key advantages of blockchain voting is **verifiability without compromising voter anonymity**. This is achieved through:

- *Public Verifiability:* A cryptographic record of votes is available for public audit, ensuring that election results are transparent and fraud-proof. Voters can verify that their vote was counted without revealing whom they voted for.
- *Zero-Knowledge Proofs (ZKP):* To enhance privacy, ZKP cryptographic techniques allow for the verification of votes without disclosing voter identities. This ensures a balance between transparency and confidentiality.
- *Instant & Secure Tallying:* Since votes are recorded in real-time, election results can be tallied almost instantly using smart contracts, eliminating delays caused by manual vote counting.

3.2 How Blockchain Enhances Security

Blockchain technology enhances the security of electronic voting systems by addressing key vulnerabilities in traditional voting methods, such as vote tampering, centralized data control, lack of transparency, and election fraud. By leveraging the decentralized, immutable, and cryptographically secure nature of blockchain, electronic voting systems can ensure integrity, verifiability, and voter privacy while minimizing human intervention and security risks. The following aspects highlight how blockchain enhances election security:

3.2.1. Tamper-Proof Transactions: Ensuring Vote Integrity

One of the most significant threats to electronic voting systems is vote manipulation, where hackers or insiders alter vote counts. Blockchain addresses this issue through immutability, meaning that once a vote is recorded on the blockchain, it cannot be altered, deleted, or replaced.

- Every vote is cryptographically hashed and linked to the previous vote, creating a chain of records that is resistant to tampering.
- Any attempt to alter a vote would require changing all subsequent records, which is computationally impossible in a properly implemented blockchain.
- Since votes are stored across multiple nodes, even if a hacker compromises one node, they cannot alter the overall election results.

By ensuring that votes remain unchangeable, blockchain builds public trust in the electoral process and eliminates concerns about vote rigging or unauthorized modifications.

3.2.2. Decentralization: Eliminating Single Points of Failure

Traditional electronic voting systems rely on centralized databases controlled by government agencies or private entities. This centralized model is highly vulnerable to:

- Cyberattacks (e.g., hacking, data breaches, malware injections).
- Insider manipulation (e.g., election officials altering votes).
- System failures (e.g., power outages, hardware failures).

Blockchain distributes vote records across a network of nodes instead of relying on a single database. This decentralized structure offers:

- Fault tolerance: If one node fails, the network remains operational.
- Hacker resistance: A cyberattack on one node does not compromise the entire system.
- No central authority control: No single entity can manipulate the election outcome.

By decentralizing voting records, blockchain removes trusted third parties, ensuring that elections remain secure, transparent, and free from central control.

3.2.3. Transparency & Auditability: Verifiable Election Results

A major drawback of traditional voting systems is that voters must trust election officials to report accurate results. Blockchain eliminates this need for trust by providing full transparency in the voting process.

- *Public Verifiability:* Election results are publicly recorded on a tamper-proof blockchain, enabling independent audits without relying on government authorities.
- *Cryptographic Proofs:* Voters and auditors can verify that each vote was counted correctly without revealing individual voter identities.
- *End-to-End Auditability:* Blockchain ensures that every vote cast is verifiable from ballot submission to final tally, making fraud and misreporting detectable. Transparency enhances public confidence in elections and reduces disputes over election outcomes.

3.2.4. Voter Privacy Protection: Secure & Anonymous Voting

A major challenge in electronic voting is balancing vote transparency with voter privacy. While election results should be auditable, voters' choices must remain confidential. Blockchain achieves this through cryptographic encryption:

- *Anonymous Voting Records:* Each vote is encrypted and assigned a unique cryptographic hash, preventing it from being linked to a specific voter.
- *Decentralized Identity (DID):* Blockchain-based digital identities allow secure authentication while keeping voter data private. This ensures that voter identities remain confidential while votes remain secure and verifiable.

3.2.5. Smart Contracts for Vote Counting: Eliminating Human Manipulation

Manual vote counting in traditional elections is prone to human errors, fraud, and manipulation. Blockchain eliminates these risks by using smart contracts—self-executing code that automates vote tallying.

- *Automated Tallying:* Smart contracts instantly count votes as they are recorded, reducing the risk of miscounting or manipulation.
- *Fraud Prevention:* Since smart contracts execute only under predefined conditions, they cannot be altered or influenced by malicious actors.
- *Real-Time Results:* Election results are computed automatically and transparently, eliminating delays and reducing the risk of last-minute result modifications.

By removing human involvement in vote counting, smart contracts ensure that elections remain free from manipulation, bias, or errors.

4. Challenges and Limitations

While blockchain technology presents a promising solution for securing electronic voting machines (EVMs), its practical implementation faces several challenges and limitations. These include scalability constraints, privacy concerns, energy consumption, accessibility issues, and regulatory barriers. Addressing these challenges is crucial for the widespread adoption of blockchain-based e-voting systems.

4.1 Scalability Issues

A major concern with integrating blockchain into large-scale elections is scalability. The sheer volume of transactions in a national or global election could overwhelm traditional blockchain networks, leading to slow transaction processing times and high computational costs.

- High Computational Power Requirements:
    - Each vote cast on a blockchain is treated as a transaction that needs to be validated, recorded, and stored on multiple nodes.
    - Large-scale elections with millions of voters could require significant computational power, potentially slowing down vote recording and verification.
    - Blockchains with complex consensus mechanisms (e.g., Proof of Work) further strain network resources.
- Transaction Speed Constraints:
    - Blockchain networks process transactions sequentially, meaning they can only handle a limited number of transactions per second (TPS).
    - Popular blockchain networks like Bitcoin and Ethereum have low TPS (7-30 transactions per second), making them unsuitable for real-time election processing.
    - Solutions like Layer-2 scaling (e.g., sidechains, rollups) or sharding could help improve transaction speeds.

To make blockchain voting feasible for large-scale elections, optimized blockchain architectures, hybrid models, or private-permissioned blockchains must be explored to balance security, speed, and efficiency.

4.2 Privacy vs. Transparency

Blockchain voting must balance **two conflicting principles**:

1. *Voter Anonymity* – Ensuring that votes remain private and cannot be linked to specific individuals.
2. *Public Auditability* – Allowing election results to be verified transparently while preventing fraud.

This creates a paradox: a fully transparent blockchain allows public verification of all votes, but revealing individual votes compromises voter privacy.

- Challenges of Public Auditability:
    - In standard blockchains, all transactions are publicly viewable, which conflicts with the secrecy of voting.
    - If votes are recorded in an openly accessible ledger, malicious entities could attempt pattern analysis to infer voter choices.
- Zero-Knowledge Proofs (ZKP) as a Solution:
    - Zero-Knowledge Proofs (ZKPs) allow verification of a vote's legitimacy without revealing voter identities.
    - A voter can prove that their vote is valid (i.e., cast once and counted correctly) without exposing their actual selection.
    - Advanced cryptographic techniques like zk-SNARKs (Zero-Knowledge Succinct Non-Interactive Arguments of Knowledge) ensure that votes are both private and verifiable.

A privacy-preserving blockchain framework combining encryption and zero-knowledge proofs could enable both voter anonymity and election transparency.

4.3 Energy Consumption

Many blockchain networks, particularly those using Proof of Work (PoW) consensus, consume vast amounts of energy, making them environmentally unsustainable for large-scale elections.

- High Energy Costs of PoW:
    - PoW networks like Bitcoin require miners to solve complex cryptographic puzzles, leading to excessive energy consumption.
    - If an entire election were conducted on a PoW blockchain, it would generate a massive carbon footprint, making it impractical for global use.
- Eco-Friendly Alternatives:
    - Proof of Stake (PoS): Rather than relying on mining, PoS selects validators based on their stake in the network, reducing energy usage.
    - Hybrid Blockchains: Combining PoS with permissioned blockchains can optimize energy efficiency while maintaining security.
    - Private Blockchains: Election authorities could use permissioned blockchains that operate without mining, significantly lowering energy demands.

Shifting towards energy-efficient blockchain solutions is essential for making blockchain voting a scalable and sustainable option.

4.4 Voter Accessibility & Digital Divide

For blockchain voting to be widely adopted, it must be accessible to all eligible voters, including those in rural areas, low-income communities, and regions with limited technological infrastructure.

- Challenges of Digital Inclusion:
    - Many voters lack access to reliable internet, smartphones, or digital literacy, making blockchain-based voting difficult.
    - In developing nations, internet penetration remains uneven, and relying solely on online voting could disenfranchise segments of the population.
- Potential Solutions:
    - Offline Blockchain Voting: Implementing offline voting mechanisms where votes can be stored locally and later synced to the blockchain once an internet connection is available.
    - Blockchain-Enabled EVMs: Instead of requiring voters to use their own devices, governments could deploy secure blockchain-powered EVMs at polling stations.
    - Mobile & SMS-Based Voting: Leveraging lightweight blockchain solutions that allow voting via basic mobile phones.

Ensuring equal access to blockchain voting is critical to preventing digital disenfranchisement and ensuring inclusive democratic participation.

4.5 Regulatory and Legal Considerations

The adoption of blockchain-based voting systems is highly dependent on legal frameworks and government regulations, which vary across jurisdictions.

- Government Regulations on Digital Voting:
    - Many countries have strict electoral laws that do not yet accommodate blockchain-based voting.
    - Electoral commissions may be hesitant to adopt blockchain due to concerns about security, voter privacy, and legal compliance.
- Legal Challenges in Different Jurisdictions:
    - Some governments restrict the use of blockchain for voting, citing risks like foreign interference, hacking, and election integrity.
    - Countries with authoritarian regimes may oppose blockchain voting as it could reduce their control over elections by making them more transparent.
- International Standards for Blockchain Voting:
    - Global regulatory frameworks need to be established to standardize security protocols, voter authentication, and data protection.
    - Transparency guidelines must be created to ensure that blockchain voting aligns with existing democratic principles.

Developing comprehensive legal frameworks will be key to ensuring the secure and lawful implementation of blockchain voting systems.

5. Future Directions and Recommendations

5.1.Hybrid Blockchain Models for E-Voting:

- Implementing hybrid blockchain models that combine private and public chains can offer a balance between privacy and transparency in e-voting systems. Sensitive voter information, such as personal details, can be securely stored on a private chain, ensuring confidentiality, while the overall election results are maintained on a public chain for transparency and verification.

5.2.AI-Powered Fraud Detection Mechanisms:

- The integration of AI-powered fraud detection mechanisms is crucial for identifying potentially fraudulent activities in e-voting systems. These mechanisms can analyze voting patterns to detect anomalies such as fake votes or unauthorized tampering with vote counts, ensuring the integrity of the electoral process.

5.3.Quantum-Resistant Cryptography:

- To safeguard against future advancements in quantum computing, which could potentially break current cryptographic methods, it is essential to integrate quantum-resistant cryptography into e-voting systems. This ensures long-term security by employing cryptographic techniques that remain secure even in the presence of quantum computers.

5.4.Government Trials for Blockchain-Based EVMs:

- Conducting government trials using blockchain-based electronic voting machines (EVMs) is a critical step in validating the effectiveness and reliability of these systems. These trials allow for controlled testing, identification of potential issues, and refinement of the technology before full-scale implementation.

5.5.Public Awareness Campaigns:

- Launching public awareness campaigns is vital to building trust and encouraging adoption of blockchain voting systems. These campaigns should include educational content, such as infographics explaining blockchain technology in e-voting, testimonials from early adopters, and user-friendly guides to ensure voters are comfortable and confident in using the system.

5.6.International Standards for Blockchain Voting:

- Establishing international standards is necessary to ensure consistency, security, and interoperability across different countries' blockchain voting systems. These standards should address technical specifications, scalability, and regional adaptability while being overseen by a recognized authority to maintain global trust and efficiency.

6. Conclusion

Blockchain technology has the potential to revolutionize electronic voting by addressing security and transparency concerns. A decentralized, immutable, and verifiable voting system could restore public confidence in electoral processes. However, challenges such as scalability, energy efficiency, and regulatory compliance must be addressed before widespread implementation. Future research should focus on refining blockchain-based voting frameworks and conducting real-world experiments to validate their feasibility

References

1. Padma, J., Devayani, A., Devi, K. R., & Akhil, L. (2025). *Secure digital voting system*. International Journal of Engineering Research & Science & Technology (IJERST). Retrieved from https://ijerst.org/index.php/ijerst/article/download/499/458
2. Pandya, S. (2025). *Advanced blockchain-based framework for enhancing security, transparency, and integrity in decentralized voting systems*. ResearchGate. Retrieved from https://www.researchgate.net/publication/387408636_Advanced_Blockchain-Based_Framework_for_Enhancing_Security_Transparency_and_Integrity_in_Decentralised_Voting_System
3. Janjua, J. I., Aslam, U., Abbas, T., & Ihsan, A. (2025). *Implementing blockchain technology for enhanced security in voting systems*. International Journal of Politics & Social Sciences Review (IJPSSR). Retrieved from https://www.researchgate.net/publication/388318507_Implementing_Blockchain_Technology_for_Enhanced_Security_in_Voting_Systems
4. Chowdhury, M. M. R., & Leary, M. (2025). *How blockchain technologies would be impactful for ensuring free, fair, and trustful elections in developing countries*. ResearchGate. Retrieved from https://www.researchgate.net/publication/388109607_How_Blockchain_Technologies_would_be_impactful_for_ensuring_the_free_fair_and_trustful_election_system_in_Developing_Countries
5. Mutaher, H., & Hameed, R. S. (2025). *An enhanced blockchain-based e-voting system with authentic key agreement*. Al-Razi University Journal. Retrieved from http://rujms.alraziuni.edu.ye/index.php/RUJCST/article/download/247/249
6. Indrason, N., Khongbuh, W., & Baital, K. (2025). *MBCSD-IoT: A multi-level blockchain-assisted SDN-based IoT architecture for secured e-voting system*. IEEE Transactions on Blockchain and Cybersecurity. Retrieved from https://ieeexplore.ieee.org/abstract/document/10858763/
7. Duvey, A. A., Rahi, P., Basa, S. S., & Sachdeva, M. (2025). *Optimizing the EVM with internet and blockchain technology: A systematic review for enhancing secured e-voting using blockchain-based EVMs*. Recent Advances in Computing & Cybersecurity. Retrieved from

https://www.taylorfrancis.com/chapters/edit/10.1201/9781003598152-134/optimizing-evm-internet-blockchain-technology-anurag-anand-duvey-pankaj-rahi-santi-swarup-basa-mohnish-sachdeva-pramod-mathur

8. Elhoseny, M., Alyami, H., Altuwairiqi, M., & Dutta, P. (2025). *An efficient and secured voting system using blockchain and hybrid validation technique with deep learning*. Peer-to-Peer Networking & Applications. Retrieved from https://link.springer.com/article/10.1007/s12083-024-01849-x
9. Kuru, K. (2025). *Blockchain-enabled decentralized voting through biometric identification using metaverse immersive devices and deep learning*. University of Central Lancashire (UCLAN). Retrieved from https://clok.uclan.ac.uk/54204/1/Online%20voting%20with%20blockchain%20V1.pdf
10. Li, H., & Wang, H. (2025). *Principles and applications of blockchain systems: Overcoming security challenges*. Springer. Retrieved from https://books.google.com/books?hl=en&lr=&id=sD88EQAAQBAJ&oi=fnd&pg=PA15&dq=blockchain+in+electronic+voting+machines+for+security&ots=5yI6kW07Jk&sig=l4AZPucUiMVK9bJcXlAwfKScEFY