STM JOURNALS

Journal of
Software Engineering Tools & Technology Trends

ISSN: 2394-7292
Volume 12, Issue 2, 2025
May–August
DOI (Journal): 10.37591/JoSETTT

https://journals.stmjournals.com/josettt

Review JoSETTT

E-Voting Application Using Blockchain

Pratik Pawar[1,*], Shreyash Kadam[2], Harsh Thakur[3], Prabhat Thakur[4], Ambuj Kumar[5]

Abstract

Electronic voting (e-voting) is increasingly recognized as a method for improving the electoral process by enhancing security, accessibility, and efficiency. However, traditional e-voting systems present challenges, including security vulnerabilities, lack of transparency, and privacy concerns. This study presents an e-voting system powered by blockchain technology, designed to enhance decentralization, security, and protection against fraud. By leveraging blockchain's features such as immutability, transparency, and cryptographic security, this model mitigates risks related to vote tampering and unauthorized access. Smart contracts facilitate automated vote counting and verification, ensuring system integrity and auditability. Advanced cryptographic methods like zero-knowledge proofs and homomorphic encryption strengthen voter privacy while ensuring the election process remains transparent and verifiable. The paper also details the system's architecture, security evaluation, and comparison with conventional voting methods. The findings indicate that blockchain-based e-voting offers a scalable and reliable solution for more transparent electoral processes. E-voting has revolutionized the electoral process by improving accessibility and efficiency. However, traditional e-voting systems suffer from security vulnerabilities, centralization risks, and lack of transparency. This paper proposes a blockchain-based e-voting application that ensures security, decentralization, and fraud resistance. By leveraging blockchain's immutable ledger, cryptographic security, and decentralized consensus, the system mitigates risks associated with vote manipulation and unauthorized access. Smart contracts automate vote casting, verification, and counting, ensuring real-time integrity. Techniques like homomorphic encryption and zero-knowledge proofs help protect voter privacy while ensuring the voting process remains transparent and verifiable. The study presents the system's architecture, security evaluation, and comparative analysis with conventional voting systems. The results indicate that blockchain-based e-voting enhances trust, transparency, and voter confidence in democratic processes.

Keywords: Blockchain, e-voting, smart contracts, cybersecurity, transparency, cryptography, decentralization

***Author for Correspondence**
Pratik Pawar
E-mail: pratikspawar17@gmail.com

[1-4]Student, Department of Computer Engineering, Mumbai University, Vishwaniketan's Institute of Management, Entrepreneurship & Engineering Technology (iMEET) Khalapur, Raigad, Maharashtra, India
[5]Professor, Department of Computer Engineering, Mumbai University, Vishwaniketan's Institute of Management, Entrepreneurship & Engineering Technology (iMEET) Khalapur, Raigad, Maharashtra, India

Received Date: February 13, 2025
Accepted Date: March 09, 2025
Published Date: April 15, 2025

Citation: Pratik Pawar, Shreyash Kadam, Harsh Thakur, Prabhat Thakur, Ambuj Kumar. E-Voting Application Using Blockchain. Journal of Software Engineering Tools & Technology Trends. 2025; 12(2): 12–21p.

INTRODUCTION

Elections are an essential aspect of democratic governance, ensuring citizens can participate in decision-making. Conventional voting methods, whether using paper ballots or electronic systems, often struggle with inefficiencies, security vulnerabilities, and transparency concerns. These concerns affect the credibility of election results. Blockchain technology offers a promising solution for overcoming these challenges by enabling a secure and decentralized voting system [1].

Blockchain technology functions as a decentralized ledger, guaranteeing that votes cannot

be altered or manipulated. Unlike conventional electronic voting (e-voting) systems that rely on centralized servers—making them susceptible to cyberattacks and data manipulation—blockchain removes the need for a central authority, thereby increasing trust in the system. Smart contracts enhance the voting process by automatically counting and verifying votes, minimizing human involvement and the risk of errors.

The objective of this research is to design and analyze a blockchain-based e-voting application that enhances security, transparency, and voter anonymity. This study explores the implementation framework, security mechanisms, and the feasibility of blockchain in large-scale electoral systems. The proposed model uses cryptographic methods like zero-knowledge proofs and homomorphic encryption to keep votes confidential while allowing them to be verified [2].

The paper is organized as follows: In the next section, we examine current voting systems and discuss their shortcomings. The third section discusses blockchain fundamentals and their application in e-voting. The fourth section presents the proposed system architecture, while the fifth section evaluates security, scalability, and performance aspects. Finally, the sixth section concludes the paper and then discusses further research direction. With blockchain's ability to revolutionize e-voting, this research contributes to the ongoing effort to build a more secure, transparent, and democratic voting process. With blockchain's ability to revolutionize e-voting, this research contributes to the ongoing effort to build a more secure, transparent, and democratic voting process.

Voting is a fundamental pillar of democratic governance, ensuring that citizens can express their choices in leadership and policy-making. Traditional voting methods, including paper-based ballots and centralized e-voting systems, have been widely used in elections. However, these methods are often prone to inefficiencies, security vulnerabilities, and trust issue [3]. Paper-based voting is susceptible to ballot tampering, miscounts, logistical challenges, and delays in result processing, whereas e-voting systems, particularly those that rely on centralized servers, face threats such as hacking, data breaches, and unauthorized access.

This study focuses on developing a blockchain-powered e-voting system to improve security, ensure transparency, and protect voter anonymity. The study explores the system's architecture, security mechanisms, and scalability to determine its feasibility for large-scale electoral implementation.

This research paper aims to design and analyze a blockchain-based e-voting system that enhances security, transparency, voter privacy, and election integrity [4]. The key objectives of this study are:

- To examine the limitations of traditional voting systems and how blockchain can overcome these challenges.
- To explore blockchain architecture suitable for e-voting, including consensus mechanisms, cryptographic security, and smart contracts.
- To propose a secure e-voting model that ensures immutability, voter anonymity, and verifiability.
- To assess how well blockchain-based voting performs, how scalable it is, and whether it can be practically implemented in real-world elections.

With growing concerns about election security, blockchain technology offers a promising solution for creating a transparent, tamper-resistant, and decentralized voting system. This study aims to support the development of a more secure and fair electoral process for future elections.

PROBLEM STATEMENT

Ensuring the integrity and security of electoral processes is vital to democracy. Both paper-based and e-voting systems come with various challenges that can undermine their reliability. Issues include ballot tampering, logistical inefficiencies, delays in result processing, and security vulnerabilities in

centralized electronic voting systems. Cyber threats like hacking and data breaches add to the worries about maintaining transparency and fairness in elections [5].

Current e-voting solutions lack a mechanism that guarantees verifiability, transparency, and tamper resistance while preserving voter privacy. The centralized nature of these systems creates a single point of failure, increasing susceptibility to data corruption and system outages. Additionally, voter distrust stems from the inability to independently verify votes while maintaining confidentiality.

Blockchain offers a decentralized, immutable, and transparent voting method. However, issues like scalability, processing speed, and verifying voter identity continue to pose challenges. This study investigates how blockchain can be effectively implemented in e-voting to mitigate security risks, enhance transparency, and ensure election integrity while maintaining efficiency [6].

Despite advancements in digital technology, existing e-voting solutions lack a trustworthy, verifiable, and tamper-resistant mechanism that ensures voter anonymity, vote immutability, and transparent auditing. The centralized nature of these systems often results in a single point of failure, making them susceptible to hacking, data corruption, and system outages. Additionally, voter distrust arises due to the inability of voters to independently verify their votes while preserving confidentiality.

Blockchain technology provides an effective way to tackle these challenges by ensuring decentralization, transparency, security, and data integrity. However, challenges remain regarding scalability, transaction speed, voter authentication, and accessibility in large-scale elections. This research aims to investigate how blockchain can be effectively implemented in e-voting systems to mitigate security risks, enhance transparency, and ensure election integrity while maintaining voter privacy and system efficiency.

LIMITATION OF EXISTING SYSTEMS

Despite the growing adoption of e-voting systems, current implementations—whether centralized or partially decentralized—face several challenges that impact election integrity, security, and trust. Below are some key limitations of existing e-voting systems:

1. *Centralization Risks* – Conventional electronic voting systems depend on centralized servers, which exposes them to cyber threats and potential tampering. A single security lapse could jeopardize the integrity of the entire election [7].
2. *Lack of Transparency* – Conventional e-voting systems do not provide an independent audit trail, reducing voter confidence in election results.
3. *Cybersecurity Threats* – Existing systems are vulnerable to hacking, malware, and insider threats, leading to possible vote tampering or system failures.
4. *Privacy Concerns* – Many e-voting platforms fail to protect voter anonymity, risking exposure of voter identities and vote choices [8].
5. *Scalability Problems* – Large-scale elections require systems capable of handling millions of votes simultaneously without performance degradation.

METHODOLOGY

The development of a secure and transparent e-voting application using blockchain (Figure 1) requires a systematic approach to designing, implementing, and evaluating the proposed system. This methodology outlines the framework, components, and techniques used to achieve a decentralized, immutable, and verifiable voting system [9].

Research Approach

This study follows a structured approach consisting of literature review, system design, prototype development, and performance evaluation.

- *Literature Review* – Analyzing existing e-voting systems, their limitations, and blockchain-based voting solutions.

- *System Architecture Design* – Defining the structure and components of the blockchain-based e-voting system.
- *Implementation* – Developing a prototype using blockchain technology, smart contracts, and cryptographic security techniques.
- *Testing and Evaluation* – Assessing the system's security, transparency, scalability, and efficiency.

System Architecture

The proposed blockchain-based e-voting system consists of several key components:

- *Blockchain Network* – A decentralized ledger for immutable vote recording.
- *Smart Contracts* – Automate vote casting, authentication, and result computation.
- *Cryptographic Security* – Techniques like zero-knowledge proofs help maintain the privacy of voters by ensuring their identities remain anonymous.
- *User Authentication Module* – Implement reliable identity verification methods to block unauthorized access.
- *Decentralized Nodes* – Validators ensure transaction legitimacy and add votes to the blockchain.

Implementation Process

- *Blockchain Selection* – Choosing an appropriate blockchain platform (e.g., Ethereum, Hyperledger) based on security and scalability.
- *Voter Registration* – Secure authentication using biometric data or decentralized identity verification.
- *Vote Casting and Encryption* – Votes are securely encrypted before being recorded on the blockchain.
- *Vote Validation* – Blockchain nodes verify transactions to ensure vote integrity.
- *Vote Counting and Results* – Smart contracts automate vote tallying, ensuring tamper-proof results.

Security Measures

- *Zero-Knowledge Proofs* – Allow voters to prove eligibility without revealing identity.
- *Homomorphic Encryption* – Ensures encrypted votes can be counted without decryption.
- *Elliptic Curve Cryptography* – Strengthens voter authentication and digital signatures.

RESULTS

Figure 1 is the front page for a blockchain-based voting system. It explores how blockchain technology is incorporated into electronic voting (e-voting) to improve security, ensure transparency, and build trust as shown in Figure 2.

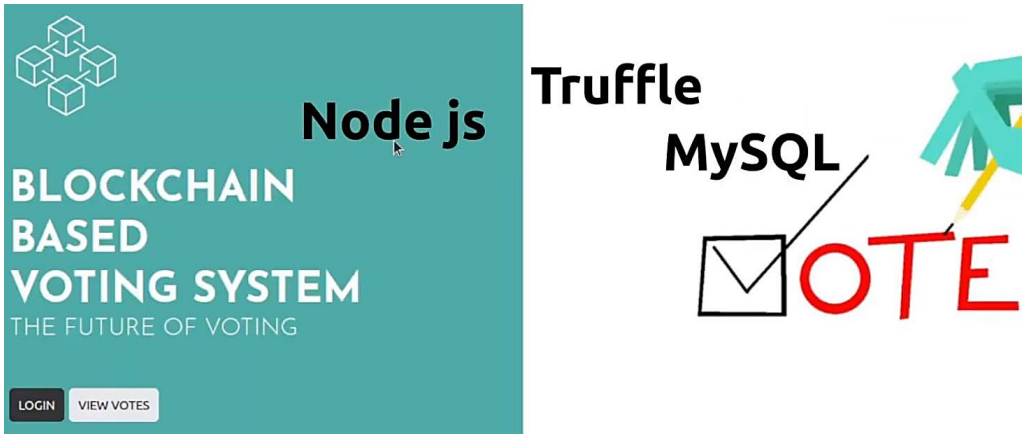

Figure 1. Blockchain-based voting system.

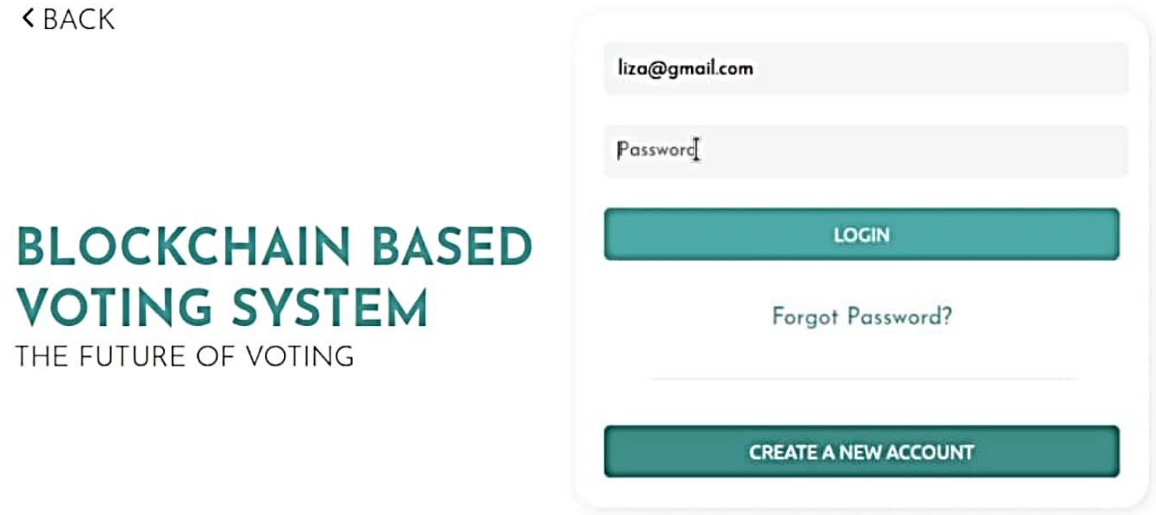

Figure 2. Voting login page.

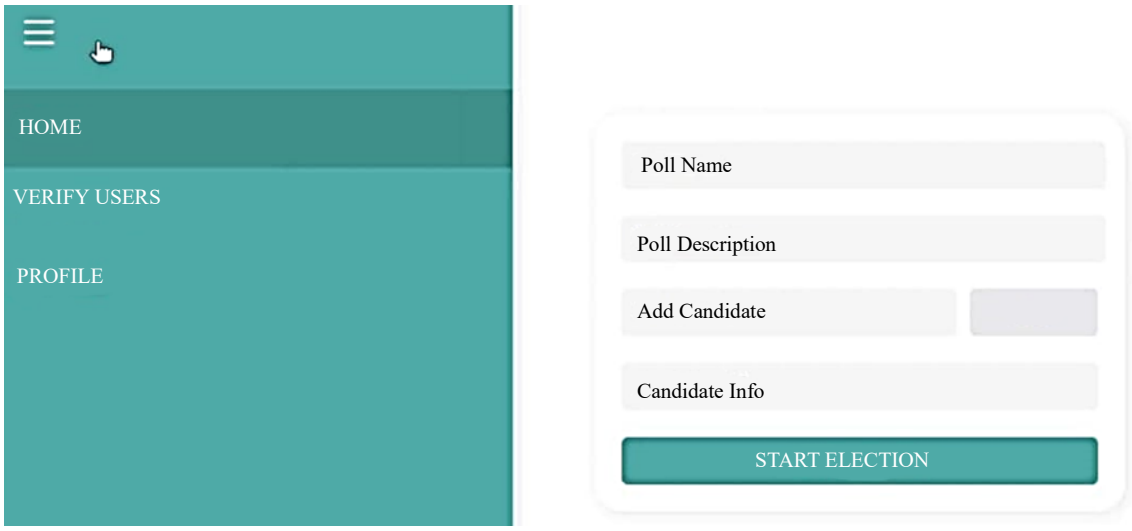

Figure 3. Credentials.

Key Elements

1. *Title:* "Blockchain-Based Voting System – The Future of Voting"
   - Suggests a modernized approach to elections using blockchain.
2. *Technology Stack:*
   - *Node.js* – Likely used for backend development.
   - *Truffle* – A structured approach to creating and evaluating smart contracts on the Ethereum blockchain.
   - *MySQL* – A relational database, possibly used for storing user credentials or vote metadata.
3. *Voting Representation:*
   - The image includes a hand marking a checkbox and the word "VOTE", symbolizing election participation.
4. *Login and View Votes Buttons:*
   - Indicates a web-based application where users can log in to vote and view results.

Figure 3 represents the login interface of a blockchain-based voting system, highlighting the authentication process for users participating in an electronic voting system. It has a simple and intuitive design with key login features, providing secure access to the platform.

The image showcases the login screen of a blockchain-based voting system, built to ensure a secure and transparent digital election process [10].

Key Elements

System Title

- Blockchain-Based Voting System – The Future of Voting
- Blockchain technology plays a crucial role in strengthening the security and integrity of elections.

User Authentication Interface

- *Email and Password Fields:* Allows access to the system exclusively for individuals who are registered voters.
- *Login Button:* Grants access to the voting platform upon successful authentication.
- *Forgot Password Option:* It helps users regain access to their accounts by recovering their credentials.
- *Create a New Account Button:* Facilitates new user registrations, ensuring inclusivity in the voting process.

Figure 4 depicts the admin dashboard of a blockchain-based voting system, which allows election administrators to set up and manage digital elections securely [11].

Key Elements

Sidebar Navigation Menu

- *Home:* The main dashboard for election management.
- *Verify Users:* Ensures only authenticated and eligible voters participate in elections.
- *Profile:* Displays admin profile and settings.

Election Setup Form

- *Poll Name and Description Fields*: Allows the admin to define the election details.
- *Add Candidate Section:* Facilitates adding candidates to the election ballot.
- *Start Election Button:* Initiates the election process, making it available for voting.

The image represents the results visualization page of a blockchain-based e-voting system, displaying the current vote count for a presidential election [12].

Key Elements in the Image

Election Title and Description

- "FOR PRESIDENT" indicates that this election is for selecting a president.
- A short description underneath provides clarity about the election.

Vote Results Representation

- Two candidates, Donald Trump and Joe Biden, are displayed.
- A bar chart illustrates how many votes each candidate received.
- The numeric count at the bottom of each bar provides precise vote counts (Trump: 1, Biden: 0).

User-Friendly Interface

- The simple and clean user interface allows voters and election officials to quickly understand the election results.
- The sidebar menu allows users to explore various sections of the platform with ease.

WORKFLOW DIAGRAM

The workflow diagram is presented in Figure 5.

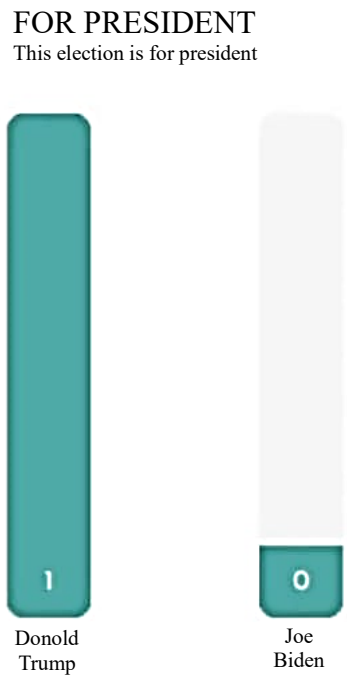

Figure 4. Election for president result.

LITERATURE REVIEW

Introduction

The increasing demand for secure, transparent, and tamper-proof voting systems has led to the exploration of blockchain technology in e-voting applications. Traditional voting systems face challenges such as fraud, coercion, and lack of transparency, which blockchain technology aims to address.

Blockchain and Its Application in E-Voting

Blockchain is a distributed digital ledger that securely logs transactions, ensuring they remain unalterable and transparent. Researchers have explored its potential in e-voting due to its ability to ensure integrity, security, and verifiability of votes. Different consensus mechanisms, including proof-of-work (PoW), proof-of-stake (PoS), and Byzantine fault tolerance (BFT), have been explored to determine their suitability for e-voting systems.

Security and Privacy Concerns

Ensuring security is a fundamental concern in e-voting systems. Blockchain offers cryptographic encryption and decentralized validation, reducing the risk of tampering and fraud.

However, privacy concerns persist, as blockchain's transparency can conflict with voter anonymity. To improve voter privacy, techniques like zero-knowledge proofs (ZKPs) and ring signatures have been suggested as potential solutions.

Existing Blockchain-Based E-Voting Systems

Several blockchain-based e-voting models have been proposed and implemented. Notable examples include Follow My Vote, which utilizes blockchain for end-to-end verifiability and transparency; Agora, a decentralized voting platform that ensures immutability and auditability; and Ethereum-based voting systems that leverage smart contracts to create tamper-resistant election processes.

Challenges and Limitations

Although blockchain-based e-voting offers several benefits, it also encounters challenges like scalability issues, high computational demands, and regulatory hurdles.

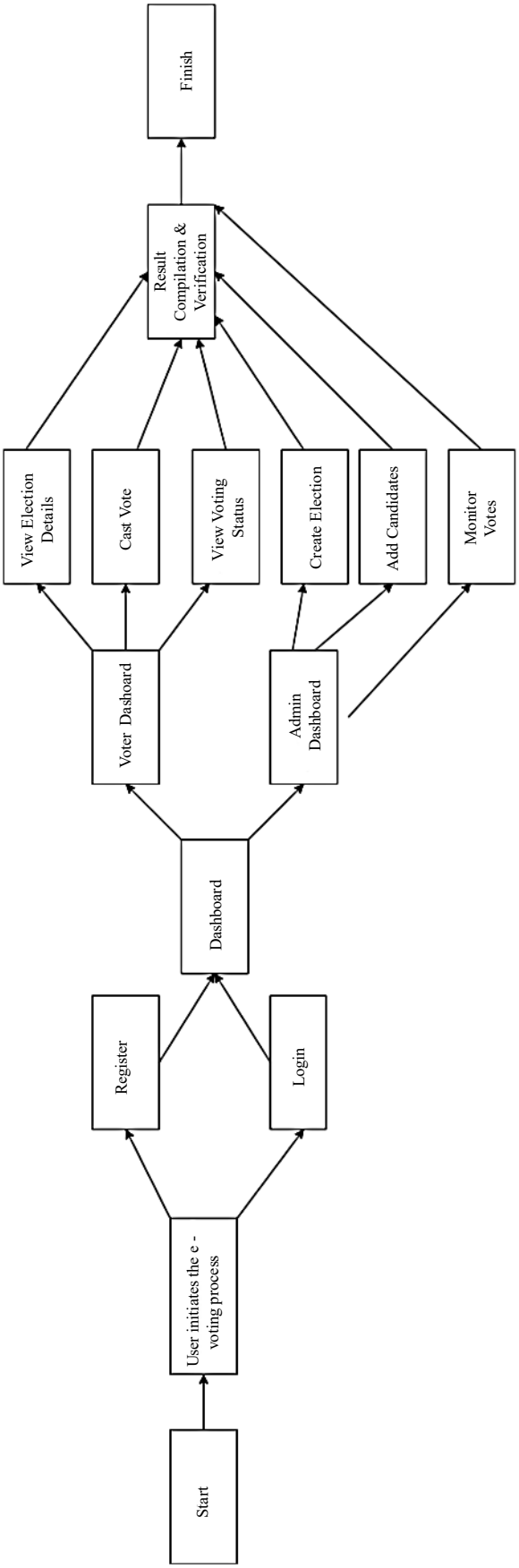

Figure 5. Work flow of E-voting application

High energy consumption in PoW-based systems and the potential for 51% attacks are also significant obstacles. Making the platform easy to use and accessible for non-technical users is an important challenge that must be tackled.

Future Directions and Research Gaps

Further research is required to address scalability, interoperability, and hybrid approaches that combine blockchain with other secure technologies. To enable the adoption of blockchain-based e-voting systems, it is essential to develop appropriate regulatory frameworks. Exploring novel consensus mechanisms that are energy-efficient and secure can also enhance the feasibility of blockchain e-voting.

CONCLUSION

Blockchain technology offers a promising way to create secure and transparent e-voting systems. Although challenges remain, continuous research and advancements are improving its implementation, making it a strong contender for future elections. By integrating blockchain into e-voting, elections can become more secure, transparent, and efficient, paving the way for a more trustworthy voting process. By leveraging the decentralized and immutable nature of blockchain, e-voting applications can mitigate risks associated with traditional voting methods, such as fraud, tampering, and unauthorized access.

Additionally, features like cryptographic encryption, smart contracts, and decentralized consensus mechanisms ensure voter anonymity, data integrity, and trustworthiness in the electoral process.

To achieve widespread adoption, it is essential to overcome challenges like scalability, verifying voter identities, and meeting regulatory requirements.

Future research should focus on optimizing blockchain protocols for large-scale elections, improving user accessibility, and ensuring compliance with legal frameworks. Despite these challenges, blockchain-based e-voting has the potential to revolutionize democratic systems by fostering greater voter confidence and participation. With the advancement of technology, blockchain has the potential to revolutionize electoral processes globally by ensuring greater security and transparency.

REFERENCES

1. Swan M. Blockchain: Blueprint for a New Economy. Sebastopol, CA, USA: O'Reilly Media, Inc; 2015.
2. Zheng Z, Xie S, Dai HN, Chen X, Wang H. Blockchain challenges and opportunities: a survey. Int J Web Grid Serv. 2018; 14 (4): 352–375.
3. Jafar U, Ab Aziz MJ, Shukur Z, Hussain HA. A systematic literature review and meta-analysis on scalable blockchain-based electronic voting systems. Sensors. 2022; 22 (19): 7585.
4. Kshetri N, Voas J. Blockchain-enabled e-voting. IEEE Softw. 2018; 35 (4): 95–99.
5. Hjálmarsson FÞ, Hreiðarsson GK, Hamdaqa M, Hjálmtýsson G. Blockchain-based e-voting system. In: 2018 IEEE 11th International Conference on Cloud Computing (CLOUD), San Francisco, CA, USA, July 2–7, 2018. pp. 983–986.
6. Wu HT, Yang CY. A blockchain-based network security mechanism for voting systems. In: 2018 1st International Cognitive Cities Conference (IC3), Okinawa, Japan, August 7–9, 2018. pp. 227–230.
7. Xiao S, Wang XA, Wang W, Wang H. Survey on blockchain-based electronic voting. In: Barolli L, Nishino H, Miwa H, editors. Advances in Intelligent Networking and Collaborative Systems: The 11th International Conference on Intelligent Networking and Collaborative Systems (INCoS-2019). Cham, Switzerland: Springer International Publishing; 2020. pp. 559–567.
8. Jafar U, Aziz MJ, Shukur Z. Blockchain for electronic voting system—review and open research challenges. Sensors. 2021; 21 (17): 5874.
9. Hajian Berenjestanaki M, Barzegar HR, El Ioini N, Pahl C. Blockchain-based e-voting systems: a technology review. Electronics. 2023; 13 (1): 17.

10. Jafar U, Ab Aziz MJ, Shukur Z, Hussain HA. A systematic literature review and meta-analysis on scalable blockchain-based electronic voting systems. Sensors. 2022; 22 (19): 7585.
11. Spanos A, Kantzavelou I. A blockchain-based electronic voting system: Ethervote. arXiv preprint. arXiv:2307.10726. July 20, 2023.
12. Mukherjee A, Majumdar S, Kolya AK, Nandi S. A privacy-preserving blockchain-based e-voting system. arXiv preprint. arXiv:2307.08412. July 17, 2023.

