iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 14 **Issue:** VI **Month of publication:** June 2026

DOI: https://doi.org/10.22214/ijraset.2026.83396

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue VI June 2026- Available at www.ijraset.com

A Modified E-Voting System based on Enhanced Block Chain Process for Transparent and Secure Voting

Khushabu Parte
School of Information Technology *Department, Rajiv Gandhi Prodhyogiki Vishvidhyalya University Bhopal*

Abstract: ***This dissertation mostly focuses on a block-chain based voting systems. It aims at identifying the strategies and the guidelines as well as provides a comprehensive end-to-end electronic voting system based on block-chain, with the help of encryption private and public techniques such as zero-knowledge proofs to improve privacy. The proposed method is to provide Security and Privacy, Transparency and Trust, Accessibility, Efficiency and Convenience to voters and Security and Fraud Prevention in Election Outcomes. The proposed online voting system using cloud-based hybrid block-chain technology eradicates the flaws that persist in the existing voting system, and it is carried out in three phases: The registration phase, Vote casting phase and Vote counting phase. The integration of SHA-512 encryption ensures that the voter's identity remains confidential and the integrity of the vote is maintained. The system also demonstrates improved security, reduced operational cost, real-time vote counting, and transparency for both voters and election authorities. The proposed method shows better result as compare to other previous method in terms of different result parameters such as block size, encryption, decryption, Block size (64 bits), Word size, hash output and number of Rounds. In the nut shall the proposed method perform better due to SHA 512 technique and provide better security as compare to other methods.***

Keywords: Blockchain, SHA-512, Smart Contracts, E-Voting, MetaMask, Ethereum

I. INTRODUCTION

Elections are a crucial foundation of democratic society, and safeguarding their integrity, transparency, and accessibility is essential. Conventional voting methods, whether paper or electronic, often exhibit deficiencies like voter fraud, vote manipulation, insufficient transparency, restricted accessibility, and ineffective manual tallying procedures [1]. These issues have prompted academics and engineers to investigate more safe and reliable solutions. In this scenario, Block-chain technology has emerged as a revolutionary alternative capable of redefining election procedures [3]. A block-chain is a decentralized, distributed ledger that securely, immutably, and transparently records transactions. In the context of voting systems, block-chain offers a platform where each vote is encrypted, time stamped, and documented as a secure transaction, hence precluding the potential for illegal modifications or duplicate voting [7]. A Block-chain-Based Voting System utilizes essential attributes such as immutability, decentralization, cryptographic security, smart contracts, and consensus algorithms to improve electoral security, safeguard voter privacy, and bolster public confidence [5].It enables comprehensive verifiability and instantaneous auditability while preserving anonymity, making it especially appropriate for governmental and organizational elections [4]. This thesis investigates the design, implementation, and assessment of a block-chain based voting system, with the objective of advancing a tamper-proof, transparent, and accessible digital voting framework [3]. The research further investigates the technological, legal, and societal ramifications of implementing such systems on a large scale [6].

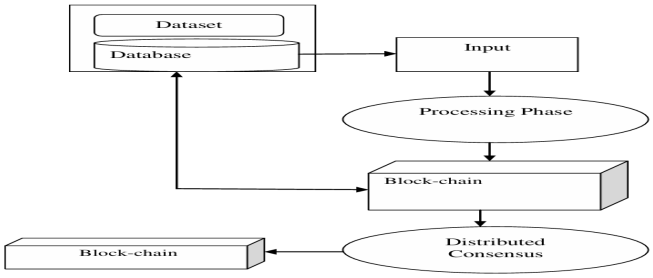


Fig. 1 Block Chain Technology

©IJRASET: All Rights are Reserved

II. LITERATURE REVIEW

Ohize et al. (2025) offer an extensive overview of blockchain e-voting schemes, in which they define and compare public, private and consortium architectures. They emphasize security characteristics (hashing, smart contracts, digital signatures) and also address issues such as scalability, consensus bottlenecks, accessibility, and regulatory problems. They stress the importance of standardization and post-quantum cryptography for later deployment[1].ayakumari et al. (2024) propose a cloud-based hybrid blockchain e-voting model, using public chains for vote storage and private chains for voter authentication. It combines zero-knowledge proofs, digital signatures, and cloud scalability to ensure security, transparency, and real-time auditability, outperforming centralized and pure blockchain systems[2].Daraghmi et al. (2024) explore blockchain e-voting in politically sensitive regions like Palestine, emphasizing trust-building, transparency, and permissioned blockchains. They address voter privacy, identity management, and highlight infrastructure and education challenges in fragile democracies[3].Spanos & Kantzavelou (2023) introduce Ethervote, an Ethereum-based voting system using smart contracts, zero-knowledge proofs, and hashing to ensure anonymity and verifiability. It's modular but faces gas costs, congestion, and usability challenges[4].Sanjeeva et al. (2023) propose a fully decentralized voting system with smart contract automation, real-time results, and reduced intermediaries. Challenges include scalability, digital literacy, and legal readiness[5].Charan et al. (2022) present a conceptual Ethereum-based model with smart contracts, government ID/biometric authentication, and cryptography to secure votes. It improves integrity and transparency but struggles with scalability and accessibility[6].Benabdallah et al. (2022) systematically review 50+ blockchain e-voting studies, noting widespread use of public/consortium chains, smart contracts, zero-knowledge proofs, and homomorphic encryption. They stress trade-offs between security, scalability, and usability, and highlight unresolved issues like authentication, accessibility, and regulatory barriers[7].Singh et al. [8] highlighted how blockchain improves trust, transparency, and tamper resistance in e-voting by using immutable ledgers, cryptography, and distributed consensus. They preserved voter anonymity through pseudonymization and secure multi-party computation but noted 51% attacks, smart contract bugs, and scalability issues, recommending hybrid blockchain models.Ostern et al. [9] examined organizational adoption of blockchain, emphasizing the need for legal clarity, institutional readiness, and strategic alignment for successful integration in e-voting. They found organizations adopt blockchain cautiously, often via pilot projects and private networks.Jafar et al. [10] reviewed various blockchain e-voting architectures, classifying them by consensus algorithms, identity verification, and privacy techniques. While ensuring integrity and auditability, they highlighted persistent scalability, latency, authentication, and legal challenges, suggesting hybrid architectures and cross-disciplinary collaboration.Yadav et al. [11] proposed an Ethereum-based e-voting model using smart contracts for secure vote casting and automated counting. Although it improves transparency and reduces manipulation, limitations include voter education, scalability, and cost issues.

III. METHODOLOGY

The proposed system consists of the following components:

1) Frontend Interface: A web-based interface enabling voter authentication and vote casting.
2) Smart Contracts: Developed in Solidity, these contracts manage candidate registration, vote casting, and result tallying.
3) Ganache Blockchain: A local Ethereum test network for simulation.
4) MetaMask Wallet: Provides secure voter authentication using cryptographic key pairs.
5) SHA-512 Encryption: ensures irreversible hashing of voter identities and votes for confidentiality.

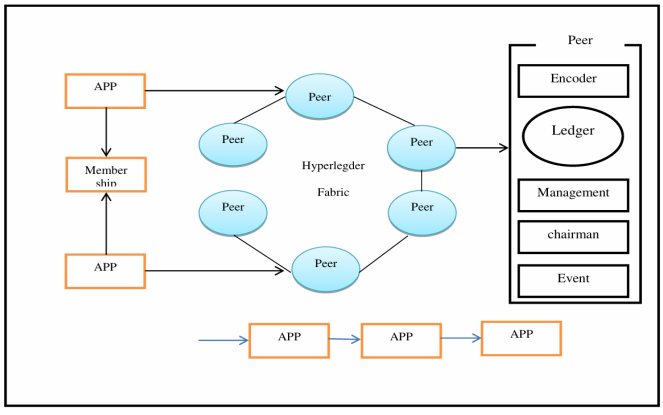


Fig. 2 Block-Chain based E-Voting System Diagram

A. Performance Parameters:

Transaction Time: Measures the delay for vote recording through smart contracts.
Deployment Cost: Gas cost required for deploying contracts on Ethereum (simulated with Ganache).
Vote Casting Cost: Gas consumed for each vote transaction.
Throughput: Number of votes processed per second under test conditions.

B. Integrity and Anonymity Parameters:

Vote Integrity: Each vote is hashed and validated to ensure no alterations.
Anonymity: Voters are identified only by wallet addresses, preserving personal identity.
One Vote per User: Enforced by smart contracts to avoid duplicate voting.
Transparency: All votes and results remain publicly verifiable on-chain.

C. Blockchain-Specific Parameters:

Gas Consumption: Evaluated for casting votes, adding candidates, and declaring results.
Block Confirmation Time: Determines how quickly transactions become finalized (instant in Ganache).
Storage Cost: Depends on encrypted vote and voter record data stored on-chain.
SHA-512 Theoretical Overview
SHA-512 generates a 512-bit (128 hex characters) hash, regardless of input size.
Features of SHA-512

TABLE I
FEATURES AND IT'S DESCRIPTION TABLE

Feature	Description
Hash Length	512 bits (64 bytes)
Input Size	Any length of data (up to 2- 1 bits)
Output Format	Fixed-size 512-bit (128 hexadecimal characters) hash
Security Level	256-bit security (pre-image and collision resistance)
Deterministic	Same input always results in the same output
Irreversible	Cannot regenerate the original input from the hash
Avalanche Effect	Small change in input causes large, unpredictable change in output

IV. RESULT DISCUSSION

A. Performance, Limitations, and Scalability

A. Performance and User Experience**:** The proposed prototype demonstrated near-instantaneous vote registration within 2–5 seconds on Ganache, attributed to its auto-mining feature. This responsiveness is sufficient for controlled demonstrations and prototype validation. However, deployment on public testnets or Ethereum mainnet would introduce inherent block delays of 15–30 seconds, necessitating appropriate UI adjustments to inform users of pending confirmations.

Security and integrity were preserved as all votes were immutably recorded on-chain, while smart contract logic ensured unique voting by preventing double submissions from the same address. The dApp was able to reconstruct the latest vote tallies directly from the blockchain upon page reload, ensuring accurate state management. MetaMask integration offered a familiar and transparent user experience, with visual confirmations (e.g., "Your vote has been recorded"), updated balances, and real-time tally updates, which improved user trust and system clarity.

1) Observed Limitations

Despite its effectiveness, several limitations were observed. The single-node Ganache setup lacks true decentralization; future tests on multi-node environments or Ethereum testnets (e.g., Goerli, Sepolia) are necessary to evaluate transaction finality and network gossip delays. Voter verification remained minimal, as any Ganache-generated address could cast a vote once per candidate. More robust implementations would integrate off-chain KYC, whitelisted addresses, or Merkle proof–based authorization. Additionally, the current front-end lacked preventive measures against replay attacks, rapid double-clicks, and proper handling of MetaMask errors (e.g., user rejection or network mismatch).

2) Scalability and Extensibility

From a scalability standpoint, the system operated efficiently with three candidates and a small voter pool, with gas consumption and state storage scaling proportionally for up to a few thousand voters or candidates. While the current design emphasizes transparency, future work could explore vote privacy mechanisms such as zero-knowledge proofs (ZKPs) or homomorphic encryption to ensure confidentiality.

The system's reliance on standard Solidity and the Ethereum Virtual Machine (EVM) makes it network-portable, enabling easy migration to public testnets or Layer-2 solutions such as Polygon for improved scalability and reduced costs. Furthermore, automated testing frameworks (e.g., Truffle or Hardhat) can be integrated to rigorously validate vote restriction rules, revert conditions, and edge cases.

Overall, the core functionalities—unique voting, real-time tallying, and immutable vote recording—are technically feasible and operational in the current prototype, providing a solid foundation for future enhancements

B. Result Parameters and Simulation Tool

In this section we have focused on the following parameters:

1) Transaction Latency

Time between initiating a vote and transaction confirmation.

Benchmarks indicated latency of 2–4 seconds per vote in Ganache's auto mine mode.

2) Vote Tally Consistency

After each vote, candidate tallies updated correctly and immutably. No repeated voting, in line with smart contract restrictions.

3) User Experience

Seamless interaction via Meta Mask and React front end.

Visual feedback: real-time vote counts, confirmation banners, and updated Ethereum balance (e.g., 99.9986 ETH after voting).

C. SHA-512 Algorithm: Step-by-Step Mathematical:

Process Step 1: Padding the Message Given a message M of arbitrary length, append: A single _1' bit • k zero bits such that total length ≡ 896 mod 1024 • Append 128-bit big-endian representation of original message length l Final padded message (L): L=M‖1‖0k‖Length(M)128−bit Step 2: Parsing the Message Split padded message L into N blocks of 1024 bits each: L=M(1),M(2),...,M(N) Step 3: Initial Hash Values (H_0 to H_7) Initialize eight 64-bit constants: H0=0x6a09e667f3bcc908, H1=0xbb67ae8584caa73b, H2=0x3c6ef372fe94f82b, H3=0xa54ff53a5f1d36f1, SHA-512 Algorithm: Step-by-Step Mathematical Process Step 1: Padding the Message Given a message M of arbitrary length, append: • A single _1' bit • k zero bits such that total length ≡ 896 mod 1024 • Append 128-bit big-endian representation of original message length l Final padded message (L): L=M‖1‖0k‖Length(M)128−bit Step 2: Parsing the Message Split padded message L into N blocks of 1024 bits each: L=M(1),M(2),...,M(N) Step 3: Initial Hash Values (H_0 to H_7) Initialize eight 64-bit constants: H0=0x6a09e667f3bcc908 H1=0xbb67ae8584caa73b H2=0x3c6ef372fe94f82b H3=0xa54ff53a5f1d36f1 Step 6: Final Hash Calculation After processing all message blocks: H0=H0+a, H1=H1+b,..., H7=H7+h Final digest: Hash=H0‖H1‖...‖H7

4.6.4 Practical Example of SHA-512 Hash "Vote: Candidate A" Output (SHA-512 hash): 0d0a65a3a2f3c7b2f3c4d6b1e13cddba2ec2aa6c5e3b503c76f2eaadf779a0f96c9cfb4577b76d5a32a5d6ad7bb79ef98e5ef42d1e02a1f6c3a42c35a61a9475 Any change in input — even a space — will drastically change the output, proving integrity protection.

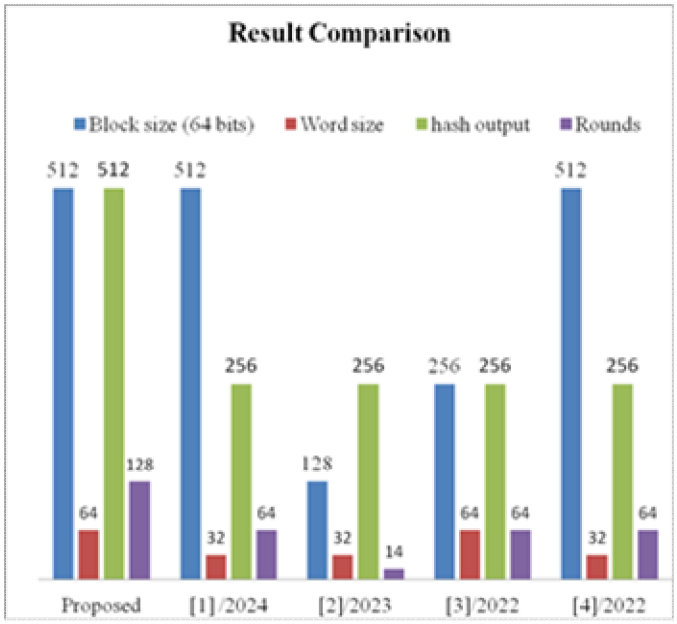


Fig. 3 graph of comparison of Encryption Techniques

V. CONCLUSIONS

In this presented work, a Block-chain Based E-Voting System has been proposed and simulated using Ethereum development tools like Ganache and Meta Mask, with strong encryption mechanisms such as SHA-512 for securing voter identity and vote data. The system aims to overcome the traditional challenges faced by paper-based and centralized electronic voting systems, such as vote tampering, duplicate voting, lack of transparency, and centralized failure points.By leveraging the decentralized, transparent, and immutable nature of block-chain technology, the system ensures a secure and trustless environment for casting and counting votes. The use of smart contracts automates the voting process, ensuring that the rules of the election are enforced programmatically without human intervention. Each vote is recorded as a unique transaction, and once added to the block-chain, it becomes irreversible and verifiable by all stakeholders.The integration of SHA-512 encryption ensures that the voter's identity remains confidential and the integrity of the vote is maintained. The system also demonstrates improved security, reduced operational cost, real-time vote counting, and transparency for both voters and election authorities.

VI. ACKNOWLEDGMENT

I wish to express my sincere thanks to my esteemed guide, Dr. Varsha Sharma, Department of Information Technology, School of Information Technology (SoIT), RGPV, Bhopal, (M.P.). Their valuable help, sage advice, blessing magnanimous attitude, keen Interest and efficient guidance coupled with their constant encouragement to channelize my workalong with the proper path to reach a stage of completion. I extended my gratefulness to the Head of Department Dr. Jitendra Agrawal, and other faculty members Dr. Sanjeev Sharma, Dr. Nishchol Mishra, Prof. Vivek Sharma, and prof. Yogendra Maravi for their advice, supervision and critical contribution. Their involvement with their originality have triggered and nourished my intellectual curiosity that will benefit me lifetime ahead. I give special thanks to Shri Neelesh Sharma and university/ collage staff members who helped us in ways immeasurable during our educational pursuits..

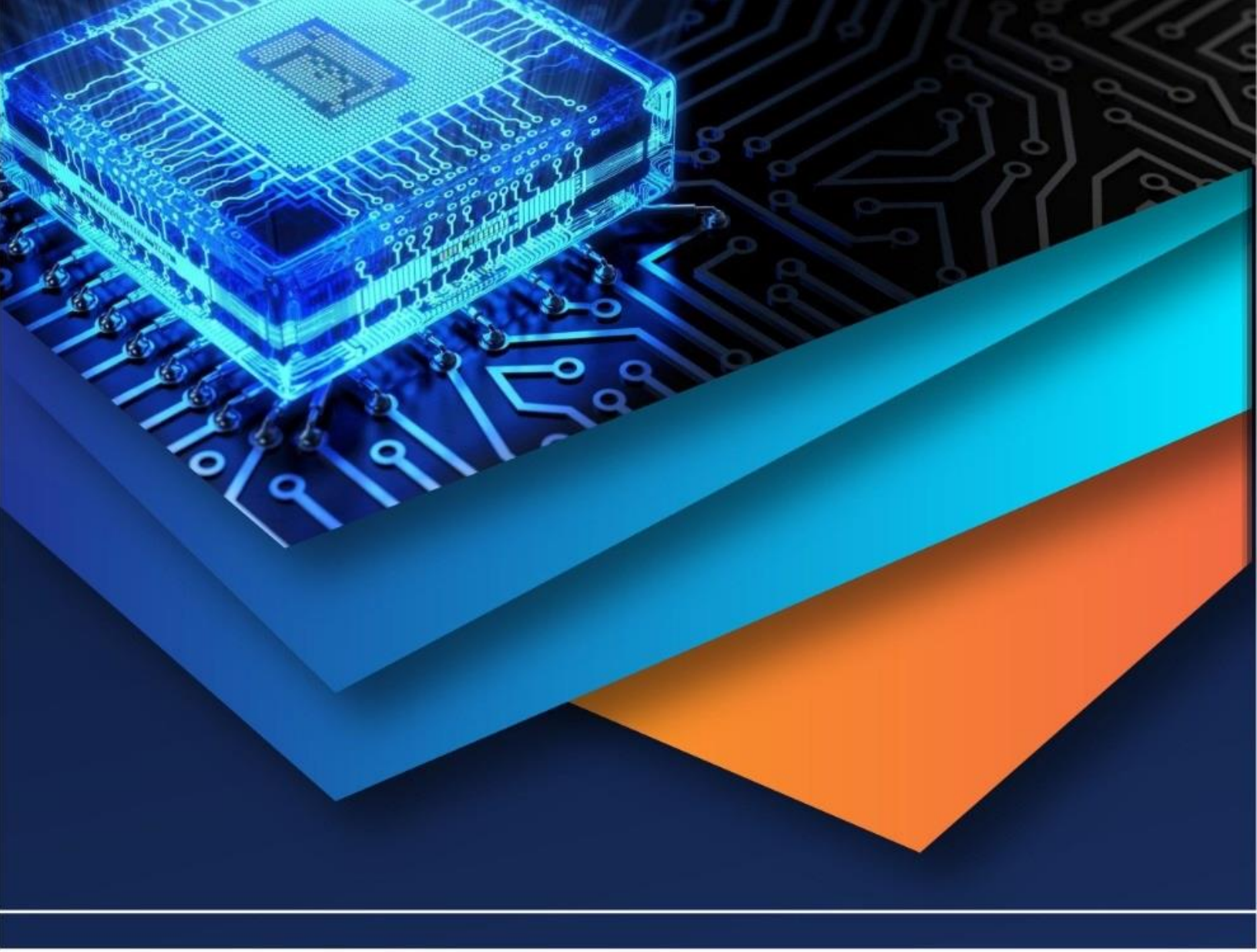
REFERENCES

[1] Ohize, Henry O., Adeiza James Onumanyi, Buhari U. Umar, Lukman A. Ajao, Rabiu O. Isah, Eustace M. Dogo, Bello K. Nuhu et al. "Block-chain for securing electronic voting systems: a survey of architectures, trends, solutions, and challenges." Cluster Computing 28, no. 2 (2025): 132.

[2] Jayakumari, Beulah, S. Lilly Sheeba, Maya Eapen, Jani Anbarasi, Vinayakumar Ravi, A. Suganya, and Malathy Jawahar. "E-voting system using cloud-based hybrid block-chain technology." Journal of Safety Science and Resilience 5, no. 1 (2024): 102-109

[3] Daraghmi, Eman, Ahmed Hamoudi, and Mamoun Abu Helou. "Decentralizing Democracy: Secure and Transparent E-Voting Systems with Block-chain Technology in the Context of Palestine." Future Internet 16, no. 11 (2024): 388.
[4] Spanos, Achilleas, and Ioanna Kantzavelou. "A block-chain-based electronic voting system: Ethervote." arXiv preprint arXiv:2307.10726 (2023).
[5] Sanjeeva, Polepaka, M. Sai Sathwik, G. Sai Prasad, G. Praneeth Reddy, Vijaylakshmi Sajwan, and Bande Ganesh. "Decentralized and automated online voting system using block-chain technology." In E3S Web of Conferences, vol. 430, p. 01046. EDP Sciences, 2023.
[6] CHARAN, TANIKELLA SAI, Mrs SRINANDA PENTAPATI, and R. PREMA. "A Research Paper on E-Voting Using Block-chain Technology." (2022).
[7] Benabdallah, Ali, Antoine Audras, Louis Coudert, Nour El Madhoun, and Mohamad Badra. "Analysis of block-chain solutions for E-voting: a systematic literature review." IEEE Access 10 (2022): 70746-70759.
[8] Singh, Jagbeer, Utkarsh Rastogi, Yash Goel, and Brijesh Gupta. "Block-chain-based decentralized voting system security Perspective: Safe and secure for digital voting system." arXiv preprint arXiv:2303.06306 (2023).
[9] Ostern, Nadine Kathrin, Friedrich Holotiuk, and Jürgen Moormann. "Organizations‘ approaches to block-chain: a critical realist perspective." Information & Management 59, no. 7 (2022): 103552.
[10] Jafar, Uzma, Mohd Juzaiddin Ab Aziz, and Zarina Shukur. "Block-chain for electronic voting system—review and open research challenges." Sensors 21, no. 17 (2021): 5874.
[11] Yadav, Abhishek Subhash, Y. V. Urade, A. U. Thombare, and Abhijeet Anil Patil. "E voting using block-chain technology." International Journal of Engineering Research & Technology (2020).
[12] Khan, Saad, Aansa Arshad, Gazala Mushtaq, Aqeel Khalique, and Tarek Husein. "Implementation of decentralized block-chain e-voting." EAI Endorsed Transactions on Smart Cities 4, no. 10 (2020): 164859.
[13] Thanekar, Gananjay Sandeep. "Decentralized Voting Application Using Ethereum Smart Contract." Diss. University of Mumbai Abou Jaoude, Joe, and Raafat George Saade. "Block-chain applications–usage in different domains." Ieee Access 7 (2019): 45360-45381
[14] Monteiro, José Diogo Soares Albergaria Serejo. "Block-chain-based Decentralized Application for Electronic Voting using an Electronic ID." Master's thesis, Universidade da Beira Interior (Portugal), 2019.
[15] Patil, Harsha V., Kanchan G. Rathi, and Malati V. Tribhuwan. "A study on decentralized e-voting system using block-chain technology." Int. Res. J. Eng. Technol 5, no. 11 (2018): 48-53.
[16] Khoury, David, Elie F. Kfoury, Ali Kassem, and Hamza Harb. "Decentralized voting platform based on ethereum block-chain." In 2018 IEEE International Multidisciplinary Conference on Engineering Technology (IMCET), pp. 1-6. IEEE, 2018.
[17] Hjálmarsson, Friðrik Þ., Gunnlaugur K. Hreiðarsson, Mohammad Hamdaqa, and Gísli Hjálmtýsson. "Block-chain-based e-voting system." In 2018 IEEE 11th international conference on cloud computing (CLOUD), pp. 983-986. IEEE, 2018.
[18] Hjálmarsson, Friðrik Þ., Gunnlaugur K. Hreiðarsson, Mohammad Hamdaqa, and Gísli Hjálmtýsson. "Block-chain-based e-voting system." In 2018 IEEE 11th international conference on cloud computing (CLOUD), pp. 983-986. IEEE, 2018.

©IJRASET: All Rights are Reserved | SJ Impact Factor 7.538 | ISRA Journal Impact Factor 7.894 |



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Call : 08813907089 (24*7 Support on Whatsapp)