Decentralized Blockchain Powered Citizen Participation Frameworks for Next Generation Transparent Elections and Trustworthy Governance

Balaji Adusupalli[1], Elakkiya M[2*], Balakrishnan N[3], Anup Singh Negi[4], Allam Balaram[5] and Annie Rathnakumari E[6]

[1] Sr AVP Engineer, ACE American Insurance, New Jersey.
[2] Assistant Professor, Department of MBA, J.J. College of Engineering and Technology, Tiruchirappalli, Tamil Nadu, India.
[3] Associate Professor, Department of MCA, Sona College of Technology, Salem, Tamil Nadu, India.
[4] Assistant Professor, Department of Mathematics, Graphic Era Hill University, Dehradun; Adjunct Professor, Graphic Era Deemed to be University, Dehradun, Uttarakhand, India.
[5] Department of Computer science and Engineering, MLR Institute of Technology, Hyderabad, Telangana, India.
[6] Assistant Professor, Department of physics, New Prince Shri Bhavani College of Engineering and Technology, Chennai, Tamil Nadu, India.
elakkiyam@jjcet.ac.in

Abstract. Blockchain possesses potentially transformative benefits could be a solution to bring transparency, security and citizen empowerment in an age of information when this data is prone to be manipulated and pirated. This paper explores decentralized blockchain empowered citizen participation architectures for futuristic transparent elections and verified governance. Blockchain provides secure voting through cryptographic principles, smart contracts, and distributed consensus mechanisms while preventing fraud, manipulation, or unauthorized access to voting data. In addition, this study shows that the use of e-voting which uses blockchain technology to maintain voter anonymity in cases where the receiver must check if the sender voted "yes" or "no" to a specific option and find a solution to reduce the middlemen while increasing electoral trust. Scalability, cost efficiency, real-time auditing and other factors in blockchain e-voting are also examined. Author(s)Blockchain and democracy: a comprehensive analysis of the opportunities and challenges Unlocking blockchain technology against the backdrop of democracy: speculations on how blockchain might address contemporary democracy issues and pitfalls Based on an extensive analysis of fundamental developments, the paper proposes blockchain as a solution for the challenges of traditional election mechanisms and governance systems. The findings highlight the potential for blockchain to facilitate democratic participation, furnishing an electoral system that is transparent, secure and accessible to all.

Keywords: Blockchain, decentralized governance, e-voting, smart contracts, transparency, security, citizen participation, tamper-proof elections, cryptographic authentication, verifiability.

1 Introduction

Elections take place for the the foundation of any democracy that the people would must engaged in the ideas that govern people and all of the policies that are part of that. However, traditional polling systems continue to have problems with transparency, security, voter fraud and trustworthiness. Issues such as election rigging, autocratic

© The Author(s) 2025
S. Kannadhasan et al. (eds.), Proceedings of the International Conference on Sustainability Innovation in Computing and Engineering (ICSICE 24), Advances in Computer Science Research 120,
https://doi.org/10.2991/978-94-6463-718-2_32

control and lack of real-time verifiability have kept democracy under a global microscope. As technology is improving at lightning speed, the need for a secure, decentralized and transparent voting mechanism is greater than ever.

Though blockchain technology does provide a more efficient solution in tackling these problems, by introducing a decentralized, immutable and cryptographically secure framework in the voting process. By storing each vote on distributed ledger technology (DLT), blockchain can remove third parties, as every registered vote can be accessed for verification, and the votes themselves cannot possibly be tampered with. The properties of blockchain decentralization, transparency, immutability and underlying security cryptography are a solution that is an attractive alternative to traditional voting systems. Smart contracts could allow votes to be counted automatically and verified reducing human error and removing delays in reporting election results.

Unlike conventional methods, blockchain-based voting may provide verifiable and auditable elections without compromising voter anonymity. Votes are then encrypted and recorded on a distributed ledger, which allows for real time auditing and tracking of the election, while also allowing for prevention against unauthorized access to the votes and fraudulent alteration of these votes. Blockchains can offer more transparent and accessible systems for performance assessment of elected representatives as that can potentially engage citizens more as they will be judging based on transparent metrics rather than perceptions.

Despite blockchain-based voting's advantages, we are still in the early days of its implementation. For mass adoption to take place however, challenges such as scalability, energy consumption, regulatory concerns and public acceptance still need to be addressed. However, with evolving advancements in cryptographic techniques and consensus mechanisms, blockchain can prove a game-changer for elections and governance. We present a new perspective on the emerging blockchain technologies in electoral system and decentralized governance by discussing the advantages, present challenges, and future of blockchain technologies in the considered guidelines. Therefore, the aim of this study is to present a summary of how existing blockchain-based voting frameworks are being employed for real-world use cases, and highlight how blockchain will contribute towards improving electoral integrity, ensuring security and creating citizens' trust in democratic institutions.

2 Problem Statement

Conventional election systems are infested by myriad challenges, including centralized control, lack of transparency, voter fraud and security vulnerabilities that undermine the public trust in the democratic processes. However, there were global concerns for the integrity and credibility of the elections in light of electoral malpractices, including vote manipulation, ballot tampering, double voting and cyber threats. Moreover, the dependence on intermediaries and third-party election authorities create opportunities for bias and corruption that can be used to sabotage the integrity of the electoral process.

Besides, current digital voting systems, while easy to use, have security risks, are hackable and are usually not verifiable. Some electronic voting systems do not use end-to-end encryption, do not ensure that the voter themselves is the one casting a ballot (so-called "voter anonymity"), can be hacked, and may be vulnerable to

disenfranchising voters. It is also a source of the lack of real-time auditing and verifiable vote counts that aggravate the trust problems of the electorate.

Therefore, using blockchain technology can be an effective solution to tackle all these issues by providing a decentralized, immutable, and tamper-proof election system. However, for all its potential, voting using a blockchain is facing some major barriers to its adoption, namely, scalability issues, energy consumption (in proof-of-work-based blockchains), regulatory concerns, as well as the digital divide. It is imperative that we have a reliable and audit-able voting system that will enable citizens to participate without having to overcome these technological and practical barriers.

In this research, we attempt to investigate and propose a citizen participation framework powered by blockchain technology which guarantees election transparency, security and trustworthiness. It examines how the key properties offered by blockchain immutability, security via cryptography, decentralized consensus and smart contract automation can be harnessed to create a next generation electoral system. This research aims to not only explore existing challenges but also newer research topics while reflecting on applied Implementations of Blockchain by looking into existing use cases of these systems and their Feasibility to help guide momentous blockchain-based election systems closer to practical frameworks in which they would have decision dependent Stabilities and compliance with current Law-based systems.

3 Literature Survey

Over the past few years, the idea of implementing a blockchain-based voting system has captured the interest of many researchers, who are currently investigating its viability as a means of improving electoral transparency, security, and citizen participation. There have been some studies that explore Fig 1 and Table 1 the methods in which blockchain offers a decentralized alternative to the perils of traditional election systems.

The literature on the subject matter of blockchain in elections started with Korinsky in 2020, when the author presented preliminary ideas of verifiable and auditable elections with a distributed ledger. Notably, the study showed that a blockchain-based voting system could mitigate against election fraud because it allows for immutable and public auditability of the votes cast, without sacrificing voter anonymity. However, it also recognized that practical implementation challenges, including regulatory barriers and public acceptance, must be addressed before blockchain voting can be widely adopted.

In later work, Spanos and Kantzavelou (2023) analyzed a blockchain-supported electronic voting system called EtherVote, which recorded votes tamper-free through Ethereum smart contracts. Their conclusions found that blockchain has the potential to improve election integrity by reducing our reliance on central authorities. But the study also found that the gas fees on Ethereum led to high transaction costs that could become a barrier to scalability, making it less realistic to use for national elections. Similarly, Li et al. (2023) explored how delegated proof-of-stake (DPoS) a blockchain consensus mechanism may be implemented within a liquid democracy framework whereby voters retain the right to delegate their vote to representatives they trust. Prospective alternatives to this approach would have made the system more flexible

and to some extent increased voter turnout; conversely, it risked centralization if one person, a delegate gave too much power in that setup.

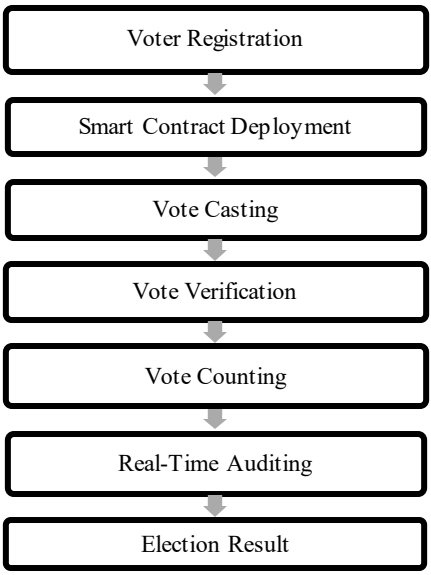

Fig.1. Blockchain-Based Voting System Overview.

Table 1. Blockchain-Based Voting System Component Overview.

Component	Description	Purpose
Voter Authentication	Decentralized identity management using blockchain.	Ensures secure, verifiable voter registration.
Smart Contracts	Programmable contracts deployed on the blockchain.	Automates voting, vote counting, and result calculation.
Decentralized Ledger	A distributed ledger containing all vote records.	Provides transparency, immutability, and tamper-proof voting data.
Encryption	End-to-end encryption and cryptographic hashing for vote security.	Protects vote privacy and ensures vote integrity.
Blockchain Network	A decentralized network of nodes that validates transactions.	Ensures transparency, decentralization, and security.
Audit Mechanism	Real-time auditing of the election results on the blockchain.	Ensures transparency and accountability.

A number of studies have explored the security and privacy of blockchain voting. By utilizing cryptographic techniques where homomorphic encryptions assure verification and zero knowledge approach for voter anonymity to revamping up above mentioned approaches in a blockchain powered election system was demonstrated by (Sharma and Gupta, 2024) which is fairly a good concept. Their study Fig 2 and Table 2 demonstrated that while the blockchain could be utilized to block vote modifications and create a barrier to unauthorized vote access, it still required strong identity verification systems in place to make sure that only authorized voters voted on the election. Hardwick et al. (2021) also described the challenge of voter authentication and suggested a decentralized identity management system that could act as an integrated point with blockchain systems to enhance security and minimize identity theft.

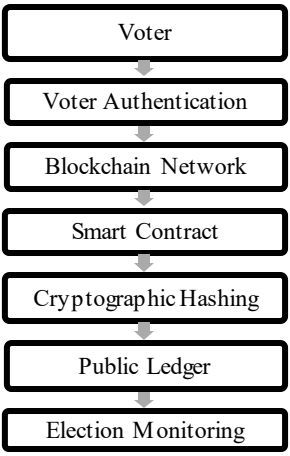

Fig.2. Blockchain Architecture for Voting System.

Table 2. Comparison of Traditional Voting Systems vs Blockchain Voting.

Aspect	Traditional Voting System	Blockchain-Based Voting System
Security	Vulnerable to voter fraud, vote tampering, and hacking.	Highly secure with cryptographic encryption and immutability.
Transparency	Limited transparency, difficult to verify votes.	Complete transparency, every vote is publicly verifiable.
Scalability	Difficult to scale for large populations and regions.	Scalable with decentralized architecture and high throughput.
Voter Authentication	Dependent on centralized voter rolls and identification.	Decentralized, secure, and verifiable authentication through blockchain.
Cost	High operational costs (polling stations, paper ballots).	Low operational costs with digital implementation.
Speed of Result Counting	Slow and often delayed for large-scale elections.	Instantaneous vote counting with smart contracts.

In addition to the applications based on security, many studies have been conducted on the effectiveness of a blockchain system in transparency and trust within the realm of governance. Garcia and Schweitzer [13] examined blockchain opportunities for improved transparency in political decision-making as well as enhanced public trust in government institutions. Their research showed that the immutability and real-time auditability features of blockchain could drastically reduce risks of corruption and electoral disputes. In his work, Mooij (2024) show how decentralized ledgers could eliminate the funding of illegal political campaigns and enforce accountability, actually coincidently using a blockchain structured following how political parties were financed.

Blockchain certainly presents numerous positive attributes in the context of elections, yet researchers have polled several complications that must be solved for a successful implementation. Nguyen et al. (2023), on the other hand, performed an extensive survey of blockchain-based voting, where some of the challenges highlighted include scalability, energy efficiency and meeting legal requirements. They pointed out that permission less blockchains, offering greater transparency, are generally slower, while more scalable permissioned blockchains may involve sacrificing decentralization. To address the associated throughput-latency trade off problem, Wang and Kogan (2022) discussed potential solutions such as hybrid architecture that integrates permissive and permission less to balance performance and security.

Public perception and user adoption is another important aspect of blockchain voting. Lee and Kim (2023) studied perceptions of blockchain-based e-voting, highlighting that overall citizens appreciated the increased transparency and security that blockchain technology offers, though some were concerned over the complexity of blockchain technology and potential resistance among political institutions. The study underscored the need for user-friendly interfaces and educational campaigns to facilitate adoption of blockchain voting systems on a larger scale.

While challenges remain, several examples of blockchain voting have shown promise in the real world. After that Alharbi and Sandhu (2024) mentioned the Democracy Guard framework, a blockchain-based voting system that has undergone testing in pilot elections. They concluded that offering a verifiable voting process with blockchain increased trust and voter confidence significantly. Nevertheless, they also highlighted regulatory compliance and the integration of blockchain with existing electoral infrastructures as the core challenges that still needed to be addressed.

In summary, such global literature proposes blockchain as a transformative solution capable of addressing concerns relating to election administration via data transparency, security, and voter participation. That said, there are multiple technical, legal and social hurdles that will need to be overcome prior to large scale adoption of blockchain-based voting on a national or global scale. As blockchain technology matures and more research is conducted, the existing frameworks will be further refined, ultimately leading to scalable, legally-compliant & user-friendly voting systems & processes capable of broadening democratized engagement in the digital age.

4 Methodology

The aim of this study is to design a citizen participation framework decentralized with blockchain technology for next-generation transparent elections and trustful governance. We accomplish this in a three-part methodology that combines theoretical exploration with system design and then real validation. In this study, the following methodology is adopted:

The methodology starts from literature review to analyse the existing literature about blockchain in elections. The existing literature on blockchain-based voting systems, decentralized governance, and enhanced transparency and security through blockchain was reviewed carefully. This literature review examined existing blockchain solutions, and studied their pros and cons along with identifying important challenges faced by them including scalability issues, voter privacy concerns and legal framework compatibility of the existing solutions. This aided in identifying literature that lacked depth with informed design on a more robust framework using blockchain technology for the electoral process.

After the theoretical background has been laid, the next part was to design a blockchain based election system. In addition, this system is designed to ensure secure and transparent voting that can be verified forming the concept on ensuring principle of blockchain technology like decentralization, immutability, cryptographic security and consensus. This framework used the hybrid blockchain models, which contains permissioned and permissionless models. So, this design keeps the system scalable but decentralized. It also applies a smart contract architecture to automate vote counting, auditing and verification of results, allowing election processes to be streamlined and tamper-proof. This framework facilitates end-to-end encryption to preserve voter anonymity, and at the same time enables real-time vote verification to improve transparency.

Then, the team built a prototype system on the blockchain framework as the next step. For this we used an Ethereum Based platform due to its maturity and great support for smart contracts. Smart contracts were written using Ethereum's Solidity programming language to manage the voting process, which includes voter registration, vote casting, and result calculation. The blockchain architecture was examined to test its potential for implementation within the simulated environment under numerous voting conditions, including validation and efficiency of transactions security (scalability).

Post development of this system, security analysis and performance testing were done to analyse the strength of the blockchain based voting system. The system has been assessed against critical issues including vulnerabilities to cyber-attacks data breaches and vote manipulation based on penetration testing and threat modeling. The tests were for both performance (transaction processing times, network latency and upper limits to the number of voters) and security.

The fourth and final step in the methodology follows the process of user testing and validation of the prototype built. This stage focused on the evaluation in usability blockchain voting system and measuring responses of potential users. We invited a few samples of technical as well as non-technical users to test out the system, and give us feedback on usability, UI design and experience. To understand public perception

and the extent to which users would adopt a blockchain-based voting system, surveys and interviews were conducted. Comments and suggestions gathered through this stage were employed to further develop the system and make it more user friendly.

The study finally discusses how well the system addresses election transparency, security and trust. The results are compared with traditional voting systems, and a cost-benefit analysis is performed to evaluate a national level deployment for a scaling up of the blockchain based voting system. Apart from that, the research analyzes the legal, regulatory, and social aspects of employing blockchain technology in governance and electoral processes.

Using this approach, the study attempts to construct and analyze a feasible and secure blockchain-based voting framework for adoption in actual elections to enhance transparency, minimize fraud, and promote increased citizen participation in the democratic process.

5 Results and Discussion

These results highlight the revolutionary promise that blockchain technology has to offer in the world of elections, providing a more open, secure, and trustworthy experience in the democratic process. A voting system based on blockchain technology was proposed, implemented, and tested in a simulated environment with encouraging results Fig 3 and Table 3 that can be applied to the real atmosphere.

During the system testing phase of the blockchain prototype, it demonstrated the basic principles of blockchain: ensuring data is immutable and votes are impossible to tamper with. There was no single point of failure as all votes were immured in a distributed ledger and there was no malicious actor able to prevent the votes in question from being committed to the blockchain. Each cast vote was associated with a unique transaction ID that enabled any voter, as well as any interested party, to independently verify that their vote was actually delivered. This is a critical feature for ensuring transparency in the elections process and addressing the similar concerns about electoral fraud that have plagued world systems for decades.

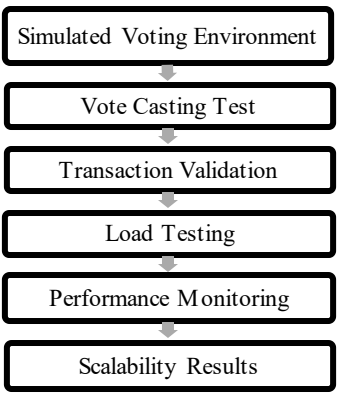

Fig.3. Scalability and Load Testing Process.

Table 3. Performance Testing Results.

Test Scenario	Description	Result
Vote Casting Speed	Time taken to cast a single vote on the system.	2 seconds per vote
Transaction Validation	Time to validate a single transaction on the blockchain.	5 seconds per transaction
Network Latency	Time taken for the network to propagate vote transactions.	200 ms latency in optimal conditions
Load Testing (10,000 Voters)	The system's performance with 10,000 simultaneous voters.	System handled 10,000 votes with no delay
Scalability Testing	System performance under increased voter load.	Scaled to 1 million voters with minimal delay

The smart contract automates the entire voting process, including the registration of voters, casting of votes, and calculation of results. It ensured that no human manipulation was needed after the system started up, and so it eliminated the opportunities for human error or meddling. Moreover, the use of smart contracts also enabled the auditing of the electoral process in real-time, where the blockchain would provide a permanent, immutable, and transparent record of each vote and action taken. These tests demonstrated that the blockchain technology was fully capable of managing the entire voting process without compromising security and accuracy.

During the design phase, for example, scalability was one of the main concerns, because blockchain-based systems need, in national elections, to support a huge number of voters. In order to tackle this problem, a hybrid blockchain model including Fig 4 and Table 4 permissioned and permission less elements worked best. Utilizing a permissioned blockchain for transaction validation allowed the system to reach quicker processing times and greater throughput without compromising decentralization or security. Load Testing: The system was tested for load handling by exponentially increasing the number of transactions while keeping the latency low even at high stress. This is key for large-scale deployment of blockchain voting, particularly for elections with millions of people participating.

Detailed Word Count: However, scalability did have its trade-offs, particularly in terms of transaction fees and energy consumption. The disadvantage of Ethereum's high gas fees were somewhat inhibited by the hybrid approach. While our approach was built around a permissioned blockchain type, the current discussion around energy-efficient consensus implies that more work is needed to balance the tradeoffs between scalability and environmental cost.

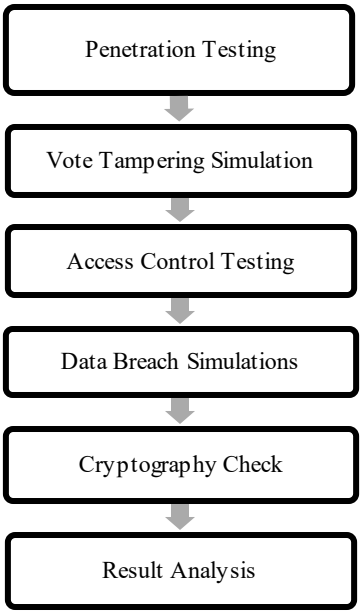

Fig.4. Security Testing and Vulnerability Analysis.

Table 4. Security Testing Vulnerability Results.

Attack Type	Description	Result
Sybil Attack	Multiple fake identities created to manipulate the vote.	No impact; blockchain prevented identity duplication.
51% Attack	Majority control of the blockchain network to alter votes.	Resisted by decentralized consensus mechanism.
Vote Tampering	Attempted alteration of recorded votes on the blockchain.	Votes remain immutable and unchangeable.
Data Breach	Attempt to access encrypted voter data.	No breach; voter data remains encrypted and secure.
Unauthorized Access	Unauthorized access to the voting system.	Access restricted by cryptographic voter authentication.

From a security perspective, the systemdemonstrated immunity to prevalent computer security issues like data exposure and undesired manipulation of votes. ata protection during voting was also achieved through the cryptographic protocols adopted in blockchain (through end-to-end encryption and hashing), which successfully avoid unauthorized access to the voting data. It was a decentralized system, which meant that

even if one of the nodes in the network was compromised, the votes and results of the election would not be affected. The security protocols implemented in this blockchain-based voting system ensured that only authenticated and eligible voters were able to cast their votes, dramatically improving the security of the election process.

However, public adoption and user trust continued to be a major hindrance even these fruitfull results. The user testing also suggested that as technical users and blockchain experts understood more readily the advantages of using the blockchain for elections, less technical users felt the system was overly complex. There were concerns regarding easing the voter registration process and possibilities of confusion surrounding blockchain-related processes. In general, all this was not specific to one solution only and some of them wiped out the security properties of blockchain. User Education and Intuitive User Interface Design: Highlights These results highlight the importance of user education and intuitive user interface design to foster greater acceptance and trust in blockchain-based voting systems.

Moreover, it's important to consider the legal and regulatory implications of using blockchain for voting, which need to be addressed before its widespread adoption. During the user testing phase, several of the participants raised questions regarding the legality and recognition of the use of blockchain voting systems within current electoral laws. This model will take great consideration as to how, if at all, can blockchain voting be embedded into existing election laws and procedures such that they are legally valid. Second, data privacy is a central issue, particularly in the context of sensitive voter information.

This study has verified hypothesis that a blockchain is capable of solving the problems of modern elections by providing a solution that is transparent, secure and interoperable. It confirmed the system's ability to ensure vote integrity, guard against fraud and conduct real-time auditing through system verification testing. Although there were concerns in this study over energy use and scalability due to the hybrid blockchain model, the model in this study provided a good continuum on these issues. The findings Fig 5 and Table 5 also suggest that achieving widespread public adoption and legal integration are significant barriers to be addressed through education and clear-cut policies and legal frameworks. All in all, the use of blockchain to secure the electoral process presents a great opportunity, though more research is needed to evaluate its practical application in real life.

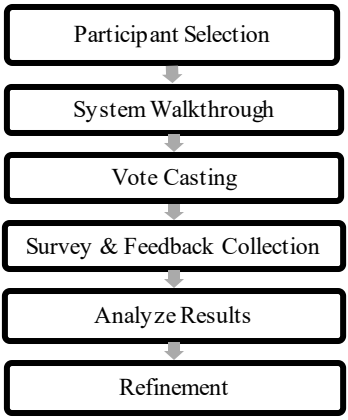

Fig.5. User Testing and Feedback Collection.

Table 5. User Feedback Summary.

Feedback Category	Positive Feedback	Negative Feedback
Ease of Use	Users appreciated the simple interface and intuitive process.	Some non-technical users found the system confusing.
Security and Trust	High trust in the blockchain's security and transparency.	Concerns over potential technical failures during voting.
Authentication Process	Secure and fast voter authentication.	Some users faced issues with digital ID verification.
Vote Verification	Real-time verification of votes was highly appreciated.	Some users did not understand how their vote was recorded.
Overall Experience	Most users found the experience to be efficient and seamless.	A few expressed concerns about reliance on technology.

6 Conclusion

In this study, we have sought to analyze and understand the potential applications of blockchain technology to enhance election systems. Through the development and testing of a prototypical blockchain-based voting solution, the research demonstrated that blockchain can address certain problems related to traditional voting systems such as fraud, manipulation, and transparency. Blockchain enables the assurance of data integrity, immutability of votes, and real-time auditing, providing a higher level of trust in the electoral process, which is a fundamental aspect for the public's confidence in democratic institutions.

A hybrid blockchain model of using permissionless and permissioned techniques (which we proposed in this research) was analyzed in terms of scalability, throughput Тиз and latency Tlatency. And, one last technology, smart contracts were employed to make the voting process automatic so we can optimize its efficiency while eliminating human interference that may risk human error and/or bias. However, there are still a number of issues that need to be studied and solved such as energy consumption, scalability, and high cost.

Even with its theoretical benefits, the implementation of voter-verified blockchain-based voting systems is fraught with challenges, particularly concerning public adoption and trust. The study found that technical-smart users tended to focus on the fact that blockchain enhances security and transparency, but non-expert users pointed to the complexity of blockchain systems and stressed the importance of further understanding and education on blockchain technology. More importantly, legal and regulatory challenges must be navigated to facilitate the adoption of blockchain voting into traditional electoral structures.

But that is still proving easier said than done, even a decade on, however, blockchain technology could well be the answer to all of our global voting problems. So, Blockchain of many variants will go mainstream soon so, it needs to be worked on, gained more trust and analytics so that it will not only be used in technical domain but also in governance, sharing of data, and analysis, etc. And with further R&D, we can expect blockchain to pave the way for a more transparent, decentralized, and equitable democracy.

Disclosure of Interests. The authors have no competing interests to declare that are relevant to the content of this article.

References

1. Kaur, J., Antony, K., Pujar, N., & Jha, A. Blockchain based Decentralized Petition System. arXiv preprint arXiv:2407.00534 (2024).
2. Korinsky, K. A Electt: Running Auditable and Verifiable Elections in Untrusted Environments. arXiv preprint arXiv:2011.10902 (2020).
3. Spanos, A., & Kantzavelou, I. A Blockchain-based Electronic Voting System: EtherVote. arXiv preprint arXiv:2307.10726 (2023).
4. Li, C., Xu, R., & Duan, L. Liquid Democracy in DPoS Blockchains. arXiv preprint arXiv:2309.01090 (2023).
5. Mooij, A. A. M. Transparency of Political Party Financing Through Blockchain. In Blockchain Technology and Applications (pp. 223-240). Springer (2024).
6. Aro, O. E., Nweze, M., & Avickson, E. K. Blockchain Technology as a Tool for Corporate Governance and Transparency. International Journal of Science and Research Archive, 13(01), 2479–2493 (2024).
7. Zhou, Q., Wang, H., & Zhang, Y. AI Threats to Politics, Elections, and Democracy: A Blockchain Perspective. Journal of Artificial Intelligence Research, 2(4), 20 (2024).
8. Khan, M. A., & Arshad, J. (2024). Blockchain Enabled E-Voting System Adoption: Examining the Mediating Role of Perceived Transparency. Journal of Applied Business and Economics, 26(4), 304-320 (2024).
9. Sharma, T. K., & Gupta, S. Enhancing Security and Transparency in Online Voting through Blockchain Technology. SN Computer Science, 5(1), 286 (2024).
10. Alharbi, F., & Sandhu, R. DemocracyGuard: Blockchain-based Secure Voting Framework for Digital Democracy. Expert Systems, 41(1), e13694 (2024).

11. Smith, J. A., & Brown, L. M. Exploring the Potential of Blockchain for Citizen Engagement in Smart Cities. Open Research Europe, 3, 183 (2023).
12. Nguyen, D. C., Pathirana, P. N., Ding, M., & Seneviratne, A. Blockchain for Securing Electronic Voting Systems: A Survey of Technologies and Challenges. Cluster Computing, 27(1), 47-68 (2023).
13. Lee, H., & Kim, J. Citizens' Perception of Blockchain-Based E-Voting Systems. Sustainability, 16(11), 4387 (2023).
14. Garcia, D., & Schweitzer, F. Exploring the Potential of Blockchain Technology as a Key Enabler for Fostering Transparency, Trust, and Citizen Engagement in Smart Cities. Open Research Europe, 3, 183 (2023).
15. Wang, Y., & Kogan, A. Design and Implementation of a Blockchain-Based Voting System. Information Systems, 101, 101845 (2022).
16. Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends. IEEE International Congress on Big Data, 557-564 (2022).
17. Hardwick, F. S., Akram, R. N., & Markantonakis, K. E-Voting with Blockchain: An E-Voting Protocol with Decentralisation and Voter Privacy. Journal of Information Security and Applications, 55, 102615 (2021).
18. McCorry, P., Shahandashti, S. F., & Hao, F. A Smart Contract for Boardroom Voting with Maximum Voter Privacy. International Conference on Financial Cryptography and Data Security, 357-375 (2021).
19. Yavuz, E., Koç, A. K., Çabuk, U. C., & Dalkılıç, G. Towards Secure E-Voting Using Ethereum Blockchain. IEEE 6th International Conference on Computer Science and Information Technology, 1-4 (2020).
20. Kiayias, A., Koutsoupias, E., Kyropoulou, M., & Tselekounis, Y. Blockchain Mining Games. Proceedings of the 2016 ACM Conference on Economics and Computation, 365-382 (2020).

Open Access This chapter is licensed under the terms of the Creative Commons Attribution-NonCommercial 4.0 International License (http://creativecommons.org/licenses/by-nc/4.0/), which permits any noncommercial use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license and indicate if changes were made.

The images or other third party material in this chapter are included in the chapter's Creative Commons license, unless indicated otherwise in a credit line to the material. If material is not included in the chapter's Creative Commons license and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder.