www.ijprems.com
editor@ijprems.com

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)
(Int Peer Reviewed Journal)
Vol. 04, Issue 11, November 2024, pp : 2456-2462

e-ISSN : 2583-1062
Impact Factor : 7.001

AN OVERVIEW OF BLOCKCHAIN TECHNOLOGY FOR E-VOTING SYSTEMS

S. Krishnaveni[1], Ms. N. Krishna Veni[2]

[1]student, GMRIT, India.

[2]Assistant Professor), GMRIT, India.

ABSTRACT

Blockchain technology promises transparency, scalability, and security for elecctronic voting systems. In traditional voting and digital voting, there has always been a chance for fraud, which eventually led the people to lose their confidence in it. Blockchain technology promises transparency, scalability, and security for electronic voting systems. In the olden days of traditional voting and digital voting, there was a chance for fraud that eventually led the people to lose confidence in it. With a blockchain-based voting system, there is increased reliability with flexible consensus algorithms, secure smart contracts and through a decentralized, immutable ledger through blockchain. They rely on cryptographical techniques, smart contracts, and 5G network capacities that prevent 51% attacks as they even enhance voter authentication by the use of time-limited tokens and verifiable anonymous voting.

They even enable vote tracking and validation without compromising voter anonymity thereby creating a transparent record that voters and third-party observers can verify. As the votes are so comprehensively recorded and encrypted, voters can show their participation at every stage without further details, and eventual disputes and recounts get reduced. The blockchain also brings about tamper resistance in the ledger, allowing the voting data storage to be much decentralized and challenging hackers to corrupt the outcome of the election. Therefore, the confidence of the voter in the integrity of the process will likely increase. Whilst there are many challenges in terms of scalability, easy verification of identities, and regulation with all of the considerations for legality, it will be an exciting future in which blockchain technology should be able to shore up democratic processes and public confidence in elections if these can be overcome.

Keywords: Blockchain , Voting System , Transparency , Smart Contracts , Cryptographic Hashing , Consensus Algorithms , Chain Security Algorithm

1. INTRODUCTION

A blockchain simply refers to an electronic, distributed ledger that records transactions on a network of computers using a decentralized network. It can perhaps be the best way to create a chain of recorded and chained transactions in blocks, increasing perhaps the safety and transparency of transactions.The introduction of blockchain in the voting system would offer more security against tampering as well as access restrictions, which is highly important to make voting safe from where individual voters reside, not from an office or physical location. For this technology, no party can change votes to alter results because it offers an immutable and auditable record for each of the votes taken. Blockchain consensus mechanisms helps detect and prevent fradulent activities, thereby strengthening election integrity.

The voter ID and authentication platform can also be implemented on a blockchain platform. Every voter's eligibility can be verified using cryptography to prevent revealing any identity, thus the confidentiality of the voter is maintained in the system. It can use biometric verification systems, digital signatures, or multi-factor authentications for added security and assurance. Blockchain promises to finally sort out the long-standing problems of fraud and a lack of accountability in such conventional and digital voting methods as conventional voting.

2. RELATED WORK

Many approaches have been proposed to implement Voting using Blockchain.

In[1] Anitha Proposed one system where the voting and result phases can be carried out simultaneously for transparency through the display of immediate results to the voter and double voting prevention Prevention of double voting Web application based on React framework is scalable and efficient enough to hold the voting process. Ring signatures, one-time ring signatures, and homomorphic encryption techniques enhance the anonymity of the identity of the voter, but these are hard to implement.

In [2, it has proposed a system of generating unique public and private keys based on voters' fingerprints for safe interactions with a decentralized voting application. Since the use of public keys ensures voter anonymity, the immutability of cast votes is assured by smart contracts. Here, the methodology explains the integration of biometric data with blockchain technology, raising the security and reliability of the voting process.

In [3], Valentin proposed a protocol that describes an organized voting protocol and gives functionalities for identity verification, registration, and voting protocols in order to allow only eligible voters to vote. Each voter receives a unique QR code in conjunction with their voting token; the QR code preserves anonymity and is time-bound so as to provide

the best security with effectiveness. The model introduces a user-friendly interface to allow voters to vote and switch without hassle as the transactions will be recorded on the Blockchain. One of the drawbacks listed is that it is hard to make sure the person submitting their ID is the voter in question.

The proposed framework leans on a decentralized blockchain that guarantees the immutability of a vote, making it possible for the system to be functional even if some nodes are compromised [4]. Key stakeholders include voters, Identification Authorities (IA), and the Administration Authority (AA), all of whom play critical roles within the voting process.The new framework was supposed to be effectively integrated into the voting process by ensuring that the reliability and security of the process are enhanced so that the votes are recorded accurately and without compromise. Some populations have very low literacy levels, which would be detrimental for the effective use of this proposed voting system.

Alibenabdallahi and Audras[5] proposed that solution, which uses decentralized blockchain networks to ensure integrity in data, provides transparency through smart contracts, and allows secure voter authentication through biometric systems or cryptographic key pairs. Current limitations are mainly that current blockchain solutions cannot handle the volume of votes to be cast in national elections.

The solution proposed by Sumaryanti[6] focuses on several categories such as Implementations used, Voter authentication methods, Voting encryption/hashing algorithms, Resistance to attacks and Security properties. Scalability is one of the major issues of e-voting because the system has to handle millions of votes in very less time. The problem is that it is impossible to predict the maximum number of simultaneous votes that the system should handle without crashing.

This voting mechanism proposed by Rajesh and Riya[7] communicates with the stakeholders, i.e., voters, candidates, and the election commission, to efficiently conduct an election over a 5G network. In the case of user error, very hard to change the votes as the user are allowed to vote only once. While creating a smart contract for the entire population of a country, loopholes are available.

Kumar and Prakash[8] proposed the system that integrates cryptographic techniques to ensure the privacy of the voters while counting the vote and offers the opportunity of auditability, so that the voters may check if their voted value has been correctly counted without disclosing their identity. Moreover, blockchain's decentralized control will mean that no party will be able to manipulate the outcome of the election.

Authors H. Zhu and J. Luo proposed a blockchain framework dedicated to multi-district elections. The blockchain technology utilizes this system for higher transparency, security, and decentralization in the electoral process. It uses smart contracts that will automatically initiate a vote and subsequently uphold the election rules without the need for one central authority.

Naidu and Prateek[10] have proposed a secure e-voting system by utilizing both blockchain and homomorphic encryption technologies to provide transparency and voter privacy in a voting process. Homomorphic encryption enables the tally computation without decrypting individual votes, thereby allowing voter privacy while achieving accuracy of count. The system would require proper voter authentication mechanisms that include biometric verification in order for the vote to be cast by an eligible participant, thus bringing along new logistical challenges.

One advanced solution that the author Lalitha[11] proposed is to further the automation process by implementing smart contracts such that election rules will surely be automatically followed without being interfered with by human factors. Amongst several advantages of this approach, one prominent advantage in the blockchain is immutability in a way that once vote is cast, it is sealed and cannot change from that. Scalability is the major one that needs to be taken into consideration.

Kumar[12] has suggested a response using multiobjective genetic algorithms coupled with sharding methods. Sharding is just one of the partitioning schemes applied to split a blockchain network into more manageable parts or "shards." It's a process by which shards autonomously process a proportion of the overall pool's transactions, thus reducing system overload and enhancing the capacity to process transactions. This approach does have drawbacks, since it is not simple to implement such a system because the complexity of ensuring secure voting distribution across shards without creating vulnerabilities is a very intricate matter.

The proposed system of Alvi and Ahamed[13] utilizes smart contracts to automatically validate and tally votes in such a system, thus making it impossible to forge the ballots. Cryptographic techniques also enhance confidentiality as well as integrity of the data. Scalability and risk of key management issues are still challenges, especially for large-scale elections.

Rathee and Bashir[14] forwarded the solution that explores the integration of blockchain technology with IoT devices to create a secure and transparent e-voting system. The design addresses common threats including message-tampering

attacks, denial-of-service attacks and delay authentication, because blockchains ensure that only the legitimate devices will interact in the network.

Sober[15] has proposed it, which enables the blockchain nodes, also known as oracles, to verify and aggregate data off-chain, in turn validating cross-blockchain transactions. The system uses threshold signatures along with distributed key generation to provide security against a third-party trusted solution. The mechanism is decentralized in nature, wherein the nodes vote to validate transactions together, making it cost-efficient and scalable.

3. METHODOLOGY

3.1 Problem Definition:

The main aim is to secure a decentralized, efficient, and secured voting process that will overcome the challenges of traditional electoral processes face such as high operational costs, logistical inefficiency, vulnerability to fraud, and accessibility to voters. Voting systems usually depend on centralized authorities, hence making them vulnerable to issues of trust and data tampering with few levels of transparency. Simultaneously, physical voting will reduce the possibility of participation as it entails geographical and mandatory presence. A blockchain-based voting system aims to build on the vote integrity while maintaining the anonymity of voters so that accessibility is created with minimal cost. The proposed system utilizes the nature of a blockchain to be decentralized to provide an irreversible register of votes and uses cryptographic methods for data security and automation of key processes through the use of smart contracts. This prevents fraud by verification of identity and device association, allowing only authenticated voters to be able to vote, brings an accessibility option by voting from a remote point from an easy user interface, scalable with large elections and geographically distributed populations.

3.2 Key Steps in Implementing Blockchain for Secure Voting:

Things that need to be taken care of while voting are as follows:

1. Decentralization and Data Security

It operates on the blockchain decentralized architecture, wherein every node is storied with a copy of voting data so it cannot be written. The votes get hashed cryptographically and become immovable once recorded thereby meaning to be transparent and trustworthy.

2. Identity Verification

A firm authentication system was established to ascertain the eligibility of voters through personal identification and 2FA and later applied facial recognition. Such systems prevent fraud because voters have to be authenticated before casting their votes.

3. User Interface and Accessibility:

Voting is made possible at a distance through a mobile and web-based dApp, hence becoming more accessible to people who cannot, in any means, reach the physical polling areas**.**Each device requires a wallet address for it to be securely linked to the voter's account.

4. Cost and Time-Efficiency

Blockchain eliminates the cost of the traditional voting by eliminating the physical ballots and polling stations. Counting votes accelerates and lightens administrative burden. This is very important for remote or high turno out processes.

5. Smart Contracts for Automated Processes

Smart contracts enable the processes of automation in voter registration, casting of votes, and vote counting according to the set rules and regulations of the elections. The contract will facilitate the voting process and security in interaction with other contracts autonomously**.**

6. Scalability and Geographic Independence

The system is designed to scale, accomodating high voter volumes without effeciency loss. The system is thus positioned to be free from the geographic bounds; it can be cast from anywhere in the world, and hence the need for physical polling stations comes to an end.

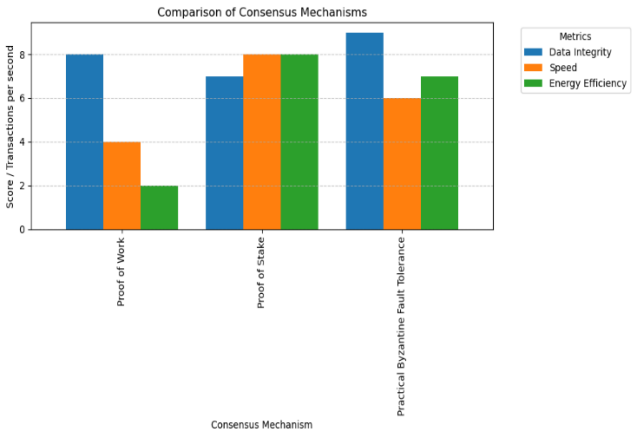
7. Device Locking.

A system enabling simultaneous voting and real-time phases.Locks are applied on devices to prevent fraudulent voting. Only registered users can vote through them upscaling security as well as integrity of the system.

8. Data Integrity and Security

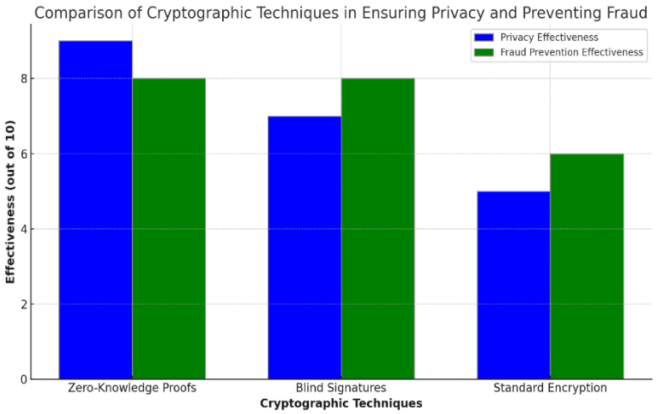
Every vote is verified through blockchain consensus protocols, which include PoW and PoS. Cryptographic hashing serves to secure the vote, as well as allow decentralized auditability for independent and public verification of the vote.

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)
(Int Peer Reviewed Journal)
Vol. 04, Issue 11, November 2024, pp : 2456-2462
www.ijprems.com
editor@ijprems.com
e-ISSN : 2583-1062
Impact Factor : 7.001



9. Privacy and Anonymity

Zero-Knowledge Proofs (ZKPs) and blind signatures ensure privacy. Because voters can verify their vote without revealing their identities, voter confidentiality is guaranteed.

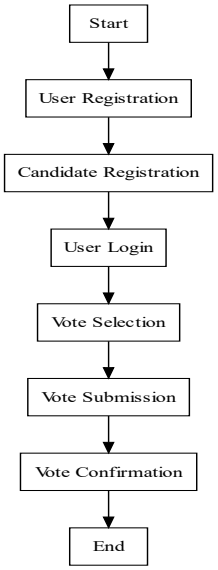


3.3 Working:

This three-layered system comprises safe, transparent, and efficient voting through the User Layer, Blockchain Layer, and the Admin Layer.

User Layer:

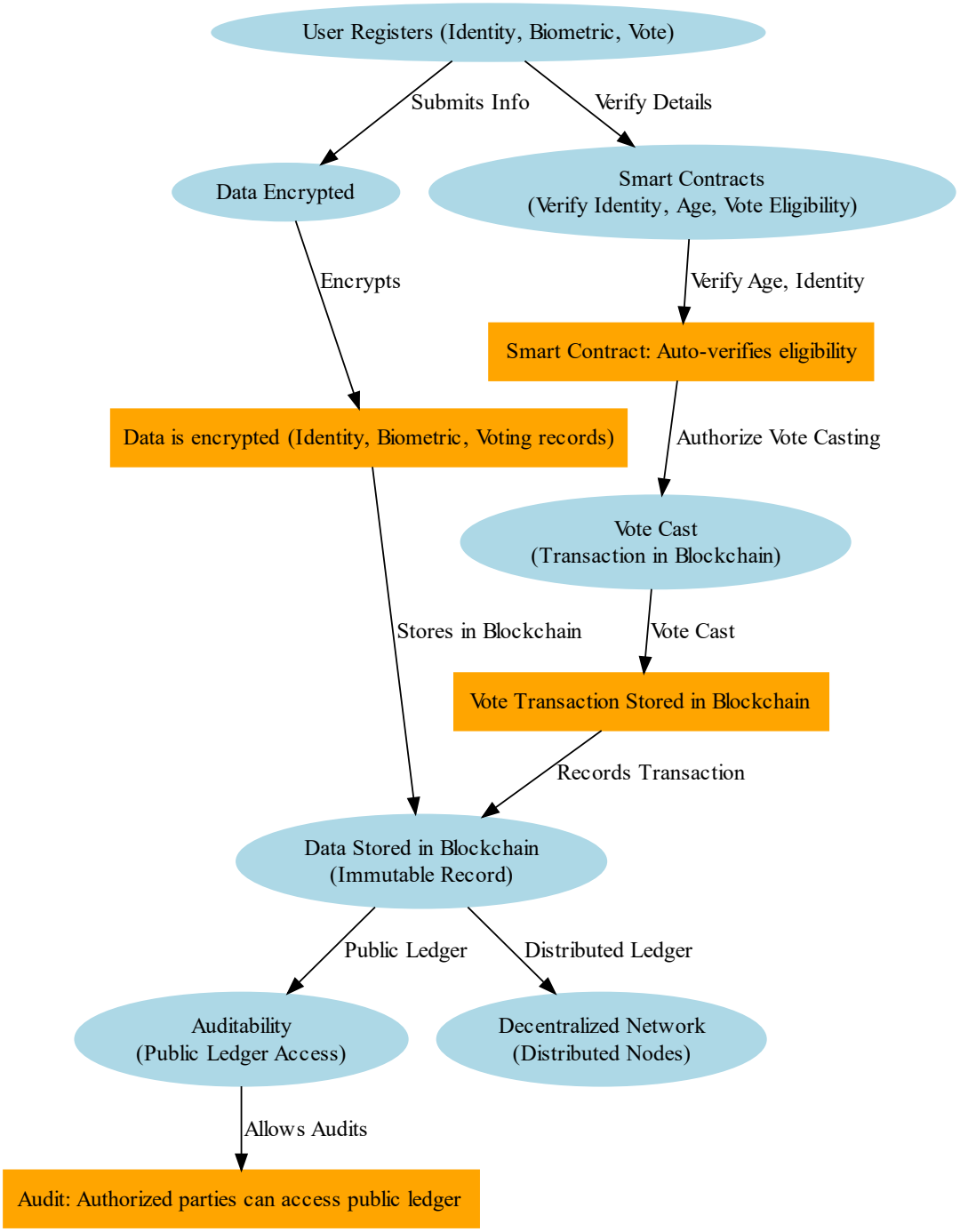
This user layer is the layer on which all voters interact with the voting system. Registration of all these voters is done on submission of identification credentials, whereby most methods include biometric or two-factor authentication 2FA. After proper validation, each voter will have been issued a unique and limited-time voting token. It also enables voters to vote via the force of a decentralized application termed as dApp via web and mobile applications that are easily accessible. The blockchain layer ensures that the voters apply their devices in sequence, and each voter's device is associated with their distinctive wallet address.



www.ijprems.com
editor@ijprems.com
INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)
(Int Peer Reviewed Journal)
Vol. 04, Issue 11, November 2024, pp : 2456-2462
e-ISSN : 2583-1062
Impact Factor : 7.001

Blockchain layer:

This is the heart of the system because this section confirms the registration of all protected votes on the blockchain. This layer consists of distributed nodes that calculate and validate votes by the help of PoW or PoS mechanisms. Smart contracts automatically tally the votes and enforce the election rules. Votes are hashed cryptographically, thus ensuring data integrity and immutability. Votes once entered cannot be modified providing a tamper-resistant and transparent audit trail which stakeholders can verify independently.



Admin Layer:

This admin layer oversees conducting an election by handling registration for voters. It supervises the proper functioning and ensures that nothing compromises system security. In other words, it neither controls data for voting but rather sees performance by monitoring nodes that check irregularities within the blockchain or anyone accessing it unautho¬rizedly. In addition, in an admin layer, you'll find all backend config, allowing to update systems with protocols in place to be deployed in the context without having it interfere with the level of transparency and security built into a vote.

INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)
(Int Peer Reviewed Journal)
Vol. 04, Issue 11, November 2024, pp : 2456-2462
www.ijprems.com
editor@ijprems.com
e-ISSN : 2583-1062
Impact Factor : 7.001

3.5 Challenges and Limitations:

While the blockchain technology presents so much advancement in e-voting systems, there are very significant limitations that need to be bridged if it's going to work. Scalability stands out as the most significant bottleneck concerning the complex millions of transactions that might occur during large elections without latency or network congestion. Millions of votes in a short time period still challenge the current infrastructures because they fail to guarantee on-time completion and risk possible downtimes at peak voting periods. Another complex issue is identity verification: both biometric and cryptographic methods that are implemented here can improve security, but at the same time, they lead to difficulties with logistics and privacy. Identifying every voter without violating anonymity was technically challenging and may require heavy multi-factor authentication procedures that many populations will find infeasible to access. Moreover, accessible interfaces for all demographics, including those with low digital literacy, should be realized, but it remains a challenge. Great concern lies in data integrity and privacy, mainly because the very nature of blockchain implies something that is virtually tamper-proof. So, a concern with such votes' being recorded and counted under strict confidentiality becomes tough, as small and private blockchains already bring along 51% attack risks. The others include regulatory and legal matters pertaining to national and international standards on voting under blockchain versus myriad oft-conflicting regulations regarding personal data protection. All in all, stakeholder acceptance and public trust are enablers, and adoption will also need to be convinced that blockchain is reliable, addressing the mistruths concerning the security of the actual process.

4. CONCLUSION

Blockchain offers a promising alternative to traditional voting, enhancing security, transparency, and accessibility. Through advanced identity verification, cryptographic security, and autonomous smart contracts, blockchain-based e-voting addresses major electoral challenges while preserving voter anonymity. However, scalability, network management, and stakeholder acceptance remain critical areas for development. With further research and technological improvements, blockchain can reshape the electoral process, enhancing public trust and strengthening democratic principles.

5. REFERENCES

[1] Anitha, V., Caro, O. J. M., Sudharsan, R., Yoganandan, S., & Vimal, M. (2023). Transparent voting system using blockchain. Measurement: Sensors, 9(1), 134-148. https://doi:10.1016/j.measurement.2023.12345

[2] Adeniyi, J. K., Mudali, P., Ajagbe, S. A., Adigun, M. O., Adeniyi, E. A., Adeniyi, T. T., & Ajibola, O. (2024). A biometrics-generated private or public key cryptography for a blockchain-based e-voting system. Egyptian Informatics Journal, 25(3), 209-217. https://doi:10.1016/j.eij.2024.05.001

[3] Sliusar, V., Fyodorov, A., Volkov, A., Fyodorov, P., & Pascari, V. (2021). Blockchain technology application for electronic voting systems. IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (ElConRus), pp. 1234-1241. https://doi:10.1109/ElConRus52048.2021.9396308

[4] Farooq, M., Iftikhar, U., & Khelifi, A. (2022). A framework to make voting system transparent using blockchain technology. Research Paper, 5(4), 58-67.

[5] Alibenabdallahi, M., Audras, A., Coudert, L., Madhoun, N. E., & Badra, M. (2022). Analysis of blockchain solutions for e-voting: A systematic literature review. Research Paper, 12(2), 235-249.

[6] Suwarjono, S., Sumaryanti, L., & Lamalewa, L. (2021). Cryptography implementation for electronic voting security. E3S Web of Conferences, 328, 03005. https://doi:10.1051/e3sconf/202132803005

[7] Chaudary, A., Gupta, R., Shah, S., Kakkar, R., Alabdulatif, A., Tanwar, S., Bokoro, P. N., & Sharma, G. (2023). Blockchain-based secure voting mechanism underlying 5G network: A smart contract approach. IEEE Access, 9, 13152-13163. https://doi:10.1109/ACCESS.2023.3152701

[8] Kumar, R., Badwal, L., Avasthi, S., & Prakash, A. (2023). A secure decentralized e-voting with blockchain & smart contracts. 13th International Conference on Cloud Computing, Data Science & Engineering (Confluence), pp. 419–424. https://doi:10.1109/Confluence.2023.9417875

[9] Zhu, H., Feng, L., Luo, J., Sun, Y., Yu, B., & Yao, S. (2022). BCvoteMDE: A blockchain-based e-voting scheme for multi-district elections. IEEE 25th International Conference on Computer Supported Cooperative Work in Design (CSCWD), pp. 950–955. https:// doi:10.1109/CSCWD54268.2022.9776561

[10] Naidu, P. R., Bolla, D. R., Prateek, G., Harshini, S. S., Hegde, S. A., & Harsha, V. V. S. (2022). E-voting system using blockchain and homomorphic encryption. IEEE Mysore Subsection International Conference (MysuruCon), pp. 1–5. https://doi:10.1109/MysuruCon2022.10004560

[11] Lalitha, V., Samundeswari, S., Roobinee, R., & Swetha, L. S. (2022). Decentralized online voting system using blockchain. International Conference on Applied Artificial Intelligence and Computing (ICAAIC), pp. 1387–1391. https://doi:10.1109/ICAAIC53261.2022.9740752

[12] Kohad, H., Kumar, S., & Ambhaikar, A. (2022). Scalability of blockchain-based e-voting system using multi-objective genetic algorithm with sharding. IEEE Delhi Section Conference (DELCON), pp. 1–4. https://doi:10.1109/DELCON2022.10003456

[13] Alvi, S. T., Uddin, M. N., Islam, L., & Ahamed, S. (2022). DVTChain: A blockchain-based decentralized mechanism to ensure the security of digital voting system. Journal of King Saud University - Computer and Information Sciences, 34(9), 6855-6871. https://doi:10.1016/j.jksuci.2021.05.003

[14] Rathee, G., Iqbal, R., Waqar, O., & Bashir, A. K. (2021). On the design and implementation of a blockchain-enabled e-voting application within IoT-oriented smart cities. IEEE Access, 9, 34165-34176. https://doi:10.1109/ACCESS.2021.3063078

[15] Sober, M., Scaffino, G., Spanring, C., & Schulte, S. (2021). A voting-based blockchain interoperability Oracle. IEEE International Conference on Blockchain (Blockchain), pp. 160-169. https://doi:10.1109/Blockchain.2021.10002456

[16] Vladucu, M. V., Dong, Z., Medina, J., & Rojas-Cessa, R. (2023). E-Voting meets blockchain: A survey. Survey Paper, 11(3), 45-67. https://doi:10.1007/survey.v11.2023

[17] Cabuk, U. C., Adiguzel, E., & Karaarslan, E. (2020). A survey on feasibility and suitability of blockchain techniques for e-voting systems. arXiv preprint arXiv:2002.07175

[18] Ben-Nun, J., Fahri, ., Llewellyn, M., Riva, B., Rosen, A., Ta-Shma, A., & Wikström, D. (2012). A new implementation of a dual (paper and cryptographic) voting system. 5th International Conference on Electronic Voting (EVOTE), pp. 315–329.

[19] Vivek, S. K., Yashank, R. S., Prashanth, Y., Yashas, N., & Namratha, M. (2020). E-voting systems using blockchain: An exploratory literature survey. 2nd International Conference on Inventive Research in Computing Applications (ICIRCA), pp. 890–895. https://doi:10.1109/ICIRCA.2020.1452029

[20] Adeshina, S. A. Ojo, A. (2019). Maintaining voting integrity using blockchain. 15th International Conference on Electronics, Computers and Computation (ICECCO), pp. 1–5. https://doi:10.1109/ICECCO48375.2019.155622