ISSN 2319-5991 www.ijerst.com
© 2026 IJERST. All Rights Reserved
Peer Reviewed, Referred & Indexed Journal

Research Paper

DESIGN AND DEVELOPMENT OF A SECURE BLOCKCHAIN-BASED ELECTRONIC VOTING SYSTEM WITH TRANSPARENT AUDIT MECHANISM

B CHANDRU[1] **A J RAJA SEKHAR**[2]

[1]mrbchandru2003@gmail.com [2]rajasekhar.arjs@gmail.com

[1]PG Scholar, Dept. of Master of Computer Application, Vemu Institute of technology. P. Kothakota, Tirupati–Chittoor Highway, Chittoor District, Andhra Pradesh, India – 517112.

[2]Associate professor, Dept. of Master of Computer Application, Vemu Institute of technology. P. Kothakota, Tirupati–Chittoor Highway, Chittoor District, Andhra Pradesh, India – 517112.

ABSTRACT

Electronic voting systems aim to modernize the electoral process by improving efficiency, accessibility, and auditability. However, conventional e-voting systems suffer from critical challenges such as centralized control, security vulnerabilities, privacy concerns, insider manipulation, and lack of public trust. To address these limitations, this paper proposes a blockchain-based electronic voting system that ensures transparency, immutability, and verifiable election processes. The proposed system integrates blockchain technology, smart contracts, and cryptographic authentication to create a secure and tamper-resistant voting environment. Each vote is validated through smart contract logic and recorded as an immutable transaction in a distributed ledger, preventing double voting and unauthorized modifications. The decentralized architecture eliminates single points of failure and enhances trust through transparent and auditable records. The system design includes voter registration, authentication, vote casting, validation, and result tallying modules. Experimental analysis demonstrates improved security, integrity, and reliability compared to traditional voting systems. The proposed framework provides a scalable and trustworthy solution for modern digital elections.

Keywords: Blockchain, Electronic Voting System, Smart Contracts, Distributed Ledger, Security, Transparency, Audit Trail

1.INTRODUCTION

The transition from traditional paper-based elections to digital voting systems has significantly improved the efficiency and accessibility of electoral processes. However, conventional electronic voting (e-voting) systems often rely on centralized architectures, which introduce critical vulnerabilities such as single points of failure, unauthorized access, data manipulation, and lack of transparency [1]. These limitations reduce public trust and raise concerns about the integrity and reliability of election outcomes. In recent years, blockchain technology has emerged as a promising solution to address these challenges. Blockchain provides a decentralized and distributed ledger that records transactions in a secure, transparent, and immutable manner.

Each transaction is cryptographically linked to previous records, making it extremely difficult to alter or tamper with stored data [2]. These properties make blockchain highly suitable for applications requiring trust, auditability, and data integrity, such as electronic voting systems.

A blockchain-based voting system eliminates dependence on a central authority by distributing trust across multiple network nodes. This ensures that no single entity can manipulate the election data. Additionally, smart contracts enable automated validation of voting rules, such as voter eligibility and prevention of duplicate voting, thereby enhancing system reliability and fairness [3]. Cryptographic techniques further ensure voter authentication while preserving ballot secrecy.

The motivation for this work arises from the growing need for secure, transparent, and verifiable voting mechanisms. Existing digital voting platforms often lack proper auditability, making it difficult to independently verify election results. Blockchain technology addresses this issue by maintaining a permanent and auditable record of all voting transactions, thereby increasing transparency and public confidence in the electoral process [4].

This paper proposes a secure blockchain-based electronic voting system that integrates smart contracts, cryptographic identity verification, and distributed ledger technology. The system is designed to ensure vote integrity, prevent fraudulent activities, and provide real-time auditability. By combining decentralization with strong security mechanisms, the proposed solution aims to deliver a scalable and trustworthy platform for modern Digital Elections.

2. LITERATURE REVIEW

Blockchain-based electronic voting systems have gained significant attention in recent years due to their potential to improve transparency, security, and trust in electoral processes. Several researchers have explored different architectures, cryptographic techniques, and consensus mechanisms to address the limitations of traditional e-voting systems.

Sharp et al. [1] presented a comprehensive survey of blockchain-based e-voting mechanisms, highlighting their advantages in terms of decentralization, transparency, and auditability. The study also identified challenges such as scalability and voter privacy. Similarly, El Kafhali et al. [2] analyzed the significance of blockchain in secure voting and emphasized the importance of addressing privacy and performance constraints.

Chaudhary et al. [3] proposed a secure smart contract-based voting system integrated with 5G networks, demonstrating improved efficiency and reduced latency. Their work highlights how emerging communication technologies can enhance blockchain-based voting systems. Madhani et al. [4] introduced a decentralized and anonymous voting system using blockchain combined with ring signatures, which ensures voter anonymity while maintaining vote integrity.

Patidar and Jain [5] developed a decentralized e-voting portal using blockchain concepts, focusing on eliminating centralized control and improving transparency. Their work demonstrated that blockchain can effectively prevent vote tampering and duplication. Bhavani et al. [6] explored recent trends in blockchain voting systems and emphasized the importance of transparency and reliability in modern electoral systems.

The Ethereum platform [7] has been widely used for implementing decentralized applications due to its support for smart contracts and secure transaction processing. Its programmable nature enables the development of automated voting mechanisms with strong validation rules. On the other hand, Hyperledger Fabric [8] provides a permissioned blockchain environment, making it

suitable for institutional voting systems that require controlled access and governance.

3.METHODOLOGY

The proposed blockchain-based electronic voting system is designed to satisfy critical properties required for secure, transparent, and reliable election processes. These properties ensure that the system maintains integrity, confidentiality, and trust throughout the voting lifecycle.

1) Security

Security is a fundamental requirement of the system. Cryptographic techniques such as hashing and digital signatures are used to protect voter data and ballot information. Smart contracts enforce strict validation rules, preventing unauthorized access and fraudulent activities.

2) Privacy and Confidentiality

The system ensures that the voter's identity is separated from the ballot data. Votes are encrypted or hashed before being stored on the blockchain, ensuring that no unauthorized entity can trace a vote back to a specific voter.

3) Integrity

Data integrity is maintained through the immutable nature of blockchain technology. Once a vote is recorded as a transaction, it cannot be modified or deleted without detection. Each block is cryptographically linked to the previous block, ensuring consistency of records.

4) Transparency

The system provides a transparent voting process by maintaining a distributed ledger that can be verified by authorized parties. All transactions are recorded and can be audited, increasing trust in the election results.

5) Decentralization

Unlike traditional voting systems, the proposed system eliminates dependence on a central authority. The distributed nature of blockchain ensures that no single entity can control or manipulate the voting data.

6) Non-Repudiation

Once a vote is cast and recorded, the voter cannot deny participation. Digital signatures provide proof of authenticity, ensuring accountability in the system.

7) Availability

The system is designed to remain accessible during the voting period. Distributed nodes ensure continuous operation even if some parts of the network fail.

8) Scalability

The architecture supports scalability to accommodate large numbers of voters. Efficient transaction handling and optimized data storage mechanisms ensure system performance during high loads.

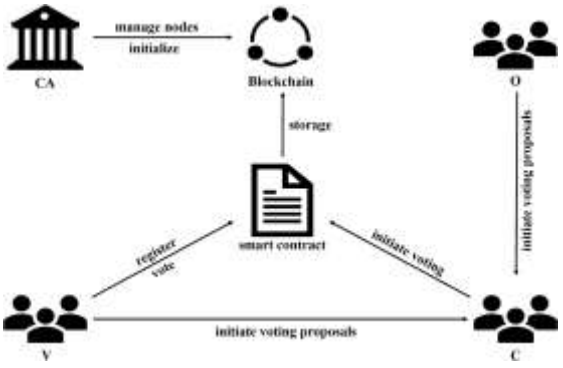
9) Auditability

Every action in the system is recorded in the audit log and blockchain ledger. This allows independent verification of election results without relying on a central authority.

10) Usability

The system provides a user-friendly interface for voters and administrators. Clear workflows and minimal steps ensure ease of use while maintaining strong security controls.

SYSTEM ARCHITECTURE DIAGRAM



ALGORITHMS USED IN THE SYSTEM

1. Voter Registration Algorithm

Input: Voter details (ID, Name, Age)

Output: Unique voter ID

Step 1: Accept voter details

Step 2: Verify eligibility (Age ≥ 18, valid identity)

Step 3: Check if voter already exists

Step 4: Generate unique voter ID or token

Step 5: Store voter data in database

Step 6: Confirm registration

2. Authentication Algorithm

Input: Login credentials / digital signature

Output: Access granted or denied

Step 1: User enters credentials

Step 2: Validate credentials from database

Step 3: Verify digital signature (if applicable)

Step 4: Check whether voter has already voted

Step 5: If valid, allow access; otherwise deny

3. Vote Casting Algorithm

Input: Selected candidate

Output: Encrypted vote

Step 1: Display ballot options

Step 2: Voter selects candidate

Step 3: Encrypt or hash the vote

Step 4: Create vote transaction

Step 5: Send transaction to smart contract

4. Smart Contract Validation Algorithm

Input: Vote transaction

Output: Valid or invalid vote

Step 1: Receive vote transaction

Step 2: Verify voter eligibility

Step 3: Check for duplicate voting

Step 4: Validate ballot format

Step 5: If all conditions satisfied, approve vote; otherwise reject

5. Blockchain Block Creation Algorithm

Input: Validated vote

Output: New block added

Step 1: Collect validated transactions

Step 2: Create block with vote hash, timestamp, previous hash

Step 3: Generate block hash

Step 4: Broadcast block to network nodes

Step 5: Add block to blockchain after validation

6. Consensus Algorithm

Input: Proposed block

Output: Approved or rejected block

Step 1: Broadcast block to validator nodes

Step 2: Nodes verify block integrity

Step 3: Collect approvals from nodes

Step 4: If approvals meet threshold, accept block; otherwise reject

7. Vote Tallying Algorithm

Input: Blockchain transactions

Output: Final vote count

Step 1: Retrieve all vote transactions from blockchain

Step 2: Decrypt or interpret vote data

Step 3: Count votes for each candidate

Step 4: Store and display results

4. IMPLEMENTATION

The proposed blockchain-based electronic voting system is designed using a modular architecture that ensures security, transparency, and reliability. The methodology integrates blockchain technology, smart contracts, and cryptographic mechanisms to provide a tamper-resistant and verifiable voting process.

A. System Workflow Overview

The overall workflow of the system follows a sequential process from voter registration to result publication. Each stage is interconnected and validated to ensure correctness and integrity. The system flow is designed to eliminate unauthorized access, prevent duplicate voting, and maintain auditability throughout the election lifecycle.

B. Detailed System Flow

The operational flow of the system is described below:

Step 1: Voter Registration

Eligible voters are registered in the system with verified identity details. A unique voter ID or cryptographic token is generated for each user. This ensures that only authorized participants can access the voting platform.

Step 2: Authentication

Registered voters log in using secure credentials. Authentication is performed using cryptographic methods such as digital signatures or token-based verification. The system checks whether the voter is valid and has not already voted.

Step 3: Ballot Access

Once authenticated, the voter is granted access to the ballot interface. The system verifies whether the election is currently active and whether the voter is eligible to participate.

Step 4: Vote Casting

The voter selects a candidate or option from the ballot. The selected vote is then encrypted or hashed before submission to preserve confidentiality.

Step 5: Smart Contract Validation

The submitted vote is processed by a smart contract deployed on the blockchain. The contract performs:

- Voter eligibility verification
- Duplicate vote prevention
- Ballot format validation

If all conditions are satisfied, the vote is approved.

Step 6: Blockchain Transaction Recording

The validated vote is recorded as a transaction in the blockchain ledger. Each transaction includes:

- Vote hash
- Timestamp
- Previous block reference

This ensures immutability and prevents any post-submission modifications.

Step 7: Vote Confirmation

The system generates a transaction receipt or confirmation message for the voter. This serves as proof that the vote has been successfully recorded.

Step 8: Vote Tallying

After the voting period ends, the system aggregates all validated transactions from the blockchain. The tally is computed automatically without manual intervention.

Step 9: Result Publication and Audit

The final results are displayed along with an auditable transaction record. Independent auditors can verify the results by examining the blockchain ledger.

5. MATHEMATICAL MODEL

A. Hash Function

A cryptographic hash function is used to secure vote data and ensure integrity.

$$H(x) = SHA256(x)$$

where x represents the input data (vote or transaction), and H(x) is the fixed-length hash output.

This ensures that even a small change in input produces a completely different hash, making tampering detectable.

B. Block Formation

Each block in the blockchain is linked to the previous block using a hash function:

$$Hash_n = H(Data_n + Hash_{n-1})$$

where:

- $Data_n$ = current block data
- $Hash_{n-1}$ = previous block hash

C. Digital Signature Model

To ensure authentication and non-repudiation, digital signatures are used:

$$S = Encrypt_{private}(H(m))$$

where:

- m = message (vote data)
- $H(m)$ = hash of the message
- S = digital signature

Verification is done using the public key:

$$Decrypt_{public}(S) =$$

D. Consensus Condition

A block is added to the blockchain only after validation by network nodes:

$$Block\ Accepted \Rightarrow \sum_{i=1}^{n} Validation_i \geq Thresh$$

E. Tally Function

The final vote count is computed as:

$$Result(c) = \sum_{i=1}^{N} Vote_i(c)$$

OUTPUT SCREENS (FORMS & REPORTS)

In a report-based prototype, output screens are presented to explain how users would interact with the completed system. The following wireframe-style visuals show the expected structure of the login page, the ballot page, and the result/audit view. These layouts are designed to be clean, minimal, and easy to understand.



Figure 9.1: Login Screen

The login screen should be simple and immediately understandable. Its role is to protect access to the voting portal while keeping the number of required steps small. A clear login screen helps users identify the system quickly and reduces confusion during election day.



Figure 9.2: Ballot Casting Screen

The ballot screen is the most important interface for the voter. It must display the available options with enough spacing and clarity to avoid accidental input. The submit button should be visually distinct, and the page should show the current election title, instructions, and any eligibility notices.



Figure 9.3: Result and Audit Screen

The result screen combines a vote summary with an audit-friendly transaction list.

This dual presentation allows users to view the outcome while also checking the evidence that supports it. Such a screen is especially important when the system is expected to prove that no tampering occurred after the ballots were cast.

6.FUTURE ENHANCEMENT

The current design can be extended in several important directions. One future enhancement is stronger identity verification, such as biometric authentication or multi-factor approval, which would make it harder for unauthorized users to

impersonate eligible voters. Another enhancement is more advanced privacy support, for example by adding privacy-preserving proof systems that allow ballot verification without revealing the voter's choice. A second area of improvement is scalability. A larger election may require optimized consensus settings, off-chain batching, or more efficient storage of non-critical metadata. The system could also be adapted to support federation across multiple election districts or institutions while still maintaining a common audit framework. A third enhancement is analytics. After the election closes, the platform could generate richer dashboards showing turnout patterns, time-based voting trends, and verification metrics. Such analytics would help administrators understand the practical behavior of the system and improve future deployments. Another valuable extension is support for external review tools. Independent observers could be given access to read-only audit dashboards, cryptographic verification utilities, and election archives. This would improve public transparency and provide additional confidence in the published outcome. Finally, the application could be expanded into a more complete civic technology platform that supports voter notifications, candidate profiles, multilingual interfaces, accessibility features, and secure mobile participation. These improvements would make the system more inclusive and closer to real-world election requirements.

7.CONCLUSION

The design and development of a blockchain-based electronic voting system demonstrates how distributed ledger technology can strengthen the reliability, transparency, and auditability of digital elections. Unlike a centralized architecture, the proposed model distributes trust, preserves the history of transactions, and makes tampering visible. This significantly improves confidence in the result and gives the system a stronger foundation for public use. The project report has presented the problem definition, system analysis, requirements, design diagrams, module breakdown, technology overview, coding logic, testing plan, output screens, future enhancements, and references in a structured chapter format. By following the same general style as the online-exam report, the document remains familiar in layout while being technically tailored to the blockchain voting domain. The result is a formal and readable project report that can be used for academic submission, presentation, or future development planning.

REFERENCES

[1] Sharp, M., Njilla, L., Huang, C.-T., & Geng, T. (2024). Blockchain-Based E-Voting Mechanisms: A Survey and a Proposal. Network, 4(4), 426–442.

[2] Ethereum Foundation. Introduction to Smart Contracts. Ethereum Documentation.

[3] Ethereum Foundation. Consensus Mechanisms. Ethereum Documentation.

[4] Ethereum Foundation. Smart Contract Security. Ethereum Documentation.

[5] Ethereum Foundation. Technical Intro to Ethereum. Ethereum Documentation.

[6] Hyperledger Foundation. A Blockchain Platform for the Enterprise. Hyperledger Fabric Documentation.

[7] Hyperledger Foundation. Smart Contracts and Chaincode. Hyperledger Fabric Documentation.

[8] Hyperledger Foundation. What Is a Blockchain Network? Hyperledger Fabric Documentation.

[9] Patidar, K., & Jain, S. (2019). Decentralized E-Voting Portal Using Blockchain. ICCCNT.

[10] Chaudhary, S., Shah, S., Kakkar, R., Gupta, R., Alabdulatif, A., Tanwar, S., Sharma, G., & Bokoro, P. N. (2023). Blockchain-Based Secure Voting Mechanism Underlying 5G Network: A Smart Contract Approach. IEEE Access, 11, 76537–76550.

[11] Madhani, N., Gajria, V., & Kanani, P. (2021). Distributed and Anonymous E-Voting Using Blockchain and Ring Signatures.

[12] El Kafhali, S. et al. (2024). Blockchain-Based Electronic Voting System: Significance and Research Directions.