iJRASET
International Journal For Research in Applied Science and Engineering Technology



INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 13 **Issue:** IV **Month of publication:** April 2025

DOI: https://doi.org/10.22214/ijraset.2025.68118

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 13 Issue IV Apr 2025- Available at www.ijraset.com

E-VoteChain: Securing Digital Elections

Prof. Mahadevi Namose, Teemira Bhale[3], Shivaranjani Darshale[4], Devashree Mali[2]
[1]*Faculty of Computer Science, International Institute of Information Technology, Pune, India*
[2, 3, 4, 5]*Computer Engineering, International Institute of Information Technology, Pune, India*

Abstract: ***The use of electronic voting (e-voting) is becoming more common instead of traditional voting systems, but it still faces a big issue: trust. E-voting systems can be easily manipulated, with potential changes to election results from hacking or tampering by those who create the systems. In centralized networks, data is managed by one party, which raises trust concerns. However, this problem can be solved by using a distributed system where data is shared among all users. Blockchain technology serves this purpose well, as it keeps a shared record that cannot be changed, making it ideal for e-voting. This research introduces a Blockchain-based e-voting system using Ethereum and MetaMask, which meets six key principles of a fair election: secret ballots, one vote per person, voter eligibility, transparency, accurate recording and counting of votes, and reliability. Additionally, testing shows that using a slower gas price option results in the best value for costs. This introduces a Blockchain-based e-voting system utilizing Ethereum and MetaMask, ensuring adherence to essential electoral principles such as secret ballots, voter eligibility, and accurate vote recording. Performance evaluations indicate that using a slow gas price option offers the best cost-efficiency for this system. Overall, the proposed model not only addresses the vulnerabilities of traditional e-voting systems but also has potential applications beyond elections, including corporate governance and various voting scenarios.***
Keywords: Electronic voting, blockchain, smart contract, Ethereum

I. INTRODUCTION

The increasing digitization of electoral processes has highlighted the need for secure, transparent, and tamper-resistant voting systems. Traditional electronic voting (e-voting) methods often suffer from security vulnerabilities, including unauthorized access, vote manipulation, and lack of verifiability. These challenges have raised concerns about the reliability and integrity of elections worldwide. To address these issues, blockchain technology has emerged as a promising solution due to its decentralized, immutable, and transparent nature.

Blockchain-based e-voting systems leverage smart contracts to automate vote recording, storage, and counting while eliminating the need for centralized authorities. By ensuring that votes are permanently recorded on a distributed ledger, blockchain prevents data tampering and enhances voter confidence. Furthermore, cryptographic techniques integrated into blockchain networks provide secure authentication, protecting voter privacy while ensuring election transparency.

This paper presents the implementation of a blockchain-driven e-voting system using Remix IDE, MetaMask, and Ganache. Remix IDE serves as the development environment for writing and deploying Ethereum-based smart contracts, while MetaMask facilitates secure authentication and interaction with the blockchain network. Ganache is used as a local Ethereum blockchain for testing and validating the system before real-world deployment.

The proposed system is designed to address key challenges in e-voting, including vote integrity, voter authentication, and real-time verifiability. The smart contract enforces a secure voting mechanism where only registered voters can participate, votes cannot be altered once cast, and election results are computed automatically without human intervention. Additionally, by eliminating central control, the system mitigates risks associated with election fraud and external manipulation.

This paper provides a detailed implementation of the blockchain-based e-voting system, discussing its architecture, functional components, and security mechanisms. It also examines the benefits and limitations of using blockchain for electoral processes, highlighting potential improvements for scalability, user adoption, and regulatory compliance. The results demonstrate that blockchain technology can significantly enhance election security and transparency, paving the way for future advancements in digital democracy. As society progresses into the digital era, there is an increased call for the voting infrastructure to be more robust and secure in order to fill the gap in available systems. Recent research and practice have focused on exploring innovative solutions to this problem. Blockchain technology is one such prominent solution that has received gigantic attention over the last few years for its potential to revolutionize many sectors of operations, including finance, healthcare, and supply chain management. At its core, it is decentralized and distributed ledger technology, which allows securing as well as recording transactions across many nodes in the network.

©IJRASET: All Rights are Reserved

Unlike other databases being controlled by a single organization, blockchain has no central authority, which minimizes the possibilities of tampering with data and makes it more resilient for the system. Some modern alternative has been identified in electronic voting systems. Voters can use electronic voting machines at the polling station or be able to vote online from their devices. This method is speedier and convenient since it will automatically count the results, saving time and resources in tallying. However, electronic voting is not without its challenges. There are also grave concerns about the security of the votes, where it is possible to manipulate or leak. Most electronic systems work like "black boxes," hence results cannot be checked or audited. Centralized systems are also not immune to denial-of-service attacks, that would disrupt the voting process and affect the public's trust. The paper deals with the integration of blockchain technology into voting systems to achieve security, transparency, and accessibility in the electoral process. It is a review of different platforms on the block chain and their respective potential applications in voting situations. But by reviewing these existing implementations, challenges, and future directions for blockchain-based voting, we hope to help shed light on how this technology might be used to help address the ills of traditional and electronic voting systems. We will seize this opportunity to further contribute to the already seminal debate around improving electoral integrity and building greater public confidence in democratic processes.

II. EASE OF USE

The simplicity of executing the suggested E-Voting System based on Blockchain is attained in a properly constructed process that has security, transparency, and easiness. The system starts at the registration phase, where candidates and voters are taken through an easy process of obtaining distinct ID numbers. With this distinct ID, there is a tamper-proof record that keeps track of eligible voters and candidates, in which only authentic people take part in the election. The system's admin side is liable for authenticating the registered user's details prior to allowing access to the system, thus becoming a controlled process that is effective. After completion of the registration process, each voter and candidate has a unique identity in the system, while impersonation and illegal voting are prevented. On election day, the voter logs in using a secure verification process through multi-factor authentication mechanisms like a password, a biometric, or an OTP mechanism.

The authentication process is important in verifying that only genuine voters can access the electoral system and that no fraud is carried out. The system has a simple and intuitive user interface with easy navigation to enable voters to vote and participate without much technical expertise.

On successful verification, the voter enters the voting phase, where the voter gets to choose their chosen candidate. On casting the vote, the blockchain instantly logs the vote in an irreversible ledger to ensure that no votes can be changed, replicated, or removed. The blockchain technology automatically avoids double voting since every vote is associated with a distinct voter ID, and the system automatically cross-checks if a voter has already voted. This system greatly minimizes the possibility of electoral fraud and increases the overall integrity of the voting process. The system candidate side verifies that the votes are received accurately, and the admin is always monitoring the system for any irregularities. A validation mechanism verifies if the votes are according to the rules of the system and ensures that only valid votes are tallied. The execution of smart contracts is important in automating the process of verifying the votes, eliminating manual verification and the possibility of manipulation or human errors. Blockchain provides transparency such that the whole voting process can be audited and verified at any given time, which boosts confidence among the voters.

After all the voters have voted, the process proceeds to the counting of votes, where the blockchain computes and authenticates the results automatically. Because every vote is safely kept on a distributed ledger, no tampering, miscounting, or data loss is possible. The use of automation for the system ensures that manual vote counting is eliminated, which lowers the time and resources needed to compute the results considerably. The ultimate results are presented in a transparent manner so that voters and candidates alike have faith in the outcome.

The winner is determined by the candidate receiving the most valid votes, and the outcome is made publicly verifiable. With the use of blockchain technology, the system provides high security along with a user-friendly framework for all parties involved, such as voters, candidates, and administrators.

The processes of various kinds, i.e., voter verification, ballot validation, and result calculation, are automated to minimize human interference and make the whole election process efficient. The system as proposed here is highly secure as well as efficient in nature and is also easy to implement, thus suitable for digital elections in the present day.

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

A. Equation

$$T(c_j) = \sum_{i=1}^{N_V} \delta(v_{cast}(v_i), c_j)$$
$$V_{cast}(v_i) \neq 0$$

Where,

N_V be the total number of voters N_V=|V|

C_j = {name,id,election…promise}

$V_{cast}(v_i)$=Vote cast function

T(C_j) = Total no. of candidates

δ = function represents a small change in vote count

III.LITERATURE SURVEY

1) Benaloh et al. (2014) propose a verifiable online voting system that ensures voter privacy and vote integrity. Their research emphasizes the importance of cryptographic techniques, such as homomorphic encryption and zero-knowledge proofs, to maintain secrecy while enabling auditability. However, the study notes that large-scale implementation requires optimizing computational efficiency.

2) Zyskind et al. (2015) explore the use of blockchain for decentralized identity management, which can be applied to e-voting systems for secure voter authentication. Their study concludes that blockchain-based identity verification enhances security by reducing risks associated with centralized databases but requires user-friendly implementations for practical adoption.

3) Kshetri and Voas (2018) analyze blockchain's role in securing elections by preventing vote tampering and increasing transparency. They highlight that while blockchain can address issues of election fraud, its effectiveness depends on consensus mechanisms, network scalability, and resistance to cyberattacks.

4) Hardwick et al. (2018) investigate the use of smart contracts in e-voting to automate vote counting and verification. Their findings indicate that while smart contracts can improve election efficiency and eliminate human errors, they must be carefully designed to prevent vulnerabilities such as reentrancy attacks and contract manipulation.

5) Yang et al. (2019) propose a hybrid e-voting framework that combines blockchain with traditional voting methods. Their study concludes that while blockchain enhances security and transparency, integrating it with existing electoral infrastructure ensures broader accessibility and compliance with legal frameworks.

6) McCorry et al. (2017) develop a blockchain-based voting system using Ethereum smart contracts. Their research demonstrates that blockchain enables verifiable and tamper-resistant elections, but network congestion and transaction costs remain critical limitations.

7) Chaudhry et al. (2020) explore the impact of consensus mechanisms on e-voting performance. They compare Proof-of-Work (PoW), Proof-of-Stake (PoS), and Delegated Proof-of-Stake (DPoS) in voting scenarios. The study concludes that while PoW ensures security, it is computationally expensive, whereas PoS and DPoS provide better scalability but may introduce centralization risks.

8) Ahmad et al. (2021) present a privacy-preserving e-voting system leveraging zk-SNARKs (Zero-Knowledge Succinct Non-Interactive Argument of Knowledge). Their findings indicate that zk-SNARKs can enhance voter anonymity while ensuring verifiability, though their computational complexity needs further optimization.

9) Shrestha et al. (2022) evaluate blockchain e-voting systems in developing countries, identifying challenges such as digital literacy, infrastructure limitations, and regulatory barriers. Their research suggests that successful adoption depends on government policies and public awareness initiatives.

10) Patel and Shah (2023) propose an AI-enhanced blockchain voting system that utilizes machine learning for voter fraud detection. Their study concludes that integrating AI with blockchain improves security but raises ethical concerns regarding data privacy and algorithmic biases.

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue IV Apr 2025- Available at www.ijraset.com

IV. PROPOSED SYSTEM

A. Registration

Before any person votes, each eligible voter receives a unique public address and with a private key. These two concepts are central to ensuring the voting system is secure and private. The public address is like an account number, while the private key is like the password. Each voter's account also loaded with a sufficient amount of ether, a form of cryptocurrency, to make one transaction. This configuration enables the voters to vote without anyone knowing their preference. The public address and the private key of the voters should remain private, thus ensuring that they get to vote anonymously.

B. Authentication

The process now moves on to voting, and authentication is at the very initial stage. In this, every voter needs to input the public address along with their private key in the system to authenticate himself or herself. This happens because only a registered voter has the right to vote. Whatever credentials entered by the user must be validated against the one that is registered with the system for any entry to vote. Authentication keeps frauds at bay and prevents only illegitimate people from voting in an election.

C. Voting

After getting authenticated, one goes through the voting phase and can then vote. They are presented with a list of accessible candidates on a friendly application. A voter may scrutinize the options and pick his preferred candidate. In essence, when the voter makes a request to a smart contract, which is truly a self-executing contract with the terms written directly into codes, they submit their vote officially. At the same time, the voter also includes the ID of the chosen candidate so that his or her vote can be recorded accurately for them through this request.

1) Algorithm

a) Candidate Registration and Voter Registration (Mapping Lookup)

Algorithm: Hash-based Lookup (Mapping)
Explanation: Solidity's mapping allows for constant-time (O(1)) lookups when registering candidates and voters. Each voter and candidate is assigned a unique key (voter address or candidate ID), making insertion and retrieval efficient .
Use Case in the Project: Adding and verifying candidates and voters.

b) Vote Casting (Direct Vote Counting)

Algorithm: Incremental Counter
Explanation: When a voter casts a vote, the candidate's vote count is incremented by 1. This is a simple operation with constant-time complexity (O(1)).
Use Case in the Project: Each vote directly increments the selected candidate's vote count.

c) Displaying Results

Algorithm: Direct Retrieval (Mapping)
Explanation: Once the election ends, the results (winner’s details) are stored in state variables, and anyone can view them in constant time (O(1)) by retrieving the pre-calculated values .
Use Case in the Project: Retrieving election results and displaying winner information.

2) Program Code

```
// SPDX-License-Identifier: MIT
pragma solidity ^0.8.10;

contract Voting {
   struct Candidate {
      string name;
      string electionPromise;
      uint8 id;
   }
```

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

ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 13 Issue IV Apr 2025- Available at www.ijraset.com

```
struct Voter {
    uint8 id;
    string name;
    uint256 registrationTime;
    bool isRegistered;
}

address public owner;
mapping(uint8 => Candidate) public candidateDetailsList;
mapping(address => Voter) public voters;

address[] public voterAddresses; // Array to store all voter addresses

uint8 public candidatesCount;
uint8 public votersCount;

event CandidateAdded(string name, uint8 id);
event VoterRegistered(address voterAddress, uint8 voterId, string voterName);

constructor() {
    owner = msg.sender;
}

modifier onlyOwner() {
    require(owner == msg.sender, "Only Owner has access to this functionality");
    _;
}

modifier onlyBeforeElection() {
    _;
}
function addCandidate(string memory name, string memory electionPromise) public onlyOwner onlyBeforeElection {
    candidatesCount += 1;
    uint8 candidateId = candidatesCount;

    require(candidateDetailsList[candidateId].id == 0, "Candidate already registered");

    candidateDetailsList[candidateId] = Candidate(name, electionPromise, candidateId);
    emit CandidateAdded(name, candidateId);
}

function registerVoter(uint8 voterId, string memory voterName) public {
    require(voters[msg.sender].isRegistered == false, "Voter already registered");

    voters[msg.sender] = Voter(voterId, voterName, block.timestamp, true);
    voterAddresses.push(msg.sender); // Add voter address to the array
    votersCount += 1;

    emit VoterRegistered(msg.sender, voterId, voterName);
```

©IJRASET: All Rights are Reserved

```
    }

    // Get voter details (returning voter addresses, IDs, and names)
    function getVoters() public view returns (address[] memory, uint8[] memory, string[] memory) {
        uint8 voterCount = uint8(voterAddresses.length);
        address[] memory voterAddressesList = new address[](voterCount);
        uint8[] memory voterIds = new uint8[](voterCount);
        string[] memory voterNames = new string[](voterCount);

        for (uint8 i = 0; i < voterCount; i++) {
            address voterAddress = voterAddresses[i];
            Voter memory voter = voters[voterAddress];
            voterAddressesList[i] = voterAddress;
            voterIds[i] = voter.id;
            voterNames[i] = voter.name;
        }

        return (voterAddressesList, voterIds, voterNames);
    }
}
```

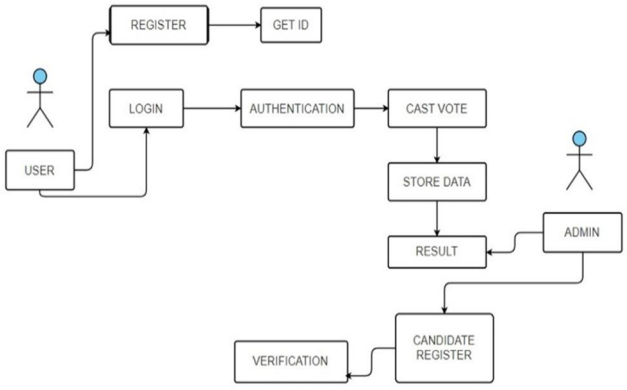


Fig 1. Detailed UML Diagram

V. SYSTEM ARCHITECTURE

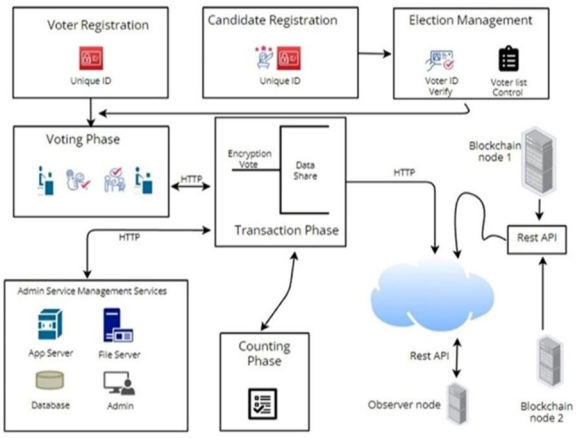


Fig 2. System Architecture

This blockchain-driven e-voting system is designed to provide a secure, transparent, and tamper-proof electoral process. It begins with voter and candidate registration, where each participant is assigned a unique ID to prevent duplication and fraud. Election management verifies voter identities and maintains a secure voter list, ensuring only eligible participants can cast their votes.

During the voting phase, voters submit their encrypted ballots through a secure HTTP connection. These votes are then processed in the transaction phase, where they are recorded on a decentralized blockchain network. Multiple blockchain nodes ensure data integrity, while REST APIs facilitate seamless communication between the voting system and the blockchain. An observer node continuously monitors transactions, enhancing transparency and preventing manipulation or unauthorized modifications.

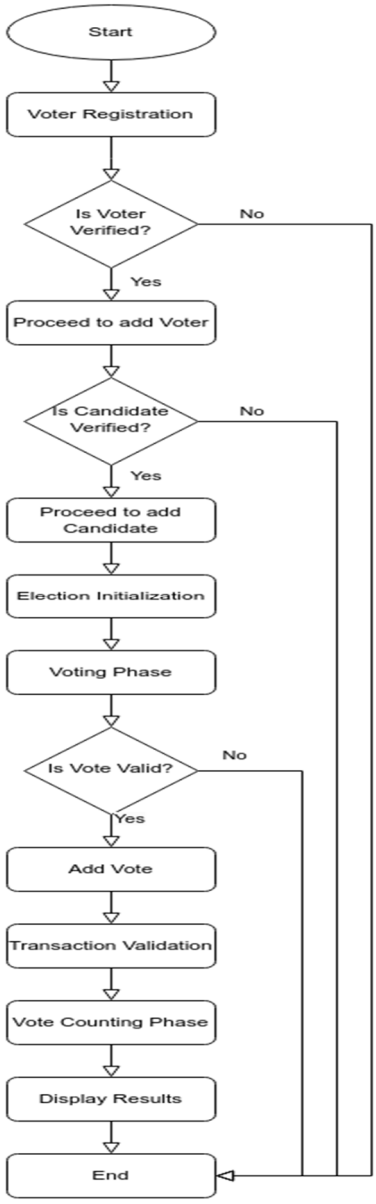


Fig 3. Flowchart of E Voting System

VI. METHODOLGY

A voting system using the technology of Ethereum blockchain. An Ethereum blockchain network is used to implement this voting system. Ethereum is a decentralized and open-source network that supports smart contracts. In this platform, the cryptocurrency used is called Ether (ETH). It uses a method called Proof of Work, where those who can quickly solve complex problems with their computer power can add new blocks to the network. Setting up the blockchain provides a safeguard from vote tampering. Each block in the blockchain is linked to the previous and next blocks.

This means any attempt of hackers to a particular block will be caught by the next block. Attempting on changes will also result in the corrupting of the following blocks, thus it would be extremely difficult to alter records without being detected. The hash value produced by the block is responsible for ensuring the data's integrity. Additionally, MetaMask is a well-known digital wallet that people use to manage crypto holdings and interact with blockchain apps, especially with the Ethereum network. Through MetaMask, it is possible for the users to connect to decentralized applications (DApps) directly from their web browsers simply, to send and receive funds, sign transactions, and to participate in blockchain activities without needing to run a full Ethereum node. Solidity is a programming language dedicated to developing smart contracts within the Ethereum blockchain. Solidity is typically used because it offers the necessary instruments to make fully decentralized applications (DApps) and transaction management in a secure way on the blockchain. Moreover, Remix IDE is an online development environment used for writing, testing, and deploying smart contracts written in Solidity. It gives a nice interface with features such as syntax highlighting, debugging tools, and a built-in Ethereum Virtual Machine (EVM) for testing contracts. Team Remix can prototype and perform quick tests on their smart contracts with Remix.

VII. RESULTS

Our project focuses on automating the process of conducting secure and transparent elections using blockchain technology. This system streamlines the identification, authentication, and validation of voters while ensuring tamper-proof voting and result computation. By leveraging blockchain's decentralized and immutable nature, the proposed system enhances the efficiency, security, and accuracy of digital elections, mitigating risks such as double voting, voter fraud, and unauthorized access. The implementation of smart contracts further automates the process, reducing human intervention and ensuring real-time vote validation, making the election process more reliable and transparent.

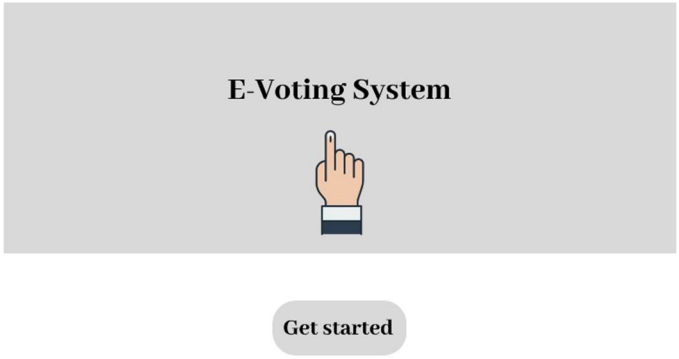


Fig 4. Home page



Fig 5. Voter Registration Page



Fig 6. Candidate Registration Page



FIG 7. FINAL RESULT PAGE

VIII. CONCLUSION

Electronic voting (e-voting) has been in existence since the 1970s, which on paper offers some advantages over the paper-based systems in terms of higher efficiency and fewer errors. Also, along with cybersecurity, there is more and more support for a fair market-free voting system from blockchain enthusiasts. The fast headway of blockchain technology is behind numerous attempts to investigate its suitability in the context of enlarged e-voting systems. This however does not rule out the fact that some crypto-currencies have difficulties as every true technology born is not perfect. This paper details one such project that leverages the powers of a blockchain that are cryptographically secure and transparent to make e-voting systems better. The proposed system is built using Multichain, and it was observed that it fully met the requirements for a reliable e-voting system.

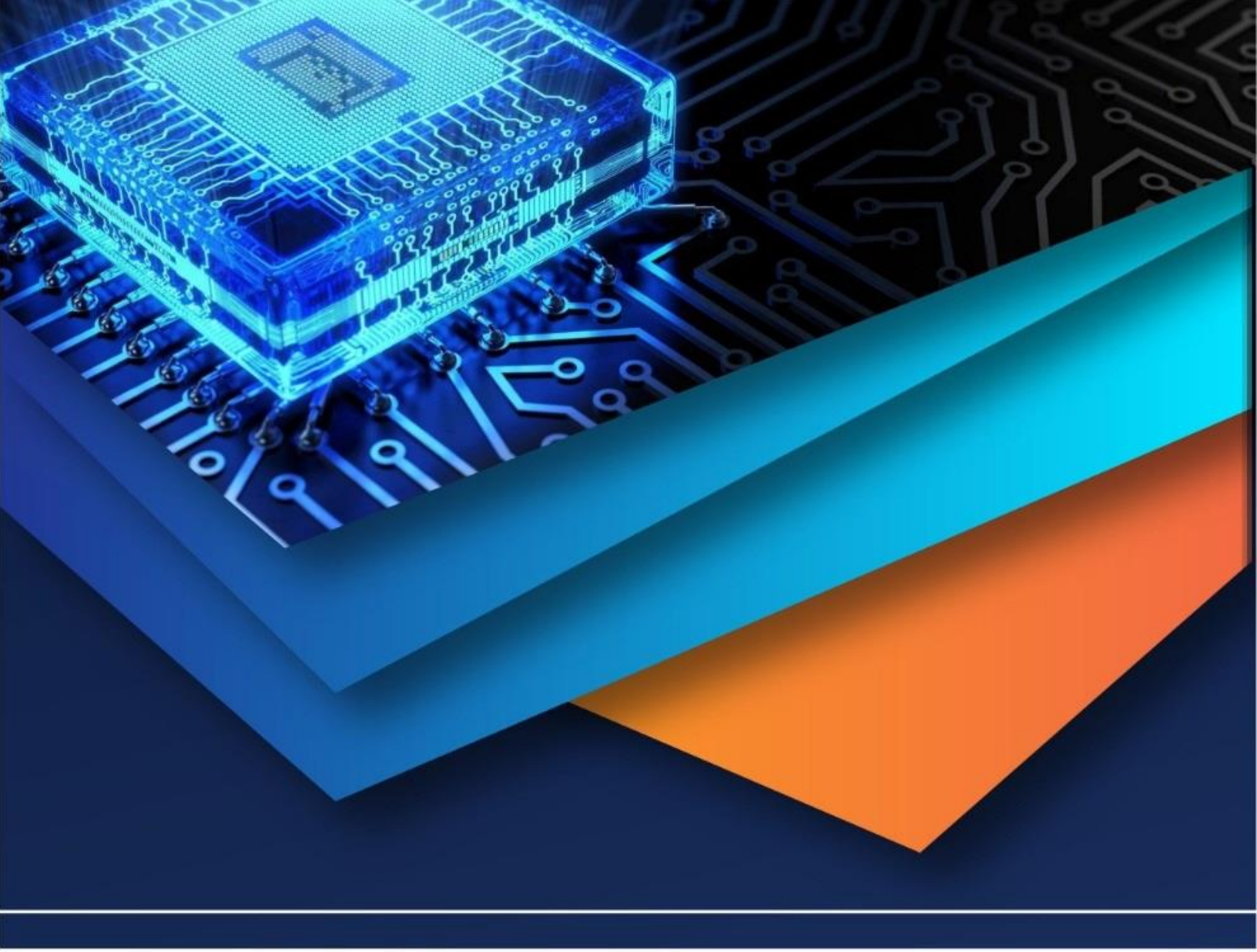
This work is a continuation of the one pinpointing the focus on the strengthening of blockchain's "double spending" problem resistance that arises, for example, in e-voting by fear of the "double voting" case which is misuse of a particular token. Mostly, users rely on this technology for the regular interpretations of transactions. If there are any deviations, they follow them. It therefore means that the secure technology works; however, when weaknesses are demonstrated, a rethink is necessary. This is the driving force to the need for studying this problem in greater depth. We hold the view that soon we are going to witness the development of a trust assured vote-tracking model (provenance) that will help us implement secure and fully verifiable e-voting systems. Adding a provenance layer to the current blockchain infrastructure is one of our ongoing projects which are intended to help in this

IX. ACKNOWLEDGMENT

This research is supported by International Institute of Information Technology College under the ' Savitribai Phule University '

REFERENCES

[1] Always on Voting: A Framework for Repetitive Voting on the Blockchain Sarad venugopalan , Ivana Stancíková , Ivan 0 Homoliak
[2] Blockchain based Voting system in Local Network, vairam
[3] An Integrated and Robust E voting Application Using Private Blockchain, Lakshmi Priya k (Phd)
[4] E-Voting System using Hyperledger Sawtooth, Namratha M*Vivek S K* Yashank R S*
[5] Implementation and evaluation of blockchain based e-voting system with Ethereum and Metamask, Bayu Anggorojati, Deni Pramuli
[6] Blockchain Technology Application for Electronic Voting Systems Valentin Sliusar
[7] U. Can Cabuk, E. Adiguzel, and E. Karaarslan, ''A survey on feasibility and suitability of blockchain techniques for the E-voting systems,'' 2020, arXiv:2002.07175.
[8] J. Ben-Nun, N. Fahri, M. Llewellyn, B. Riva, A. Rosen, A. Ta-Shma, and D. Wikström, ''A new implementation of a dual (paper and cryptographic) voting system,'' in Proc. 5th Int. Conf. Electron. Voting (EVOTE), 2012, pp. 315–329.
[9] S. K. Vivek, R. S. Yashank, Y. Prashanth, N. Yashas, and M. Namratha, ''E-voting systems using blockchain: An exploratory literature survey,'' in Proc. 2nd Int. Conf. Inventive Res. Comput. Appl. (ICIRCA), Jul. 2020, pp. 890–895.
[10] S. A. Adeshina and A. Ojo, ''Maintaining voting integrity using blockchain,'' in Proc. 15th Int. Conf. Electron., Comput. Comput. (ICECCO), Dec. 2019, pp. 1–5.
[11] J. P. Gibson, R. Krimmer, V. Teague, and J. Pomares, ''A review of E-voting: The past, present and future,'' Ann. Telecommun., vol. 71, nos. 7–8, pp. 279–286, Aug. 2016.
[12] R. Taş and Ö. Ö. Tanriöver, ''A systematic review of challenges and opportunities of blockchain for E-voting,'' Symmetry, vol. 12, no. 8, p. 1328, Aug. 2020.
[13] P. Y. Ryan, D. Bismark, J. Heather, S. Schneider, and Z. Xia, ''Prêt à Voter: A voter-verifiable voting system,'' IEEE Trans. Inf. Forensics Security, vol. 4, no. 4, pp. 662–673, Dec. 2009.
[14] S. Bell, J. Benaloh, M. D. Byrne, and D. DeBeauvoir, ''STAR-Vote: A secure, transparent, auditable, and reliable voting system,'' in Proc. Electron. Voting Technol. Workshop/Workshop Trustworthy Elections (EVT/WOTE), 2013, pp. 1–20.
[15] S. Al-Maaitah, M. Qatawneh, and A. Quzmar, ''E-voting system based on blockchain technology: A survey,'' in Proc. Int. Conf. Inf. Technol. (ICIT), Jul. 2021, pp. 200–205
[16] Antoine Audras1, Louis Coudert1 "Analysis of Blockchain Solutions for E-Voting: A Systematic Literature Review" LIP6, CNRS, Sorbonne Université, 75005 Paris, France
[17] S. Gao, D. Zheng, R. Guo, C. Jing, and C. Hu, "An anti-quantum e-voting protocol in blockchain with audit function," IEEE Access, vol. 7, pp. 115304–115316, 2019. https://doi. org/10.1109/ACCESS.2019.2935895
[18] B. Shahzad and J. Crowcroft, "Trustworthy electronic voting using adjusted blockchain technology," IEEE Access, vol. 7, pp. 24477–24488, 2019. https://doi.org/10.1109/ ACCESS.2019.2895670
[19] K. M. Khan, J. Arshad, and M. M. Khan, "Investigating performance constraints for blockchain based secure e-voting system," Future Generation Computer Systems, vol. 105, pp. 13–26, 2020. https://doi.org/10.1016/j.future.2019.11.005
[20] C. K. Adiputra, R. Hjort, and H. Sato, "A proposal of blockchain-based electronic voting system," in 2018 Second World Conference on Smart Trends in Systems, Security and Sustainability (WorldS4), IEEE, 2018, pp. 22–27. https://doi.org/10.1109/ WorldS4.2018.8611593
[21] T. Dimitriou, "Efficient, coercion-free and universally verifiable blockchain-based voting," Computer Networks, vol. 174, p. 107234, 2020. https://doi.org/10.1016/j.comnet. 2020.107234
[22] X. Sun, Q. Wang, P. Kulicki, and M. Sopek, "A simple voting protocol on quantum blockchain," International Journal of Theoretical Physics, vol. 58, no. 1, pp. 275–281, 2019. https://doi.org/10.1007/s10773-018-3929-6
[23] D. Pawade, A. Sakhapara, A. Badgujar, D. Adepu, and M. Andrade, "Secure online voting system using biometric and blockchain," in Data Management, Analytics and Innovation, N. Sharma, A. Chakrabarti, and V. E. Balas, Eds., in Advances in Intelligent Systems and Computing, vol. 1042. Singapore: Springer Singapore, 2020, pp. 93–110. https:// doi.org/10.1007/978-981-32-9949-8_7
[24] [C. Braghin, S. Cimato, S. R. Cominesi, E. Damiani, and L. Mauri, "Towards blockchain-based E-voting systems," in International Conference on Business Information Systems, Springer, 2019, pp. 274–286. https://doi.org/10.1007/978-3-030-36691-9_24



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)