STM JOURNALS

Journal of
Web Engineering & Technology

ISSN: 2455-1880
Volume 11, Issue 3, 2024
September–December
DOI (Journal): 10.37591/JoWET

https://journals.stmjournals.com/jowet

Review JoWET

Digital Voting System Using Blockchain

Gopalakrishnan R.J.[1,*], Mandira D.N.[1], Rithik Kumar[1], Hemanth B.[1], Mary Dhivya Shamili[2], J. Ghayathri[3]

Abstract

The advent of blockchain technology has ushered in a new era of secure, transparent, and decentralized systems, providing a promising foundation for various applications, including electronic voting (e-voting). This report examines the development and deployment of a blockchain-based e-voting system designed to tackle the ongoing issues of security, transparency, and voter privacy in elections. The system utilizes blockchain's core features, including immutability, decentralization, and cryptographic security, to establish a secure and tamper-resistant voting process. The report begins with an overview of traditional e-voting systems, highlighting their vulnerability to fraud, hacking, and centralization issues. It then delves into the principles of blockchain technology, elucidating how its decentralized ledger can enhance the integrity of voting systems. The architecture of the blockchain-based e-voting system is meticulously detailed, encompassing voter registration, vote casting, vote storage, and vote tallying processes. Each stage is fortified with cryptographic techniques to ensure voter authentication, data encryption, and privacy preservation. Moreover, the report presents a comprehensive analysis of the smart contracts utilized to automate and enforce the rules of the election, thereby eliminating the need for trusted intermediaries. The analysis of consensus mechanisms, such as Proof of Stake (PoS), illustrates how they improve the system's security and efficiency. Additionally, the scalability of the system is addressed, proposing solutions to manage large-scale elections without compromising performance or security. To assess the practicality and effectiveness of the proposed system, a prototype is created and evaluated in a simulated setting. The results demonstrate significant improvements in security, transparency, and trustworthiness compared to conventional e-voting systems. The report concludes with a discussion of potential challenges, including regulatory hurdles, voter accessibility, and technological limitations, along with recommendations for future research and development to further enhance the system's capabilities. This blockchain-based e-voting system represents a significant step towards modernizing electoral processes, offering a secure, transparent, and decentralized alternative that can restore public confidence in the democratic process.

Keywords: Blockchain, voting, solidity, Truffle suite, Ethereum

***Author for Correspondence**
Gopalakrishnan R.J.
E-mail: gopiravi.edu@gmail.com

[1]Student, School of Information Science, Presidency University, Bengaluru, Karnataka, India
[2]Assistant Professor, School of Computer Science and Engineering, Presidency University, Bengaluru, Karnataka, India
[3]Associate Professor, Department of Computer Science, Presidency University, Bengaluru, Karnataka, India

Received Date: August 22, 2024
Accepted Date: September 05, 2024
Published Date: September 16, 2024

Citation: Gopalakrishnan R.J., Mandira D.N., Rithik Kumar, Hemanth B., Mary Dhivya Shamili, J. Ghayathri. Digital Voting System Using Blockchain. Journal of Web Engineering & Technology. 2024; 11(3): 8–14p.

INTRODUCTION

The rise of digital technology has profoundly changed many aspects of contemporary life, including the elections. Conventional voting methods, which depend on physical ballots and centralized databases, encounter several problems such as voter fraud, limited transparency, and inefficiencies in vote tallying. These ongoing challenges have prompted the exploration of new solutions to improve the security, transparency, and accessibility of voting processes. One particularly promising solution that has gained significant attention is the implementation of digital voting systems utilizing blockchain technology.

© STM Journals 2024. All Rights Reserved

Blockchain technology is renowned for its decentralized, transparent, and secure characteristics, offering substantial benefits that can effectively address the shortcomings of traditional voting systems. Using distributed ledger technology, blockchain-based voting systems provide tamper-proof transparent voting processes. This guarantees that votes are securely recorded and permanently stored, making it almost impossible for unauthorized individuals to alter or manipulate outcomes. In a blockchain voting system, every vote is encrypted and recorded on either a public or a private blockchain. This not only protects voter anonymity but also enables real-time auditing and verification by authorized parties. The decentralized nature of blockchain technology guarantees that no single organization can oversee the entire voting process, thereby mitigating the risk of centralized control or data breaches. Additionally, blockchain technology can significantly improve voter accessibility by allowing remote voting, particularly benefiting individuals who cannot physically attend polling stations owing to geographical constraints, disabilities, or public health concerns.

However, the transition to blockchain-based voting systems presents several challenges. Technical complexities, scalability issues, regulatory compliance, and the need for widespread public trust and understanding of technology are critical concerns that must be addressed. Additionally, safeguarding voting infrastructure from advanced cyber threats continues to be a key priority. This study delves into the intricacies of blockchain-based digital voting systems, examining their potential benefits, challenges, and the current state of their implementation across different regions to provide valuable insights into how blockchain technology can transform the electoral process, making it more secure, transparent, and accessible to all stakeholders involved.

LITERATURE REVIEW

Traditional and current digital voting systems lack transparency and can easily be exploited, leading to a lack of trust among voters. The proposed framework employs blockchain technology to guarantee transparency, dependability, and security within a voting system. The application layer of the framework handles user verification encapsulates voting system data in online databases and manages blockchain transactions. Blockchain technology offers a decentralized and unchangeable ledger, which helps prevent tampering and ensures voting system security [1].

This study proposes a framework for trustworthy electronic voting using adjusted blockchain technology, addressing the security and privacy flaws observed in electronic voting systems over the years. The framework employs efficient hashing methods, block generation and finalization, data aggregation, and result announcements through a flexible blockchain approach. This study emphasizes the importance of security, privacy, anonymity, and verifiability in the electronic voting process and highlights the suitability of blockchain technology in addressing these challenges. This study aimed to model the entire e-voting process to identify errors and flaws before implementation. This study covers the choice of appropriate hash algorithms, modifications in the blockchain, management of voting data, and measures for securing and authenticating the voting process. The study also mentions the use of biometric authentication and the orientation of electronic voting based on it to improve trust in the electoral process [2].

The study reviews various e-voting solutions based on blockchain technology, focusing on their security, reliability, and transparency. It discusses the use of biometric authentication methods such as fingerprint, iris, and facial recognition, as well as other authentication methods like mobile phone numbers and ID documents. The study compares different blockchain-based e-voting systems based on properties such as verifiability, dependability, consistency, audibility, anonymity, transparency, scalability, eligibility, authentication, and fairness. It emphasizes the importance of security properties in e-voting systems, including audibility, voter-verifiability, and data integrity The study also highlights the challenges and limitations of employing blockchain technology in e-voting include the necessity for comprehensive testing of consensus mechanisms and cryptographic systems [3].

© STM Journals 2024. All Rights Reserved

This study introduces a blockchain-based voting system (BBVS) designed for parliamentary elections in Jordan, focusing on the requirements for secure, private, and trustworthy electronic voting. BBVS is a private, centralized blockchain tested in a simulated environment to ensure election transparency and security. It employs synthetic voter benchmarks to assess the system's performance, accuracy, and integrity and incorporates new algorithms and techniques for blockchain creation, vote casting, and authenticity verification. This study underscores the benefits of blockchain technology in elections by addressing issues such as denial-of-service attacks, reliability, security, integrity, transparency, voter exclusion, and anonymity. It eliminates the necessity for a trusted third-party and lowers the costs and challenges associated with traditional voting systems. The system is tailored and evaluated for the Jordanian Parliamentary election, implementing a two-tier voting process in which voters cast ballots for both groups and specific members within that group. The winners were determined by using the open proportional list method. This study examines various iterations of the system, such as sequential voting, multi-threaded voting with synchronization across all voting processes, and multi-threaded voting with synchronization managed separately for each district. Performance improvements are achieved through algorithms and techniques, such as Quicksort [4].

This study provides a comprehensive review by various authors of different BBVSs, aiming to pinpoint the challenges and solutions associated with using blockchain in voting. It helps researchers develop an appropriate voting framework tailored to their country's needs while highlighting the advantages of blockchain in voting systems, such as minimizing identity uncertainty and enhancing accountability and transparency. They also highlight issues with traditional electronic voting processes, such as lack of accessibility, vulnerability to hacking and falsification, and the inability of voters to verify the outcomes. The study mentions that many researchers have proposed solutions that inherit the diverse features of the blockchain for voting. This underscores the necessity of grasping these features and their relevance in blockchain voting. The authors also mention the use of a virtual agreement system and the separation of the polling process from the counting phase to ensure that the outcome is not revealed during the polling process. They discussed the importance of verification in allowing only qualifying electors to cast their ballots and prevent alteration of voting data. They also highlighted the weaknesses of traditional paper-based voting methods, such as the need for all electors to vote and the vulnerability to multiple nominees. The study concludes by asserting that blockchain offers a novel approach to data storage, distribution, and updating and is expected to be crucial in the development of future interactive internet systems. The survey conducted in this study helps researchers find the best way of voting with blockchain and identifies the limitations and solutions of voting mechanisms based on blockchain. The study concludes by highlighting that blockchain offers a unique method for storing, distributing, and updating data and is anticipated to be essential in the evolution of future interactive internet systems. The survey conducted in this study helps researchers find the best way of voting with blockchain and identifies the limitations and solutions of voting mechanisms based on blockchain [5].

This study introduces a new consensus protocol called Credit-Delegated Byzantine Fault Tolerance (CDBFT) to improve efficiency and reduce abnormal node participation in the consensus process. CDBFT utilizes a voting reward and punishment scheme based on credit evaluation to stimulate reliable node enthusiasm and enhance system stability. The protocol includes mechanisms for credit rewards and punishments based on node behavior and involvement in the consensus process. Various stages, such as View-Change, View-Change-Ack, and New-View, are implemented to ensure data consistency and monitor block generation in the system. This research received support from the Natural Science Foundation of China, and the authors thank the anonymous reviewers for their valuable feedback [6].

The evolution of research on electronic voting systems has progressed from public cryptographic concepts to blockchain-based proposals. Literature surveys on e-voting systems prior to blockchain protocols were limited, with early examples focusing on Direct Recording Electronic (DRE) voting machines. A systematic literature review analyzed both centralized and decentralized e-voting systems

© STM Journals 2024. All Rights Reserved

with a focus on common characteristics and technological trends. Various publications have delved into the classification criteria and challenges of implementing e-voting systems, with a shift towards blockchain-based surveys in recent years [7].

The Secure Internet Voting Protocol (SIVP) is designed to meet security requirements like eligibility, democracy, privacy, verifiability, accuracy, fairness, robustness, receipt-freeness, and coercion-resistance. The protocol is based on blind signatures and public key cryptography, ensuring secure electoral processes Colombia aims to implement electronic voting, and the SIVP protocol offers a comprehensive solution with reduced computational load using ECC [8].

This study introduced a novel method for strengthening online voting systems by utilizing Rivest-Shamir-Adleman (RSA) and decryption techniques to ensure strong data protection. The online voting management system ensures the authenticity and confidentiality of the voting process through advanced technologies such as face recognition, fingerprint scanning, and One Time Password (OTP) transmission [9].

This study explores the application of intelligent agents and multi-agent system principles within the Auditable Blockchain Voting System (ABVS), emphasizing how blockchain technology enhances the ability to create an auditable and verifiable electronic voting system. Electronic voting systems are described as solutions to traditional voting issues, with e-voting encompassing the registration, authentication, authorization, voting, counting, and verification processes. Smart contracts in the Ethereum network have been proposed to enhance the ABVS system by enabling the automatic execution of contract terms without third-party involvement. The ABVS voting process involves casting votes broadcast to nodes for verification and processing within a multi-agent system framework [10].

METHODOLOGY

The methodology section outlines the detailed processes and techniques employed to develop a blockchain-based voting system. This encompasses system design, smart contract development, security protocols, and testing methods, with an emphasis on developing a secure, transparent, and tamper-resistant voting platform. Ethereum was chosen for its strong smart contract features and broad usage, while the Proof of Stake (PoS) mechanism was selected to improve scalability and minimize energy usage. Multiple nodes were deployed to ensure redundancy and availability, and the nodes were geographically distributed to enhance security. The system components included a front-end interface developed using React.js to ensure a user-friendly experience, back-end services handled by Node.js to interact with the blockchain, and smart contracts written in Solidity to manage voter registration, ballot creation, vote casting, and result tallying.

In smart contract development, the voter registration contract's purpose is to register voters securely and assign unique identifiers. Voters submit encrypted personal details to the system and the smart contract verifies eligibility based on predefined criteria. After verification, the voter's information was recorded on the blockchain with a distinct ID. The ballot creation contract aims to create and manage ballots for elections, where election officials input candidate information and election parameters, and the smart contract generates a ballot stored on the blockchain, accessible only to registered voters. The vote casting contract allows secure and anonymous vote casting; voters log in using their unique ID and cast an encrypted vote through the smart contract, which then validates and records the vote on the blockchain. The result tallying contract counted votes and published results automatically after the voting period, ensuring transparency.

Security measures were paramount, with all sensitive data, including voter information and votes, encrypted using the Advanced Encryption Standard (AES-256) before storage or transmission. Multi-factor Authentication (MFA) was implemented, requiring voters to pass the MFA to access the voting system, adding an extra layer of security. All smart contracts undergo independent security audits to

© STM Journals 2024. All Rights Reserved

detect and address vulnerabilities. Distributed denial-of-service (DDoS) protection was implemented using cloud-based services to prevent disruptions during the voting process. Testing and validation included unit testing on individual smart contracts; integration testing to ensure seamless system component interaction; user acceptance testing (UAT) involving potential voters and election officials to test usability and effectiveness; and security testing, which included penetration testing and vulnerability scanning to identify and mitigate security risks.

Deployment began with pilot testing, where a pilot election was conducted with a small group of voters to test the system under real-world conditions, and feedback was gathered and utilized to implement the required improvements. Following successful pilot testing, the system was deployed for a large-scale election with continuous monitoring and support to ensure smooth operation. This methodology outlines the comprehensive steps taken to develop, secure, test, and deploy BBVSs. The system uses blockchain technology to guarantee transparency, security, and integrity during the electoral process. Further research and development should focus on scalability and usability improvements to cater to larger populations and diverse electoral contexts.

RESULTS AND DISCUSSIONS

The blockchain-based voting system demonstrated high security and transparency during the pilot testing. Voter registration was seamless, and smart contracts accurately managed vote casting and result talking without human intervention. Data encryption and MFA ensure voter privacy and system integrity. Integration and security testing revealed no significant vulnerabilities, thereby confirming the robustness of the system. User feedback highlighted ease of use and trust in the system. However, scalability remains a concern for large populations, as shown in Figures 1–4. Future efforts should aim to optimize the system to handle higher transaction volumes and improve user interfaces to better serve a diverse range of voters.

Figure 1. Home page.

Figure 2. Voting page.

© STM Journals 2024. All Rights Reserved

Figure 3. Confirming of the vote.

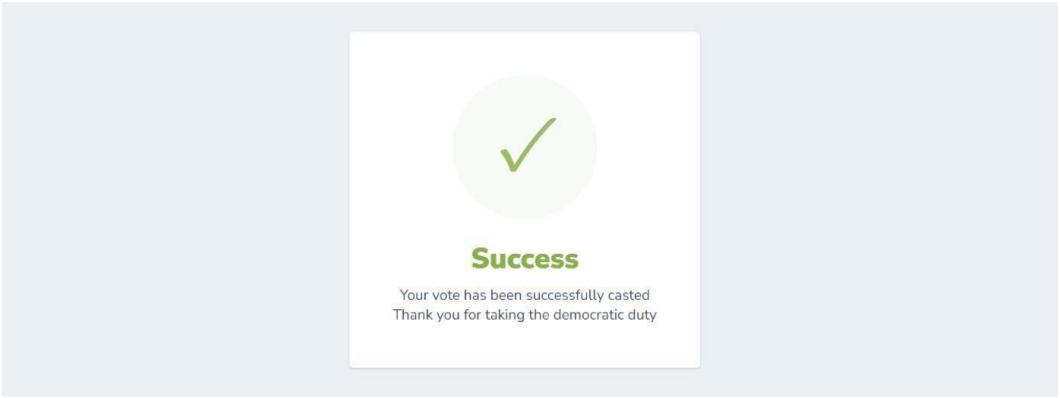

Figure 4. Voting success.

CONCLUSION

The blockchain-powered voting system effectively improves the security, transparency, and reliability of the election process. Pilot testing confirmed its ability to securely manage voter registration, voting, and tallying of results. Although scalability needs improvement for larger elections, the system's robust security measures and user-friendly interface show significant promise. Further development will focus on optimizing performance and expanding usability.

REFERENCES

1. Farooq MS, Iftikhar U, Khelifi A. A framework to make voting system transparent using blockchain technology. IEEE Access. 2022;10:59959–69. doi:10.1109/ACCESS.2022.3180168.
2. Pramulia D, Anggorojati B. Implementation and evaluation of blockchain-based e-voting system with Ethereum and Metamask. 2020 International Conference on Informatics, Multimedia, Cyber and Information System (ICIMCIS), Jakarta, Indonesia. 2020, pp. 18–23. doi: 10.1109/ICIMCIS51567.2020.9354310.
3. Sliusar V, Fyodorov A, Volkov A, Fyodorov P, Pascari V. Blockchain technology application for electronic voting systems. 2021 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (ElConRus), St. Petersburg, Moscow, Russia. 2021, pp. 2257–61. doi:10.1109/ElConRus51938.2021.9396400.
4. Chaudhary S, Shah S, Kakkar R, Gupta R, Alabdulatif A, Tanwar S, et al. Blockchain-based secure voting mechanism underlying 5G network: A smart contract approach. IEEE Access. 2023;11:76537–50. doi:10.1109/ACCESS.2023.3297492.
5. Oprea SV, Bâra A, Andreescu AI, Cristescu MP. Conceptual architecture of a blockchain solution for e-voting in elections at the university level. IEEE Access. 2023;11:18461–74. doi:10.1109/ACCESS.2023.3247964.

© STM Journals 2024. All Rights Reserved

6. Jayakumari B, Sheeba SL, Eapen M, Anbarasi J, Ravi V, Suganya A, et al. E-voting system using cloud-based hybrid blockchain technology. J Saf Sci Resilience. 2024;5:102–9. doi:10.1016/j.jnlssr.2024.01.002.
7. Dhulavvagol PM, Bhajantri VH, Totad SG. Blockchain Ethereum clients performance analysis considering E-voting application. Procedia Comput Sci. 2020;167:2506–15. doi:10.1016/j.procs.2020.03.303.
8. Satizábal C, Páez R, Forné J. Secure Internet Voting Protocol (SIVP): A secure option for electoral processes. J King Saud Univ Comput Inf Sci. 2022;34:3647–60. doi:10.1016/j.jksuci.2020.12.016.
9. Rathee G, Iqbal R, Waqar O, Bashir AK. On the design and implementation of a blockchain-enabled e-voting application within IoT-oriented smart cities. IEEE Access. 2021;9:34165–76. doi:10.1109/ACCESS.2021.3061411.
10. Pawlak M, Poniszewska-Marańda A, Kryvinska N. Towards the intelligent agents for a blockchain e-voting system. Procedia Comput Sci. 2018;141:239–46. doi:10.1016/j.procs.2018.10.177.

© STM Journals 2024. All Rights Reserved