International Journal of Computer Techniques–IJCT Volume 12 Issue 6, November 2025
Open Access and Peer Review Journal ISSN 2394-2231 https://ijctjournal.org/

Blockchain based E-Voting system-LITERATURE SURVEY

Dhruthana S ,Chandana PY ,Inchara BS ,Vandana G Raj ,Guruprasad YK

dhruthanaysa@gmail.com

1.E-voting system using cloud-based hybrid blockchain technology

1.1 Abstract

The advancement of blockchain and cloud technologies has enabled secure and transparent online voting systems. Traditional voting mechanisms often suffer from issues such as vote tampering, identity fraud, and lack of transparency. The proposed E-voting framework integrates cloud computing with hybrid blockchain technology to ensure a reliable, flexible, and tamper-proof voting process. The system operates through three phases—registration, vote casting, and vote counting—utilizing a timestamp-based authentication protocol and digital signatures for validation. Smart contracts automate transactions while eliminating third-party involvement, and the Practical Byzantine Fault Tolerance (PBFT) algorithm guarantees secure and consistent vote tallying. Performance evaluation demonstrates reduced authentication delay, minimized vote alteration, and improved system latency, offering a more secure and efficient E-voting solution compared to traditional systems.

1.2 Approach

The proposed approach combines blockchain, cloud, and IoT technologies to build an end-to-end verifiable E-voting system.

1. Hybrid Blockchain Architecture: Merges public and private blockchains to balance transparency and security—public visibility for results and private encryption for sensitive data.

2. Phased Process:

Registration Phase: Voters and candidates register through the Election Commission Authority using unique digital identities generated by the Key Generation Center (KGC).

3. Vote Casting Phase: Voters cast encrypted votes authenticated via timestamp and digital signatures, which are securely recorded as blockchain transactions using Elliptic Curve Digital Signature Algorithm (ECDSA).

4. Vote Counting Phase: Smart contracts automatically tally votes based on PBFT consensus, ensuring immutability and correctness of results.

5. Performance Optimization: Authentication delay, response time, and latency are measured and improved through blockchain decentralization and optimized cloud storage.

1.3 Contributions

1. Secure Voter Authentication: Introduced a timestamp-based digital signature protocol enhancing voter and candidate verification beyond biometric methods.

2. Elimination of Third-Party Dependence: Used smart contracts for self-executing and tamper-resistant vote validation, reducing chances of manipulation.

3. Integrity through Consensus: Adopted PBFT consensus to prevent data corruption during block validation and vote counting.

4. Enhanced System Efficiency: Demonstrated lower authentication delays (up to 50% reduction) and improved response times in large-scale testing.

5. Transparency and Trust: The hybrid blockchain allows public verifiability of results while preserving vote confidentiality.

1.4 Limitations

1. Scalability Concerns: System performance may degrade under extremely large-scale national elections due to blockchain network expansion.

2. Infrastructure Dependency: Requires continuous and stable Internet connectivity along with sufficient cloud resources.

3. Technical Complexity: Implementation involves complex cryptographic mechanisms, demanding skilled personnel for maintenance and auditing.

4. User Accessibility: Non-technical voters or regions with limited digital literacy may face usability challenges.

5. Legal and Regulatory Issues: Adoption requires alignment with electoral laws, data privacy regulations, and government approval for nationwide deployment.

2. E-Voting System Using Blockchain and Web Engineering

2.1 Abstract

The traditional voting process often faces challenges related to security breaches, lack of transparency, and inefficiency. To overcome these issues, this research introduces an electronic voting (E-voting) system built using blockchain and web engineering principles. The proposed model utilizes blockchain's decentralized and immutable ledger to ensure data integrity and transparency throughout the election process. It eliminates the need for centralized control while incorporating cryptographic techniques and smart contracts for secure,

verifiable, and tamper-resistant voting. The integration of Aadhar-based authentication enhances voter identity verification, reducing fraudulent activities. Experimental results demonstrate significant improvements in security, transparency, voter authentication, and cost-effectiveness, establishing the proposed system as a robust alternative to conventional voting methods.

2.2 Approach

The study proposes a hybrid blockchain-based architecture that leverages Web technologies for a secure, scalable, and user-friendly E-voting process.The approach includes:

1. System Design: Implementation of a decentralized blockchain ledger where each vote is securely recorded as a unique, immutable transaction.

2. Authentication Mechanism: Integration of Aadhar-based identity verification and digital signatures to ensure that each voter can cast only one vote.

3. Smart Contracts: Automated validation and vote counting are executed through smart contracts, minimizing human intervention and ensuring accuracy.

4. Scalability Enhancements: Incorporation of interoperability protocols, zero-knowledge proofs, and state rent mechanisms to optimize storage and reduce computational overhead.

5. Hybrid Blockchain Architecture: Combination of public and private blockchains to maintain transparency for authorized parties while preserving voter privacy.

6. User Interface: A web-based platform for both administrators and voters that supports secure login, candidate management, and real-time result visualization.

2.3 Contributions

1. Enhanced Security and Privacy: Utilized blockchain immutability and cryptographic encryption to prevent data tampering and unauthorized access.

2. Decentralization and Transparency: Removed dependency on a central authority by using distributed nodes for vote validation and storage.

3. Improved Voter Authentication: Integrated Aadhar-based digital identity verification, ensuring that only legitimate voters participate.

4. Automation through Smart Contracts: Enabled real-time vote tallying and verification, reducing human error and bias.

5. Scalable and Efficient System: Introduced dynamic block size adjustment and off-chain governance to improve throughput and reduce latency.

6. User-Centric Design: Developed an accessible and intuitive web interface that enhances usability while maintaining security.

7. Performance Gains: Achieved approximately 80–85% improvement in efficiency and reliability compared to conventional e-voting systems.

2.4 Limitations

1. Scalability Challenges: Despite optimizations, large-scale national elections may still face network congestion and transaction delays.

2. High Computational Demand: Blockchain operations, encryption, and consensus mechanisms require substantial computing power and energy.

3. Technical Complexity: Implementation demands advanced infrastructure and expertise, which may limit deployment in low-resource environments.

4. Regulatory and Legal Barriers: The absence of standardized laws for blockchain-based voting could hinder official adoption.

5. User Accessibility: Citizens lacking digital literacy or access to reliable internet may face difficulties using the system.

6. Privacy Concerns: Although voter data is encrypted, improper key management could potentially compromise anonymity.

3. E-Voting using Blockchain Technology

3.1 Abstract

Electronic voting (e-voting) systems are increasingly recognized as essential tools for modernizing democratic elections, improving transparency, and encouraging voter participation. However, conventional e-voting approaches face critical challenges related to cybersecurity threats, data integrity, voter privacy, and system transparency. To address these issues, blockchain technology has emerged as a transformative innovation, providing decentralized, immutable, and verifiable mechanisms for recording and auditing votes. This survey paper presents a comprehensive overview of current advancements, architectures, and global trends in blockchain-based e-voting systems. It systematically analyzes how distributed ledger technologies, cryptographic algorithms, and smart contracts can strengthen vote authentication, confidentiality, and auditability. Furthermore, the paper highlights recent improvements in blockchain scalability and performance that make it suitable for large-scale elections. Despite these advantages, blockchain-based e-voting still encounters obstacles such as high resource demands, legal and infrastructural limitations, and cybersecurity vulnerabilities.

3.2 Approach

1. Research Design: The study adopts a systematic literature review (SLR) guided by the PRISMA (Preferred Reporting Items for Systematic Reviews and Meta-Analyses) framework. This structured approach ensures transparency, reproducibility, and comprehensive coverage of all relevant studies.

2. Data Collection and Search Strategy- Databases: IEEE Xplore, Scopus, ACM Digital Library, SpringerLink, MDPI, and Google Scholar. Keywords: "Blockchain," "Electronic voting," "E-voting architectures," "Security," "Transparency," and "Consensus algorithms." Boolean operators (AND/OR) were used to refine search results. Initial results: Over 22,000 publications were identified.

3. Inclusion and Exclusion Criteria-Included: Peer-reviewed journal/conference papers directly addressing blockchain-based e-voting, architectures, and security. Excluded Non-peer-reviewed, incomplete, or irrelevant studies, and preprints without detailed methodology.

4. Methodological Strength: PRISMA methodology ensured systematic and unbiased coverage. Use of multiple databases provided a wide research scope. Comprehensive categorization helped map the evolution of blockchain-based e-voting systems

5. Research Objectives: The study was guided by key questions focusing on: Architectural design and scalability of blockchain-based e-voting systems. Implementation strategies of blockchain technologies in voting. Identification of security challenges and cryptographic solutions.

3.3 Contributions

1. Integration of Key Blockchain Technologies: Explains the use of smart contracts for automated vote verification and tallying. Discusses cryptographic mechanisms such as digital signatures, homomorphic encryption, and zero-knowledge proofs to ensure privacy and integrity.Examines consensus algorithms (PoW, PoS, PBFT) and their role in achieving distributed trust.

2. Identification of Research Gaps: Highlights the lack of scalable, energy-efficient, and legally adaptable blockchain frameworks for large-scale elections. Emphasizes the need for privacy-preserving yet verifiable mechanisms that balance transparency and anonymity.

3. Framework for Future Research: Suggests new directions for improving blockchain-based e-voting systems through lightweight consensus algorithms, quantum-resistant cryptography, and AI-based security enhancement.

4. Scalability and Performance Limitations: Blockchain networks may face transaction delays and congestion during large-scale elections. Consensus algorithms like PBFT and PoW become less efficient with increased voter participation and data volume.

5. High Computational and Energy Requirements: Blockchain operations demand substantial computational power and storage capacity, increasing energy consumption and operational costs.

3.4 Limitations

1. Infrastructure and Network Dependency: Continuous and reliable internet connectivity and cloud infrastructure are essential. Areas with weak digital infrastructure may struggle to implement or maintain the system effectively.

2. Complexity in Implementation: Requires advanced technical expertise in cryptography, blockchain development, and cybersecurity auditing.

3. Legal and Regulatory Challenges: Lack of clear legal frameworks for blockchain-based voting systems limits their national adoption. Issues of jurisdiction, data privacy, and regulatory compliance remain unresolved.

4. Dependency on Internet and Infrastructure: The system requires stable internet connectivity and blockchain infrastructure, which may not be available in all regions.

5. Computational and Financial Costs: Every transaction consumes gas fees, which can increase operational costs when scaled to millions of voters.

4. Blockchain for securing electronic voting systems

4.1 Abstract

The evolution of digital technologies has transformed the way democratic elections can be conducted, making electronic voting (e-voting) a practical and efficient alternative to conventional ballot or Electronic Voting Machine (EVM) systems. However, traditional methods often suffer from issues such as vote tampering, identity fraud, lack of transparency, and low voter turnout. To address these challenges, this study introduces a blockchain-based e-voting framework that utilizes the decentralized, transparent, and immutable nature of blockchain technology. The system is implemented on the Ethereum network using smart contracts, programmed through the Solidity language, to ensure that each vote is securely recorded, verified, and counted without the need for a central authority. Each transaction consumes a limited amount of “gas” to prevent duplicate voting while maintaining accountability and auditability.

4.2 Approach

1. System Design and Framework: The proposed e-voting system is designed using a Model-View-Controller (MVC)architecture to ensure modularity and maintainability. The system integrates blockchain technology, smart contracts, OTP-based authentication, and web technology for end-to-end secure voting.

2. Registration Phase: Each voter registers on the web platform with a unique ID and attributes such as name, roll number, and mobile number. Registration details are stored in a MySQL database, and a digital identity is created for each voter.

3. Login and Authentication: Users log in with credentials and authenticate using a real-time OTP verification system. This two-factor authentication mechanism strengthens voter verification and prevents unauthorized access.

4. Blockchain Layer: Ethereum blockchain serves as the backbone of the voting system. Votes are encrypted using an asymmetric encryption algorithm where a public key is used for verification and a private key is held by the host for secure processing. Each vote is recorded as a transaction on the blockchain, ensuring immutability and traceability.

5. Smart Contract Deployment: The voting logic is implemented as smart contracts on the Ethereum network using Solidity. Smart contracts manage candidate data, record votes, prevent double voting, and automatically tally results.

4.3 Contributions

1. Development of a Secure Blockchain-Based E-Voting Framework :Introduced a decentralized voting system that eliminates the need for a trusted third party (TTP) by leveraging Ethereum blockchain and smart contracts.

2. Integration of Smart Contracts for Automated Voting: Designed and implemented smart contracts in Solidity to handle vote registration, authentication, and result tallying autonomously. The contract ensures one vote per voter and enforces immutability in vote records.

3. Enhanced Security with Multi-Layer Authentication: Introduced OTP-based two-factor authentication for real-time voter verification. Combined with blockchain encryption, this mechanism strengthens system security against impersonation and fraudulent voting.

4. Transparency and Auditability: Each vote is recorded as an encrypted transaction visible on the blockchain, providing complete traceability without compromising privacy. Voters can verify their vote records using their unique blockchain address.

5. Prevention of Double Voting and Data Manipulation: Implemented a gas mechanism in Ethereum to limit vote transactions per voter, preventing double voting. Smart contracts automatically reject repeated vote attempts.

4.4 Limitations

1. Scalability Constraints: The proposed model is suitable for small-scale elections (e.g., campus or local polls). Ethereum's current transaction capacity and gas costs make large-scale national elections impractical at this stage.

2. Voter Anonymity Challenges: Although transactions are encrypted, blockchain transparency may expose patterns between voter and candidate addresses. Achieving complete anonymity without losing auditability remains a key research challenge.

3. Dependency on Internet and Infrastructure: The system requires stable internet connectivity and blockchain infrastructure, which may not be available in all regions.

4. Computational and Financial Costs: Every transaction consumes gas fees, which can increase operational costs when scaled to millions of voters. Ethereum-based smart contract execution is resource-intensive and may cause network delays.

5. Implementation Complexity: Developing, auditing, and maintaining smart contracts requires technical expertise in blockchain development, cryptography, and network management voter Anonymity Challenges

5. BLOCKCHAIN BASED E-VOTING SYSTEM

5.1 Abstract

The paper explores the potential of blockchain technology to create a secure, transparent, and trustworthy evoting system. Traditional voting methods face challenges of accuracy, transparency, and security, which blockchain's decentralized and immutable nature aims to resolve. Using cryptographic techniques and consensus mechanisms, the proposed system ensures anonymity, prevents vote manipulation, and maintains verifiable records. The research demonstrates that blockchain can enhance election integrity, increase public trust, and modernize democratic processes.

5.2 Approach

The proposed system is implemented using the Ethereum blockchain and Solidity smart contracts. It has two main modules:

1. Admin Module: Logs in, adds candidates and voters, starts and ends elections, and views results.
2. User Module: Logs in, views candidate details, casts a single vote, and views results once the election ends.

Phases:

1. Frontend Design: Development of the user interface for admin and voters.

2. Backend Implementation: Smart contract creation using Solidity on Ethereum.
3. Integration & Testing: Connecting frontend and backend using Truffle framework, ensuring functionality and security.

5.3 Contributions

1. Secure & Transparent E-Voting: Demonstrates how blockchain ensures data integrity and voter privacy.
2. Smart Contract Automation: Utilizes Ethereum-based smart contracts to manage election logic without intermediaries.
3. Prototype Implementation: A working prototype validating blockchain's practical use for voting systems.
4. Comparative Evaluation: Highlights improvements over traditional and electronic voting in terms of security, transparency, reliability, and trust.
5. Promotes Trust in Democracy: Suggests blockchain as a viable path to rebuild confidence in electoral systems.

5.4 Limitations

1. Technical Complexity: Implementation and maintenance require blockchain expertise.
2. Scalability Issues: May face challenges when handling large-scale elections.
3. Cybersecurity Risks: Vulnerable to network attacks or system compromise if not properly secured.
4. Vote-Buying Risk: Difficult to ensure that all votes are cast freely without external influence.
5. Limited Adoption: Blockchain-based voting systems are still new and not widely implemented.
6. Infrastructure Dependency: Requires stable internet and computational resources for all participants.

6. Digital Voting with Blockchain using Interplanetary File System and Practical Byzantine Fault Tolerance

6.1 Abstract

The paper proposes a secure and tamper-proof digital voting system that combines blockchain technology, the InterPlanetary File System (IPFS), and Practical Byzantine Fault Tolerance (pBFT) consensus. Traditional voting systems are prone to fraud, manipulation, and lack of transparency. The proposed system ensures data

integrity, voter anonymity, and transparency through distributed ledger technology and cryptographic techniques.

The blockchain ledger guarantees immutability, IPFS ensures data integrity and decentralized storage, and pBFT enhances fault tolerance and transaction validation. The system allows voters to cast votes remotely via the internet while preserving trust, reliability, and verifiability in the election process.

6.2 Approach

The proposed approach integrates blockchain, IPFS, and pBFT to form a decentralized e-voting framework with enhanced security and efficiency.

Key Components:

1. Blockchain Layer:Acts as an immutable ledger where each vote is securely recorded using cryptographic seals.
2. Employs smart contracts to automate voting logic, user permissions, and access control.
3. InterPlanetary File System (IPFS):Used for secure decentralized storage of voting data, linked to blockchain via unique content hashes. Reduces data redundancy, improves scalability, and cuts transaction costs.
4. Practical Byzantine Fault Tolerance (pBFT):Used for secure decentralized storage of voting data, linked to blockchain via unique content hashes. Reduces data redundancy, improves scalability, and cuts transaction costs.
5. Practical Byzantine Fault Tolerance (pBFT):Ensures consensus and fault tolerance, even if some nodes behave maliciously. Improves transaction validation speed and network scalability.
6. Frontend and Backend Integration: Developed using ReactJS, HTML, CSS, JavaScript, and Third Web framework with Solidity smart contracts. Authentication handled through token-based secure login and cryptographic verification.
7. System Flow: Admin registers voters and candidates. Voters log in securely, view candidates, and cast encrypted votes. Votes are stored via IPFS and verified through blockchain smart contracts using pBFT.

   Final results are viewable by both admin and voters, ensuring transparency.

6.3 Contributions

1. Integration of IPFS with Blockchain: Enables efficient decentralized storage and retrieval of largescale voting data.

2. Use of pBFT Consensus Mechanism: Enhances speed, scalability, and fault tolerance compared to proof-based consensus algorithms.
3. Smart Contract Optimization: Introduces gas cost reduction mechanisms, lowering blockchain transaction fees by up to 33%.
4. Improved Security & Transparency: Prevents vote alteration and tampering while maintaining voter privacy through encryption.
5. Empirical Validation: Tested with 30,000 voters, showing improvements of:

- 15–33% reduction in gas cost
- 25–55% improvement in latency
- 35–71% improvement in authentication delay
- 29–67% reduction in vote alteration rate.

6.4 Limitations

1. Maintenance Cost: Despite optimization, running blockchain and IPFS nodes still incurs maintenance overhead.
2. Gas Fees Fluctuation: Ethereum-based transactions are subject to variable gas costs depending on network congestion.
3. Complex Deployment: Implementation requires technical expertise in blockchain and smart contracts.
4. Limited Real-world Testing: Experiments were conducted in a simulated environment; large-scale national-level validation remains pending.
5. Dependence on Internet Access: Digital divide and network outages may restrict participation for remote or underprivileged users.

CONCLUSION

TITLE AND YEAR	AUTHORS	PROS	CONS
E-voting system using cloud-based hybrid blockchain technology(2024)	Beulah jayakumari,S. LillySheeba, Maya Eapen	Ensures transparency, security, and reliability through hybrid blockchain.	Complex implementation requiring high computational power

E-Voting System Using Blockchain and Web Engineering (2024)	Zunjarrao Aastha Girish, Kirtik Ganeshan, Srushti More, Shrutam Tambe	Aadhar-based voter authentication improves verification accuracy by 95%	Requires high technical expertise for deployment.
E-Voting using Blockchain Technology(2020)	Abhishek Subhash Yadav, Abhijeet Anil Patil	Good for students or developers learning blockchain-based application building.	No formal comparison with existing systems or security audits.
Blockchain for Secure electronic voting system(2024)	Henry o, Adeiza james onumanyi, Rabiu O	Covers a wide range of e-voting architectures (centralized and decentralized), blockchain integration,	Primarily a survey — lacks implementation or experimental validation.
Blockchain Based E-Voting system(2023)	Aarti Goel, Abhishek Singh	Demonstrates a working Ethereum-based e-voting system with Solidity smart contracts, Truffle framework, and front–back-end integration.	No experimental results such as throughput, latency, or gas cost are provided.
Digital voting with blockchain using interplanetary file system(2024)	Sreedhar jinka, Anusha Marouthu, Giddaluru Somasekhar	Discusses scalability, evolving legal compliance, and continuous improvement.	Despite optimization, the Ethereum network still incurs transaction fees and energy costs.