Advanced International Journal of Multidisciplinary Research
E-ISSN: 2584-0487
editor@aijmr.com
Volume 4, Issue 2, March-April 2026
CrossRef DOI: 10.62127/aijmr.2026.v04i02.1260

Electronic Voting System Using Blockchain

R. Venkata Hemanth Goud[1], B. Venkateswar Reddy[2], M. Sandhya[3], A. Shirisha[4], B. Javeed Basha[5]

Department of CSE, Tadipatri Engineering College, Tadipatri.

Abstract
Electronic voting systems must guarantee high levels of security, transparency, and trust in order to prevent fraud and protect voter privacy. This paper presents a blockchain-based electronic voting system that utilizes smart contracts deployed on the Ethereum network to create a secure and tamper-resistant voting environment. The system enables authenticated interaction between voters and administrators, allowing secure vote casting, election configuration, and result verification without reliance on centralized authorities. By employing decentralized blockchain storage and automated smart contract execution, the proposed approach prevents duplicate or unauthorized voting while ensuring the integrity and immutability of election data. Each vote is permanently recorded on the blockchain, enabling public verification while maintaining voter anonymity. The system also enhances transparency by allowing election results to be independently validated. The implementation demonstrates that blockchain technology can provide a scalable, reliable, and cost-effective solution for modern electronic voting systems, strengthening confidence in digital electoral processes.

Keywords: Electronic Voting System, Blockchain Technology, Smart contracts, Secure voting.

I.INTRODUCTION:

Block chain is one of the first technologies within the IT global. It is a new block chain era that works in transactional methods. It ambitions to provide a secure and at ease business device the use of virtual crypto currencies that cannot be changed by means of absolutely everyone with an ulterior purpose. A block is a group of blocks that contain data about transactions with whom, and everything is shipped for the duration of the community within the shape of a digital post, which could be very at ease and not possible to exchange, hack, or screw. Machine The block is confirmed and demonstrated via every community node to hold the technique of completing transactions [1]. In this paper, we propose a self-tallying e-voting protocol using a smart contract deployed on Ethereum, which can be replaced by any blockchain that supports smart contracts. We use the paradigm of score voting introduced into make our scheme suitable for more scenarios. Electronic voting systems are prone to a relied upon authority, which poses threats of manipulating or losing ballots [2]. To get around the above shortcomings, self-tallying e-voting models enable any party to check and calculate the final results without a central party. Such systems with the aid of blockchain and contemporary cryptographically tools can provide transparency, privacy, and manipulation resistance. The paper introduces a decentralized voting scheme that provides strong vote submission, verifiability and equitable publicizing of results [3]. The increasing distrust in both the traditional and digital voting system has brought up the issue of fairness, security and transparency in the election process. The centralized systems are usually prone to manipulation and thus there is the need to have a more secure way of defending the democratic rights. A viable alternative provided by blockchain technology is its ability to guarantee immutability, decentralization, and proper recording of votes with no need of physical polling centers. This work presents a blockchain-powered voting system that is going to

Advanced International Journal of Multidisciplinary Research
E-ISSN: 2584-0487
editor@aijmr.com
Volume 4, Issue 2, March-April 2026
CrossRef DOI: 10.62127/aijmr.2026.v04i02.1260

offer a high level of transparency, high level of security, and scalable online elections [5]. One-vote veto systems, where the vote only counts as anonymous, demand great privacy, particularly when one no-vote is enough to turn the vote. Due to the emergence of quantum technology, qubits provide an alternative means of voting privately. This paper presents a straightforward quantum-based vetoing protocol, which guarantees the privacy, fairness, and verifiability. The initial Open Vote Network (OV-Net) was a decentralized and private voting system, which was ineffective at scale with a large number of candidates. Its tallying cost was soaring and hence it could not be used in large elections. This paper presents a better version of OV-Net in which tallying is only linearly related to the size of the candidate set, and secrecy and verifiability are maintained [4] [7]. The classic forms of voting are physical presence, and in most cases, they are not very secure and private. As the level of digitization increases, e-voting technologies can provide remote voting, although they are subject to such threats as manipulation and data leakage. Blockchain-based architectures address these challenges because it ensures the transparency, immutability, and safe authentication of reliable e-voting [9]. The existing voting systems, including forms of voting that are both safe and reachable, are especially crucial in a time when people cannot physically turn up to cast their vote due to the COVID-19 pandemic. In such areas as Iraq, the lack of infrastructure and the problems of post-conflict makes the traditional voting unreliable. The alternative solution is the use of mobile-based voting where citizens can vote safely through the devices they already possess [10].

II.LITERATURE REVIEW:

J. Yao, B. Yang, T. Wang and W. Zhang. (2024), The existing literature on self-tallying e-voting concentrates on homomorphic encryption and zero-knowledge proofs, with most having difficulties in dealing with abortive voters and adaptive attacks. Earlier models of blockchain enhanced transparency, however, they still relied on partial trust or did not produce low computational costs. Recent protocols based on ElGamal and group encryption are better, but they do not effectively deal with inactive voters. All these holes indicate that a large scale and fully decentralized system is required to support large scale elections [1].

M. S. Farooq, U. Iftikhar and A. Khelifi. (2022), The previous blockchain-aided voting systems reviewed enhanced automatization, but many of them relied on a set of trusted actors and thus left systems vulnerable to intrusion and vote manipulation. Other suggestions minimized the administrative role but had issues with voter privacy and long turnaround time, particularly in large scale elections. There were also systems where end to end verification was allowed and was prone to latency and low protection against technical failures. These shortcomings indicate that a safer, privacy-friendly, and high-performance blockchain voting solution is required, and the presented framework is provided with the option of flexible consensus, encryption, and an improved chain verification to meet the requirements [2].

According to S. Wu et al. (2021), Traditional veto methods are not that anonymous and are susceptible to threats of quantum-era attacks. Previously, quantum based solutions to privacy issues enhanced the privacy, but those methods were usually based on complicated computations or unrealistic conditions. These inadequacies indicate the need of a viable, safe, and convenient quantum veto protocol, which will be an endeavour of our solution [3].

S. Wei, H. Zhang, W. Zhang and H. Yu (2020), With N- variant and mimic defence systems, earlier studies used pairwise similarity to test diversity, but again it loses its reliability as the type of variants grows. The current selection algorithms do not have an attack-based model to demonstrate their resistance. Recent

Advanced International Journal of Multidisciplinary Research
E-ISSN: 2584-0487
editor@aijmr.com
Volume 4, Issue 2, March-April 2026
CrossRef DOI: 10.62127/aijmr.2026.v04i02.1260

results mention the necessity of more comprehensive metrics of heterogeneity and superior voting, which provokes the enhanced strategy adopted in this paper [4].

S. Majumder, S. Ray, D. Sadhukhan, M. Dasgupta, A. K. Das and Y. Park. (2023), Previous research on e-voting was based on paperless and electronic systems, however, failed at their attempt to provide privacy, attack resistance and results that were verifiable. Recent studies have centred on blockchain, Merkle trees and other cryptographic methods such as zero-knowledge proofs to enhance security. Nevertheless, the majority of current models do not have effective consensus and lightweight mechanisms, which inspires better blockchain-based e-voting schemes [5].

N. A. J. Al-Habeeb, N. Goga, H. A. Ali and S. M. S. Al-Gayar. (2020), The benefits of electronic and mobile voting have been mentioned in the previous works, however, most of the existing literature is found in technologically advanced areas with high digital infrastructure. Studies of post-conflict or infrastructure restricted regions are relatively few; particularly in Asia Minor. Available evidence indicates that solutions which are balanced in terms of ease of use, security, and accessibility are required-something that needs to be filled in this study [6].

III.PROPOSED METHODOLOGY

Executor's best has the right to hold elections, appointments and votes. The control can test the votes. Administrative exams are reversed every term, so attempt to show a manner to save you voters from balloting at the ballot. You can discover a winner, however victory is not a system or a vote. It makes use of a blocking tool. This method of recording protects your identity with every phrase.

Advantages of Proposed Methodology

A voter cannot verify the overall voting statistics, and individual votes are not uniquely identifiable. The blockchain is used to record and manage the voting process.

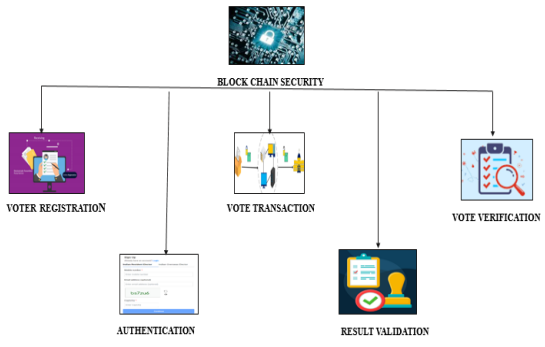

Fig: 1 BLOCK CHAIN SECURITY

Blockchain is a technology which utilizes the structured distributed blocks which exist in a blockchain network to allow individuals and businesses to store and process data. Each new block stores a transaction or chain of transactions which are connected to all the previous blocks with a cryptographic chain.

Advanced International Journal of Multidisciplinary Research
E-ISSN: 2584-0487
editor@aijmr.com
Volume 4, Issue 2, March-April 2026
CrossRef DOI: 10.62127/aijmr.2026.v04i02.1260

Validation Transaction
This involves checking the wallet of the sender and the e-mail of the recipient and ensuring that the transaction is comfortable and impeccable. Block chain verification is implemented by applying consensus algorithms and cryptographic strategies, which guarantee the integrity and impossibility of changes.

Authentication
A visual cryptography and QR codes-based system of voter authentication was digital. The purpose of usability is to provide electorate with a minimum technical delight with a profitable machine. All the consumer needs is a tool that combines a QR code reader, such as a telephone. Such a method relies on visible cryptography as a running device: e-vote casting cards are coded and encrypted in the form of QR codes to prevent authentication and implicit transparency. Thus, transparency will not disclose any records but reveal hidden keys during the organization of layers.

Vote Transaction
The volume of trade in the shape of a digital ledger which is circulated throughout the network, makes it safer and unfeasible to alter or defraud the system. It is thus checked and confirmed by all the nodes of the block chain network to get the process of making the transactions.

Result Validation
Checking. if the e-voting system meets the specified goals, checking if the e-voting system performs functions it is supposed to perform.

Vote Verification
checking whether e-voting system is consistent, checking whether e-voting system complies with the standards, checking whether the e-voting system employs sound techniques and reasonable practices, checking whether the e-voting system fulfils the chosen functions in the right way, checking whether the e-voting protocol is compatible with e-voting system,

1. Administrative Block
In this module, the administrator maintains all required records and documentation for reporting purposes. The admin is responsible for managing candidate details, voter information, and overall election activities. Vote counting and result evaluation are carried out under administrative control to ensure accuracy. The administrator also verifies the validity of ballots to identify any irregular or compromised votes. Once verification is complete, the election process is formally closed and the final results are published.

2. Custom Block
In this module, users are authenticated to ensure secure access to the information provided by the system. To view data or submit queries, a user must first register and log in with valid credentials. During registration, essential details such as email address, username, password, and display name are collected. The display name is used within the system to identify users according to their personal preferences.

3. Records Entry Module
Each voter is permitted to view the candidates and cast a vote, while only the final winner is visible after the election without revealing individual vote counts. The use of blockchain ensures that the voting process remains secure and tamper-resistant.

Advanced International Journal of Multidisciplinary Research
E-ISSN: 2584-0487
editor@aijmr.com
Volume 4, Issue 2, March-April 2026
CrossRef DOI: 10.62127/aijmr.2026.v04i02.1260

4. Secure Vote Platform

Blockchain technology combined with smart contracts provides a robust solution for electronic voting systems, making them secure, cost-effective, reliable, and easy to use. Since every vote is recorded as a separate block, it ensures that votes remain tamper-proof and cannot be altered.

PROPOSED ALGORITHM

HMAC- HMAC is a hash-based MAC which utilizes a hash function. It no longer includes any cryptographic functionalities such as md5, sha1 and sha256 as well as a multitude of others. To the extent that the only parameter used in the HMAC is the hash characteristic, the magnitude is surpassed to the magnificence, and the wrapper magnificence bears the majority of effective static capability which encompasses the hash attribute. HMAC uses shell capability in-house. The HMAC set of rules has been designed in a such way that it is highly flexible due to combination with the hash function.

Security:

The security comparison highlights the ability of each voting system to resist manipulation, unauthorized access, and data tampering. Traditional and EVM-based systems show limited protection due to centralized control, while the proposed blockchain system demonstrates stronger resilience through decentralization and cryptographic safeguards.

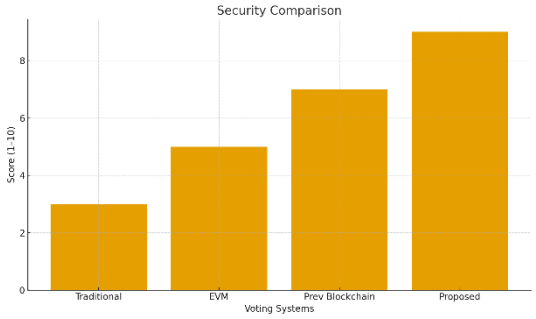

FIG 2. SECURITY BAR GRAPH

Transparency:

This graph illustrates how openly election processes and results can be verified by participants. Conventional systems depend on administrative audits, whereas the proposed model enables public verification through an immutable ledger, ensuring greater openness in vote recording and counting.

Advanced International Journal of Multidisciplinary Research
E-ISSN: 2584-0487
editor@aijmr.com
Volume 4, Issue 2, March-April 2026
CrossRef DOI: 10.62127/aijmr.2026.v04i02.1260

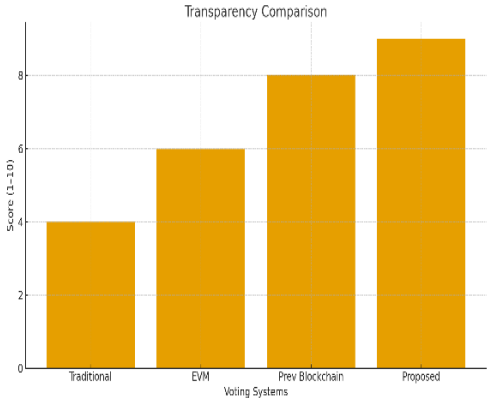

FIG 3. TRANSPARENCY

Privacy:

The privacy comparison reflects how well voter identities and choices are protected. Earlier systems expose voters to risks through physical or centralized records, while the proposed system preserves anonymity by separating identity verification from vote storage using cryptographic methods.

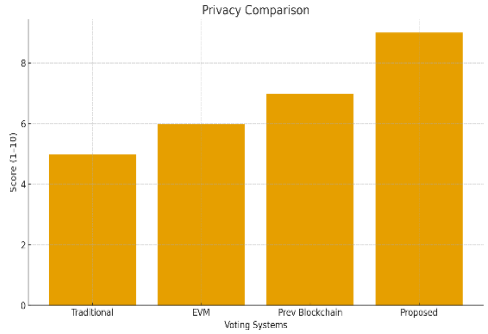

FIG 4. PRIVACY

Trust:

Trust levels indicate public confidence in the fairness of the voting process. Centralized systems require reliance on authorities, whereas the proposed blockchain-based approach builds trust through distributed validation and tamper-proof records.

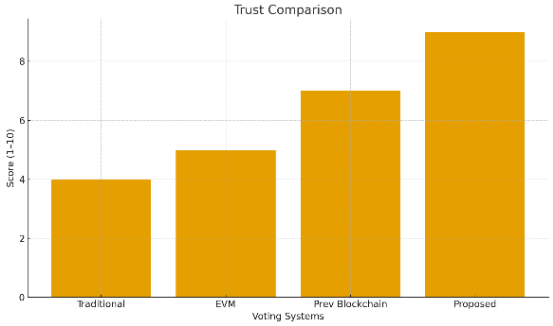

FIG 5. TRUST

Advanced International Journal of Multidisciplinary Research
E-ISSN: 2584-0487
editor@aijmr.com
Volume 4, Issue 2, March-April 2026
CrossRef DOI: 10.62127/aijmr.2026.v04i02.1260

IV. RESULT AND DISCUSSION

In the initial stages of its progress, citizens rely on the vote casting issues. They either vote in person or through mail and feel that their vote has been changed, discarded or changed. The possibility of manipulation after the casting and before counting of votes can be reduced by using electronic voting era with a safety clause. In this system the citizens submit their votes in voting points by polling through electronic vote casting machines that store data regarding the ballots and provide voters with a paper receipt to attend to their ballot. The voters are able to certify themselves that they have made a choice of their minds. In such a manner, block chain arrangements aid in properly presenting the election results and rely on votes without the possibility of human errors. The voting enterprise can now benefit the enhancement of block chain provision which provides a comfortable and transparent vote casting system with the support of block chain time and custom block chain solutions. The machine that is mainly based on blockchain will help in developing a cozy environment in which residents will think and take action in uncertain scenarios. The lock plays a significant role within the former registration. People and government members might refresh their voter registration with additional security of the fact that the blockchain is not ended randomly, but it is constantly being updated with facts concerning what account the alternate became was made in and at what time. Big independent agencies may modify voter registration in real-time metrics to detect purge or dubious pastime. Also, proper vote-counting and hundred percent electoral transparency.

Fig: 2 Screenshot

Fig: 3 Screenshot

V. CONCLUSION

This paper presents a structured approach to logo identification. Protecting data privacy is highlighted as a key user right in content verification, and several new logical frameworks are proposed. Authentication of content in hybrid cloud environments is addressed, where replicated data files are stored on private cloud servers using individual encryption keys. Security analysis shows that the system is resilient against both internal and external threats. A standard attack model is used to validate the protection mechanism. To illustrate the concept, a prototype version of the proposed framework was developed and tested. Results

Advanced International Journal of Multidisciplinary Research
E-ISSN: 2584-0487
editor@aijmr.com
Volume 4, Issue 2, March-April 2026
CrossRef DOI: 10.62127/aijmr.2026.v04i02.1260

demonstrate that the dual-injection mechanism requires minimal overhead compared to conventional encryption methods when transmitting data over the network.

REFERENCES:

[1] J. Huang, D. He, Y. Chen, M. K. Khan and M. Luo, "A Blockchain-Based Self-Tallying Voting Protocol with Maximum Voter Privacy," in IEEE Transactions on Network Science and Engineering, vol. 9, no. 5, pp. 3808-3820, 1 Sept.-Oct. 2022, doi: 10.1109/TNSE.2022.3190909.

[2] J. Yao, B. Yang, T. Wang and W. Zhang, "A Distributed Self-Tallying Electronic Voting System Using the Smart Contract," in Chinese Journal of Electronics, vol. 33, no. 4, pp. 1063-1076, July 2024, doi: 10.23919/cje.2023.00.233.

[3] M. S. Farooq, U. Iftikhar and A. Khelifi, "A Framework to Make Voting System Transparent Using Blockchain Technology," in IEEE Access, vol. 10, pp. 59959-59969, 2022, doi: 10.1109/ACCESS.2022.3180168.

[4] S. Wu et al., "A Secure Quantum Protocol for Anonymous One-Vote Veto Voting," in IEEE Access, vol. 9, pp. 146841-146849, 2021, doi: 10.1109/ACCESS.2021.3123681.

[5] Y. Yang, Z. Guan, Z. Wan, J. Weng, H. H. Pang and R. H. Deng, "PriScore: Blockchain-Based Self-Tallying Election System Supporting Score Voting," in IEEE Transactions on Information Forensics and Security, vol. 16, pp. 4705-4720, 2021, doi: 10.1109/TIFS.2021.3108494.

[6] D. Xu, W. Shi, W. Zhai and Z. Tian, "Multi-Candidate Voting Model Based on Blockchain," in IEEE/CAA Journal of Automatica Sinica, vol. 8, no. 12, pp. 1891-1900, December 2021, doi: 10.1109/JAS.2021.1004207.

[7] S. Seol, H. Kim and J. H. Park, "An Efficient Open Vote Network for Multiple Candidates," in IEEE Access, vol. 10, pp. 124291-124304, 2022, doi: 10.1109/ACCESS.2022.3224798.

[8] S. Wei, H. Zhang, W. Zhang and H. Yu, "Conditional Probability Voting Algorithm Based on Heterogeneity of Mimic Defense System," in IEEE Access, vol. 8, pp. 188760-188770, 2020, doi: 10.1109/ACCESS.2020.3031323.

[9] S. Majumder, S. Ray, D. Sadhukhan, M. Dasgupta, A. K. Das and Y. Park, "ECC-EXONUM-eVOTING: A Novel Signature-Based e-Voting Scheme Using Blockchain and Zero Knowledge Property," in IEEE Open Journal of the Communications Society, vol. 5, pp. 583-598, 2024, doi: 10.1109/OJCOMS.2023.3348468.

[10] N. A. J. Al-Habeeb, N. Goga, H. A. Ali and S. M. S. Al-Gayar, "A New M-voting System for COVID-19 Special Situation in Iraq," 2020 International Conference on e-Health and Bioengineering (EHB), Iasi, Romania, 2020, pp. 1-4, doi: 10.1109/EHB50910.2020.9280275.

[11] L. Bai and L. Liu, "Research on Software Defined Network Security Model Based on Blockchain," 2021 6th International Conference on Intelligent Computing and Signal Processing (ICSP), Xi'an, China, 2021, pp. 150-153, doi: 10.1109/ICSP51882.2021.9409008.

[12] S. Khedkar, K. Mahajan and M. Shirole, "Optimization of Blockchain Based E-voting," 2023 8th International Conference on Business and Industrial Research (ICBIR), Bangkok, Thailand, 2023, pp. 700-705, doi: 10.1109/ICBIR57571.2023.10147663.

[13] A. K. Goel, A. Rai, A. Narain, A. Richard and K. Kumar, "Trusted Vote: Reorienting eVoting using Blockchain," 2022 Sixth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), Dharan, Nepal, 2022, pp. 129-138, doi: 10.1109/I-SMAC55078.2022.9987301.

[14] A. Madhuri, P. R. Lakshmi, P. John, T. Ganesh, S. Asma and P. Nahila, "Blockchain Ballotbox: Empowering Democracy Through Tamper-Proof E-Voting," 2023 3rd International Conference

on Innovative Mechanisms for Industry Applications (ICIMIA), Bengaluru, India, 2023, pp. 232-239, doi: 10.1109/ICIMIA60377.2023.10425872.

[15] F. Þ. Hjálmarsson, G. K. Hreiðarsson, M. Hamdaqa and G. Hjálmtýsson, "Blockchain-Based E-Voting System," 2018 IEEE 11th International Conference on Cloud Computing (CLOUD), San Francisco, CA, USA, 2018, pp. 983-986, doi: 10.1109/CLOUD.2018.00151.

[16] R. Barelli, M. D'Onghia and S. Longari, "Toward Secure Electronic Voting: A Survey on E-Voting Systems and Attacks," in IEEE Access, vol. 13, pp. 89600-89626, 2025, doi: 10.1109/ACCESS.2025.3569334.

[17] D. Dabpimjub and S. Kiattisin, "Success Factors for Conceptual Digital Voting Model," in Journal of Mobile Multimedia, vol. 20, no. 4, pp. 785-819, July 2024, doi: 10.13052/jmm1550-4646.2042.

[18] A. Qureshi, D. Megías and H. Rifà-Pous, "SeVEP: Secure and Verifiable Electronic Polling System," in IEEE Access, vol. 7, pp. 19266-19290, 2019, doi: 10.1109/ACCESS.2019.2897252.

[19] Y. -X. Kho, S. -H. Heng, S. -Y. Tan and J. -J. Chin, "Relationships Among e-Voting, e-Auction, e-Cheque, and e-Cash," in IEEE Access, vol. 13, pp. 71773-71791, 2025, doi: 10.1109/ACCESS.2025.3560552.

[20] W. Ali Mahmood, J. Waleed, A. R. Abbas, H. Alaskar, M. Altulyan and A. Jaafar Hussain, "Intelligent Gesture-Enhanced Blockchain Voting: A New Era of Secure and Accessible E-Voting," in IEEE Access, vol. 12, pp. 144055-144068, 2024, doi: 10.1109/ACCESS.2024.3468338.

[21] R. L. Almeida, F. Baiardi, D. Di Francesco Maesa and L. Ricci, "Impact of Decentralization on Electronic Voting Systems: A Systematic Literature Survey," in IEEE Access, vol. 11, pp. 132389-132423, 2023, doi: 10.1109/ACCESS.2023.3336593.

[22] M. -V. Vladucu, Z. Dong, J. Medina and R. Rojas-Cessa, "E-Voting Meets Blockchain: A Survey," in IEEE Access, vol. 11, pp. 23293-23308, 2023, doi: 10.1109/ACCESS.2023.3253682.

[23] S. Al-Maaitah, M. Qatawneh and A. Quzmar, "E-Voting System Based on Blockchain Technology: A Survey," 2021 International Conference on Information Technology (ICIT), Amman, Jordan, 2021, pp. 200-205, doi: 10.1109/ICIT52682.2021.9491734.