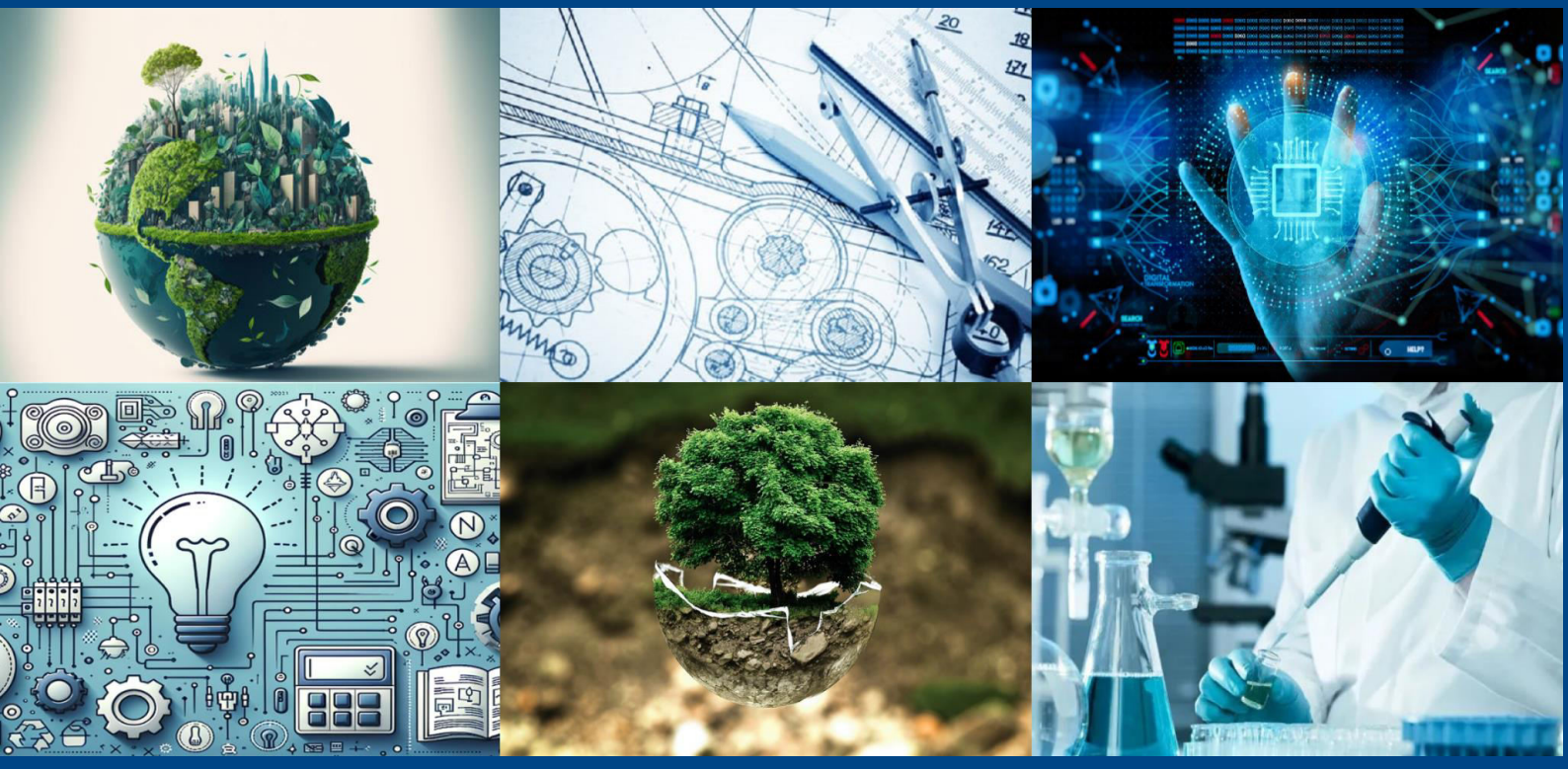
ISSN: 2582-7219

International Journal of Multidisciplinary Research in Science, Engineering and Technology

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)



Impact Factor: 8.206

Volume 8, Issue 3, March 2025

© 2025 IJMRSET | Volume 8, Issue 3, March 2025| DOI: 10.15680/IJMRSET.2025.0803169

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

VoteGuardian: A Blockchain Based Voting System

Srilakshmi CH[1], Sreena K[2], Srimathi P[3], Swetha S S[4]

Faculty, Department of Computer Science and Business Systems, R.M.D. Engineering College, Chennai, India[1]

Student, Department of Computer Science and Business Systems, R.M.D. Engineering College, Chennai, India[2]

Student, Department of Computer Science and Business Systems, R.M.D. Engineering College, Chennai, India[3]

Student, Department of Computer Science and Business Systems, R.M.D. Engineering College, Chennai, India[4]

ABSTRACT: Ensuring secure and transparent elections is crucial for democracy. Traditional voting systems often face issues like fraud, lack of transparency, and accessibility challenges. This paper presents a blockchain-based e-voting system that enhances security, transparency, and efficiency. Blockchain's decentralized and immutable nature ensures secure vote recording and verification, while smart contracts automate vote validation and counting, reducing human involvement and potential manipulation. Cryptographic techniques maintain voter anonymity while ensuring vote authenticity. A distributed ledger enables real-time vote verification, preventing unauthorized modifications. By integrating blockchain, this system reduces fraud, increases voter trust, and ensures a fair and verifiable electoral process.

KEYWORDS: Blockchain, E-Voting, Smart Contracts, Cryptographic Security, Transparency, Decentralization, Electoral Integrity, Distributed Ledger, Vote Authentication, Tamper-Proof Voting.

I. INTRODUCTION

Elections are a fundamental pillar of democracy, enabling citizens to express their choices in a free and transparent manner. However, traditional voting systems face numerous challenges, including fraud, vote tampering, lack of transparency, and accessibility issues. While electronic voting (e-voting) has been introduced to address some of these concerns, most e-voting systems rely on centralized databases, making them vulnerable to cyberattacks, data manipulation, and unauthorized access. Ensuring election security and integrity is crucial to maintaining public trust and confidence in the democratic process.

Blockchain technology provides a decentralized, immutable, and tamper-proof solution to these challenges. By leveraging blockchain's distributed ledger and cryptographic security, this project aims to develop a secure and transparent e-voting system. The system employs smart contracts to automate vote validation, counting, and result generation, reducing human intervention and minimizing potential manipulation. Additionally, cryptographic techniques ensure voter anonymity while preserving vote authenticity, preventing identity fraud and unauthorized alterations.

The objective of this project is to design and implement a blockchain-based e-voting system that enhances electoral integrity, prevents fraud, and increases voter trust. The decentralized nature of blockchain ensures that votes remain immutable, preventing unauthorized modifications and ensuring verifiable election results. By integrating blockchain, this system offers a reliable, efficient, and transparent approach to modern digital voting. This paper presents the system architecture, security mechanisms, and performance evaluation of the proposed solution.

II. SYSTEM DESCRIPTION

A. Hardware Requirements:

- Network Infrastructure: The system requires a robust distributed network infrastructure comprising multiple nodes representing partitions of the voting population. Each geographical voting jurisdiction should host at least one

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

dedicated server node with high-speed internet connectivity (minimum 100 Mbps) and redundant power sources to ensure uninterrupted service during the election period.

- Server Specifications: Each node server should meet minimum specifications of quad-core processors (3.0 GHz or higher), 16GB RAM, and 1TB SSD storage to handle concurrent transaction processing and maintain blockchain integrity. For large-scale national elections, server specifications should be scaled accordingly to accommodate increased user load and transaction volume.
- Voting Devices: The system supports various voter access points including mobile phones, tablets, and computers that meet minimum security requirements. These devices serve as interfaces through which voters interact with the blockchain network.
- Security Hardware: Hardware security modules (HSMs) should be deployed at each node to securely store cryptographic keys and execute sensitive cryptographic operations. Biometric authentication devices may be integrated at registration centers to enhance voter identity verification while maintaining privacy through Zero Knowledge Proof implementations.

B. Software Requirements:

- Blockchain Platform: The system utilizes a private blockchain network with Proof of Authority (PoA) consensus protocol to optimize performance while maintaining security. This architecture balances transaction throughput with decentralization requirements specific to the electoral process. The blockchain implementation should support smart contract functionality compatible with election-specific operations.
- Smart Contract Implementation: Election rules are encoded as Solidity-based smart contracts that serve as digital ballots. A factory smart contract creates and deploys individual ballot contracts for each voting partition, allowing for scalable and modular implementation. These contracts must enforce voting rules, including single-vote verification, candidate selection validation, and proper vote recording.
- Consensus and Validation: The Proof of Authority consensus mechanism governs transaction validation, providing efficient block generation while maintaining security through authorized validators.
- Identity Management: The system implements a secure voter registration process incorporating Zero Knowledge Interactive Proofs to authenticate voters without revealing their identities. Each eligible voter receives a digital wallet secured through public-private key cryptography using libraries like OpenSSL. The system issues a single voting coin to each verified voter, which is consumed upon casting a vote to prevent multiple voting.
- User Interface: A user-friendly web application interface built using frameworks like React or Angular, allows voters to authenticate, view ballot information, and cast votes securely. The interface should be accessible across different devices and platforms while maintaining security standards. Administrative interfaces with appropriate access controls enable election officials to manage the election lifecycle.
- Security Protocols: End-to-end encryption protects all data transmissions within the system. Hash functions anonymize voter data while maintaining verification capabilities. The system implements UTXO (Unspent Transaction Output) mechanisms to prevent incomplete or malicious transactions.

III. SYSTEM ARCHITECTURE

The operational process of the Blockchain-Based Electronic Voting System starts from the authentication process for users, during which voters identify themselves via an authentic authentication module. Having done so, the voter proceeds to choose his candidate through a web or mobile-based application. Then, his choice is encrypted utilizing cryptographic processes so that his security and anonymity remain intact, then submitted to a smart contract deployed on the blockchain. The election rules are enforced by the smart contract and send the vote to be validated by a consensus mechanism, whereby legitimacy and tamper- proofing are guaranteed.

After verification, the encrypted vote is kept forever in the blockchain ledger (on-chain storage), whereas related metadata like timestamps and voter credentials (excluding personally identifiable information) are stored in off-chain storage by employing secure databases such as IPFS or cloud storage. Once the voting process concludes, the votes tally module retrieves votes from the blockchain and automatically tallies them through smart contracts. The results of the election are ultimately presented to users via application interface.

To ensure transparency and integrity, an audit verification module enables election officials and the public to verify election records without invading voter privacy. This decentralized, tamper-evident process provides a secure,

© 2025 IJMRSET | Volume 8, Issue 3, March 2025| DOI: 10.15680/IJMRSET.2025.0803169

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

transparent, and fraud-proof election system, taking advantage of blockchain's immutability and cryptographic security.

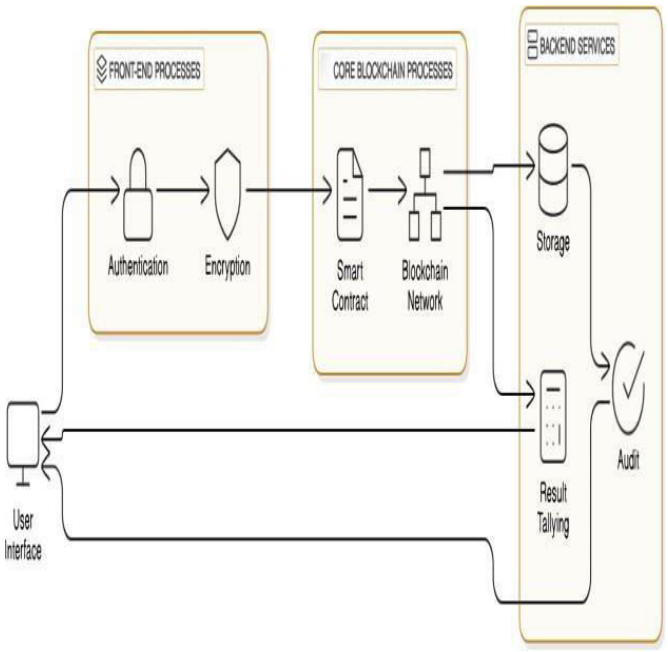


Fig. 3.1 Architecture Diagram

IV. WORKING MECHANISM

The operational process of the Blockchain-Based Electronic Voting System starts from the authentication process for users, during which voters identify themselves via an authentic authentication module. Having done so, the voter proceeds to choose his candidate through a web or mobile-based application. Then, his choice is encrypted utilizing cryptographic processes so that his security and anonymity remain intact, then submitted to a smart contract deployed on the blockchain. The election rules are enforced by the smart contract and send the vote to be validated by a consensus mechanism, whereby legitimacy and tamper- proofing are guaranteed.

After verification, the encrypted vote is kept forever in the blockchain ledger (on-chain storage), whereas related metadata like timestamps and voter credentials (excluding personally identifiable information) are stored in off-chain storage by employing secure databases such as IPFS or cloud storage. Once the voting process concludes, the votes tally module retrieves votes from the blockchain and automatically tallies them through smart contracts. The results of the election are ultimately presented to users via application interface.

To ensure transparency and integrity, an audit verification module enables election officials and the public to verify election records without invading voter privacy. This decentralized, tamper-evident process provides a secure, transparent, and fraud-proof election system, taking advantage of blockchain's immutability and cryptographic security.

© 2025 IJMRSET | Volume 8, Issue 3, March 2025| DOI: 10.15680/IJMRSET.2025.0803169

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

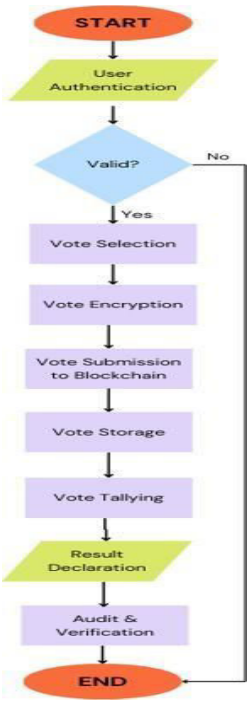


Fig. 4.1 Flow Chart

V. IMPLEMENTATION

The implementation of the blockchain-based e-voting system integrates multiple components to ensure secure, transparent, and tamper-proof voting. The system is built on a blockchain network, utilizing smart contracts, cryptographic security, and a decentralized ledger. These elements work together to maintain vote integrity while preserving voter anonymity. A smart contract automates vote validation, counting, and result declaration, reducing manual intervention and minimizing manipulation risks. The system also employs cryptographic methods for secure voter authentication and ensures the confidentiality of votes.

A. Technologies Used

The following technologies are utilized in the system:

- Blockchain Network – Ethereum ensures decentralized, immutable vote storage.
- Smart Contracts – Solidity-based contracts automate vote validation and counting.
- Cryptographic Security – ECDSA ensures secure voter authentication.
- Web Development – React.js provides an intuitive user interface.
- Backend & Blockchain Communication – Node.js and Web3.js handle blockchain interactions.
- Data Encryption – SHA-256 hashing secures vote confidentiality.

B. Smart Contract Implementation

Smart contracts play a critical role in enforcing election rules and automating voting procedures. The contract ensures that each voter can cast only one vote, preventing duplication and fraudulent activities. Once recorded, votes cannot be altered, ensuring transparency and security. The smart contract handles voter registration, vote casting, vote validation, and result computation, reducing human involvement and errors. Each vote is treated as a transaction and is permanently stored on the blockchain, making unauthorized modifications impossible.

© 2025 IJMRSET | Volume 8, Issue 3, March 2025| DOI: 10.15680/IJMRSET.2025.0803169

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

C. Security Measures

Security is a fundamental aspect of the system, with multiple layers of protection. The decentralized nature of blockchain eliminates control by any single entity, reducing risks of manipulation. The immutability of blockchain ensures that once a vote is recorded, it cannot be altered or deleted. Cryptographic techniques safeguard voter anonymity, preventing any link between a vote and a voter. Additionally, blockchain's consensus mechanisms make tampering nearly impossible, ensuring the integrity of the election process. *D. System Workflow*

The blockchain-based e-voting system follows a structured workflow to ensure secure and transparent elections. The steps involved are:

- Voter Authentication – Users log in using a secure authentication mechanism, verifying their identity through cryptographic techniques.
- Eligibility Check – The system verifies if the user is registered and has not voted already. If eligible, access is granted; otherwise, voting is restricted.
- Vote Casting – The voter selects their preferred candidate using a user-friendly web interface.
- Vote Encryption & Storage – The selected vote is encrypted and stored securely on the blockchain ledger, ensuring immutability.
- Vote Validation – The smart contract validates each vote to prevent duplicate or unauthorized submissions.
- Vote Confirmation – The voter receives confirmation that their vote has been securely recorded.

Result Computation – After the voting period ends, the system automatically counts the votes and publishes verifiable results on the blockchain

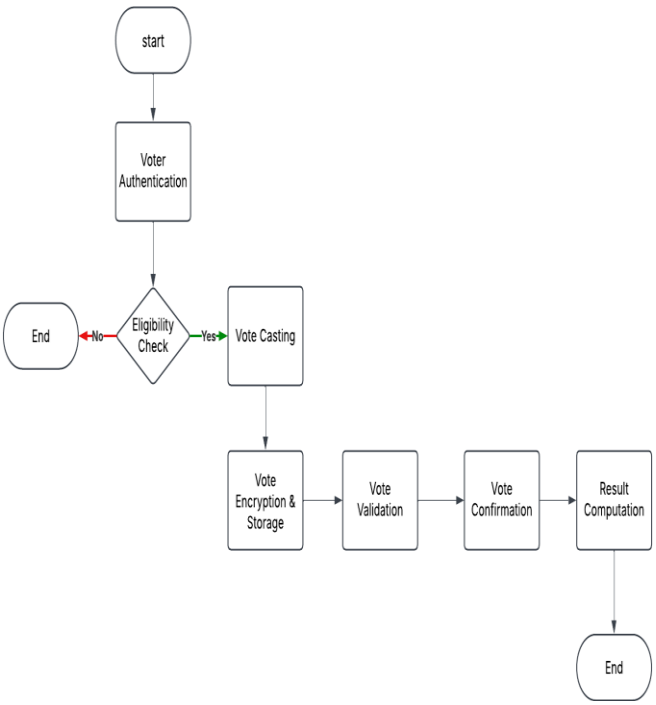


Fig. 5.1 Flow Chart

E. Performance Analysis

The system is evaluated based on multiple factors, including transaction speed, security performance, and scalability. Blockchain-based e-voting eliminates the delays associated with traditional voting methods, ensuring faster processing and error-free vote counting. Gas consumption on Ethereum is optimized to minimize transaction costs, while cryptographic mechanisms provide robust security. The decentralized approach guarantees election transparency, increasing voter confidence in the process.

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

VI. ADVANTAGES

- Enhanced Security: Blockchain's decentralized nature makes it resistant to tampering and fraud. Each transaction is cryptographically secured and immutable, ensuring that once a vote is recorded, it cannot be altered or deleted.
- Transparency and Auditability: Every transaction on the blockchain is publicly accessible, allowing for real-time auditing of votes. This transparency fosters trust among voters, as they can independently verify the integrity of the election results.
- Voter Privacy: Utilizing advanced cryptographic techniques, such as Zero Knowledge Proofs, allows voters to cast their ballots without revealing their identities or choices. This protects voter privacy while maintaining the ability to verify votes.
- Accessibility: The system can be accessed from various devices, including smartphones and tablets, enabling voters to participate in elections from remote locations. This increased accessibility can lead to higher voter turnout, particularly among marginalized populations.
- Cost Efficiency: By reducing the need for physical polling stations and paper ballots, blockchain voting systems can lower operational costs associated with traditional voting methods. Furthermore, the automation of processes through smart contracts can streamline election management.
- Reduction of Human Error: Automated processes minimize the risk of human error in vote counting and result tabulation. Smart contracts ensure that votes are counted accurately and consistently according to predefined rules.

VII. FUTURE WORK

- Scalability Enhancements: Future work should focus on optimizing the system to handle larger voter populations and increased transaction volumes without compromising performance or security.
- Interoperability with Existing Systems: Research is needed to develop standards and protocols that allow blockchain voting systems to integrate seamlessly with existing electoral infrastructure, including voter registration databases and election management systems.
- User Experience Improvements: Continuous refinement of the user interface is essential to ensure that it remains intuitive and accessible for all voters, including those with disabilities or limited technological proficiency.
- Regulatory Compliance: Future studies should explore how blockchain voting systems can align with existing electoral laws and regulations across different jurisdictions, ensuring legal validity and acceptance by electoral authorities.
- Pilot Programs and Real-World Testing: Conducting pilot programs in controlled environments will provide valuable insights into the practical challenges of implementing blockchain-based voting systems in real elections. These tests will inform necessary adjustments before large-scale deployment.

VIII. CONCLUSION

The proposed blockchain-based voting system represents a significant advancement in the quest for secure, transparent, and accessible electoral processes. By leveraging the inherent strengths of blockchain technology—such as decentralization, immutability, and cryptographic security—the system addresses many vulnerabilities associated with traditional voting methods. The advantages outlined demonstrate its potential to enhance public trust in elections while promoting higher voter participation rates.

REFERENCES

1. M.-V. Vladucu, Z. Dong, J. Medina, and R. Rojas-Cessa, “E-Voting Meets Blockchain: A Survey,” IEEE Access, vol. 11, pp. 23293–23306, Mar. 2023, doi: 10.1109/ACCESS.2023.3253682.
2. A. Subhash Yadav, A. U. Thombare, Y. V. Urade, and A. A. Patil, “E-Voting Using Blockchain Technology,” Int. J. Eng. Res. Technol. (IJERT), vol. 9, no. 7, pp. 375-380, Jul. 2020.
3. R. Hanifatunnisa and B. Rahardjo, “Blockchain Based E- Voting Recording System Design,” in Proc. IEEE, 2017, pp. 1-6, doi: 10.1109/ICoICT.2017.8074663.

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

4. S. Suralkar, S. Udasi, S. Gagnani, M. Tekwani, and M. Bhatia, "E-Voting Using Blockchain With Biometric Authentication," Int. J. Res. Anal. Rev. (IJRAR), vol. 6, no. 1, pp. 77-85, Mar. 2019.
5. M. Pathak, A. Suradkar, A. Kadam, A. Ghodeswar, and P. Parde, "Blockchain Based E-Voting System," Int. J. Sci. Res. Sci. Technol. (IJSRST), vol. 8, no. 3, pp. 134-140, May- Jun. 2021, doi: 10.32628/IJSRST2182120.
6. Friðrik Þ. Hjálmarsson, Gunnlaugur K. Hreiðarsson, Mohammad Hamdaqa, and Gísli Hjálmtýsson, "Blockchain-Based E-Voting System," in Proc. IEEE 11th Int. Conf. Cloud Comput., 2018, pp. 983-990, doi: 10.1109/CLOUD.2018.00151.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH

IN SCIENCE, ENGINEERING AND TECHNOLOGY

| Mobile No: +91-6381907438 | Whatsapp: +91-6381907438 | ijmrset@gmail.com |

www.ijmrset.com