iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 11 **Issue:** I **Month of publication:** January 2023

DOI: https://doi.org/10.22214/ijraset.2023.48676

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 11 Issue I Jan 2023- Available at www.ijraset.com

Voting System Using Blockchain Technology

Tushar Ganotra[1], Sachin Garg[2]
[1, 2]*Department of Information and Technology, Maharaja Agrasen Institute of Technology Rohini*

Abstract: ***Electronic voting, or e-voting, has been used in various forms since the 1970s. B. Increase efficiency and reduce errors. However, wide adoption of such systems remains a challenge, especially in terms of improving resilience to potential failures. Blockchain is a disruptive technology of our time and promises to improve the overall resilience of electronic voting systems. The democratic system is fundamentally based on the right to vote that Allow individuals within the community to express their opinions. While voter turnout has declined in recent years, concerns about the integrity, security, and accessibility of the current voting system have increased. Electronic voting was introduced to address these concerns. However, it is not cost-effective and requires full oversight by a central authority. Blockchain is an emerging decentralized and decentralized technology that promises to improve many aspects of many industries. Extending e-voting to blockchain technology could be a solution to alleviating current concerns about e-voting. In this paper, I proposed a voting system that leverages the Ethereum blockchain and smart contracts to achieve voter management and verifiable voting records.***

Keywords: Blockchain , Blockchain Voting , Ethereum Voting , Voting system using solidity , Decentralized voting system

I. INTRODUCTION

Democracy is defined as the right of the people to choose their leaders. Elections are an important process that allows people to choose their leaders. Electoral systems must be democratic, independent and fair. Therefore, we need a transparent and safe process where everyone can freely share their perspectives. Many people in the world do not believe in voting systems. Traditional voting is controlled and full of middlemen. In addition, people complain about booth inspections, dummy voting, problems with proper supervision, large numbers of people queuing in front of booths, improper voting, pre-voting, duplicate voting, lack of legal enforcement, political We are dealing with a variety of issues such as issues. Instability and private encroachment Lack of awareness. In this context, approaches to voting are an evolving field. This development is primarily driven by efforts to make the system secure, auditable, and transparent. Given its importance, continuous efforts have been made to improve the overall efficiency and resilience of the electoral system. Electronic voting or e-voting plays an important role. Since its first use as punch card voting in the 1960s, electronic voting systems have made remarkable progress with adaptations using Internet technology. However, electronic voting systems must meet certain benchmark parameters to encourage wide adoption. Such parameters include, but are not limited to, voter anonymity, vote integrity, and disapproval.

Blockchain technology is the solution to the above problems with blockchain technology not only we can save lot of money and human resources but also make voting process more transparent and fair. Blockchain is one of the emerging technologies with a strong cryptographic foundation that allows applications to leverage these capabilities to deliver robust security solutions. A blockchain is like a data structure that manages and shares all transactions that occur during its creation. It is primarily a decentralized, decentralized database that maintains a complete list of constantly sprouting and growing datasets protected from unauthorized manipulation, tampering, and revision. Blockchain CORE Metadata, citation and similar papers at core.ac.uk Provided by UWL Repository allows every user to connect to the network, send new transactions to it, verify transactions and create new. Each block is assigned a cryptographic hash (which can also be treated as the block's fingerprint) that remains valid as long as the data in the block remains unchanged. As soon as the block is changed, the cryptographic hash is changed, indicating possible data modification by malicious activity. Due to its strong cryptographic foundation, blockchain is therefore increasingly being used to mitigate fraudulent transactions across various domains.

Objective of writing this paper is to propose a Voting system which is more secure , transparent, immutable, reliable and fair using blockchain technology , with the goal is to minimize the expense of running an election, while ensuring the integrity of election by fulfilling the security, privacy and compliance requirements.

1) Some of the disadvantages of Existing System Centralized architecture.
2) Attack prone.
3) Not trustable.
4) Non-transparent vote casting process.

This paper focuses on proposing the decentralized voting system that can replace traditional ways of voting with a new election system the has the potential to limit fraud while making the voting process traceable, verifiable and decentralized

II. LITERATURE SURVEY

1) In Khan et al. (2020) propose a way to eliminate the pain points of traditional elections using blockchain technology. This work establishes a decentralized rather than a centralized electronic voting method through blockchain technology and an easily accessible voting mechanism that guarantees the security of voter identification and data transmission and verification. It is intended to The proposed system uses multiple technologies such as Ganache, Truffle Framework and Metamask. A limitation of this system is that the votes cast are visible during voting and does not provide voter anonymity.
2) In Jorge Lopes (2019) Smart He proposes a blockchain-based electronic voting system using contracts. There are three categories of people who can communicate with the program: directors, developers and voters. Record, Creator, and Election are his three contracts. The record contract is responsible for storing voter registration information for authentication verification. After authentication, the API will send the transfer to the creator contract. Creator contracts are responsible for setting up new election contracts.
   An election contract is created and the address is sent to the creator contract for voting. Before the votes are included in the blockchain, they are encrypted using homomorphic encryption, a type of symmetric encryption.
3) Boshriet al. Proposed a blockchain-based democratic process based on the Ethereum network (Bosri et al., 2019). With this approach, the Electoral Commission set up an Ethereum account to store voter data. Voters without smartphone access can vote at designated polling places. You must complete the biometric authentication process before voting. Although it uses blockchain technology, there are many third parties involved in the system. Only cast votes added by third parties are recorded in the chain. In this case wrong tuning is possible . Election Administrator manages the election lifecycle.
4) The electronic voting system is described by Hjálmarsson et al. Presented. (2018) Create a decentralized electronic voting system using using blockchain as a service. There are two types of he nodes in this system: district nodes and starting nodes. A district node identifies each member, and each district node is equipped with a software application that connects to the boot node. Boot nodes allow district nodes to identify themselves and connect to them. This system fails to adequately protect voter privacy (Qu et al., 2020, Tso et al.,2019, Roh and Lee,2020) and does not consider the self-counting process.
5) In Shahzad et al. (2019), the framework proposed an improved form of electronic voting using blockchain. This integrity proof algorithm deals with block development, block locking, information management, blockchain design, especially voting machine network design. For block formation, the Electoral Commission (PO) verifies a voter's unique ID and biometrics. When a voter casts a ballot, the machine creates a hash using her SHA-256 and sends that data to the chairman to create a block. The main drawback of this strategy is that it requires more security, privacy, and transparency to be considered a fully trustworthy voting method (Toapanta et al., 2019).

III. TOOLS AND TECHNOLOGIES

A. *Blockchain*

Blockchain is best described as a public database that is updated and shared among many computers on a network. "Block" refers to the fact that data and state are stored in a contiguous stack or "block". When sending ETH to another person, the transaction data must be added to the block for the transfer to succeed. “Chain” refers to the fact that each block cryptographically references its parent block. A block's data cannot be changed without changing all subsequent blocks, requiring approval from the entire network.

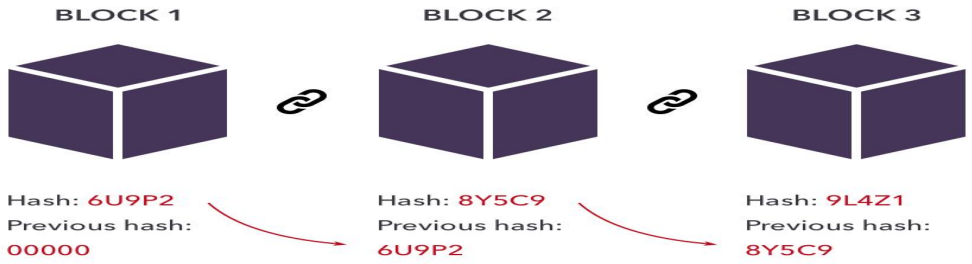


Fig- 1 (Chain of Blocks)

B. *Ethereum*

Ethereum is a decentralized software platform built suing blockchain technology. Natively known for its cryptocurrency Ether Ethereum can be used by anyone to create secure digital technology. While there are tokens intended to pay for work done to support the blockchain, participants can also use it to pay for tangible goods and service if accepted.

Ethereum is scalable, programmable, secure and decentralized. It is the blockchain of choice for developers and the companies building technology on it, transforming the way many industries work and how we conduct our daily lives. It natively supports smart contracts, essential for developing Dapps

C. *Dapps*

Decentralized Applications or Dapps are open source distributed software applications that run in a peer-to-peer decentralized network. Imagine a Twitter application on your mobile phone. You can post anything you want on Twitter, but unfortunately it's controlled by a single company that can remove tweets for violating community guidelines or for any other reason. But with the Twitter dApp, it's decentralized and not owned by anyone else. If you post something there, nobody can remove it, including its creator.

Some of the requirements for Dapp are -

1) *Open Source:* dApps should be open source and its code should be freely available for all. Any changes in the structure or working of the apps should only be taken with the agreement of the majority
2) *Decentralized:* dApps should be decentralized with all the information and operations stored on a public and decentralized Blockchain which would ensure security and transparency
3) *Incentive:* dApps should offer some sort of incentive to their users in the form of cryptographic tokens. These are sort of liquid assets and they provide incentives for users to support the Blockchain
4) *Protocol:* dApps should have a particular protocol to demonstrate proof of value. This means showing the value of a particular process in a way that can be easily verified by others.

D. *EVM*

The Ethereum Virtual Machine or EVM is a piece of Software that executes smart contracts and computes the state of Ethereum network after each new block is added to the chain.

The EVM sits on top of Ethereum's hardware and node network layer . Its main purpose is to compute the state of the network, execute various kinds of smart contracts and compile them into a readable format called "ByteCode".

E. *Nodes*

Nodes are the Real machines that store the EVM state. Nodes communicate with each other to disseminate information about EVM states and new state changes. Any user can request code execution by submitting a code execution request from a node.

The Ethereum network itself is the totality of all Ethereum nodes and their communications.

F. *Smart Contracts*

Smart contracts are similar to real-world contracts. The only difference is that they are digital. In fact, a smart contract is a computer program stored on the blockchain. A smart contract is self-executing code that executes when preset conditions of the parties are met. For example, a smart contract that issues tokens when someone deposits fiat currency. smart contracts enable secure and trusted transactions between anonymous parties without consulting a central authority. Ethereum smart contracts are written in Solidity.

Advantages of Smart Contract

1) *Speed, Efficiency, Accuracy:* Contracts are executed immediately once the conditions are met. Because smart contracts are digitized and automated, no paperwork is required and no time is spent reconciling errors that often occur with manual entry.
2) *Trust and Transparency:* No third parties are involved and encrypted records of transactions are shared between participants, so there is no need to question whether information has been falsified for personal gain.
3) *Security:* Blockchain transaction records are encrypted, making them extremely difficult to hack. Additionally, each record is linked to the previous and next record on the distributed ledger, requiring a hacker to change the entire chain to change a single record.

4) *Savings:* Smart contracts eliminate the need for intermediaries to process transactions, eliminating associated time delays and fees.

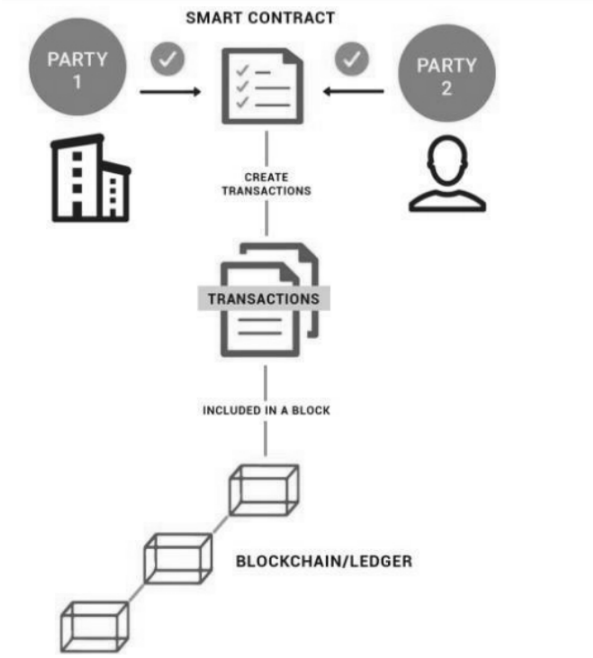


Fig – 2 (Smart Contract Flow Chart)

G. Solidity

Solidity is an object-oriented programming language specially developed by the Ethereum Network team for creating and designing smart contracts on the blockchain platform.

It is used to create smart contracts that implement business logic and generate chains of transaction records in blockchain systems.

It serves as a tool for writing machine-level code and compiling it on the Ethereum Virtual Machine (EVM).

H. Ether (ETH)

Ether (ETH) is the main token of the Ethereum blockchain and the second largest cryptocurrency in the world by market capitalization. Similar to Bitcoin, the largest cryptocurrency, Ether can be used to send payments directly to other people without the need for intermediaries like banks. Ethereum's long-term vision is to enable more than just financial transactions. Software developers can build applications on Ethereum, from decentralized money lending platforms to social networks.

Ether serves as the primary "fuel" for any Ethereum-based app. All activity on the blockchain requires large amounts of Ether, also known as “gas,” to send Ether to another user. And like cash, payments do not require third-party processing or authorization. 20 Tokens Transaction Fees from Yield Farming to Execution Functions such as Governance Voting: From payments to using dapps, every Ethereum action requires a fee.

I. Truffle

Truffle is the development environment, asset pipeline and testing framework for the Truffle Suite ecosystem.

Truffle is a very popular development framework for Ethereum dApp development and has a large community behind the tool. Additionally, Truffle uses his EVM as a foundation and one of its goals is to make smart contract development easier and more accessible.

Truffle offers several different features:

1) *Smart Contract Management:* This means that Truffle helps manage all smart contract artifacts used in dApps. Truffle takes care of that so you can focus on other parts of your development process. This also means that Truffle supports library linking, custom deployments, and more complex Ethereum dApps.

2) *Automatic Contract Revie:* Another useful feature of Truffle is that it supports automatic contract review. This means he can bring his bring his developer experience into the 21st century and create automated tests for every contract. The main advantage is that it shortens the smart contract development process.
3) *Scriptable Migration and Deployment:* Truffle allows you to create deployment scripts that can react to your dApps changing over time. This means that smart contracts can be maintained long-term into the future.
4) *Network Management:* Truffle helps you manage your network by managing your artifacts so you can focus on other tasks.
5) *Interactive Console:* Truffle has an interactive console where you can access all the Truffle commands and contracts you've created.

J. *Ganache*

Ganache is a private Ethereum blockchain environment that can emulate the Ethereum blockchain, allowing you to operate smart contracts on your own private blockchain.

Here are some features provided by Ganache:

1) Shows blockchain log output
2) Provides advanced mining control
3) Built-in block explorer
4) Ethereum blockchain environment
5) Ganache has a desktop application and command line tools

K. *Metamask*

MetaMask is a cryptocurrency wallet available as a browser extension that helps store tokens, interact with decentralized applications, and trade on Ethereum. By connecting the user to his MyEtherWallet, MetaMask eliminates the need to enter a private key when performing each transaction when creating, storing or trading tokens. Users can store and manage Bitcoin, Ethereum, and other cryptocurrencies with a blockchain wallet available as a digital or online wallet. Blockchain wallets enable the transfer of cryptocurrencies, prevent theft of crypto assets, and allow users to convert them into their local currency as needed.

L. *Remix IDE*

The Remix Project is a development tool platform that uses a plugin architecture. It contains sub-projects such as Remix Plugin Engine, Remix Libraries and of course Remix IDE. Remix IDE is an open source web application. It facilitates a rapid development cycle and features various plugins for development of interactive GUI.

IV. PROPOSED SYSTEM

We proposed to design an existing online voting system integrated with blockchain technology.

The proposed system has the following advantages over the existing system:

1) Users can vote from anywhere in the world until they obtain citizenship of that country.
2) Votes are tamper-proof as they are stored on the blockchain.
3) Not having to wait in line to vote saves a lot of time and effort.

The proposed system has 2 modules

a) *Admin Module*: Admin or Administrator is basically an authorized person who is responsible for creating an election, changing the state of the election, and registering voters into the contract so they can cast a vote.

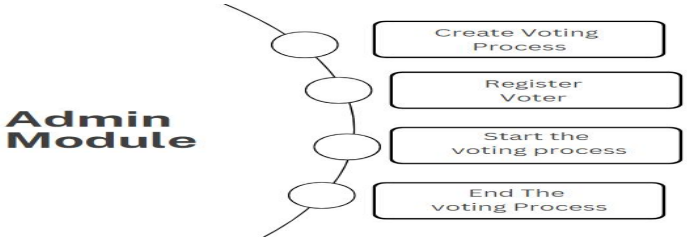


Fig – 3 (Admin Module)

b) *Voter Module:* Voters, or users, are those who can cast their vote only if they are registered. Voters can cast a vote only once (a vote will not be counted if a voter tries to cast a vote multiple times). Once a vote is cast, it can not be changed or undone. A voter's vote will be anonymous or secret (no one will know who the voter is or who he voted for).

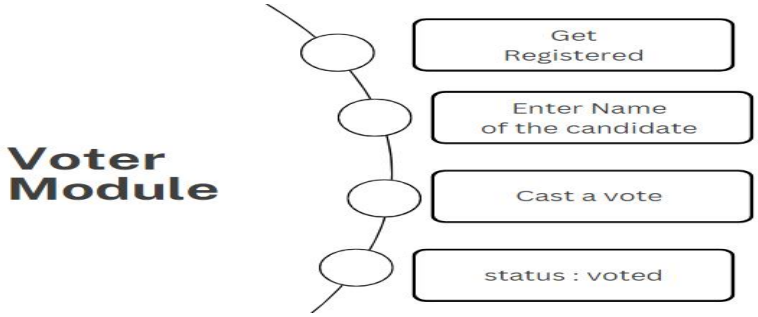


Fig – 4(Voter Module)

Below is the complete flow of how blockchain based voting system work

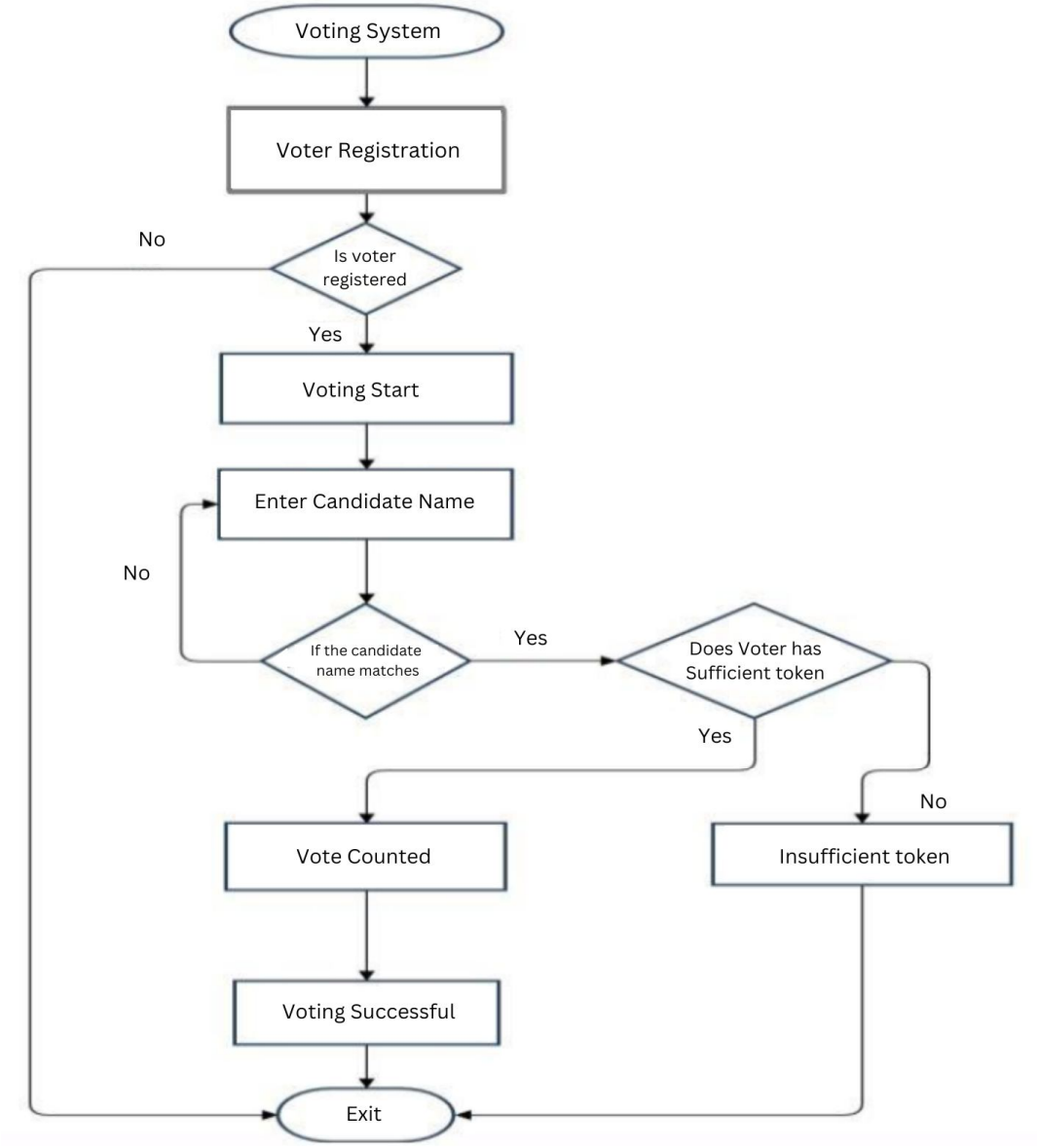


Fig – 5 (Flow Chart)

The proposed voting mechanism is divided into four phases

- *First Phase: Registration Phase*

The registration phase is the first phase in which voters are added to the smart contract by the admin (as only those users can vote whose public keys are registered into the contract along with their name).
It is the administrator's responsibility to manually add all public keys and names of voters to the contract prior to beginning of second phase of the election.

- *Second Phase: Voting Start phase*

Voting Start phase or second phase, is implemented once voters are registered in the contract by the admin.
Admin is responsible for staring this phase by changing the state of the contract to 1. In this phase, voters can cast their vote by adding the name of the respective candidate. Once the voter cast a vote it gets checked by the contract if the name entered by the voter of respected candidate matches with that registered in the smart contract then only the vote is counted otherwise it will not be counted . Once a vote is casted, it can not be changed or undone.
A voter is only allowed to vote once.
Once a voter has cast a vote, his status will be changed to "voted".

- *Third Phase: End Phase*

The end phase, or third phase, comes when the start phase, or second phase, is over, which means after voters have cast their respective votes. Admin is responsible for starting this phase by changing the state of the voting system to 2.
When the state is changed to 2, the voting process is stopped, and no one, not even registered users, can vote after that.

- *Fourth Phase: Result Phase*

The result phase is the final phase in which all the votes that were casted by the voters in the second phase are counted by the smart contract, and the candidate with the maximum number of votes is displayed as the winner of the election.

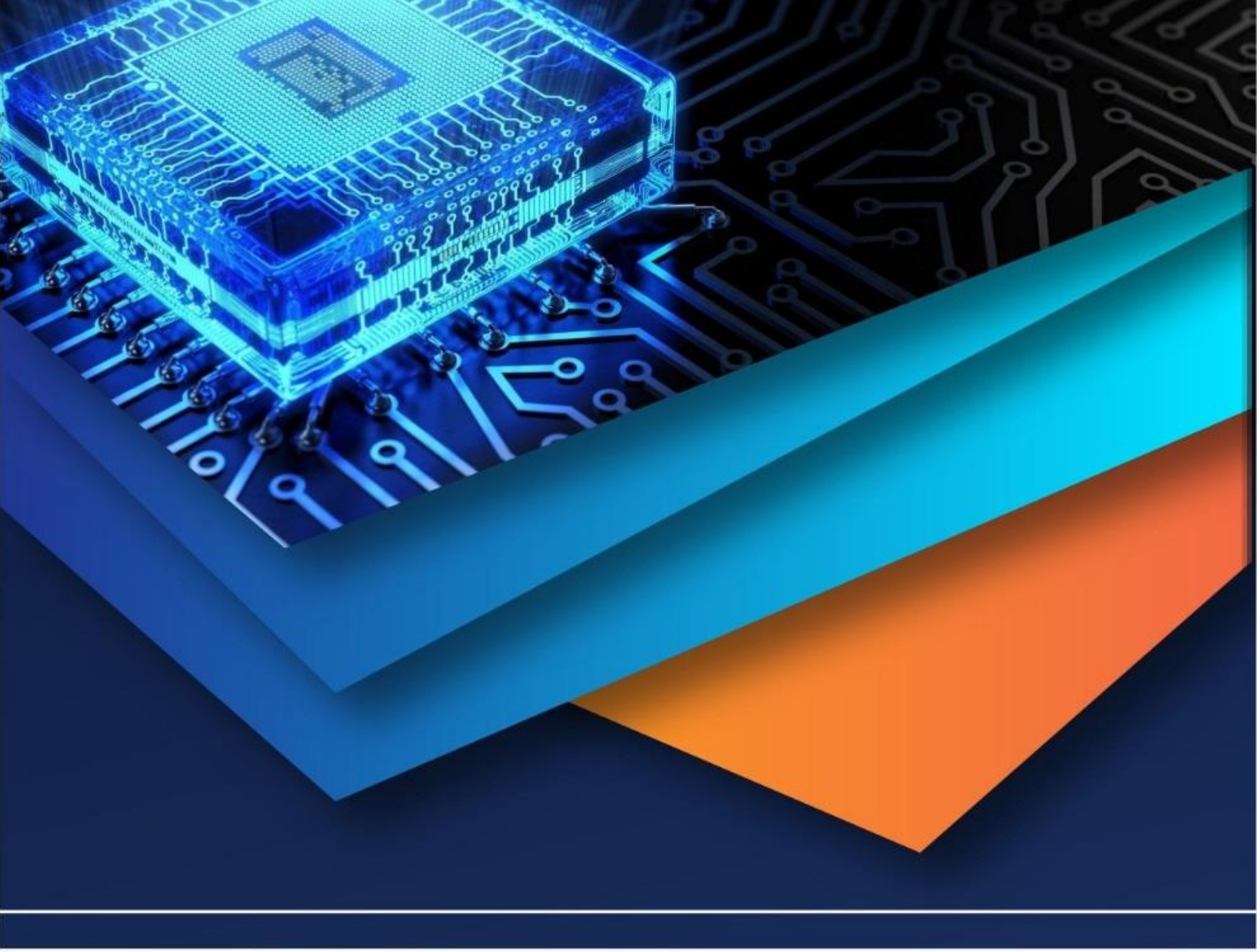
V. CONCLUSIONS

A credible and honest electoral system is essential for a democratic society. Democracy depends on trustworthy elections, and citizens must trust their electoral system for a strong democracy. However, traditional paper-based elections do not provide credibility. The idea of employing a digital voting system to make the popular voting process cheaper, faster and easier is appealing in today's world.
Making the election process cheaper and faster normalizes it in the eyes of voters, removes power barriers between voters and elected officials, and puts some pressure on elected officials. It also opens the door to more direct forms of democracy, allowing voters to express their views on individual bills and proposals.
This paper introduced a blockchain-based electronic voting system that leverages smart contracts to enable secure and cost-effective elections while maintaining voter privacy.
This research paper shows that blockchain technology offers new ways to overcome the limitations and barriers to acceptance of electronic voting systems, ensuring election securityand integrity, and laying the foundation for transparency

REFERENCES

[1] Wolchok, Scott, et al. "Security analysis of India's electronic voting machines." Proceedings of the 17th ACM conference on Computer and communications security. ACM, 2010.
[2] Ohlin, Jens David. "Did Russian cyber interference in the 2016 election violate international law." Tex. L. Rev. 95 (2016): 1579.
[3] Ayed, Ahmed Ben. "A conceptual secure blockchain-based electronic voting system." International Journal of Network Security & Its Applications 9.3 (2017): 01-09.
[4] Hanifatunnisa, Rifa, and Budi Rahardjo. "Blockchain based e-voting recording system design." 2017 11th International Conference on Telecommunication Systems Services and Applications. IEEE, 2017.
[5] Yu, Bin, et al. "Platform-independent secure blockchain-based voting system." International Conference on Information Security. Springer, Cham, 2018.
[6] Himanshu Agarwal and GN Pandey. Online voting system for india based on aadhaar id. In 2013 Eleventh International Conference on ICT and Knowledge Engineering, pages 1–4. IEEE, 2013.
[7] Soumyajit Chakraborty, Siddhartha Mukherjee, Bhaswati Sadhukhan, and Kazi Tanvi Yasmin. Biometric voting system using aadhar card in india. International journal of Innovative research in Computer and Communication Engineering, 4(4), 2016.

[8] Basit Shahzad and Jon Crowcroft. Trustworthy electronic voting using adjusted blockchain technology. IEEE Access, 7:24477–24488, 2019.
[9] Scott Wolchok, Eric Wustrow, J Alex Halderman, Hari K Prasad, Arun Kankipati, Sai Krishna Sakhamuri, Vasavya Yagati, and Rop Gonggrijp. Security analysis of india's electronic voting machines. In Proceedings of the 17th ACM conference on Computer and communications security, pages 1–14, 2010.
[10] Komal K. Sharma, Prof. Mrunalinee Patole, "Securing E-Voting System using Blockchain" International Journal of Innovative Research
[11] Narayanan, A., Bonneau, J., Felten, E., Miller, A. and Gold, S. (2015) Bitcoin and Cryptocurrency Technologies, Chapter 2 and 3, Draft October 2015.
[12] Rockwell, M. (2017) Bitcongress – Process for block voting and law, http://bitcongress.org/ last accessed: December 2017.
[13] Rosenfeld. M. (2017). Analysis of hashrate-based double-spending. [Online]. Available: http://arxiv.org/abs/1402.2009 last accessed: December 2017.
[14] Rura L., Issac B., and Haldar M. K. (2016) Implementation and evaluation of steganography based online voting, International Journal of Electronic Government Research.
[15] Ryan, P. Y. A, (2008) Prêt à Voter with Paillier Encryption, in the Mathematical and Computer Modelling, in Vol. 48, issue 9-10,1646-1662, 2008.
[16] Shahandashti, F. S. and Hao, F. (2016) DRE-ip: A Verifiable E-Voting Scheme without Tallying Authorities, the 21st European.
[17] Symposium on Research in Computer Security (ESORICS), 2016. Shahandashti S. F. and Hao, F. (2016). DRE-ip: A Verifiable E-Voting Scheme Without Tallying Authorities. Cham: Springer International Publishing, 2016, pp. 223-240.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY