Bima Journal of Science and Technology, Vol. 8(3) Sept, 2024 ISSN: 2536-6041

DOI: 10.56892/bima.v8i3.762

A Review of Blockchain-Based E-Voting Systems: Enhancing Security and Transparency

Muhammed Kabir Ahmed[1], Raymond Dangdat Delmut[2] and Mikailu Habila[3]

[1]Department of Computer Science, Gombe State University, Gombe, Nigeria
[2]Department of Computer Science, Federal Polytechnic Kaltungo, Gombe, Nigeria
[3]Department of Computer Science, Army University Biu, Borno, Nigeria.

ABSTRACT

The concept of e-voting, which is to eliminates the need for manual paper ballots is gaining traction, particularly in large-scale implementations where security and reliability are crucial. Blockchain technology, recognized for its transformative impact across various industries, is increasingly being considered for its potential to enhance electoral systems through e-voting. This study aims to review the potential of blockchain technology in transforming e-voting systems, examines the prospects of blockchain-based e-voting systems, highlighting how blockchain's core attributes; decentralization, immutability, and cryptographic security could address the significant challenges of traditional voting methods. By analyzing case studies, the advantages of blockchain in e-voting, and the various challenges involved, the work presents a roadmap for the adoption of blockchain-based e-voting as a means to strengthen democratic processes by enhancing transparency, security, and inclusivity.

Keywords: Voting, E-voting Systems, Blockchain, Security, Transparency

INTRODUCTION

In contemporary societies, democracy stands as a cornerstone of governance, valuing citizen participation and collective decision-making. However, traditional electoral systems have faced persistent challenges, ranging from voter fraud and manipulation to issues of transparency and accessibility, which have cast doubt on the integrity and inclusivity of democratic processes. An electronic voting system, or e-voting system, has been proposed as an improved alternative to the traditional ballot system as societies strive for more transparent, secure, and inclusive electoral processes. Because of its potential to minimize manual intervention and save costs, e-voting has been implemented in select scenarios (Vivek et al., 2020). However, worries about data integrity, privacy, distributed authority, security, and compliance requirements have postponed the widespread use of e-voting systems.

With the intention of guaranteeing fair and accurate elections, e-voting was first put out as a remedy for the problems with paper-based voting (Daramola & Thebus, 2020). E-voting system security issues have been thoroughly investigated in the literature (Ryan et al., 2015). Research suggests that using electronic voting could provide a number of difficulties, such as issues with data integrity, dependability, transparency, ballot secrecy, possible malfunctions, illiterate voters, the requirement for specific IT skills, equipment storage, security, possibility for fraud, and expense (Esteve et al., 2012).

But the introduction of blockchain offers a revolutionary way to deal with these issues and bring about a decentralized democratic future (Taş & Tanrıöver, 2020) . In recent years, blockchain technology—which was first created as the backbone of bitcoin transactions—has witnessed an expansion of its uses. Given that the blockchain is unchangeable and may therefore be thought of as a distributed and decentralized ballot box, blockchain-enabled voting systems have been suggested as the next generation of contemporary electronic voting. (Taş & Tanrıöver, 2020).

Taş & Tanrıöver, (2020) encourages governments to incorporate sustainability data and implement intelligent, sustainable

DOI: 10.56892/bima.v8i3.762

voting methods in order to guarantee that all participants have access to accurate information on sustainable assets. Although blockchain technology is being used more often to improve security in electronic voting systems, a number of issues still exist.

Security, transparency, and scalability are three persistent issues with both traditional and electronic voting systems that are addressed in this paper. It looks at how blockchain technology, which has security, immutability, and decentralization as its main characteristics, could be able to solve these problems with the way e-voting works now. The goal of the study is to find weaknesses in current e-voting systems, assess how blockchain technology could strengthen them, examine case studies to gain useful knowledge, and provide a path for implementing blockchain-based e-voting systems to strengthen democratic processes. A conceptual study of e-voting, blockchain technology, a review of associated literature, a discussion of the implications of blockchain-based e-voting systems, an examination of potential future developments, and a conclusion will be covered in the following sections.

BACKGROUND OF THE STUDY

This section provides an overview of e-voting system, blockchain technology and its concept.

E-Voting

According to Karanikolas et al., (2023), Electronic voting refers to any voting process that uses electronic methods for conducting or counting votes.

More specifically, electronic voting refers to the use of electronic techniques to facilitate or oversee the casting and tallying of votes. This can include computers with an Internet connection for online voting or stand-alone electronic voting machines (EVMs). The first implementation of e-voting occurred in the U.S. in 2000, followed by France (2001), the UK (2002), Spain (2003), Ireland (2004), Estonia (2005), Portugal (2005), the Netherlands (2004, 2006, 2007), Paraguay (2008), Finland (2008), Austria (2009), Germany (2009), and Norway (2011) (Esteve et al., 2012) . Faster vote counting, reduced expenses, and improved accessibility for voters with disabilities are some benefits of electronic voting. On the other hand, drawbacks include the possibility of hacking and vote rigging. Voting procedures have changed throughout time. Paper ballots replaced traditional public voting, and punch cards gave way to optical scanning devices at polling places and online voting for electronic voting. Phases of the electronic voting process include registration, authentication, voting, and counting (Figure 1).

The following features are essential for e-voting systems;

1. Receipt-Freeness: There should be no receipts available through the system demonstrating a voter's preference for a particular candidate. (Ali & Murray, 2016).
2. Fairness: Preliminary results should not influence the decisions of other voters (Anane et al., 2007; Fujioka et al., 1993).
3. Data Integrity: Each vote must be noted as intended and must not be altered once logged (Keshk & Abdul-Kader, 2007).
4. Privacy/Voter Anonymity: The identity of voters and their choices must kept confidential (Anane et al., 2007).
5. Eligibility: Only registered voters should be permitted to vote (Zhang et al., 2018).
1. Reliability/Robustness: Election systems must work consistently without losing votes. Software and methods should be designed to be free from malicious code and errors (Ryan et al., 2009).
2. Uniqueness: The system should allow voters from voting more than once (Bokslag & de Vries, 2016; Sun et al., 2019).
3. Verifiability: Voters should be able to confirm that their ballots have been counted accurately (Liu & Wang, 2017).

Bima Journal of Science and Technology, Vol. 8(3) Sept, 2024 ISSN: 2536-6041

DOI: 10.56892/bima.v8i3.762

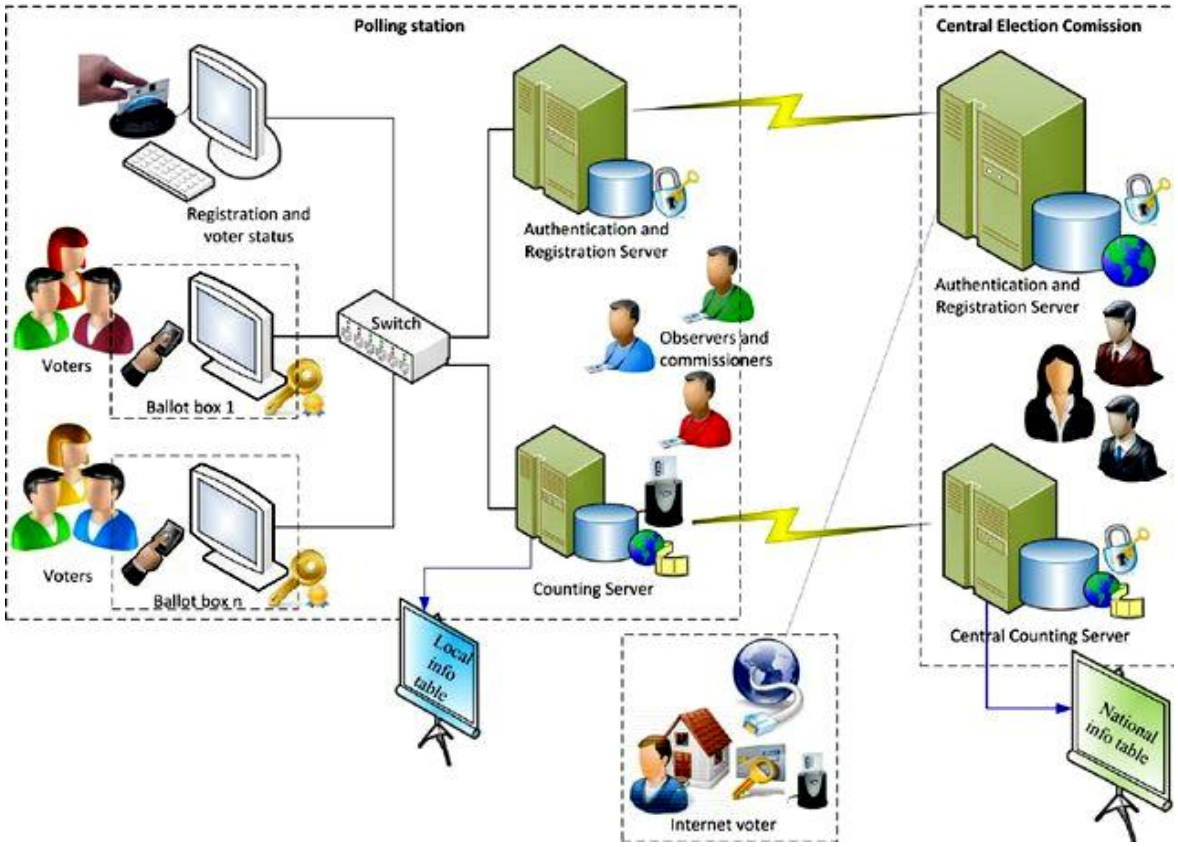

Figure 1: General architecture of e-Voting system (Rexha et al., 2011)

Blockchain Technology

In 2008, a whitepaper outlining the Bitcoin, a brand-new digital money, presented blockchain technology. Many more uses for blockchain have surfaced since then. Using a peer-to-peer distributed timestamp server to offer computational verification of the transaction sequence, blockchain technology mitigates the double-spending issue, which is one of its main advantages (Nakamoto, 2008). Although blockchain is mostly linked to cryptocurrencies and the financial industry, it can be used in many other transaction-related domains as well. As a result, in the years to come, blockchain will be seen as a crucial component of Industry 5.0 applications. (Taş & Tanrıöver, 2020). Although blockchain is widely recognized in the realm of digital currency, its potential applications may extend well beyond just digital money. According to Anders & Jørgen (2016), blockchain can be compared to an enormous Google Doc spreadsheet that serves as a register for both material and immaterial assets, including money, records, and real estate. A blockchain is essentially a distributed ledger with several transactions recorded in each block. Every time a transaction takes place, a record of it is added to each participant's ledger. Distributed Ledger Technology is the name given to this decentralized database that is managed by several parties (DLT).

Bima Journal of Science and Technology, Vol. 8(3) Sept, 2024 ISSN: 2536-6041

DOI: 10.56892/bima.v8i3.762

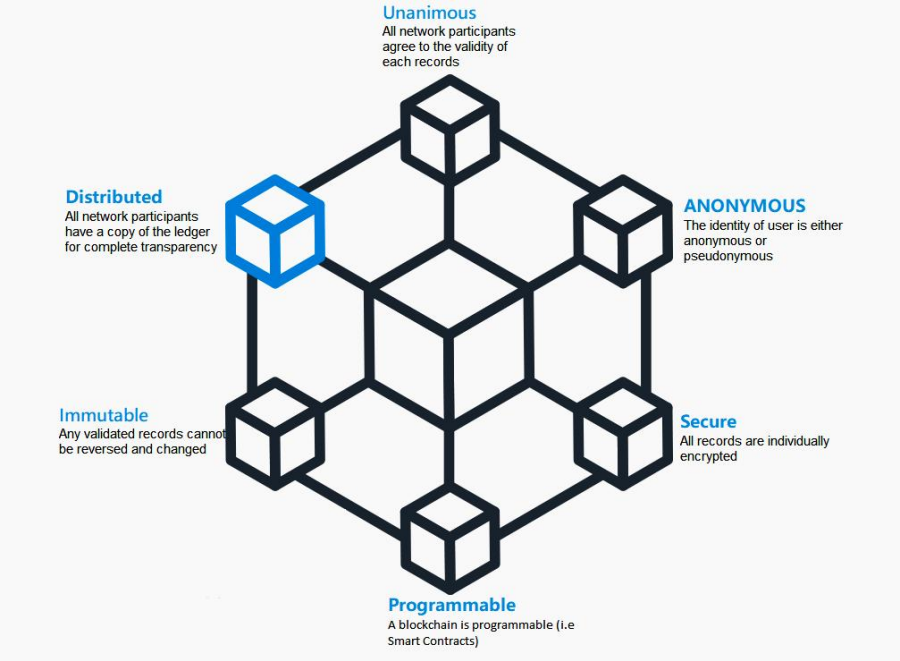

Figure 2: Properties of Distributed Ledger Technology (DLT)

Figure 2 illustrates the properties of Distributed Ledger Technology (DLT). Important characteristics are covered in the section that follows. Notably, tampering is instantly visible if a block in the chain is changed. A blockchain system is extremely secure since hackers would have to alter each block in the chain across all distributed copies in order to compromise it.

According to Gatteschi (2018), blockchain technology's main objective was to facilitate internet payments between parties without the need for middlemen. According to the study, blockchain acts as the primary ledger for Bitcoin transactions, guaranteeing payment authenticity and non-repudiation via cryptographic processes. Gatteschi et al. identified the following core concepts underlying blockchain technology:

- **Transactions**: all transfers of cryptocurrency between subjects are denoted as transactions from A to B. Since its inception, the Blockchain has recorded every transaction that has taken place.
- **Blocks:** are used to group transactions. Every block gathers every transaction that takes place during a specified time period and maintains a reference to the block before it (this is where the term "chain" originates).
- **Nodes:** Rather of being kept in a single database, the Blockchain is distributed among network computers, or "nodes," each of which has a local copy of the complete Blockchain.
- **Majority consensus**: because there isn't a central authority, choices on the network are decided by the majority. To make its local copy of the Blockchain reflect the majority of the network's nodes' status, every node alters it.
- **Mining**: nodes have two options: they can actively participate in the so-called "mining" process to actively maintain the Blockchain, or they can passively hold a copy of it. In the process of mining, nodes examine past transactions to confirm if a subject is authorized to spend a specific amount of cryptocurrency. They also solve a challenging mathematical problem that requires a lot of calculation each time a block needs to be added to the chain. This issue was created expressly to reduce the likelihood that a malevolent

DOI: 10.56892/bima.v8i3.762

party may influence the Blockchain by fabricating transactions. Since controlling the majority of network nodes is necessary to add a new (malicious) block or alter one that has already been put to the chain, the likelihood of attacks is very low.

- **Wallet**: are used by people to transfer cryptocurrency. Cryptocurrency is the outcome of prior transactions rather than anything that can be kept in physical memory. As a result, the wallet only keeps login information that allows Blockchain users to move the cryptocurrency they possess. A wallet has one (or more) distinct addresses connected to it. If a user wants to transmit a certain amount of cryptocurrency to a peer, they must use their credentials to confirm the transaction and provide the recipient's address and desired quantity.

Blockchain Technology Structure

A blockchain consists of a series of blocks, with each block containing transaction data, its own hash value (a unique cryptographic string of characters and numbers generated by a complex algorithm), and a reference to the hash of the preceding block (Aneesa, 2022).

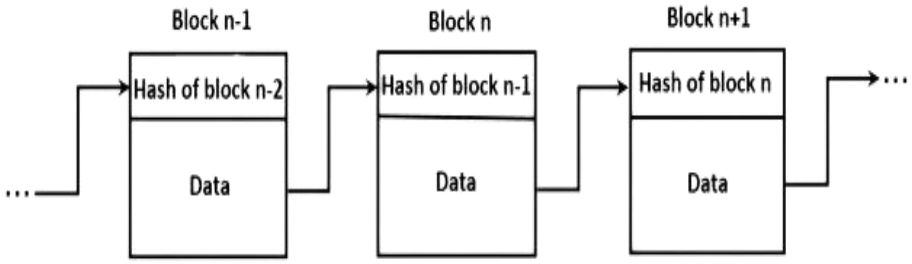

Figure 3: The Structure of Blockchain (Shahsavari et al., 2019)

A block is composed of a header and a body as shown in figure 3, where a header contains a reference hash of previous block links these blocks to each other, a timestamp, Nonce and the Merkle root. The Merkle root, stored in a block's body, represents the root hash of a Merkle tree. Using the example of the 3rd block, containing only four transactions, as an example to illustrate the structure of a Merkle tree.

Characteristic of Blockchain

According to Zheng, Xie, Dai, Chen, & Wang, (2017), some of the main characteristics of blockchain are as follows:

- ***DECENTRALIZATION:*** Decentralization in transaction systems shifts from centralized authorities to peer-to-peer (P2P) blockchain networks, eliminating the need for trust in intermediaries. This paradigm uses blockchain's consensus processes to lower costs and increase efficiency. Decentralization has trade-offs, such as increased server and energy costs, but overall, the advantages—such as improved security and efficiency—outweigh these disadvantages. Consensus algorithms in blockchains provide data consistency across dispersed networks, eliminating the need for middlemen.
- ***IMMUTABLE:*** Within a short period of time, transactions are validated, and any unlawful transactions are rejected by miners before being added to the blockchain. A transaction cannot be removed or changed after it is recorded on the blockchain, making it irreversible.

DOI: 10.56892/bima.v8i3.762

- ANONYMITY: To maintain anonymity, users can interact with a Blockchain network using various randomly generated addresses (Wang et al., 2017). Because Blockchain is decentralized, it doesn't rely on a central authority to gather or store user private data. A considerable amount of anonymity is provided by this decentralized configuration.
- AUDITABILITY: In a Blockchain network, transactions are documented and verified through a digital distributed ledger and timestamp, facilitating straightforward auditing and tracking of historical records if any network node is accessed (Yu et al., 2018). With Bitcoin, for instance, every transaction can be methodically tracked, guaranteeing the audibility and transparency of the Blockchain's data state. When money passes across several accounts, it becomes more difficult to trace its original source.

2.2.3 Types of Blockchain

In practice, blockchain technology can typically be classified into the following categories (Zheng et al., 2017):

- Public Blockchain: A public blockchain is accessible to all network participants, enabling anyone to verify transactions and take part in the consensus process. Examples of public blockchains include Bitcoin and Ethereum (Bashir, 2017).
- Private Blockchain: In a private blockchain, participation is limited to authorized nodes, with access controlled by designated authorities. Examples include Hyperledger Fabric, developed by the Linux Foundation (Antwi et al., 2021)
- Hybrid Blockchain: A semi-private blockchain blends features of both public and private blockchains. Authorized nodes are pre-approved, typically reflecting business-to-business partnerships. The data remains partially decentralized. Examples of this model include consortium blockchains like Hyperledger and R3CEV (Bashir, 2017).

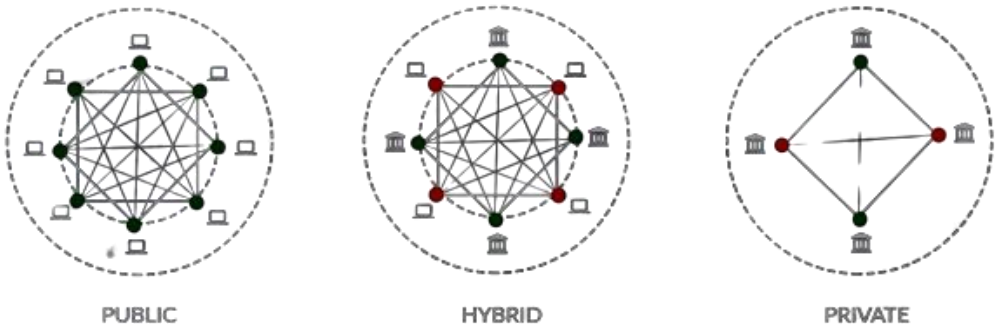

Figure 4. Types of blockchain (Desai et al., 2022)

Related Work

Studies investigating blockchain technology's applications in e-voting seek to assess its feasibility, security, and effectiveness in improving the transparency and integrity of the electoral process.

Cheema et al., (2020) addresses the critical concerns of privacy, authentication, and integrity in e-voting systems by proposing a model that integrates blockchain and machine learning. The study utilizes blockchain to ensure the security and integrity of votes, while a machine learning

DOI: 10.56892/bima.v8i3.762

model is employed to detect intrusions in voting data centers and e-voting stations. The proposed system distinguishes between personal and public blockchains; the personal blockchain handles voter registration and voting, whereas the public blockchain maintains the integrity of voters' personal data by storing the root hash from the Merkle hash tree and revealing voting results after the process concludes. Their model offers transparency, trust, and security in e-voting systems, preventing intrusions into the information exchange network.

Febriyanto et al., (2020) explore the challenges in current electronic voting systems, particularly the manipulation of election results. The study highlights a case from the 2019 election where discrepancies between fast-count technology and electronic media reports raised concerns about vote manipulation. To address these issues, the authors propose using blockchain technology to ensure the validity and authenticity of voting data. The decentralized nature of blockchain allows each server to connect within a peer-to-peer network, enabling easier data tracking and robust backup mechanisms. If a server encounters issues, other servers can temporarily take over, ensuring continuous integrity. The application of blockchain technology in electronic voting, as suggested by Febriyanto et al., can produce tamper-proof data, thereby maintaining the authenticity and trustworthiness of election results.

Soud et al., (2020) address the ongoing challenges in developing trusted e-voting systems by exploring the potential of blockchain technology to enhance their integrity and modernity. The authors provide a comprehensive review of existing blockchain-based e-voting implementations, identifying the strengths and limitations of various approaches. Building on this analysis, they propose a blockchain-based e-voting system called TrustVote, which utilizes both public and permissioned blockchains. Their findings indicate that the permissioned blockchain implementation of TrustVote outperforms its public blockchain counterpart in terms of meeting e-voting requirements. While acknowledging that several challenges and requirements remain, Soud et al. argue that permissioned blockchain offers a promising pathway for creating reliable e-voting systems that can foster public trust.

Jafar et al., (2021) presented a conceptual description of a blockchain-based e-voting application in addition to an introduction to the blockchain's fundamental structure and characteristics in relation to e-voting where they also examine the growing trend of online voting and its potential to reduce organizational costs and increase voter turnout, while also addressing the significant security challenges associated with electronic voting systems. The authors explore how blockchain technology, with its decentralized nodes and end-to-end verification capabilities, can serve as a robust alternative to traditional electronic voting systems. Their study provides a conceptual overview of blockchain-based e-voting applications, highlighting the fundamental structure and characteristics of blockchain in the context of elections. Jafar et al. identify key issues in current blockchain-based voting research, such as privacy protection and transaction speed, noting that while blockchain can address many of the security concerns in election systems, these challenges must be resolved to achieve a sustainable and scalable e-voting solution. The authors conclude that existing frameworks need significant improvements before they can be effectively utilized in voting systems.

Huang et al., (2021) provided a comprehensive review of blockchain-based voting systems, highlighting the shift from traditional centralized voting methods to decentralized solutions leveraging blockchain technology. Their study categorizes blockchain-based voting systems

DOI: 10.56892/bima.v8i3.762

based on various features, including the types of blockchain used, consensus approaches, and participant scale. By systematically analyzing and comparing these systems, Huang et al. identify several limitations and research opportunities, offering valuable insights into the potential advantages of blockchain for enhancing voting systems. The review aims to deepen understanding of blockchain's utility in voting and outline future research directions to address existing challenges and advance the field.

Jafar & Aziz, (2021) review the evolution of electronic voting systems and their transition from paper ballots to digital solutions aimed at enhancing accuracy, security, and convenience. Despite these advancements, security and privacy vulnerabilities have persisted over time. The authors highlight the potential of blockchain-based e-voting systems to mitigate voter fraud and enhance voter access, emphasizing blockchain's advantages in end-to-end authentication, distributed nature, non-repudiation, and overall security. Their analysis covers various blockchain-based e-voting implementations, assessing current e-voting structures and exploring the decentralized voting mechanisms offered by blockchain technology. The study provides a comprehensive evaluation of the benefits and challenges associated with blockchain-based e-voting systems, outlining its potential as a robust alternative to traditional e-voting solutions.

Vladucu et al., (2023) provided a thorough review of the global adoption of electronic voting systems for public office elections, highlighting their benefits such as remote voting capabilities, faster vote counting, improved privacy, and reduced voting bias. The authors focus on the role of blockchain technology in strengthening the voting process through its immutable vote storage, which helps prevent vote tampering and ensures election legitimacy. The study examines the implementation of blockchain-based e-voting systems in countries like Germany, Russia, Estonia, and Switzerland, and assesses various proposed systems in academic research. Vladucu et al. also analyze the challenges associated with blockchain e-voting systems and identify key areas for future research to enhance their reliability and trustworthiness.

Table 1: Summary of Review on Related work

Author Name	Paper Title	Strength	Weakness
Cheema et al., (2020)	Machine learning with blockchain for secure e-voting system	Uses blockchain for security and integrity, machine learning for intrusion detection	Not mentioned
Febriyanto et al., (2020)	Using blockchain data security management for E-voting systems	Uses blockchain for tamper-proof data, decentralized network for integrity	Focuses on a specific case study
Soud et al., (2020)	TrustVote: On elections we trust with distributed ledgers and smart contracts	Comprehensively reviews existing blockchain-based e-voting systems, proposes TrustVote with permissioned blockchain	Permissioned blockchain may limit access
Jafar et al., (2021)	Blockchain for electronic voting system review and open research challenges	Conceptual overview of blockchain for e-voting, highlights security benefits	Does not address scalability or privacy concerns
Huang et al., (2021)	The application of the blockchain technology in voting systems: A review	Comprehensive review with categorization based on features, identifies limitations and opportunities	Not focused on specific solutions

DOI: 10.56892/bima.v8i3.762

Jafar & Aziz, (2021)	A state-of-the-art survey and research directions on blockchain based electronic voting system	Reviews e-voting evolution, highlights blockchain's security advantages	Does not dig into technical details of blockchain implementation
Vladucu et al., (2023)	E-voting meets blockchain: A survey	Reviews global adoption of e-voting systems, analyzes blockchain's role and challenges	Does not provide specific solutions for identified challenges

Case Studies

In the below, we present several use cases of e-voting that have been proposed and implemented on blockchain.

- Voatz: Introduced in 2018, Voatz is a blockchain-based mobile voting platform used in West Virginia for overseas military voters during the 2018 U.S. midterm elections. The system incorporates biometric validation, including fingerprint and retinal scans, to authenticate voters. However, recent research has identified significant security vulnerabilities in Voatz, which could enable attackers to monitor, modify, or block large numbers of votes (Berenjestanaki et al., 2023).
- Votereum: An e-voting system built on the Ethereum platform, designed to ensure an open, fair, and universally verifiable voting process. The system architecture includes a primary server managing the entire system and another server dedicated to handling blockchain-related requests. The authors deploy Votereum on the Rinkeby Testnet to observe its feasibility and address potential security concerns. Their study underscores the promise of blockchain in establishing trust in e-voting systems, while also acknowledging the need for further exploration of security challenges (Vo-Cao-Thuy et al., 2019).
- VID: The system is further strengthened by integrating Aadhar, India's biometric identification system, to prevent vote duplication and tampering. The proposed scheme uses biometric details and Virtual IDs (VID) from the Aadhar database for voter authentication, and digital signatures are employed to encrypt votes within the blockchain. This approach aims to create a secure and verifiable e-voting system that leverages both blockchain and biometric authentication to maintain the integrity of the electoral process (Roopak & Sumathi, 2020).
- VoteChain: A blockchain-based voting system designed to enhance transparency and security in elections. By leveraging blockchain technology, which has proven effective in creating secure and scalable distributed systems across various sectors, VoteChain eliminates the single point of failure associated with centralized systems. The authors detail the implementation of VoteChain and report on its successful testing in a real-world poll, demonstrating its viability for large-scale elections and its potential to significantly improve the trustworthiness of e-voting systems (Pandey et al., 2019).
- DecentraVote: Developed by a team at iteratec in Vienna, DecentraVote is a blockchain-based solution for virtual meetings. It operates on the public Ethereum network using Proof of Authority consensus with permissioned validator nodes. The system employs a smart contract to create a Merkle tree of all voting rights on-chain, while Zero-Knowledge Succinct Non-Interactive Argument of Knowledge (zk-SNARK) provides off-chain proofs for each voting right. DecentraVote is not designed for national political elections. (Berenjestanaki et al., 2023).

DOI: 10.56892/bima.v8i3.762

DISCUSSION

blockchain in E-Voting

E-voting has gained considerable interest in recent years due to its potential to improve the transparency and security of the voting process. Blockchain technology, in particular, emerges as a promising solution to overcome the challenges and limitations faced by traditional e-voting systems.

Blockchain-based e-voting systems provide significant benefits such as enhanced transparency, security, and integrity (Taş & Tanrıöver, 2020). Blockchain technology ensures secure information storage through a distributed, digitized, and consensus-driven approach (Taş & Tanrıöver, 2020) . By encrypting data and distributing it across the network, blockchain improves information security and privacy (Walde & Yadav, 2022). This technology can enhance transparency, prevent fraud, and boost citizen confidence in the electoral process (Walde & Yadav, 2022).

A key benefit of blockchain-based e-voting is its transparency. Voting results recorded on the blockchain can be verified by participants or independent external observers, ensuring the integrity of the election (Taş & Tanrıöver, 2020). The immutable nature of blockchain transforms it into a decentralized, distributed ballot box, which supports the adoption of smart, sustainable voting systems (Taş & Tanrıöver, 2020) . Blockchain technology also allows for the integration of sustainability information into voting systems (Taş & Tanrıöver, 2020).

In addition to transparency, blockchain-based e-voting systems offer robust privacy protection. Voter identities can remain anonymous while ensuring the integrity of the voting results (Kim et al., 2021). Cryptographic techniques, such as homomorphic encryption, can further safeguard voter data (Kim et al., 2021). By encrypting voter information, the system facilitates statistical analysis of vote results while preserving the privacy and verifiability of the e-voting system (Kim et al., 2021).

Future Perspectives

Blockchain technology could profoundly change democratic processes, especially in electronic voting (e-voting). The following viewpoints highlight how blockchain could impact e-voting and democratic systems (Treiblmaier et al., 2020; Khan et al., 2020; Hu et al., 2021):

. Improved Transparency and Trust: Blockchain technology enhances transparency and trust in e-voting by offering a decentralized and immutable ledger of voting records. The transparent nature of blockchain allows for independent verification of election results, boosting confidence in the electoral process. Additionally, the immutability of blockchain makes it nearly impossible to tamper with or manipulate the data, further strengthening transparency and trust.

. Secure and Tamper-Resistant System: Blockchain-based e-voting systems provide a secure and tamper-resistant method for recording and storing votes. The decentralized architecture of blockchain makes it highly resistant to tampering and manipulation, while cryptographic techniques safeguard the integrity and security of voting data. This ensures that votes remain unaltered, maintaining the integrity of the democratic process.

. Decentralized Control: Blockchain technology allows for the decentralization of control within e-voting systems. Rather than depending on a central authority, blockchain enables distributed consensus among participants, reducing the risk of single points of failure and increasing system resilience. This decentralization also fosters inclusivity and prevents the concentration of power in a few entities.

. Enhanced Accessibility and Inclusivity: Blockchain-based e-voting systems have the potential to improve accessibility and

DOI: 10.56892/bima.v8i3.762

inclusivity in democratic processes. By utilizing digital technologies, e-voting can overcome geographical barriers, allowing for remote participation and potentially increasing voter turnout and engagement, particularly among marginalized or remote communities. Additionally, blockchain systems can incorporate features to accommodate individuals with disabilities, ensuring that the voting process is inclusive for all citizens.

5. Cost Reduction and Efficiency Gains: Blockchain technology offers the potential to reduce costs and increase the efficiency of e-voting processes. By removing intermediaries and manual procedures, blockchain-based systems can streamline the voting process, thereby lowering administrative costs. Automation through smart contracts can further enhance the efficiency and accuracy of implementing voting rules, leading to more cost-effective and efficient democratic processes.

CONCLUSION

Blockchain technology integration offers a possible path forward for improving the security, transparency, and integrity of electronic voting systems. Blockchain's intrinsic qualities—decentralization, immutability, and cryptographic security—provide a strong basis for resolving the issues that have beset conventional e-voting systems, as several studies and case studies have shown. Blockchain has the potential to greatly boost public confidence in election results by offering an auditable and transparent record of votes. The electoral process is protected by the decentralized structure of blockchain, which reduces the possibility of fraud and manipulation. Furthermore, blockchain-based electronic voting systems have the potential to increase inclusion and accessibility, which could increase democratic participation

Although blockchain technology is still being incorporated into electronic voting, there are a lot of potential advantages. To fully achieve the transformative potential of blockchain in electronic voting, more research and development is required to overcome technical problems like scalability and user experience. Societies can get closer to having transparent, safe, and fair elections that accurately represent the will of the people by adopting this technology. But it's important to recognize that careful consideration of legal, regulatory, and ethical frameworks is necessary for the successful adoption of blockchain-based electronic voting systems. Strong cybersecurity safeguards must also be in place to stave against such dangers. We can create a more safe, open, and democratic future by tackling these issues and taking use of the potential that blockchain technology offer

REFERENCES

Anane, R., Freeland, R., & Theodoropoulos, G. (2007). e-Voting Requirements and Implementation. *9th IEEE International Conference on E-Commerce Technology and the 4th IEEE International Conference.* Tokyo, Japan.

Aneesa, I. R. (2022). *Types of Blockchain Structures.* Fintech.

Antwi, M., Adnane, A., Ahmad, F., Hussain, R., Rehman, M. H., & Kerrache, C. A. (2021). The case of HyperLedger Fabric as a blockchain solution for healthcare applications. . *Blockchain: Research and Applications*, 100012.

Bashir, I. (2017). *Mastering blockchain.* Packt Publishing Ltd.

Berenjestanaki, M., Barzegar, H. R., El Ioini, N., & Pahl, C. (2023). Blockchain-based e-voting systems: a technology review. *Electronics, 13*(1), 1-38.

Bokslag, W., & de Vries, M. (2016). *Evaluating e-voting: Theory and practice.* arXiv.

Cheema, M. A., Ashraf, N., Aftab, A., Qureshi, H. K., Kazim, M., & Azar, A. T. (2020). Machine learning with blockchain for secure e-voting system. *In 2020 first international conference of smart systems and*

DOI: 10.56892/bima.v8i3.762

emerging technologies (SMARTTECH). Riyadh, Saudi Arabia: IEEE.

Daramola, O., & Thebus, D. (2020). Architecture-Centric Evaluation of Blockchain-Based Smart Contract E-Voting for. *Informatics, 7*(2), 16.

Desai, K., Gosar, D., & Pachorkar, R. (2022). BLOCKCHAIN BASED E-VOTING SYSTEM. *International Journal of Engineering Applied Sciences and Technology, 7*(12), 21-30.

Esteve, J. B., Goldsmith, B., & Turner, J. (2012). International experience with e-voting. *Norwegian E-Vote Project. International Foundation for Electoral Systems. Document disponibil online la adresa http://www. ifes. org/Content/Publications/News-in-Brief/2012/June/% 7E/media/B7FB434187E943C18F4D 4992A4EF75DA.pdf*.

Esteve, J., Goldsmith, B., & Turner, J. (2012). International Experience with E-Voting. *Norwegian E-Vote Project. International Foundation for Electoral Systems. Document disponibil online la adresa http://www. ifes. org/Content/Publications/News-in-Brief/2012/June/% 7E/media/B7FB434187E943C18F4D 4992A4EF75DA. pdf.*

Febriyanto, E., Rahayu, N., Pangaribuan, K., & Sunarya, P. A. (2020). Using blockchain data security management for E-voting systems. *In 2020 8th International Conference on Cyber and IT Service Management (CITSM).* Pangkal, Indonesia: IEEE.

Fujioka, A., Okamoto, T., & Ohta, K. (1993). A practical secret voting scheme for large scale elections. *Advances in Cryptology—AUSCRYPT'92: Workshop on the Theory and Application of Cryptographic Techniques Gold Coast, Queensland, Australia, December 13–16, 1992 Proceedings 3.* Springer Berlin Heidelberg.

Gatteschi, V. e. (2018). Blockchain and Smart Contracts for Insurance: Is the Technology Mature Enough? Future Internet. (www.mdpi.com/journal/futureinternet.), 10, 20.

Hu, B., Zhang, Z., Liu, J., Liu, Y., Yin, J., Lu, R., & Lin, X. (2021). A Comprehensive Survey On Smart Contract Construction and Execution: Paradigms, Tools, And Systems. *Patterns, 2*(2), 100179.

Huang, J., He, D., Obaidat, M. S., Vijayakumar, P., Luo, M., & Choo, K. K. (2021). The application of the blockchain technology in voting systems: A review. *ACM Computing Surveys (CSUR), 54*(3), 1-28.

Jafar, U., & Aziz, M. J. (2021). A state of the art survey and research directions on blockchain based electronic voting system. *In Advances in Cyber Security: Second International Conference, ACeS 2020.* Penang, Malaysia: Springer Singapore.

Jafar, U., Aziz, M. J., & Shukur, Z. (2021). Blockchain for electronic voting system review and open research challenges. *Sensors, 21*(17), 5874. https://doi.org/https://doi.org/10.3390/s21175874

Karanikolas, N., Kaklamanis, C., & Nikolopoulos, S. (2023). AQUA: A blockchain based multi-winner e-voting system. *Technium, 11*, 32-43.

Keshk, A., & Abdul-Kader, H. (2007). Development of remotely secure e-voting system. *In Proceedings of the 2007 ITI 5th International Conference on Information and Communications Technology.* Cairo, Egypt.

Khan, K. M., Arshad, J., Khan, & M, M. (2018). Secure digital voting system based on blockchain technology.

DOI: 10.56892/bima.v8i3.762

International Journal of Electronic Government Research (IJEGR), 53-62.

Khan, K., Arshad, J., & Khan, M. (2020). Investigating Performance Constraints For Blockchain Based Secure E-voting System. *Future Generation Computer Systems, 105*, 13-26.

Kim, H., Kim, K. H., Park, S., & Sohn, J. (2021). *E-voting System Using Homomorphic Encryption and Blockchain Technology To Encrypt Voter Data.* arXiv preprint arXiv:2111.05096 .

Liu, Y., & Wang, Q. (2017). An E-voting Protocol Based on Blockchain. *International Association for Cryptologic Research*.

Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System.* . Available online: https://bitcoin.org/bitcoin.pdf (accessed on 21 December 2021).

Pandey, A., Bhasi, M., & Chandrasekaran, K. (2019). VoteChain: A Blockchain based e-voting system. *In 2019 Global Conference for Advancement in Technology (GCAT).* Bangalore, India: IEEE.

Rexha, B., Dervishi, R., & Neziri, V. (2011). Increasing the trustworthiness of e-voting systems using smart cards and digital certificates–Kosovo case. *Proceedings of the 10th WSEAS International Conference on E-Activities (E-ACTIVITIES'11), Jakarta, Island of Java, Indonesia*, 208-212.

Roopak, T. M., & Sumathi, R. (2020). Electronic voting based on virtual id of aadhar using blockchain technology. *In 2020 2nd International Conference on Innovative Mechanisms for Industry Applications (ICIMIA).* Bangalore, India: IEEE.

Ryan, P., Bismark, D., Heather, J., Schneider, S., & Xia, Z. (2009). PrÊt À Voter: A Voter-Verifiable Voting System. *IEEE transactions on information forensics and security, 4*(4), 662-673.

Ryan, P., Schneider, S., & Teague, V. (2015). End-to-End Verifiability in Voting Systems, from Theory to Practice. *IEEE Secur. Priv., 13*, 59-62.

Shahsavari, Y., Zhang, K., & Talhi, C. (2019). Performance modeling and analysis of the bitcoin inventory protocol. *2019 IEEE International Conference on Decentralized Applications and Infrastructures (DAPPCON) (pp. 79-88).* IEEE.

Soud, M., Helgason, S., Hjálmtýsson, G., & Hamdaqa, M. (2020). TrustVote: On elections we trust with distributed ledgers and smart contracts. *In 2020 2nd Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS).* Paris, France: IEEE.

Sun, X., Wang, Q., & Kulicki, P. (2019). A Simple Voting Protocol on Quantum Blockchain. *Int. J. Theor. Phys, 58*, 275-281.

Swan, M. (2015). *Blockchain: Blueprint for a New Economy;.* Newton MA, USA: O'Reilly Media.

Taş, R., & Tanrıöver, Ö. Ö. (2020). A systematic review of challenges and opportunities of blockchain for E-voting. *Symmetry, 12*(8), 1328.

Treiblmaier, H., Rejeb, A., & Strebinger, A. (2020). Blockchain As a Driver For Smart City Development: Application Fields And A Comprehensive Research Agenda. *Smart Cities, 3*(3), 853-872.

Vivek, S. K., Yashank, R. S., Prashanth, Y., Yashas, N., & Namratha, M. (2020). E-voting systems using blockchain: An exploratory literature survey. *2020 Second International Conference on Inventive Research in*

DOI: 10.56892/bima.v8i3.762

Computing Applications (ICIRCA). IEEE, 890-895.

Vladucu, M. V., Dong, Z., Medina, J., & Rojas-Cessa, R. (2023). E-voting meets blockchain: A survey. *IEEE Access, 11*, 23293-23308.

Vo-Cao-Thuy, L., Cao-Minh, K., Dang-Le-Bao, C., & Nguyen, T. A. (2019). Votereum: An ethereum-based e-voting system. *In 2019 IEEE-RIVF International Conference on Computing and Communication Technologies (RIVF).* Danang, Vietnam: IEEE.

Walde, R. B., & Yadav, A. K. (2022). Blockchain Technology For E-government. *International Journal for Research in Applied Science and Engineering Technology, 8*(10), 1698-1703.

Zhang, W., Yuan, Y., Hu, Y., Huang, S., Cao, S., Chopra, A., & Huang, S. (2018). A Privacy-Preserving Voting Protocol on Blockchain. *In Proceedings of the 2018 IEEE 11th International Conference on Cloud Computing (CLOUD.* San Francisco, CA, USA.