Building Resilient and Trustworthy Voting Systems with Ethereum Blockchain Technology

Sameer Tembhurney[1], Dr. Tripti Arjariya[2]

[1] *M. Tech Student, Department of Computer Science & Engineering, Bhabha University Bhopal, Madhya Pradesh, India*

[2] *Professor, Department of Computer Science & Engineering, Bhabha University Bhopal, Madhya Pradesh, India*

ABSTRACT

It is possible to lower the risk of fraud caused by database manipulation in electronic voting systems by incorporating blockchain into the database distribution. The proposed system explained in this study includes the use of blockchain algorithms to record voting results from each voting location. Unlike Bitcoin's proof-of-work mechanism, the suggested system depends on pre-defined power-ups for each node in the blockchain. This system allows online voting, providing voters the ease of casting their votes from any location and at any time, which in turn enhances voter turnout. By distributing the database among several users, the proposed system decreases the chances of fraud and manipulation while also offering a more accessible and efficient voting process. Overall, the integration of blockchain technology into electronic voting systems has the potential to boost the security, dependability, and fairness of elections.

Keyword : - *Ethereum Blockchain, Electronic Voting, Smart Contracts, Decentralization, Transparency, Security*

1. INTRODUCTION

The term "blockchain revolution" can encompass a variety of ideas, which may be confusing for people and organizations. However, it essentially refers to the concept of decentralized records, where transaction data is distributed across multiple network nodes rather than being stored on a single centralized server. While the idea of blockchain technology originated in the 1980s, it was Bitcoin's emergence in 2009 that popularized it. Although it was not the first cryptocurrency, many credit Bitcoin with catalyzing the development of paperless, digital financial transactions with physical assets. However, it is worth noting that without centralized controllers overseeing transactions, this asset/currency might lack fundamental value. The blockchain's mathematical equations provided the basis for its development. Elections play a crucial role in any democratic system. With the introduction of internet technology, ensuring a fair election process has become even more critical. External factors could potentially impact a county's administration and processes, making it imperative to prioritize fairness. Many nations have dealt with authoritarian governments in the past, which is always a challenging experience for the average person.

The theft of the common people's fundamental human rights and the freedom enshrined in their constitution has left them vulnerable. In such circumstances, it is crucial to establish a fair and impartial election system for the nation's proper growth and development. Election voting machines (EVMs) have faced criticism in India due to inconsistencies in results reporting, as well as concerns about vulnerabilities and tampering. Moreover, current voting procedures have been exploited to gain control, with instances of fraud, including voter fraud, ballot fraud, and booth capturing, shaking public trust in the electoral process. Nevertheless, making the voting process more equitable, transparent, and accountable could help resolve the problems associated with the current system. It should be noted, however, that although the current method guarantees voter anonymity, it is not entirely transparent, and voters must have blind faith in election results due to the lack of systemic verifiability. Recently, internet-based voting systems have gained popularity, and the Telangana State Election Commission developed a mobile-based electronic voting application that was tested in one district.

The protection and security of voter data is crucial during the voting process, which is facilitated by the Ethereum blockchain's secure and efficient voting mechanisms. Since the data collected during the voting process is highly

sensitive, tampering or unauthorized access must be prevented, and blockchain technology can ensure this. The use of Solidity in developing smart contracts for this project makes the code used in the voting process transparent and auditable, which further strengthens the security and trust in the system.

2. METHODOLOGY

2.1 Working of Blockchain

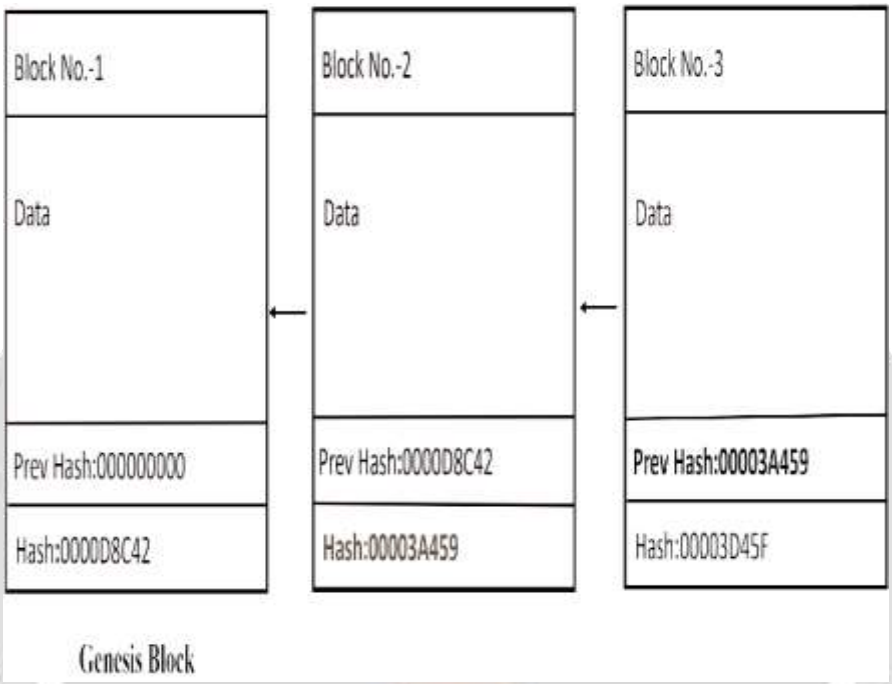


Fig- 1: Working of Blockchain

The mechanism of blockchain technology involves a network of computers that maintains a secure and decentralized ledger for recording transactions. This ledger, which is composed of linked and encrypted blocks, grows continuously and each block is comprised of a cryptographic hash of the previous block, a timestamp, and transaction data.

The blockchain is highly resistant to tampering and hacking, as any attempt to modify a block will alter all subsequent blocks, and the information stored in a block cannot be changed or deleted without the consensus of the network. This provides a high level of security to the blockchain, making it difficult for malicious actors to tamper with the data stored within it. Other participants in the network can easily detect any attempts to alter the blockchain, further reinforcing its security.

Participants in a blockchain network, known as nodes, collaborate to verify transactions and incorporate them into the blockchain. Whenever a new transaction is initiated, it is sent to all nodes in the network. The nodes then validate the transaction by verifying its authenticity and ensuring that the individual initiating the transaction has adequate funds. Once a majority of nodes agree on the transaction's validity, it is recorded in a block, which is subsequently broadcast to the whole network and appended to the blockchain.

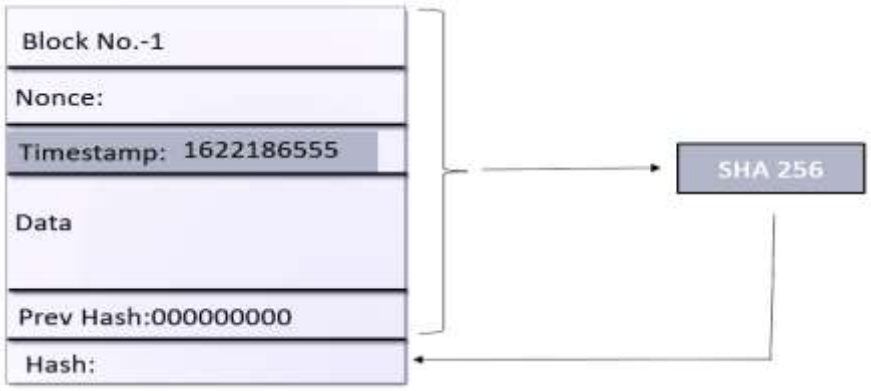


Fig- 2: SHA-256 Algorithm

Smart contracts on a blockchain operate through "if/when...then" statements that are coded and stored on the blockchain. Once predetermined conditions are confirmed, a network of computers executes the specified actions, which can include disbursing funds, registering a vehicle, issuing notifications, or generating a ticket. Upon completion of the transaction, the blockchain is updated, ensuring that it cannot be altered, and only authorized parties can access the results.

To ensure successful execution of the activity, a smart contract can include multiple conditions that reassure all participants involved. The participants must agree on the rules that govern the transactions and consider any potential exceptions while also designing a framework for dispute resolution. Additionally, the representation of transactions and their associated data on the blockchain must also be decided by the participants.

2.2 MetaMask

Metamask, a cryptocurrency wallet, enables users to interact with the Ethereum Blockchain, including exchanging tokens and cryptocurrencies based on Ethereum and managing their account keys. Users can connect to decentralized networks through a web browser or mobile device's built-in browser app. To establish a connection between a decentralized network and Metamask, developers can use the Javascript plugin Web3js. Ethers are used as gas to complete transactions between Metamask and smart contracts.Metamask is a blockchain wallet that allows users to manage their funds and complete transactions using a web browser extension. Once a transaction is initiated, a Metamask window pops up to request confirmation from the user before the transaction is executed.

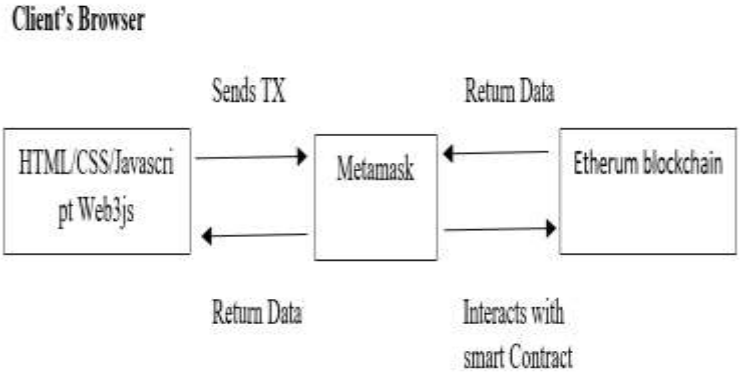


Fig- 3: Working of MetaMask

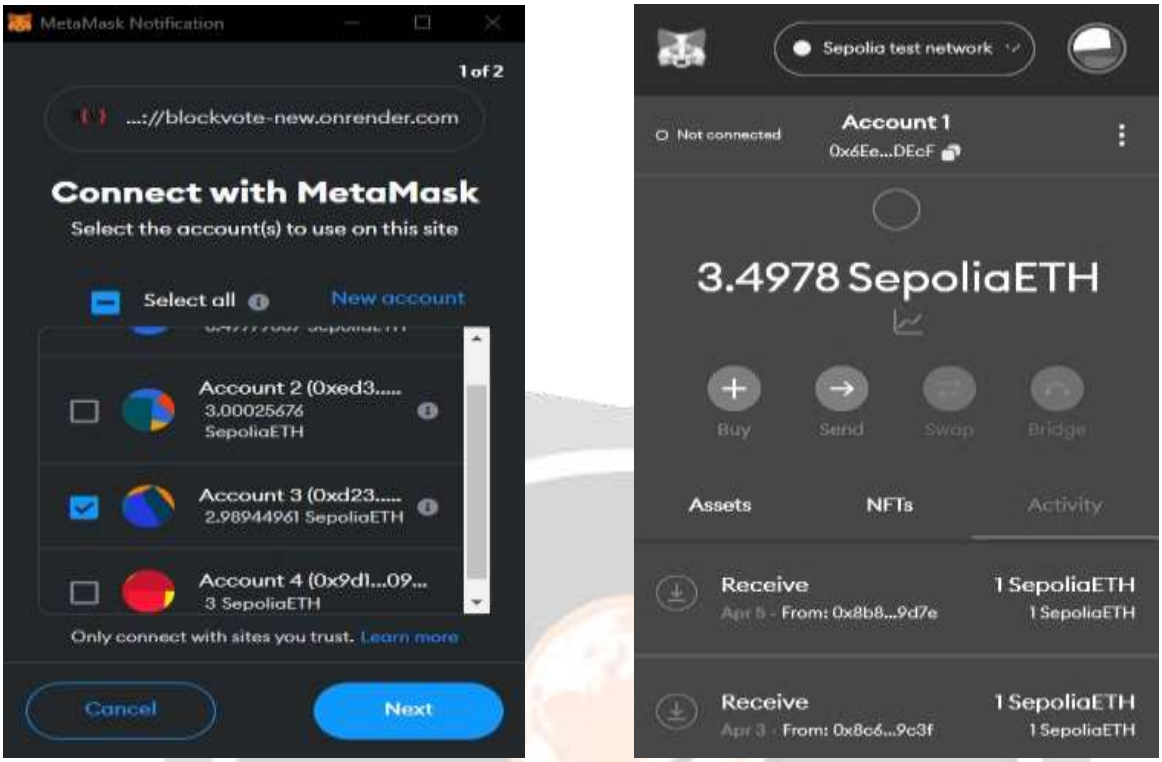


Fig- 4: MetaMask Wallet

2.3 Ethereum Virtual Machine

The Ethereum Virtual Machine (EVM) is designed as a secure runtime environment for Ethereum's smart contracts. It operates in isolation from the rest of the system, ensuring that repeated calls to a particular function on the EVM will not modify data or programs.

The Ethereum Virtual Machine (EVM) enables the execution of scripts on the Ethereum blockchain, allowing for the implementation of various activities. Creating new tokens on the Ethereum blockchain is made simple by the EVM, which executes a script consisting of instructions that guide the computer on how to perform a particular function. Access to any network node is required to execute the necessary commands and create new tokens on the blockchain using the EVM.

Ethereum Virtual machine has two parts:

i. EVM (the part that runs solidity source code)
ii. Uncles

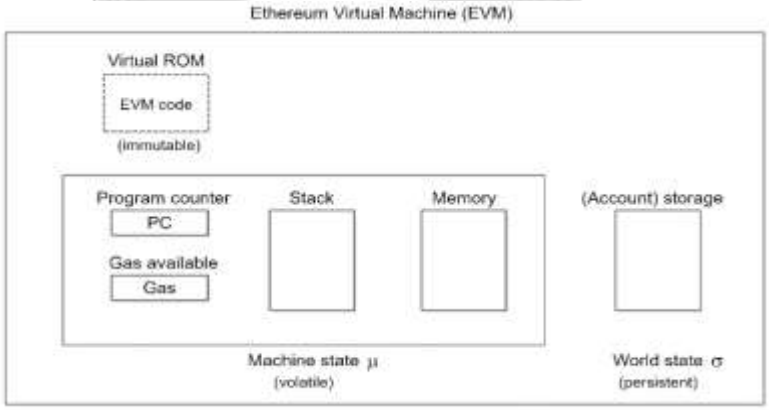


Fig- 5: Working of Ethereum Virtual Machine

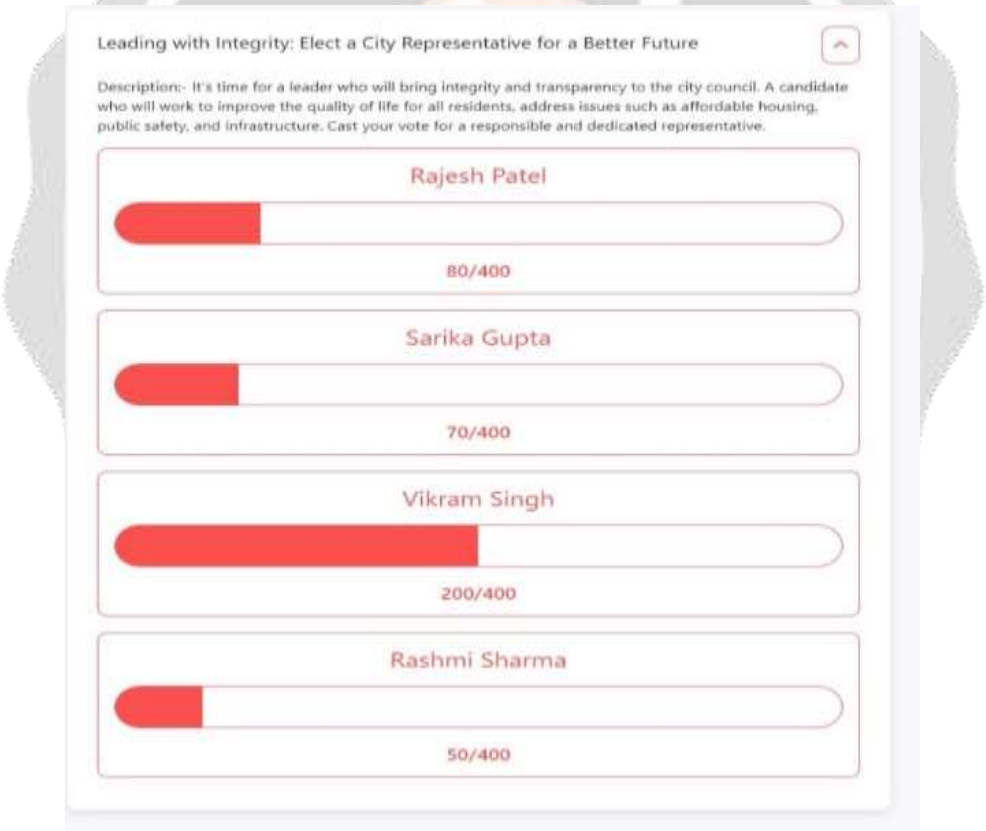
2.4 Ether.js

Originally created to support ethers.io, the ethers.js library has evolved into a versatile and comprehensive library for interacting with the Ethereum Blockchain and its ecosystem.
It is important to interface with a hub that can gain information from the blockchain and compose new exchanges. This association can be laid out in different ways, including straightforwardly from an internet browser, a product on a PC, or a back-end server. When the association is laid out, the hub can be utilized to distribute new exchanges and get information about digital currencies and NFTs. This association can empower the making of a completely decentralized site that supports decentralized applications. The ethers.js library can be utilized as a minimized and complete library for cooperating with the Ethereum Blockchain and its environment.
Ether.js Modules:

i. Ethers.Contract
ii. Ethers.Utils
iii. Ethers.Provider
iv. Ethers.Wallet

3. RESULT

The experimental result obtained by performing the project is as follow:



Blockchain-based casting a ballot framework is plan to give quick and productive strategy to cast a ballot counting, Bringing about prompt political race results. The principal objective of fostering this framework is to resolve the issue of broadened sitting tight period for acquiring results. With our task, the outcomes can be gotten in only second. Essentially diminishing the stand by time.

4. CONCLUSIONS

This paper proposes an electronic voting system that addresses several problems associated with traditional voting methods. Through the use of the internet, citizens can cast their votes from any location, at any time, thanks to this system's security and convenience. Blockchain technology is used to ensure that the vote data is stored in a tamper-proof manner, and no central authority can modify it. This produces an open-source and transparent voting platform that is available to everyone.

The proposed electronic voting system is intended to be efficient, user-friendly, and speedy, with immediate results. This would eliminate the need for manual counting, reducing both the time and resources required to obtain election results. In addition, the system would be available on any device with internet access, enabling all citizens to participate in the voting process, regardless of their technical abilities. Its implementation is a significant step forward in modernizing the electoral process, as it makes voting more convenient, efficient, and secure, encouraging greater participation while ensuring the accuracy of every vote. This system offers a practical and effective solution to conducting elections, and if widely adopted, has the potential to improve the democratic process on a global scale.

6. REFERENCES

[1]. S. Tandon, N. Singh, S. Porwal, Satiram and A. K. Maurya, "E-Matdaan: A Blockchain based Decentralized E-Voting System", 2022 IEEE Students Conference on Engineering and Systems (SCES), 2022, pp. 1-6, doi: 10.1109/SCES55490.2022.9887759.

[2]. Tanikella Sai Charan, Srinanda Pentapati, Mrs. R. Prema, "A Research Paper on E-Voting Using Blockchain Technology", in International Research Journal of Engineering and Technology (IRJET) March 2022, India.

[3]. Pradeep Katta, Mohammed Oviaz, Prabaakaran, Divya, Jayashree, Keerthika, "Smart voting using Fingerprint, Face and OTP Technology with Blockchain" in Institute of Physics (IOP) February 2021, India.

[4]. Syada Tasmia Alvi, Mohammed Nasir Uddin, Linta Islam, "Digital Voting: A blockchain based E-voting system using Biohash and smart Contract", in IEEE Third International Conference on Smart Systems and Inventive Technology (ICSSIT) 06 October 2020, India.

[5]. Spurthi Anjan, Johnson P Sequeira, "Blockchain based E-voting system for India using UIDAI's adhaar", in Journal of Computer Science Engineering and Software Testing by MAT Journals September 2019, India.

[6]. T ElGamal (1985), "A public Key Cryptosystem and a Signature Scheme Based on Discrete Logarithms", issued in IEEE Trans. Info. Theory, Volume 31.

[7]. J Jan, Y Chen, Y Lin (16−19 October 2001), "The Design of Protocol for e-Voting on the Internet", Proceedings IEEE 35th Annual 2001 International Carnahan Conference on Security Technology, London, England.

[8]. X. Xu, I. Weber, M. Staples, L. Zhu, J. Bosch, L. Bass, C. Pautasso and P. Rimba, "A Taxonomy of Blockchain-Based Systems for Architecture Design", issued in IEEE Conference on "Software Architecture (ICSA), Gothenburg", Sweden, 2017.

[9]. Jinn-Ke Jan, Yu-Yi Chen, and Yi Lin. "The Design of Protocol for E-Voting on the internet in Security Technology", issued on 2001, IEEE 35th Carnahan Conference on, pages 180 - 189. IEEE, 2001.

[10]. Hiroki Watanabe, Shigeru Fujimura, Atsushi Nakadaira, Yasuhiko Miyazaki, Akihito Akutsu, and Jay Junichi Kishigami. "Blockchain contract: A complete consensus using blockchain", In Consumer Electronics (GCCE), 2015 IEEE 4th Global Conference on, pages 577–578 IEEE, 2015.

[11]. Hjalmarsson, Fririk., Gunnlaugur K. Hreiarsson, Mohammad Hamdaqa, ´and G´ısli Hjalmt ´ ysson. "Blockchain based E-Voting system." issued on 2018 11th Conference on Cloud Computing, pp. 983 - 986. IEEE, 2018.

[12]. Jayesh Solanki , Divykant Meva, "Comparative Study Indian Electoral Reforms in Indian Context", Issue 27-28 Sept. 2019, IEEE

[13]. Z.A. Usmani, Kaif Patanwala, Mukesh Panigrahi, Ajay Nair, Conference on "Multi-purpose platform Independent Online Voting system", Issue 17 - 18 March 2017, IEEE

[14]. Bhushan M. Pawar, Sachin H. Patode, Yamini R. Potbhare, Nilesh A. Mohota, "An efficient and secure students online voting application", Issue 8 - 10 Jan. 2020, IEEE

[15]. Ramya Govindaraj, P Kumaresan, K. Sree harshitha, "Online Voting System using Cloud", Issued on 24-25 Feb. 2020, IEEE