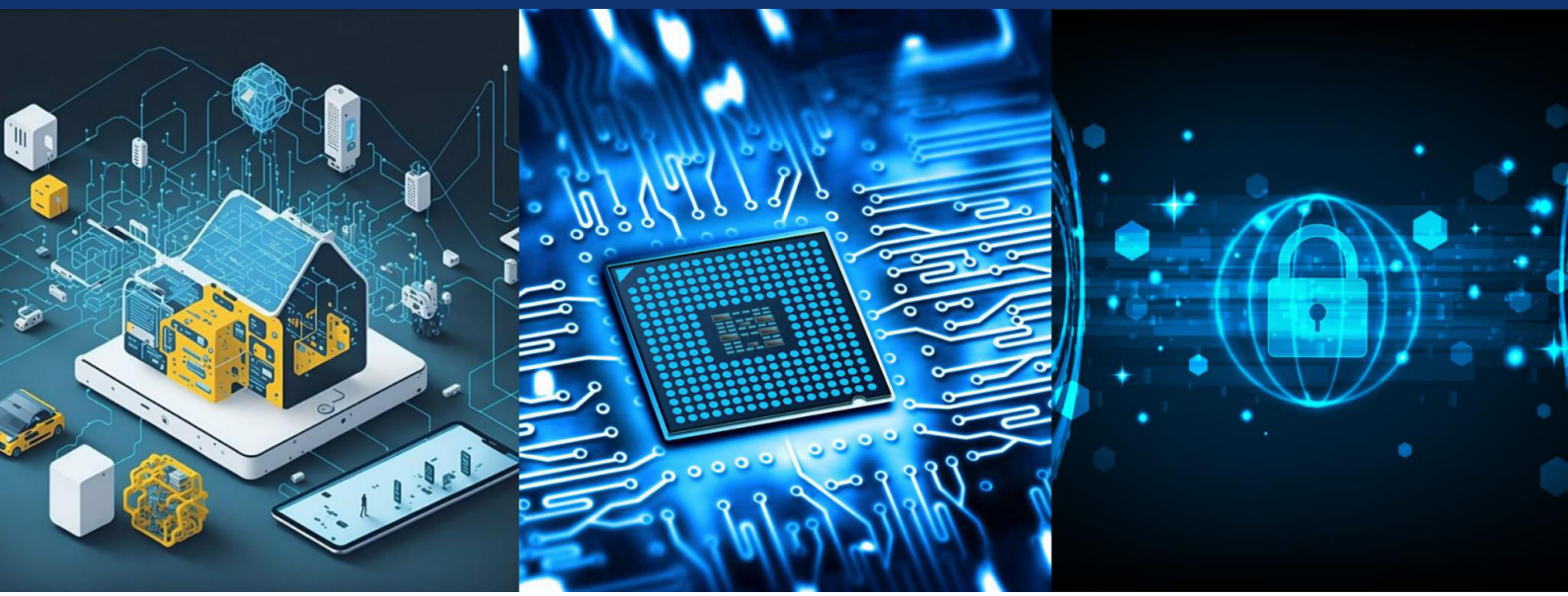
IJIRCCE

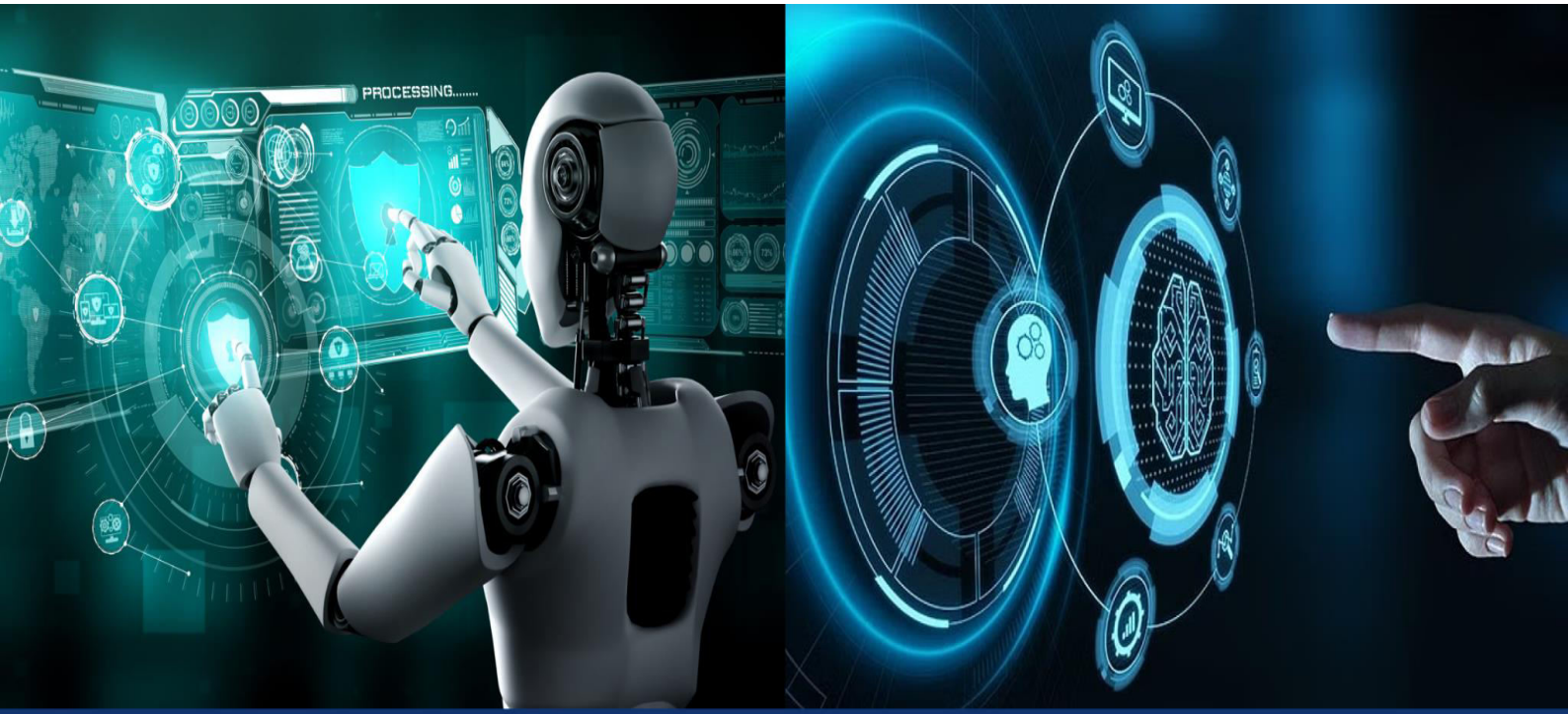
ISSN(O): 2320-9801

ISSN(P): 2320-9798



International Journal of Innovative Research in Computer and Communication Engineering

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 9.927

Volume 14, Issue 5, May 2026

© 2026 IJIRCCE | Volume 14, Issue 5, May 2026 DOI: 10.15680/IJIRCCE.2026.1405018

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Advanced & Hybrid Voting System Using Blockchain Technology

Elakkiya K[1], Eswaramoorthi M[1], Gayathiri M[1], Gowri M[1], Mr. R. Raja Mon Singh, M.E., [2]

Department of Artificial Intelligence and Data Science, Christ the King Engineering College, Coimbatore, Tamil Nadu, India[1]

Assistant Professor, Department of Artificial Intelligence and Data Science, Christ the King Engineering College, Coimbatore, Coimbatore, Tamil Nadu, India[2]

ABSTRACT: The credibility of democratic systems relies heavily on the integrity and transparency of electoral processes. Traditional voting mechanisms, including paper ballots and electronic voting machines, suffer from several drawbacks such as centralized control, susceptibility to manipulation, lack of transparency, and delayed result declaration. To address these limitations, this paper proposes a Blockchain-Based E-Voting System that leverages decentralized ledger technology to ensure secure, transparent, and tamper-proof elections. The system utilizes Ethereum-compatible blockchain networks and smart contracts written in Solidity to automate vote validation, storage, and counting. A modern frontend built using React, TypeScript, and Vite provides an intuitive voting interface, while Supabase serves as a cloud backend for authentication, election metadata, and audit logging. Wallet-based voter authentication using MetaMask ensures secure participation and prevents duplicate voting. Experimental evaluation demonstrates that the proposed system significantly improves trust, efficiency, and transparency while reducing operational overhead. The results validate blockchain as a viable solution for secure digital voting systems.

KEYWORDS: Blockchain, EVM; sharding; post-quantum attacks; deep learning; security; scalability

I. INTRODUCTION

An election system is a crucial part of democracy and a catalyst for the progression of a country. Conducting a fair and equitable election in a country in which democracy has not yet been firmly established poses significant challenges, particularly in the absence of a reliable voting system [1]. The vulnerability of paper-based voting systems to tampering and fraud by influential groups or individuals poses a significant threat. Newer Electronic Voting Machines (EVMs) that use biometrics have addressed some of these concerns. However, they often operate as “black boxes”, meaning that voters cannot accurately verify their votes. This lack of transparency undermines trust in the voting process. Furthermore, current EVM voting systems are prone to manipulation by a single authority [1].

In response to this issue, researchers have turned their attention to emerging technologies, such as blockchain, as a potential way to enhance transparency and security in voting systems. Blockchain [2] is a distributed, immutable, and tamper-resistant public ledger that offers several important characteristics. Notably, one of its key features is immutability, which ensures that once data are recorded on the blockchain, they cannot be altered or deleted. This is achieved by requiring each generated block to include the digest of the previous block, forming an unbreakable chain that guarantees the integrity and permanence of the blockchain. Any attempt to tamper with existing blocks disrupts the integrity of the chain, rendering the blockchain obsolete and unreliable [3].

To operate a blockchain, an authoritative consensus is essential, and it is one of the most critical features of this technology. In many countries, electoral systems are legally required to enforce specific regulations to prevent unauthorized activities and misconduct during elections. But consensus mechanisms that are specially designed to manage cryptocurrency operation or general-purpose blockchain are just too unsophisticated to handle the complex permission and access systems required for electoral processes [4].

© 2026 IJIRCCE | Volume 14, Issue 5, May 2026 DOI: 10.15680/IJIRCCE.2026.1405018

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

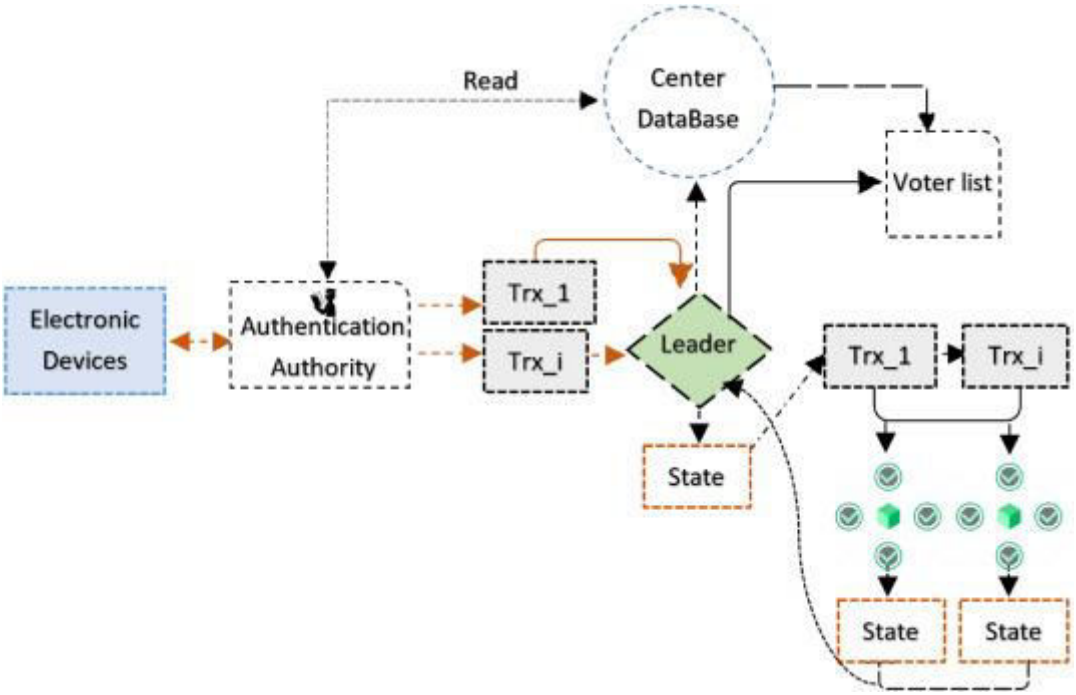


Fig 1: Blockchain-based electronic voting systems

Therefore, this paper proposes a consensus mechanism that employs a controlled level of authority, akin to an authorized block, to include or exclude specific entities based on their authorized permissions within the electoral system. This approach ensures transparency, ballot integrity, and immutability while maintaining necessary regulation without granting any entity excessive or unconventional permissions.

Blockchain technology, due to its transparency, is considered a promising tool for implementing modern and innovative voting processes [5,6]. However, scalability and performance are significant concerns in existing proposed blockchain-based e-voting systems. To address this issue, researchers have explored sharding techniques, such as [7,8], which involve partitioning the blockchain into smaller shards. Nevertheless, most of their proposed methods uses shuffle sharding that involves selecting shards and nodes randomly, failing to create data-contracted shards and introducing new latency-related issues discussed in Section 2.3. In our study, we adopt a category-based sharding approach, in which the blockchain is divided into shards based on the category or type of data stored.

Moreover, preserving the confidentiality of voter privacy while maintaining transparency in a blockchain is crucial. Several studies have employed various encryption techniques to ensure user privacy. Some proposals involve using a third-party server for verification, while others suggest storing voter information directly on the blockchain to validate voter identity. However, using a third-party server does not provide adequate security and immutability, and storing voter information on the blockchain can potentially breach voter privacy and anonymity.

II. RELATED WORK

In this section, we introduce previous work related to this research in the context of blockchain-based e-voting systems and consider three significant issues associated with this research: security, consensus and verification, and sharding.Many previous studies have attempted to develop protocols for blockchain-based e-voting systems and create incentive schemes for cryptocurrencies. Our work is motivated by recent advances.

Kevin et al. discussed blockchain voting, highlighting its elimination of central authority and enabling of vote verification by anyone. They suggested Hyperledger Fabric as a viable blockchain solution. Das et al. [17] proposed a blockchain-based voting system integrated with face recognition. However, their method and others have limitations, including scalability and extensive computational requirements. Additionally, their use of an msp system to validate voters

© 2026 IJIRCCE | Volume 14, Issue 5, May 2026 DOI: 10.15680/IJIRCCE.2026.1405018

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

undermines privacy, and the Raft consensus mechanism used by their system is not feasible for electoral system permissions and access. Khoury et al. [18] proposed a decentralized trustless voting platform using Ethereum and mobile numbers to register each voter in the system. Also proposed an Ethereum-based voting system using smart contracts. Neloy et al. [10] suggested an Ethereum network-based system with user verification via Metamask wallet, face recognition, and deepface analysis.

proposed a system using unique identification like Aadhar Card numbers or OTPs for authentication and Ethereum blockchain, integrating with traditional Electronic Voting Machines. Although researchers from [10] proposed Ethereum-blockchain-based e-voting systems aiming for secure voting, performance and scalability issues were not adequately addressed. Many of these proposals use OTPs or third-party servers, which do not provide adequate security and immutability. Additionally, storing voters' unique identifiers on solidity smart contracts can potentially breach voter privacy and anonymity. Neloy et al. [10] efficiently utilized solidity smart contracts to reduce transaction costs, but relying on an Ethereum-based network could lead to centralization and high gas costs for large-scale elections. Yousif et al. [9] proposed a hybrid blockchain (PSC-Bchain) combining Proof of Credibility and Proof of Stake to address energy consumption and scalability issues in blockchain-based e-voting systems. They employed Ethereum smart contracts and a sharding mechanism to enhance security and performance. However, this approach introduces additional computational complexity and increased gas fees. Moreover, their approach does not fully address voter privacy, as it uses a third-party server called a managed server to store node and voter information. This poses a severe risk to system integrity and voter privacy, as the data stored on the managed server are not part of an immutable ledger. Additionally, their proposal does not adequately address the potential risk of single points of failure that could occur from this server.

III. THE PROPOSED BLOCKCHAIN-BASED E-VOTING SYSTEM

Our proposed voting system is designed to ensure a secure and fair election process. It encompasses several key features such as decentralization, security, cost-effectiveness, voter verifiability, auditability, anonymity, fairness, and ease of use. These features guarantee that all voters have an equal opportunity to cast their ballots, which are then accurately and securely counted. To verify each voter's information, we use biometric and facial recognition systems. These systems authenticate user information retrieved from the National Identification Database (NID) through a secure cryptographic signature mechanism. To prevent fraud and double voting, we've developed a multiparty cryptographically secure token verification system. This system ensures the protection of the voter's identity and privacy while checking whether a valid voter has already cast their vote.

This paper presents a novel approach to consensus called the Hierarchical Authoritative Consensus (HAC) model. In this section, we discuss the details of the proposed hybrid consensus model and provide a clear perspective of its design. The consensus model integrates a dependable signing mechanism that ensures the authenticity of each participant involved in voting. This feature is crucial for maintaining the system's integrity. Furthermore, our hybrid consensus model employs a hierarchical authorization and access-control system. This innovative approach allows us to capitalize on the beneficial features of both public and private blockchains while simultaneously mitigating their drawbacks. This balance contributes significantly to the efficiency and security of the consensus model.

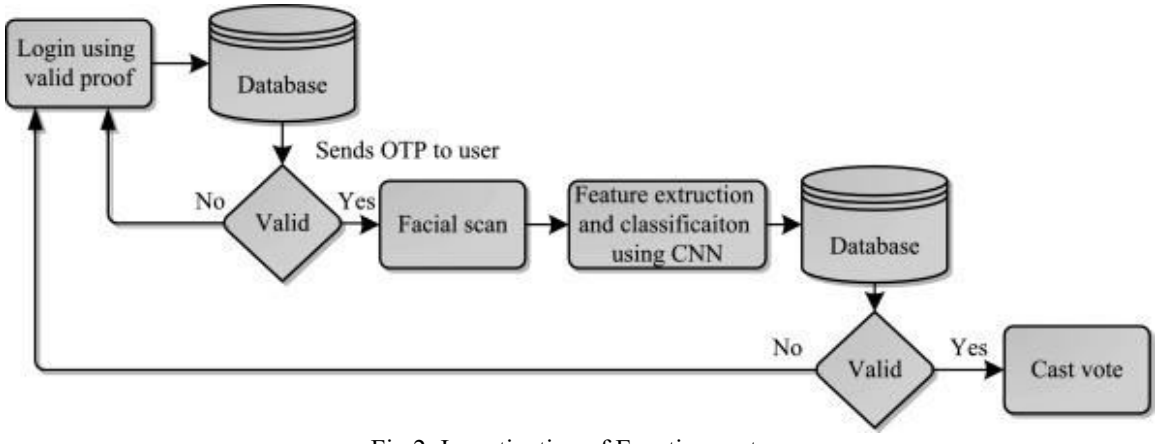


Fig 2: Investigation of E-voting system

© 2026 IJIRCCE | Volume 14, Issue 5, May 2026 DOI: 10.15680/IJIRCCE.2026.1405018

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Proposed a consensus algorithm, POV, for decentralized arbitration through voting. POV theoretically achieves transaction finality with one confirmation. However, the study lacks experimental evaluation, and multilevel access control is unclear. Wang et al. introduced CW-DPoS, a strategy to improve node activity and fairness in the DPoS consensus algorithm, resulting in performance enhancements. However, security risks and real-world election complexities are not addressed. Yuanyuan et al. proposed DT-DPoS, enhancing the DPoS consensus algorithm's security and scalability with an Eigen Trust model and ring signatures against DoS and collusion attacks. A theoretical analysis supported its effectiveness.

The hybrid blockchain system proposed differs from combining two separate blockchains, using a single blockchain with hierarchical and separate layers for permission and access based on the user within the consensus mechanism. This approach offers the benefits of public and private chains without compromising security. By maintaining sensitive election authoritative access and control of the public network, the model ensures secure, fair voting as per law regulations while preserving the transparency and accountability of a public blockchain by sharing all ledgers publicly. Operating on a public network also ensures greater immutability.

IV. RESULTS AND DISCUSSION

The proposed blockchain-based e-voting system was successfully implemented and evaluated using Ethereumcompatible blockchain networks. The system enabled secure wallet-based voter authentication, accurate vote casting, immutable storage of votes on the blockchain, and real-time result visualization. Smart contracts strictly enforced voting rules such as allowing only one vote per wallet and validating candidate selections. Any attempt at duplicate voting was automatically rejected, demonstrating the effectiveness of the system in preventing common electoral frauds. Supabase was used as a backend service to manage election metadata, candidate information, and audit logs. While vote data was securely stored on-chain, off-chain logs improved accountability by recording transaction details such as timestamps and transaction hashes. The hybrid architecture balanced decentralization with efficient system management. Performance testing showed that vote confirmation times varied depending on the blockchain network, with local Hardhat providing instant results and public test networks showing acceptable latency for small to medium-scale elections. Compared to traditional voting systems, the proposed solution reduced administrative effort, improved transparency, and increased voter trust through public verifiability of results.

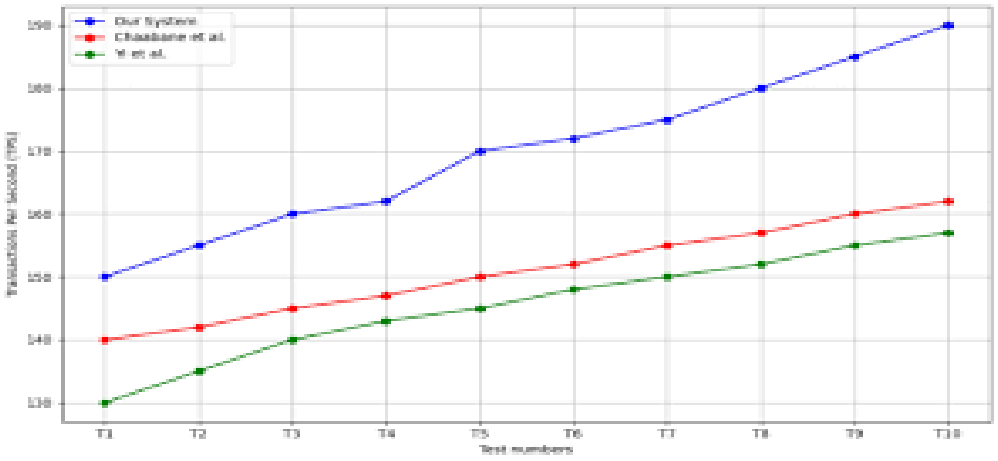


Fig 3: E-Voting System Based on Blockchain for Enhanced University Elections

The system is designed to accommodate real-world electoral systems, incorporating roles such as returning officers (election administrators) who oversee polling stations in specific areas. Polling officers, acting as block validators or miners, are authorized by returning officers, creating a multi-layer system of permission and access. This structure ensures the integrity and security of the voting process, establish voter trust and confidence. The following section discusses various users and their roles in the electronic voting system.

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

We conducted blockchain system experiments, focusing on block generation rate, throughput, and memory usage based on sharding, post-quantum cryptography, and block modularity. We integrated advanced post-quantum cryptographic algorithms (Dilithium-2 and Dilithium-3) with general elliptic curve cryptography for robust security. The experiments explored the benefits and challenges of sharding without block modularity, sharding with block modularity, and system performance without sharding. We also investigated the system's behavior without sharding and block modularity. The aim was to assess the impact of sharding and block modularity on system performance and efficiency.

V. CONCLUSION

This paper presented a secure, transparent, and decentralized blockchain-based e-voting system designed to overcome the limitations of traditional voting mechanisms. By integrating Solidity smart contracts, wallet-based authentication, and a modern web interface, the system eliminated centralized vulnerabilities and ensured election integrity. Automated vote validation and counting reduced human intervention and operational overhead. The successful implementation and evaluation confirm that blockchain technology is a promising solution for building trustworthy and efficient digital voting platforms. Future enhancements can further strengthen the system's capabilities. The integration of zero-knowledge proof techniques can provide stronger voter anonymity while maintaining verifiability. Biometric or government-issued digital identity authentication can enhance voter validation and prevent wallet misuse. Mobile application development and the adoption of Layer-2 blockchain solutions can improve accessibility, scalability, and cost efficiency. Additional improvements such as advanced analytics, multi-language support, and DAO-based election governance can make the system suitable for large-scale real-world elections.

REFERENCES

[1]. K. Patidar and S. Jain, "Decentralized E-Voting Portal Using Blockchain," Proc. 10th Int. Conf. Computing Communication and Networking Technologies (ICCCNT), 2019.
[2]. C. K. Adiputra, R. Hjort, and H. Sato, "A Proposal of Blockchain-Based Electronic Voting System," World Conf. Smart Trends in Systems, Security and Sustainability, 2018.
3]. R. Bulut, A. Kantarci, S. Keskin, and S. Bahtiyar, "Blockchain-Based Electronic Voting System for Elections," Int. Conf. Computer Science and Engineering, 2019.
[4]. G. Dagher, P. Babu, M. Milojkovic, and J. Mohler, "BroncoVote: Secure Voting System Using Ethereum's Blockchain," Int. Conf. Information Systems Security and Privacy, pp. 96–107, 2018.
[5]. A. Singh and K. Chatterjee, "SecEVS: Secure Electronic Voting System Using Blockchain Technology," Int. Conf. Computing, Power and Communication Technologies, 2019.
[6]. L. A. Ajao et al., "Blockchain Integration with Multimodal Biometric Authentication for Secure E-Voting," IEEE Access, vol. 13, 2025.
[7]. E. Tyagi et al., "Next-Generation E-Voting Security using Blockchain Technology," Int. Conf. Intelligent and Secure Engineering Solutions, 2025.
[8]. R. Barelli, M. D'Onghia, and S. Longari, "Toward Secure Electronic Voting: A Survey on E-Voting Systems and Attacks," IEEE Access, vol. 13, 2025.
[9]. Abuidris, Y.; Kumar, R.; Yang, T.; Onginjo, J. Secure large-scale E-voting system based on blockchain contract using a hybrid consensus model combined with sharding. Etri J. 2021, 43, 357–370. [Google Scholar] [CrossRef]
[10]. Neloy, M.N.; Wahab, M.A.; Wasif, S.; All Noman, A.; Rahaman, M.; Pranto, T.H.; Haque, A.B.; Rahman, R.M. A remote and cost-optimized voting system using blockchain and smart contract. IET Blockchain 2023, 3, 1–17. [Google Scholar] [CrossRef]
[11]. Vaidya, C.; Kirnapure, C.; Rithe, J.; Sonkusare, D.; Khade, P.; Kharche, K. An Approach Towards Decentralized E-Voting. In Proceedings of the IEEE 2023 11th International Conference on Emerging Trends in Engineering & Technology-Signal and Information Processing (ICETET-SIP), Nagpur, India, 28–29 April 2023; pp. 1–6. [Google Scholar]
[12]. Curran, K. E-Voting on the Blockchain. J. Br. Blockchain Assoc. 2018, 1, 1–6. [Google Scholar] [CrossRef]
[13]. Peralta, R.; Brandão, L.T.A.N. NIST First Call for Multi-Party Threshold Schemes; National Institute of Standards and Technology: Gaithersburg, MD, USA, 2023. [CrossRef]
[14]. Ducas, L.; Kiltz, E.; Lepoint, T.; Lyubashevsky, V.; Schwabe, P.; Seiler, G.; Stehlé, D. Crystals-Dilithium: A Lattice-Based Digital Signature Scheme; IACR Transactions on Cryptographic Hardware and Embedded Systems; IACR: Bochum, Germany, 2018; pp. 238–268. [Google Scholar]

www.ijircce.com | e-ISSN: 2320-9801, p-ISSN: 2320-9798| Impact Factor: 9.927| ESTD Year: 2013|

International Journal of Innovative Research in Computer and Communication Engineering (IJIRCCE)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

[15]. Ghose, P.; Sharmin, S.; Gaur, L.; Zhao, Z. Grid-search integrated optimized support vector machine model for breast cancer detection. In Proceedings of the 2022 IEEE International Conference on Bioinformatics and Biomedicine (BIBM), Las Vegas, NV, USA, 6–8 December 2022; pp. 2846–2852. [Google Scholar]

[16]. Ghose, P.; Uddin, M.A.; Acharjee, U.K.; Sharmin, S. Deep viewing for the identification of COVID-19 infection status from chest X-Ray image using CNN based architecture. Intell. Syst. Appl. 2022, 16, 200130. [Google Scholar] [CrossRef]

[17]. Das, S.K.; Saha, S.; DasGupta, S. Decentralized Voting: A Blockchain-Based Voting System. In Proceedings of the Applications of Networks, Sensors and Autonomous Systems Analytics: Proceedings of ICANSAA 2020; Springer: Berlin/Heidelberg, Germany, 2022; pp. 33–45. [Google Scholar]

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INNO SPACE SJIF Scientific Journal Impact Factor

doi crossref

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details