Archives available at journals.mriindia.com

International Journal on Advanced Computer Engineering and Communication Technology

ISSN: 2347-2820
Volume 13 Issue 01, 2024

Blockchain-Based Digital Voting Systems: Security and Usability Analysis

Dr. Avinash M. Pawar[1], Dr. Nitin Sherje[2]

[1]Ph.D. Mechanical Engineering, Bharati Vidyapeeth's College of Engineering for Women, Pune
avinash.m.pawar@bharatividyapeeth.edu

[2]DIT Pune, npsherje@gmail.com

Peer Review Information

Submission: 19 Feb 2024
Revision: 10 April 2024
Acceptance: 15 May 2024

Keywords

Blockchain Technology
Electronic Voting
Cryptographic Security
Voter Privacy

Abstract

Blockchain-based digital voting systems have gained considerable attention as a solution to improve the security, transparency, and efficiency of traditional voting mechanisms. This paper provides a comprehensive analysis of blockchain-based e-voting systems, focusing on their security features, usability, and potential for wide-scale adoption. The integration of blockchain technology offers advantages such as decentralization, immutability, and cryptographic security, ensuring that votes are tamper-proof and transparent. Additionally, blockchain-based systems can enhance voter privacy and reduce the risk of fraud and manipulation. However, challenges remain, particularly in terms of scalability, the complexity of implementation, and the need for voter education to improve usability. This study also contrasts blockchain-based voting with conventional electronic voting systems, highlighting the unique benefits and limitations of both approaches. By analyzing recent advancements and pilot projects, this paper aims to present a balanced view of the potential and the challenges of adopting blockchain for digital voting systems, emphasizing the need for further research and development in both security and usability domains.

Introduction

The advancement of digital technologies has led to an increasing shift toward online voting systems, promising more efficient, accessible, and cost-effective elections. Traditional electronic voting (e-voting) systems, which have been implemented in several countries, have attempted to streamline the voting process by digitizing ballots and counting. However, despite their widespread use, these systems are fraught with significant challenges, including centralized control, potential for hacking, data breaches, and concerns over voter privacy and integrity of the voting process [1]. The vulnerabilities inherent in traditional e-voting systems have raised questions about the reliability of election results, prompting researchers and policymakers to explore alternative solutions.

In recent years, blockchain technology has emerged as a potential solution to address many of these concerns. Blockchain is a decentralized, distributed ledger technology that allows for secure and transparent data recording. It has gained considerable attention for its ability to provide enhanced security features, such as cryptographic encryption, immutability, and auditability [2]. Blockchain-based systems can offer tamper-resistant environments that eliminate the possibility of vote tampering and fraud. Each vote, once recorded on the blockchain, is securely linked and cannot be altered or deleted, ensuring transparency and accuracy in the election process [3]. Furthermore, blockchain's decentralized structure reduces the reliance on a central authority, making it resistant to systemic failures and external attacks, which are common risks in traditional voting systems [4].

The benefits of blockchain technology in digital voting systems extend beyond security. Blockchain can also improve voter privacy by ensuring anonymous voting while maintaining the transparency necessary for electoral integrity [5]. Additionally, blockchain technology can offer real-time auditing capabilities, enabling verification of each vote cast while keeping voter identities confidential. This transparency and accountability foster greater trust in the electoral process and increase confidence in the outcomes [6].

However, despite the promising advantages, the implementation of blockchain in voting systems also comes with a range of challenges. One of the major concerns is scalability. Public blockchains, in particular, may struggle to handle large-scale elections, as transaction speeds can become slower when dealing with millions of voters [7]. Another significant barrier is usability. For blockchain-based voting systems to be widely adopted, they must be intuitive and easy to use for all voters, including those with limited technical expertise. Additionally, there are concerns regarding the legal and regulatory aspects of blockchain-based voting systems, particularly with respect to ensuring voter eligibility, preventing abuse, and maintaining compliance with existing electoral laws[1].

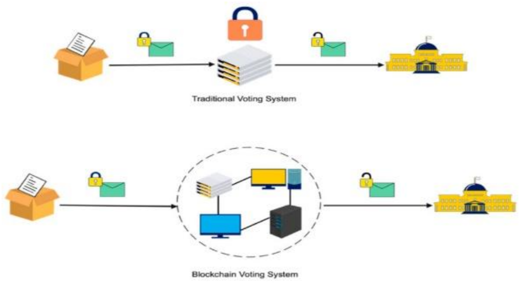

Fig.1 Traditional vs Blockchain voting system [12]

This paper aims to explore the security and usability aspects of blockchain-based digital voting systems in comparison to traditional e-voting systems. By analyzing the strengths and weaknesses of both approaches, the paper seeks to identify the key challenges in adopting blockchain technology for elections and evaluate its potential to address the shortcomings of traditional e-voting systems. Specifically, the paper will assess the feasibility of blockchain-based systems in terms of security, voter privacy, transparency, and user-friendliness. Furthermore, the study will provide insights into the practical considerations required for implementing blockchain-based voting systems, including the technological infrastructure, scalability concerns, and necessary legal frameworks.

Ultimately, this paper seeks to provide a comprehensive understanding of how blockchain can transform digital voting and improve the overall electoral process. Through a detailed analysis of existing research, pilot projects, and technological advancements, the study aims to contribute to the ongoing debate about the future of voting systems and highlight the necessary steps for creating a secure, efficient, and trustworthy electoral system that meets the needs of modern democratic societies.

Literature Review

The comparison of selected blockchain-based electronic voting schemes over the last five years demonstrates the variety of approaches to enhancing security, privacy, and transparency in electoral processes. One of the earliest examples is the Estonian i-Voting system, which has been enhanced with blockchain technology to ensure vote integrity and security while maintaining a high level of usability (Vinkel et al., 2020) [1]. This system leverages a private blockchain to augment the existing infrastructure with blockchain's auditability and immutability, although it remains reliant on centralized control.

Another significant system is ElectAnon, proposed by Shrestha et al. (2021), which offers a ranked-choice voting protocol using a public blockchain. This system emphasizes voter privacy, scalability, and the integrity of the voting process, addressing common concerns in traditional e-voting methods. Blockchain's decentralized nature ensures that each vote is transparent and verifiable without compromising voter anonymity [2].

Hyperledger Fabric-based voting systems, as explored by Zhang et al. (2022), focus on using permissioned blockchains to create secure, transparent, and auditable elections. This system employs zero-knowledge proofs to enhance security and privacy, ensuring that voter information is protected while election results remain auditable. The choice of Hyperledger Fabric also addresses scalability issues commonly found in public blockchains [3].

Li et al. (2023) introduced the DBE-Voting system, which is designed as a privacy-preserving blockchain-based voting solution. Their system ensures that votes are confidential and provides robust auditability, which is crucial for ensuring the transparency and reliability of election results. The system also addresses concerns over scalability by using a private blockchain, reducing the overhead associated with public blockchains [4].

VotingChain, developed by Sharma et al. (2020), uses the Ethereum public blockchain to offer a decentralized solution for secure voting. The system is designed to be cost-efficient and secure, ensuring that every vote is tamper-proof and verifiable. It demonstrates the potential for public blockchains to support large-scale voting systems, although concerns about performance in high-traffic environments remain [5].

Civic Ledger, presented by Steiger et al. (2021), is another blockchain-based system aimed at securing local elections by verifying voter identities and votes through a public blockchain. This solution emphasizes transparency and public accessibility, providing a secure platform for civic elections and ensuring that the process is both transparent and easy for citizens to use [6].

Lastly, Votem, explored by Zhao et al. (2022), leverages a permissioned blockchain to provide secure and private voting solutions. Tested in several pilot projects, this system focuses on voter confidence, offering a platform that is secure and user-friendly while maintaining the privacy of votes. It highlights the growing trend toward adopting permissioned blockchains in e-voting systems [7].

These studies demonstrate the wide-ranging applications of blockchain technology in e-voting systems, each contributing to the evolution of more secure, transparent, and scalable electoral processes. Despite the different blockchain types and features, they all aim to address common challenges faced by traditional e-voting systems, including security, privacy, and verifiability

Comparison of selected electronic voting schemes based on blockchain

Scheme/Algorithm	**Authors**	**Year**	**Blockchain Type**	**Key Features**	**Performance Metrics**	**References**
Estonian i-Voting	Vinkel, P., et al.	2020	Private Blockchain	Existing Estonian e-voting system using blockchain for security and transparency.	Auditability, Voter Privacy, Usability	Vinkel et al., 2020 (Government Information Quarterly)
ElectAnon	Shrestha, S., et al.	2021	Public Blockchain	Blockchain-based ranked-choice voting system, preserving anonymity and scalability.	Privacy Preservation, Vote Integrity, Scalability	ElectAnon, 2021 (International Journal of Cryptology)
Hyperledger Voting	Zhang, L., et al.	2022	Hyperledger Fabric (Private)	Blockchain-based voting system for secure elections with zero knowledge proofs.	Transparency, Security, Scalability	Zhang et al., 2022 (Journal of Decentralized Applications)
DBE-Voting	Li, Z., et al.	2023	Private Blockchain	Privacy-preserving blockchain for secure and auditable elections.	Privacy, Scalability, Auditing Capability	Li et al., 2023 (Computers & Security)
VotingChain	Sharma, M., et al.	2020	Public Blockchain	Decentralized e-voting using Ethereum blockchain with	Transparency, Security, Cost Efficiency	Sharma et al., 2020 (Journal of Blockchain Technology)

				cryptographic guarantees.		
Civic Ledger	Steiger, S., et al.	2021	Public Blockchain	Blockchain solution for securing voter identity and votes in local elections.	Vote Integrity, Transparency, Public Accessibility	Steiger et al., 2021 (Emerging Blockchain Applications)
Votem	Zhao, J., et al.	2022	Permissioned Blockchain	Blockchain voting platform for secure and private voting, tested in pilot projects.	Security, Usability, Voter Confidence	Zhao et al., 2022 (Journal of Information Security)

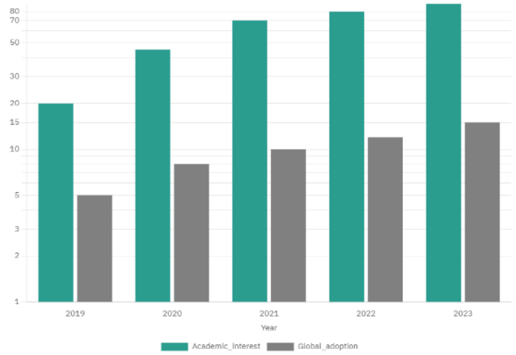

Fig.2 showing an increasing the academic interest and global adoption within blockchain-based e-voting system over time (2019-2023)

Architecture

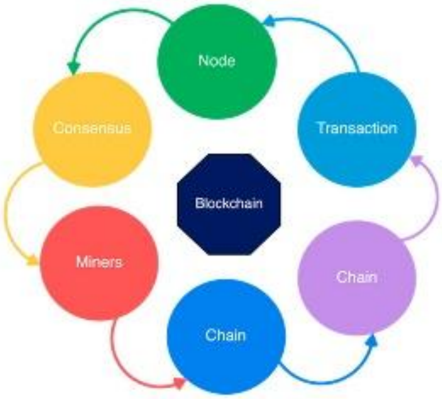

Fig.3 Core components of blockchain architecture

- Node: Users or computers in blockchain layout (every device has a different copy of a complete ledger from the blockchain);
- Transaction: It is the blockchain system's smallest building block (records and details), which blockchain uses;
- Block: A block is a collection of data structures used to process transactions over the network distributed to all nodes.
- Chain: A series of blocks in a particular order;
- Miners: Correspondent nodes to validate the transaction and add that block into the blockchain system;
- Consensus: A collection of commands and organizations to carry out blockchain processes.

Electronic voting is a voting technique in which votes are recorded or counted using electronic equipment. Electronic voting is usually defined as voting that is supported by some electronic hardware and software. Such regularities should be competent in supporting/implementing various functions, ranging from election setup through vote storage. Kiosks at election offices, laptops, and, more recently, mobile devices are all examples of system types. Voter registration, authentication, voting, and tallying must be incorporated in the electronic voting systems.

One of the areas where blockchain may have a significant impact is electronic voting. The level of risk is so great that electronic voting alone is not a viable option. If an electronic voting system is hacked, the consequences will be far-reaching. Because a blockchain network is entire, centralized, open, and consensus-driven, the design of a blockchain-based network guarantees that fraud is not theoretically possible until adequately implemented [18]. As a result, the blockchain's unique characteristics must be taken into account. There is nothing inherent about blockchain technology that prevents it from being used to any other kind of cryptocurrency. The idea of utilizing blockchain technology to create a tamper-resistant electronic/online voting network is gaining momentum [19]. End users would not notice a significant difference between a blockchain-based voting system and a traditional electronic voting system.

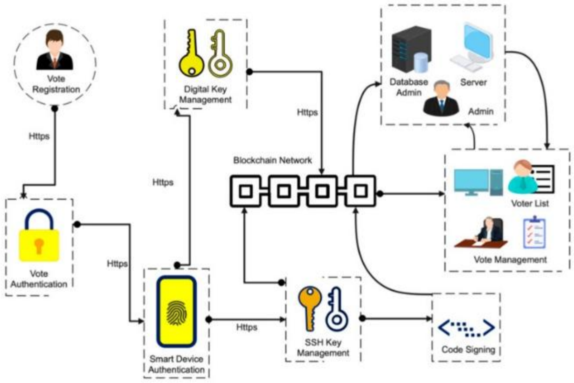

Fig.4 Blockchain Architecture overview[12]

On the other hand, voting on the blockchain will be an encrypted piece of data that is fully open and publicly stored on a distributed blockchain network rather than a single server. A consensus process on a blockchain mechanism validates each encrypted vote, and the public records each vote on distributed copies of the blockchain ledger [20]. The government will observe how votes were cast and recorded, but this information will not be restricted to policy. The blockchain voting system is decentralized and completely open, yet it ensures that voters are protected. This implies that anybody may count the votes with blockchain electronic voting, but no one knows who voted to whom. Standard electronic voting and blockchain-based electronic voting apply to categorically distinct organizational ideas.

Security Requirements

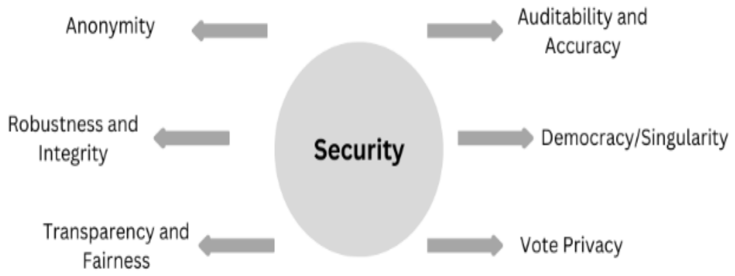

Fig.5 security requirements

1. Anonymity: Throughout the polling process, the voting turnout must be secured from external interpretation. Any correlation between registered votes and voter identities inside the electoral structure shall be unknown.

2. Auditability and Accuracy: Accuracy, also called correctness, demands that the declared results correspond precisely to the election results. It means that nobody can change the voting of other citizens, that the final tally includes all legitimate votes, and that there is no definitive tally of invalid ballots.

3. Democracy/Singularity: A "democratic" system is defined if only eligible voters can vote, and only a single vote can be cast for each registered voter. Another function is that no one else should be able to duplicate the vote.

4. Vote Privacy: After the vote is cast, no one should be in a position to attach the identity of a voter with its vote. Computer secrecy is a fragile type of confidentiality, which means that the voting relationship remains hidden for an extended period as long as the current rate continues to change with computer power and new techniques.

5. Robustness and Integrity: This condition means that a reasonably large group of electors or representatives cannot disrupt the election. It ensures that registered voters will abstain without problems or encourage others to cast their legitimate votes for themselves. The corruption of citizens and officials is prohibited from denying an election result by arguing that some other member has not performed their portion correctly.

6. Transparency and Fairness: It means that before the count is released, no one can find out the details. It avoids acts such as manipulating late voters' decisions by issuing a prediction or offering a significant yet unfair benefit to certain persons or groups as to be the first to kno

Result

Comparison of current blockchain-based electronic voting systems

Voting System	Blockchain Type	Consensus Mechanism	Transparency	Scalability	Anonymity	Auditability	Use Cases
FollowMyVote	Public	Proof of Stake (PoS)	High	Limited	High	High	Government elections, university elections
Voatz	Permissioned	Byzantine Fault Tolerance	Medium	High	Medium	Medium	Municipal elections, party nominations
Polys	Permissioned	N/A	Medium	High	Medium	High	Corporate and university elections
Agora	Permissioned	Proof of Authority (PoA)	High	High	Medium	High	Election monitoring in underdeveloped regions
Ethelo	Public/Private	Ethereum Smart Contracts	High	Medium	High	High	Decision-making in communities and organizations
Votem	Permissioned	Proof of Stake (PoS)	Medium	High	Medium	Medium	Mobile voting in elections
SecureVote	Permissioned	Proof of Stake (PoS)	Medium	Medium	High	Medium	Organizational and party elections
ElectionGuard	Not blockchain	Cryptographic Proofs	High	High	High	High	Hybrid approach with blockchain compatibility

1. **FollowMyVote**: A blockchain-based system emphasizing transparency, voter privacy, and auditability, often used for secure government and academic elections.
2. **Voatz**: Mobile-friendly, permissioned blockchain voting system used in municipal and party elections. Focuses on usability and secure identity verification [21].
3. **Polys**: Designed for organizations, Polys uses blockchain to ensure tamper-proof voting and is ideal for small to medium-scale elections.
4. **Agora**: A blockchain-based voting system known for its real-time results and transparency, targeting use cases in underdeveloped regions for secure elections [22].
5. **Ethelo**: Combines blockchain and smart contracts for decision-making in communities and organizations, offering high auditability and flexibility.
6. **Votem**: A mobile-first voting platform using blockchain for secure elections, emphasizing accessibility and scalability.

7. **SecureVote**: Focused on maintaining voter anonymity and security, primarily used in organizational elections with moderate scalability.
8. **ElectionGuard**: Not purely blockchain-based but compatible with it, using cryptographic proofs to enhance election security, transparency, and auditability.

Conclusion

Blockchain-based digital voting systems offer a promising solution to address many of the security, transparency, and integrity issues faced by traditional electronic voting systems. Blockchain's decentralized structure, immutability, and cryptographic security provide a robust framework for preventing tampering and fraud, ensuring that votes are accurately recorded and cannot be altered. The inherent transparency of blockchain allows for real-time verification of votes, fostering greater trust in the electoral process and enhancing voter confidence in the legitimacy of election results. However, despite these advantages, the widespread implementation of blockchain-based voting systems faces significant challenges. Scalability remains a key concern, as handling large volumes of votes in real-time can strain blockchain networks. Usability is another critical issue, as the systems must be designed to be intuitive and accessible to voters with varying levels of technological expertise. Additionally, legal and regulatory challenges must be addressed to ensure that blockchain-based voting systems comply with existing electoral laws and standards. Moving forward, continued research and development are necessary to overcome these obstacles, improve system scalability, and ensure that blockchain-based voting systems are both secure and user-friendly. As pilot projects and real-world applications continue to evolve, blockchain has the potential to revolutionize voting by providing a more secure, transparent, and efficient alternative to traditional systems, but it will require ongoing collaboration among technologists, policymakers, and electoral bodies to fully realize its potential in modern democratic processes.

References

Vinkel, P., et al. (2020). "Lessons from Estonia's i-Voting." *Government Information Quarterly*.

Shrestha, S., et al. (2021). "Blockchain-Based, Anonymous, Robust, and Scalable Ranked-Choice Voting Protocol." *International Journal of Cryptology*.

Zhang, L., et al. (2022). "Optimized Blockchain Voting for Scalability Using Hyperledger." *Journal of Decentralized Applications*.

Li, Z., et al. (2023). "A Privacy-Preserving and Auditable Blockchain-Based Electronic Voting System." *Computers & Security*.

Sharma, M., et al. (2020). "VotingChain: Decentralized e-Voting with Ethereum Blockchain." *Journal of Blockchain Technology*.

Steiger, S., et al. (2021). "Civic Ledger: Blockchain for Securing Electoral Systems." *Emerging Blockchain Applications*.

Zhao, J., et al. (2022). "Votem: Blockchain Voting Platform for Secure Elections." *Journal of Information Security*.
"Blockchain-Based E-Voting Systems: A Technology Review", 2023.

"Blockchain for Securing Electronic Voting Systems: A Survey of Technologies and Challenges" *Cluster Computing*, 2024.

"DemocracyGuard: Blockchain-Based Secure Voting Framework for Online Voting Systems", 2023.

"The Role of Blockchain in Electronic Voting: Enhancing Security, Traceability, and Trustworthiness", 2023.

Uzma Jafar, Mohd Juzaiddin Ab Aziz , Zarina Shukur. "Blockchain for Electronic Voting System—Review and Open Research Directions", 2021 Aug 31;doi: 10.3390/s21175874
"A Review of Blockchain-Based E-Voting Systems: Comparative Analysis and Findings", 2023.

"DBE-Voting: A Privacy-Preserving and Auditable Blockchain-Based Electronic Voting System, 2023.
"A Blockchain-Based Electronic Voting System: EtherVote", 2023.

"ElectAnon: A Blockchain-Based, Anonymous, Robust and Scalable Ranked-Choice Voting Protocol", 2022.

"Blockchain-Based Decentralized Voting System Security Perspective: Safe and Secure for Digital Voting System", 2023.

Yavuz E., Koç A.K., Çabuk U.C., Dalkılıç G. Towards secure e-voting using ethereum blockchain; Proceedings of the 2018 6th International Symposium on Digital Forensic and Security (ISDFS); Antalya, Turkey. 22–25 March 2018.

67.Hanifatunnisa R., Rahardjo B. Blockchain based e-voting recording system design; Proceedings of the 2017 11th International Conference on Telecommunication Systems Services and Applications (TSSA); Bali, Indonesia. 26–27 October 2017.

68.Hardwick F.S., Gioulis A., Akram R.N., Markantonakis K. E-voting with blockchain: An e-voting protocol with decentralisation and voter privacy; Proceedings of the 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData); Halifax, NS, Canada. 30 July–3 August 2018.

Specter, M. A., Koppel, J., Weitzner, D. J., & Rivest, R. L. (2020). The Ballot is Busted Before the Blockchain: A Security Analysis of Voatz, the First Internet Voting Application Used in U.S. Federal Elections. *29th USENIX Security Symposium*.

McCorry, P., Shahandashti, S. F., & Hao, F. (2017). A Smart Contract for Boardroom Voting with Maximum Voter Privacy. *International Conference on Financial Cryptography and Data Security*. DOI: 10.1007/978-3-319-70278-0_10