IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 5, April 2025
Impact Factor: 7.67

Blockchain-Based E-Voting Models

Prof. Pritesh Patil, Deep Pawar, Chinmay Kalokhe , Ritesh Korade
Department of Information Technology,
AISSMS Institute of Information Technology, Maharashtra, India
Corresponding Author: Deep Pawar (deeppawar640@gmail.com)

Abstract: *Elections are crucial in democracies today, but most people across the globe lack confidence in their electoral systems. This is a critical problem for democracy. Even in the best democracies such as India, America, and Japan, election processes still have serious issues. Vote rigging, EVM hacking, election fraud, and booth capturing are serious issues in holding free and fair elections.*

This research examines issues with existing election systems and presents a blockchain-based e-voting model as a potential solution. The suggested system evaluates various blockchain platforms offering Blockchain-as-a-Service (BaaS) and examines their effectiveness in providing a secure, decentralized, and transparent e-voting system. This method will surpass the drawbacks of existing voting systems and will ensure the anonymity of the voter and the openness and verifiability of the results to the public.

An electronically compliant voting system has been an area of challenge for long. Distributed Ledger Technology (DLT) is a paradigm shift in the information technology industry with secure, tamper-proof, and decentralized solutions in multiple areas. Blockchain as a disruptive technology can enhance e-voting systems as more robust, secure, and efficient.

This paper presents a blockchain-based e-voting system that applies cryptographic security, transparency, and verifiability to provide a secure and tamper-free election process. The suggested model fulfills essential e-voting needs and provides end-to-end verifiability, making it a prime candidate to replace current voting systems. Comprehensive analysis of the framework proves its effectiveness in providing a secure, transparent, and reliable election process.

Keywords: Elections

I. INTRODUCTION

Researches have been conducted on electronic voting systems that make voting easy and convenient via the mobile phone, computer, or other media. In spite of this, no large-scale uses of these technologies have been reported due to issues related to their security that can potentially affect the voting process itself. This work introduces a blockchain-based electronic voting system, targeted to improve the security, facilitate voter privacy, and enhance trustworthiness as well as transparency.

Blockchain is a distributed digital ledger, commonly known for its use in securing digital currency transactions such as Bitcoin. It is a chain of increasing records, referred to as blocks, that are cryptographically chained to provide data integrity and security. Although initially created for digital currencies, blockchain technology is now being used across industries because it is immutable, transparent, and tamper-resistant.

With the rapid advancement of digital technologies, there is growing interest in transitioning from traditional voting systems to more efficient, accessible, and technology-driven platforms. Electronic voting (e-voting) systems, which allow citizens to vote using mobile devices, personal computers, or other internet-enabled tools, have the potential to revolutionize electoral participation by eliminating logistical barriers and increasing voter turnout. These systems can also streamline the voting process, reduce human error, and accelerate vote counting and result declaration.

To address the security and trust challenges in e-voting, researchers and technologists have turned to blockchain — a decentralized, tamper-resistant ledger platform. Originally built to secure digital transactions, blockchain has shown tremendous promise in fields like supply chain management, healthcare, finance, and governance. Its key attributes —

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 5, April 2025
Impact Factor: 7.67

immutability, cryptographic protection, transparency, and decentralization — make it an ideal foundation for constructing an electronic voting system that is both highly secure and publicly trustworthy.

II. LITERATURE REVIEW

1.**Zaghloul et al. (2021) – d-BAME: Distributed Blockchain-Based Anonymous Mobile Electronic Voting**
Zaghloul, Li, and Ren propose d-BAME, an electronic voting system based on blockchain to enhance voter anonymity and security. The system uses a distributed ledger to prevent fraud and ensure transparency and verifiability for mobile voting. The authors discuss the application of zero-knowledge proofs and cryptographic techniques to ensure voter anonymity while maintaining election integrity. The research demonstrates the feasibility of anonymous and decentralized voting, overcoming common vulnerabilities in conventional e-voting systems.

2.**Jafar et al. (2021) – Blockchain for Electronic Voting System: Review and Open Research Challenges**
Jafar, Aziz, and Shukur provide an extensive overview of blockchain-based e-voting systems, examining existing frameworks, security concerns, and implementation challenges. The study highlights the advantages of blockchain, such as immutability, decentralization, and transparency. However, it also outlines open research issues including scalability, privacy, and regulatory concerns that must be addressed before widespread adoption. This work serves as a foundation for further research aimed at strengthening blockchain-based e-voting solutions.

3.**Abeyratne&Monfared (2016) – Blockchain-Ready Manufacturing Supply Chain Using Distributed Ledger**
Abeyratne and Monfared explore the use of blockchain in managing manufacturing supply chains. They demonstrate how distributed ledgers can enhance traceability, security, and operational efficiency. The study emphasizes the use of smart contracts to automate compliance and transaction verification, thereby removing intermediaries. Their research showcases blockchain's potential to create tamper-proof and decentralized logistics systems, improving authenticity and transparency in product tracing.

4.**Lin & Liao (2017) – A Survey of Blockchain Security Issues and Challenges**
Lin and Liao deliver a comprehensive review of the security vulnerabilities associated with blockchain technology. They classify key threats including 51% attacks, Sybil attacks, double-spending, and privacy leaks. The paper also assesses current cryptographic solutions and suggests enhancements to strengthen blockchain security. This survey provides critical insights into threat models, which are essential for the development of secure applications such as blockchain-based e-voting systems.

5.**Monrat et al. (2019) – A Survey of Blockchain: Applications, Challenges, and Opportunities**
Monrat, Schelén, and Andersson offer a broad overview of blockchain technology, covering its applications, advantages, and technical challenges. They examine its use across sectors like finance, healthcare, supply chains, and e-voting, emphasizing its role in enabling decentralization, transparency, and data integrity. The study also discusses challenges such as scalability and energy consumption and identifies key areas for future research. The authors conclude by underscoring blockchain's transformative potential and the hurdles that must be overcome for mainstream adoption

Table 1: Major Literature Review

Authors & Year of Publication	Title & Source	Methodology Adapted
Zaghloul, E., Li, T., & Ren, J. (2021)	"d-BAME: Distributed blockchain-based anonymous mobile electronic voting." IEEE Internet of Things Journal	Proposed a distributed blockchain-based e-voting system using zero-knowledge proofs and cryptographic tools to ensure voter anonymity and integrity.
Jafar, U., Aziz, M. J. A., & Shukur, Z. (2021)	"Blockchain for electronic voting system—review and open research challenges." Sensors	Presented a systematic review on blockchain-based voting systems, identifying major security benefits and existing research gaps.
Abeyratne, S. A., & Monfared, R. P. (2016)	"Blockchain ready manufacturing supply chain	Applied blockchain concepts to manufacturing logistics, emphasizing

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429 Volume 5, Issue 5, April 2025 Impact Factor: 7.67

	using distributed ledger." IJRET	transparency, traceability, and reliability in distributed environments.
Lin, I.-C., & Liao, T.-C. (2017)	"A survey of blockchain security issues and challenges." International Journal of Network Security	Detailed a range of blockchain vulnerabilities including 51% attacks, Sybil attacks, and data privacy issues.
Monrat, A. A., Schelén, O., & Andersson, K. (2019)	"A survey of blockchain from the perspectives of applications, challenges, and opportunities." IEEE Access	Comprehensive overview of blockchain's capabilities across sectors, highlighting technical barriers and deployment challenges.
Khan, K. M., Arshad, J., & Khan, M. M. (2020)	"Investigating performance constraints for blockchain-based secure e-voting system." Future Generation Computer Systems	Investigated bottlenecks in e-voting systems using blockchain, with focus on latency, throughput, and energy efficiency.
Adiputra, C. K., Hjort, R., & Sato, H. (2018)	"A proposal of blockchain-based electronic voting system." IEEE WorldS4 Conference	Proposed an e-voting model leveraging blockchain smart contracts to improve transparency, privacy, and auditability.
Dimitriou, T. (2020)	"Efficient, coercion-free and universally verifiable blockchain-based voting." Computer Networks	Designed a blockchain voting framework focusing on preventing voter coercion and ensuring verifiability of votes.

III. SYSTEM ARCHITECTURE

The AI-Powered Learning Platform is intended to make learning enjoyable, interactive, and accessible to students. It solves the problem of distraction caused by social media. The platform is constructed with essential elements that work together to provide a smooth and secure learning experience.

An e-voting system based on blockchain usually has a few major components that work together to make online elections safe, open, and tamper-proof. The fundamental part is the blockchain network, which is a shared ledger to record and verify votes. Each vote is treated as a transaction and is recorded as a block in the chain, thus making it unchangeable and traceable. The system comprises voter authentication modules that authenticate the identity of the voters through secure methods like biometrics, OTP, or digital signatures. Once authenticated, voters can use the voting interface, usually a web or mobile application, to cast their vote securely. The vote is then encrypted and sent to the smart contract level, which holds the election's rules in line, checks inputs, and initiates recording of the votes to the blockchain. A consensus system (like Proof of Authority or Practical Byzantine Fault Tolerance) guarantees the nodes are consistent regarding whether transactions are valid or not. Moreover, audit and result modules also allow real-time counting of votes and checking of results in a comprehensible way without violating voter anonymity. The system is usually maintained by cloud infrastructure for scalability purposes as well as ease of access, making it a secure, efficient, and irreversible online voting process.

As per this, the architecture of blockchain e-voting system integrates both front-end and back-end components to offer an end-to-end smooth, secure, and trustworthy voting process online. At the front-end, the users interact with the system using an accessible web or mobile app that is easy to use, e.g., multi-language support and assistive technologies. This interface is coupled with a middleware layer that provides secure communication, session management, and data validation before forwarding the data to the blockchain network.

The authentication module is essential to guarantee that only qualified voters can vote. It interfaces with national identity databases or other authentication services and uses methods like Public Key Infrastructure (PKI), digital certificates, facial recognition, or two-factor authentication. Once a voter is successfully authenticated, they are

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 5, April 2025
Impact Factor: 7.67

provided with a one-time, unique token or credential. This maintains their anonymity and does not allow them to vote twice.

Once a vote has been made, it is digitally signed and encrypted to safeguard voter anonymity and the integrity of the vote. The encrypted vote is then implemented using smart contracts, automated election officials programmed with voting regulations (e.g., time limits, voting eligibility, and vote duplication detection). Smart contracts timestamp each vote and maintain an auditable record.

The blockchain layer includes distributed nodes (election authorities or validators) which verify and append transactions (votes) to the ledger using a consensus algorithm optimizing speed, scalability, and fault tolerance. Nodes have a synchronized, tamper-proof version of the voting record.

A dashboard and analytics layer provides election officials and observers with timely statistics without exposing the voters. The results calculation module gathers the votes directly from the blockchain, where it is accurate and transparent, and stakeholders or third-party auditors can verify the data.

In addition, backup and recovery mechanisms, encryption standards, and regulatory compliance procedures (e.g., GDPR or local election regulations) are integrated to promote trust and resilience. This architecture, which integrates blockchain, cryptography, and secure communication, establishes a strong foundation for transacting transparent, secure, and scalable online elections**.**

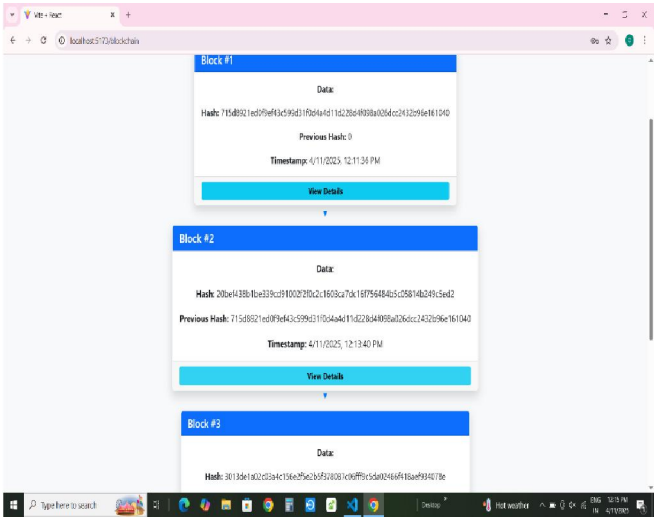

Fig. 1. System ‘s Block Diagram

IV. PROPOSED SYSTEM

The proposed blockchain e-voting system is meant to bring forth a secure, transparent, and trusted online voting system using decentralized ledger technology. Enrolled voters sign up on a secure web portal where their identity is verified via digital IDs or biometric sign-in. A voter, post-registration, may cast a single vote using an easy-to-use web or mobile app. A vote is encrypted and stored as a transaction in the blockchain and hence it becomes tamper-proof, time-stamped, and irreversible. Smart contracts are used to implement the voting rules and counting automatically without any interference from humans, and with the assurance that the result is correct and trustworthy. Since the blockchain ledger is decentralized and open to the public, it introduces transparency into the voting process and allows independent audit. Not only does the system enhance security and reduce the chance of fraud, but also bring the voters within reach by making remote participation feasible.

According to the suggested blockchain-based e-voting framework, the architecture of the system is designed to eradicate the constraints of conventional voting systems like human errors, electoral tampering, and restricted access. Voters, after verification, are issued a distinct cryptographic key that keeps their vote anonymous but verifiable on the public blockchain. The blockchain ensures that the vote cast cannot be tampered with or erased, thereby ensuring the

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 5, April 2025
Impact Factor: 7.67

integrity of the election. All the transactions for voting are pooled into blocks, verified by consensus protocols such as Proof of Stake (PoS) or Practical Byzantine Fault Tolerance (PBFT), and added to the blockchain. This distributed system removes the need for a central entity to control or monitor the process of voting, reducing the risk for manipulation or single points of failure.

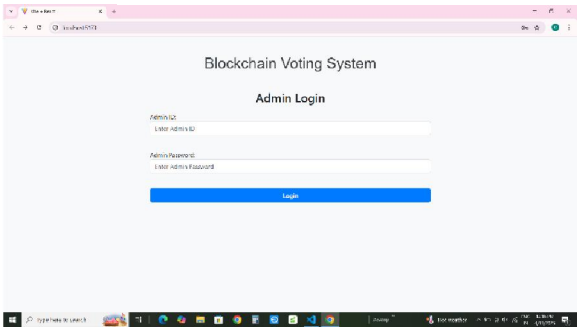

Fig. 2. Admin Login

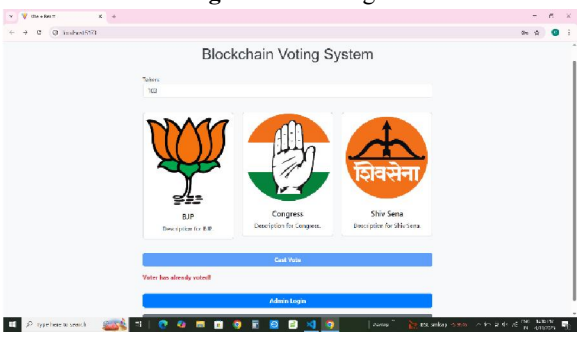

Fig. 3. Voting Option

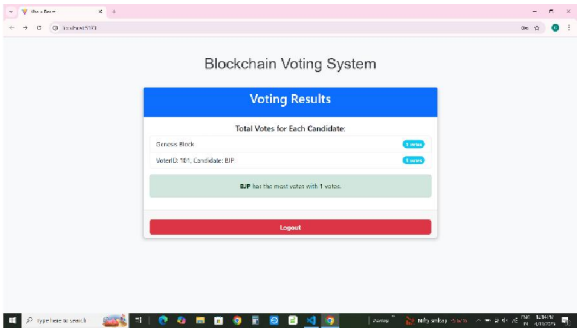

Fig. 4. Voting Result

V. CONCLUSION

The blockchain-based voting system designed in this research illustrates an open, secure, and tamper-evident method of electronic voting. Relying on the decentralization and immutability of blockchain technology, the system ensures every vote is recorded in a proper manner and cannot be tampered with, and double voting is prevented by voter verification processes. Use of cryptographic hashing, block chaining, and monitoring of the votes also adds to the election process's integrity. Not only does the proposed solution address key problems in traditional voting systems, but it also provides the basis for scalable, trustworthy digital elections in the future.

.

IJARSCT
International Journal of Advanced Research in Science, Communication and Technology
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
ISSN: 2581-9429
Volume 5, Issue 5, April 2025
Impact Factor: 7.67

REFERENCES

[1] E. Zaghloul, T. Li, and J. Ren, "d -BAME: Distributed blockchain-based anonymous mobile electronic voting," IEEE Internet Things J., vol. 8, no. 22, pp. 16585–16597, 2021. https://doi.org/10.1109/JIOT.2021.3074877

[2] U. Jafar, M. J. A. Aziz, and Z. Shukur, "Blockchain for electronic voting system—review and open research challenges," Sensors, vol. 21, no. 17, p. 5874, 2021. https://doi.org/10.3390/s21175874

[3] S. A. Abeyratne and R. P. Monfared, "Blockchain ready manufacturing supply chain using distributed ledger," International Journal of Research in Engineering and Technology, vol. 5, no. 9, pp. 1–10, 2016. https://doi.org/10.15623/ijret.2016.0509001

[4] I.-C. Lin and T.-C. Liao, "A survey of blockchain security issues and challenges," Int. J. Netw. Secur., vol. 19, no. 5, pp. 653–659, 2017. https://doi.org/10.6633/IJNS.201709.19(5).01

[5] A. A. Monrat, O. Schelén, and K. Andersson, "A survey of blockchain from the perspectives of applications, challenges, and opportunities," IEEE Access, vol. 7, pp. 117134–117151, 2019. https://doi.org/10.1109/ACCESS.2019.2936094

[6] Z. Zheng, S. Xie, H.-N. Dai, X. Chen, and H. Wang, "Blockchain challenges and opportunities: A survey," International Journal of Web and Grid Services, vol. 14, no. 4, pp. 352–375, 2018. https://doi.org/10.1504/IJWGS.2018.10016848

[7] B. Kitchenham and S. Charters, "Guidelines for performing systematic literature reviews in software engineering," 2007.

[8] F. Þ. Hjálmarsson, G. K. Hreiðarsson, M. Hamdaqa, and G. Hjálmtỳsson, "Blockchain-based e-voting system," in 2018 IEEE 11th International Conference on Cloud Computing (CLOUD), IEEE, 2018, pp. 983–986. https://doi.org/10.1109/CLOUD.2018.00151

[9] F. Sheer Hardwick, A. Gioulis, R. Naeem Akram, and K. Markantonakis, "E-voting with Blockchain: An e-voting protocol with decentralisation and voter privacy," arXiv e-prints, arXiv-1805, 2018. https://doi.org/10.1109/Cybermatics_2018.2018.00262

[10] H. Yi, "Securing e-voting based on blockchain in P2P network," EURASIP Journal on Wireless Communications and Networking, vol. 2019, no. 1, pp. 1–9, 2019. https://doi.org/10.1186/s13638-019-1473-6

[11] S. Gao, D. Zheng, R. Guo, C. Jing, and C. Hu, "An anti-quantum e-voting protocol in blockchain with audit function," IEEE Access, vol. 7, pp. 115304–115316, 2019. https://doi.org/10.1109/ACCESS.2019.2935895

[12] B. Shahzad and J. Crowcroft, "Trustworthy electronic voting using adjusted blockchain technology," IEEE Access, vol. 7, pp. 24477–24488, 2019. https://doi.org/10.1109/ACCESS.2019.2895670