Journal of Analysis and Computation (JAC)
(An International Peer Reviewed Journal), www.ijaconline.com, ISSN 0973-2861
Volume XVIII, Issue II, July-December 2024

BLOCKCHAIN BASED DIGITAL VOTING SYSTEM

[1]Nimisha swami, [2]Nikita Agarwal, [3]Dixit Bansal, [4]Deepanshu Moorjani

[1]Assistant Professor, Department of Information Technology, JECRC College
[2]B. Tech Student, Department of Information Technology, JECRC College
[3]B. Tech Student, Department of Information Technology, JECRC College
[4]B. Tech Student, Department of Information Technology, JECRC College

ABSTRACT:

Election stands as cornerstone of democracy, pivotal for maintaining a fair and equitable society. However, conventional voting systems suffer from inherent flaws such as opacity, susceptibility to manipulation, and potential human errors. In response to these challenges, blockchain technology has emerged as a promising solution, offering enhanced election security and transparency. This research paper presents a detailed blueprint and implementation of a blockchain-based electronic voting system. Leveraging distributed ledger technology, the proposed system ensures the secure and transparent recording of votes, thus mitigating the risk of manipulation or alteration of results. Notably, the system prioritizes voter anonymity and guards against in stances of double voting. Built upon the Ethereum blockchain platform, the system utilizes smart contracts to automate the voting process, including tasks such as vote counting and tallying. This decentralized approach eliminates the need for centralized authority, enhancing the system's integrity and resilience. Compared to traditional voting mechanisms, the proposed blockchain-based electronic voting system demonstrates superior performance in terms of transparency, security, and efficiency Moreover, its adaptable design facilitates seamless integration with existing election processes, rendering it a viable option for future adoption. While platforms like Simply Voting and Election Buddy offer secure and customizable online voting services for businesses, blockchain-based e-voting systems present unique advantages in terms of security, transparency, and decentralization.

Keywords- Blockchain, Electronic Voting, Smart Contracts, Consensus Algorithms, identity verification, privacy, security, trust, authentication.

[1] INTRODUCTION

The process of voting within organizations varies depending on factors such as size, structure, and governance model. Common steps include issuing as all to vote, verifying eligibility, selecting a voting method, preparing the ballot, conducting the voting period, tallying votes, announcing results, and acting based on the outcome. It is imperative that the voting process remains fair, transparent, and accessible to all eligible participants.

Organizational voting presents concerns regarding eligibility verification, accessibility, security, privacy, transparency, fairness, and the accuracy and integrity of results. Addressing the concerns requires meticulous planning, clear communication, and robust systems and processes to uphold the integrity of the voting process.[1]

The primary objectives of this research are:

- To validate the voting system to ensure that only legitimate voter scan participate.
- To safeguard voter identity by separating it from the cast vote.

In the context of shares in organizations, two common types are ordinary shares and preferred shares. Ordinary shareholders may benefit from pre-emptive rights, which allow them to maintain their ownership stake by purchasing additional shares before they are offered to the public or new investors.[2]

Voting shares differ significantly from preferred shares in situations of bankruptcy or solvency. In such cases, preferred shareholders are typically entitled to receive payment a head of common shareholders. Additionally, common shareholders may receive lower dividend payments compared to preferred shareholders or may not receive dividends at all.

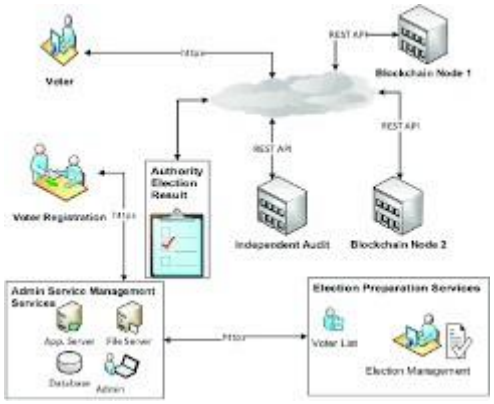
Regarding voting rights, shareholders typically have the authority to elect or remove company directors, inspect corporate and financial records, and appoint auditors. In companies limited by shares with equity share capital, each shareholder usually holds one vote on each are solution affecting the company.

Furthermore, a shareholder in a company limited by shares may assign all or part of the outstanding debt on their shares, even I fit hasn't been called up. However, until the relevant amount is called up, the shareholder does not possess voting rights pertaining to that portion of the debt.

[2] BACKGROUND STUDY

This paper provides an in-depth analysis of existing literature concerning scalable blockchain-based electronic voting systems. They begin by defining electronic voting and examining the

potential advantages and disadvantages as sociated with implementing blockchain technology in this context. The paper synthesizes various studies on the usability, scalability, and security aspects of blockchain-based electronic voting systems.[2] Additionally, the authors conduct a meta-analysis of the compiled content, offering insights into the current state of research on scalable blockchain-based electronic voting systems. This comprehensive examination of the literature serves as a valuable resource for academics, professionals, and legislators considering the adoption of blockchain technology in electronic voting systems.



2.1 Blockchain Technology

The blockchain functions as a decentralized and distributed ledger, comprising interconnected blocks. Within each block, there resides a set of transactions, each representing an event or action. An essential component of each block is its header, containing the previous block's hash, timestamp, nonce, and Merkle root. This header serves as the unique identifier for the block, linking it to its predecessor. The timestamp verifies the block's data and assigns a creation time for digital documents, while the nonce, a single-use number, plays a crucial role in the proof-of-work mechanism. The Merkle root act salsa data structure, encapsulating all transactions within the block by generating a digital fingerprint of the entire transaction set.[3] This design ensures the immutability and security of blockchain transactions. Once data are recorded within a block, altering them requires modifying all subsequently recorded blocks. Consequently, blockchain transactions become tamper-proof. Figure 1 illustrates the blockchain's structure, showing a chain of blocks securing transactions with has his and other data. These blocks are distributed and replicated across a network of peers.

Blockchain technology relies on robust security measures grounded in cryptographic principles, effectively mitigating manipulation and fraudulent activities. Its decentralized nature enables universal access to the distributed database among network participants, governed by a consensus algorithm. As a result, blockchain data remains immutable, tracing

and validating transactions transparently and securely.

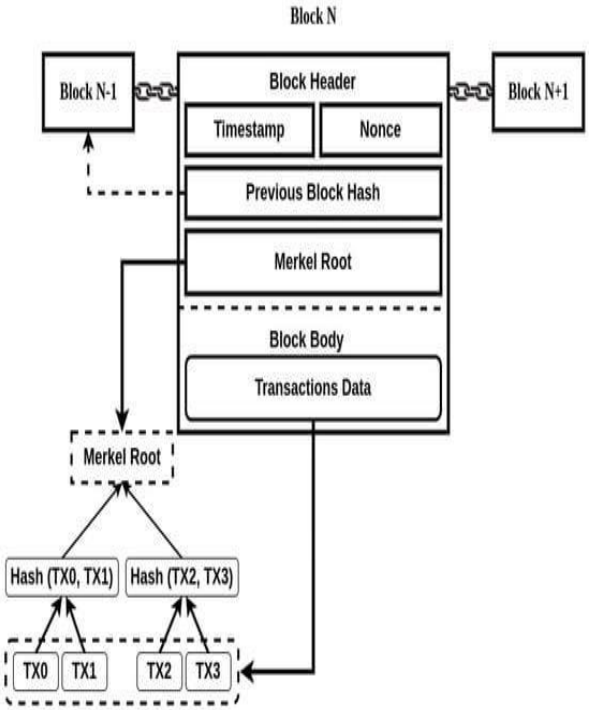


Fig 2.1 The blockchain structure.

2.2 Blockchain Applications across Domains

Blockchain technology has become a revolutionary trend across various sectors, with its application in e-voting systems garnering significant interest due to its potential to enhance electoral integrity and transparency. However, blockchain's utility extends beyond e-voting, as it is equally valuable in other domains, each with distinct requirements and objectives. This section aims to compare and analyze blockchain applications in different domains such as healthcare, financial services, supply chain management, cloud computing, education, and the Internet of Things (IoT), highlighting their parallels and contrasts with their use in e-voting systems.[5]

2.2.1 Blockchain in Healthcare

In healthcare, blockchain is utilized for secured sharing, patient privacy, and interoperability among different healthcare systems. While it shares some aspects withe-voting, such as an emphasis on data security and privacy, blockchain in healthcare deals with continuous data flow and personal health records, contrasting with the singular event of casting and recording votes in e-voting systems.

2.2.2 Blockchain in Financial Services

In financial services, blockchain technology revolutionizes transactions and trust mechanisms, bringing transparency and verifiability like its role in e-voting. However, it differs in handling continuous financial transactions compared to the discrete event of voting.

2.2.3 Blockchain in Supply Chain Management

Blockchain technology in supply chain management focuses on improving transparency, reducing fraud, and enhancing efficiency. While both supply chain management and e- voting systems benefit from blockchain's immutability and transparency, supply chain management uniquely utilizes blockchain for continuous tracking of goods and transactions, contrasting with the periodic nature of elections.

2.3 Implementations of Blockchain-Based E-Voting Systems

1. Lux oft: Lux oft Holding Inc., a global IT service provider, is developing an e-voting infrastructure for the world's first consultative vote on blockchain in Zug, Switzerland. They utilized Hyperledger Fabric to create an authorized blockchain network, including applications and algorithms. Zug's digital ID registration app, based on Ethereum and authorized through Port, enables voters to cast their ballots. Lux oft intends to open source this technology and establish a Government Alliance Blockchain to promote blockchain adoption in public institutions.
2. Votem: Specializing in election management, Votem offers the Cast Iron platform built on blockchain technology. This platform provides features such as a distributed database, immutability, permission-based access, and an audit trail. Votem has successfully managed over 13million voters without any instances of fraud, compromise, attacks, or hacking, underscoring the security and reliability of their system.
3. Voat z: Voat z is a blockchain-based mobile voting tool launched in 2018 in West Virginia for overseas military voters in the 2018 midterm elections in the United States. It incorporates biometric validation, such as fingerprints or retinal scans, to ensure voter authentication. However, a recent study revealed major security flaws in Voat z, allowing attackers to monitor, edit, or block ballots in large quantities.
4. POLYAS: POLYAS offers an electronic voting system utilizing blockchain technology, which has been used in both public and private sectors since the company's inception in1996. Their online voting system has received certification from Germany's Federal Office for Information Security and meets requirements such as anonymity, accuracy, singularity, verifiability, and auditability. POLYAS is employed by several significant companies in Europe and the USA for managing electronic voting systems.
5. Polys: Polys is an online voting system leveraging blockchain technology to ensure security and transparency in the voting process and results. The system guarantees immutability of

both voting procedure and results, with transparent cryptographic techniques employed to protect voter anonymity. Voters can verify the validity and integrity of their votes at any time.

6. Dicentra Vote: Developed by a team at an iterate location in Vienna, Dicentra Vote is a blockchain-based solution for virtual meetings. It uses a public Ethereum network with Proof of Authority consensus and permissioned validator nodes. The smart contract constructs a Merkle tree of all voting rights on-chain, and Zero-Knowledge Succinct Non-Interactive Argument of Knowledge (zk-SNARK) generates proofs for voting rights off-chain. Notably, Dicentra Vote does not address national political elections.[8]

[3] METHODOLOGY

This review follows the PRISMA protocol, ensuring a transparent and rigorous view process, and applies systematic literature review principles to selected papers. The objective is to provide a fair analysis of the available information using a systematic approach designed to minimize bias.

The hypothesis of this study posits that by leveraging the distinctive features of blockchain technology, such as decentralization, immutability, and transparency, it is possible to address weaknesses and constraints inherent in traditional voting systems. This hypothesis suggests that integrating blockchain technology leads to enhanced democratic procedures.

A systematic search technique is employed to discover relevant research, utilizing precise keywords and concepts related to electronic voting and blockchain. Boolean operators ("OR", "AND") are used to combine keywords and filter search results effectively.

The literature search is conducted using reputable databases (ACM, IEEE, Elsevier, Springer, and Scopus). Titles are initially screened to identify potentially relevant papers, followed by a thorough review of the full text of the articles to determine their relevance to the research questions.[9]

Inclusion criteria are established to ensure the relevance and validity of selected papers, including direct relevance to blockchain-based e-voting systems, availability in English, access to full-text versions, and alignment with the study's focus.

Exclusion criteria are also defined to maintain the quality and uniqueness of the data set, including removal of duplicate titles, exclusion of non-English papers, book chapters, officially retracted papers, and those not aligned with the topic of blockchain-based e-voting systems.

Figure 2 illustrates the methodology employed for database analysis, including the inclusion and exclusion of publications for the study's purpose.

This systematic approach ensures a comprehensive and unbiased review of the literature on blockchain-based e-voting systems.[10]

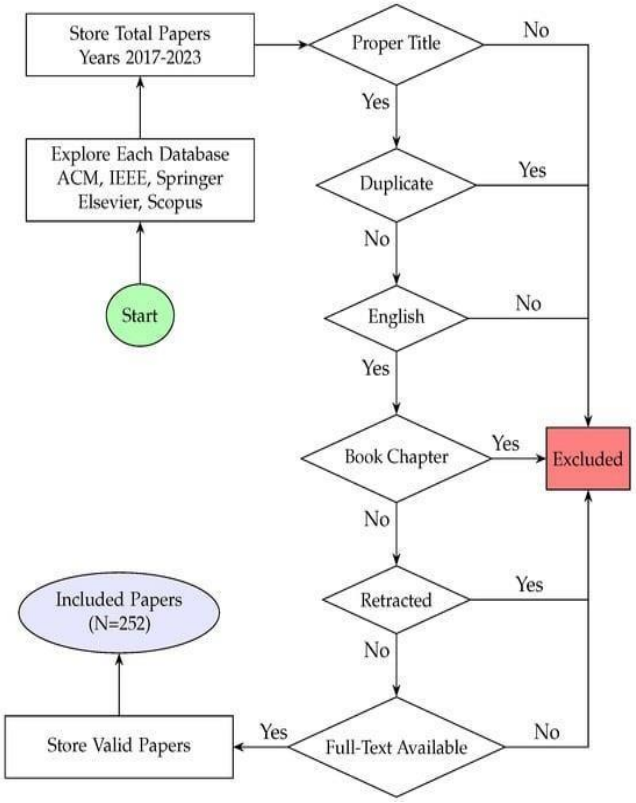


Fig 2. Procedure for database examination and paper inclusion.

[4] CONCLUSION

In conclusion, this research has provided a thorough analysis of blockchain-based digital voting systems, highlighting their potential to address weaknesses and constraints present in traditional voting systems. By leveraging blockchain technology's distinct features such as decentralization, immutability, and transparency, e-voting systems can be enhanced to ensure integrity, security, and trust in electoral processes.

Through a systematic literature review following the PRISMA protocol, we have synthesized existing research on blockchain-based e-voting systems. Our findings underscore the significance of integrating blockchain technology in electoral procedures to promote fairness, transparency, and accountability.

Furthermore, case studies of ongoing projects and implementations in the field have provided valuable insights into real-world applications of blockchain-based e-voting systems. Projects such as Lux oft, Votem, Voat z, POLYAS, Polys, and Dicentra Vote demonstrate the

diversity and potential impact of blockchain technology in revolutionizing electoral processes worldwide.

Moving forward, it is imperative to address several challenges and considerations associated with the adoption of blockchain-based digital voting systems. These include ensuring accessibility and inclusivity, mitigating security risks and vulnerabilities, addressing scalability issues, and navigating regulatory and legal frameworks.

[5] FUTURE WORK

Future research in the realm of blockchain-based digital voting systems should focus on several key is as to further advance the field:

- **Security and Privacy Enhancements:** Investigate novel cryptographic techniques and privacy-preserving mechanisms to enhance the security and privacy of blockchain-based e-voting systems, addressing concerns such as vote manipulation, coercion, and unauthorized access.
- **Scalability Solutions:** Explore scalable blockchain architectures and consensus mechanisms to accommodate large-scale electoral processes with millions of voters while maintaining efficiency and performance.
- **Usability and Accessibility Improvements:** Conduct user-centric design research to improve the usability and accessibility of blockchain-based e-voting interfaces, ensuring inclusivity for all voters, including those with disabilities or limited technical proficiency.
- **Regulatory and Legal Considerations:** Collaborate with policymakers, legal experts, and electoral authorities to develop regulatory frameworks and standards for the implementation and governance of blockchain-based e-voting systems, addressing legal challenges, and ensuring compliance with electoral laws and regulations.

REFERENCES

[1] Rihab H Sahib and Prof. Dr. Eman S. Al-Shamery.

[2] Kashif Mehboob Khan, Junaid Arshad, Muhammad Mubashir Khan Secure Digital Voting System based on Blockchain technology.

[3] Mohammad Hajian Berenjestanaki, Hamid R. Barzegar, Nabil El Ioini and Claus Pahl Blockchain-Based E-Voting Systems

[4] Neziri, V., Shabani, I., Dervishi, R. and Rexha,B.,2022.AssuringAnonymityandPrivacyinElectronicVoting with Distributed Technologies Based on Blockchain. Applied Sciences, 12(11),p.5477.

[5] V Ch, R., Kumari D, J., Gadekallu, T.R. and Iwendi, C., 2022. Distributed-Ledger-Based Blockchain Technology for Reliable Electronic Voting System with Statistical Analysis. Electronics,11(20),p.3308.

[6] Jafar, U., Aziz, M.J.A. and Shukur, Z.,2021. Blockchain for electronic voting system—review and open research challenges. Sensors, 21(17),p.5874.

[7] Ch, R. ,Kumari D,J., Gadekallu, T.R. and Iwendi,C.,2022. Distributed-Ledger-Based Blockchain Technology for Reliable Electronic Voting System with Statistical Analysis. Electronics,11(20),p.3308.

[8] Abdullah, S., Shafiq, M., Imran, M., & Malik, H. (2018). Towards Secure E-Voting Using Ethereum Blockchain. 2018 15th International Bhurban Conference on Applied Sciences and Technology(IBCAST),324-328.doi:10.1109/ ib

[9] Khoury, D., Kfoury, E.F., Kassem, A. and Harb,H., 2018, November. Decentralized voting platform based on one there um blockchain. In 2018 IEEE International Multi disciplinary Conference on Engineering Technology (IMCET)(pp.1-6). IEEE.

[10] Gupta, A., Kumar, P., Kumar, S., & Pandey, S.(2018). Blockchain-Enabled E-Voting. 2018 3rd International Conference on Computational Systems and Information Technology for Sustainable Solutions (CSITSS), 1-4. doi:10.1109/csitss.2018.8768932