iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 11 **Issue:** VII **Month of publication:** July 2023

DOI: https://doi.org/10.22214/ijraset.2023.54818

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 VII Jul 2023- Available at www.ijraset.com

E-Voting using Blockchain

Gnanavel Udayar
Department of Master of Computer Applications, Vivekanand Education Society's Institute of Technology (VESIT), Mumbai

Abstract: ***In the era of Industry 4.0, blockchain technology is quickly gaining popularity due to its unique features, such as decentralization, transparency, immutability, and security. These features make it suitable for building various applications in different industries. One such application is E-Voting. Voting is an essential tool for any democratic government. It is the most important factor that makes a government "for the people and by the people". Even though the current system has a strong foundation, there are some issues with it. One of the major issues is that if a voter stays outside of his or her home constituency on election day, it's not simple to vote in any nearby constituency. Some of the other common issues are security breaches like data leaks, vote tampering, etc. Furthermore, it requires a lot of paperwork and time to conduct an election. Therefore, this paper provides an overview of developing a reliable and secure e-voting system using blockchain technology that can help in reducing fraud and ensuring the integrity of the election process, and it also provides an added advantage of mobility.***
Keywords: Blockchain; Etheruem; Web3.js; E-Voting

I. INTRODUCTION

Traditional democracies have relied on paper ballots and electronic voting machines for conducting elections. However, concerns have been raised about the susceptibility of electronic voting machines to tampering, despite existing system checks, safeguards, and protocols. Critics argue that the proprietary code underlying these machines can be manipulated, casting doubt on the integrity of election results. In response to these challenges, governments worldwide have started exploring the potential of blockchain technology to address the issue of tamper-proof and transparent elections. The goal is to establish a system that fosters trust in the accuracy of data and eliminates the possibility of counterfeiting. By leveraging the inherent security and transparency of blockchain, governments aim to enhance the integrity and credibility of general elections.

An electronic voting system enables citizens to exercise their democratic rights conveniently from any location within the country. However, various sectors, including innovation, social media, and political organizations, have raised concerns and debates surrounding online voting. Electronic voting has the potential to revolutionize the traditional voting system by simplifying the process and making it more accessible to voters. The internet's widespread availability allows democratic structures to be displayed on any computer with an internet connection, ensuring that voters can easily access the voting platform.

Implementing online voting methods can reduce costs associated with physical voting booths and provide additional options for voters to cast their ballots. This approach eliminates the need for long queues at polling stations and offers improved accessibility for individuals with mental or physical disabilities, those serving in the military or living abroad, and those facing transportation challenges. Moreover, online voting platforms offer the flexibility for voters to submit their ballots at any convenient time. The web-based voting system also presents an opportunity to engage young voters between the ages of 18 and 30, who are often considered hard to reach through traditional means. Online voting systems have the potential to enhance the democratic process by making it more accessible, cost-effective, and convenient for citizens to exercise their voting rights. The internet serves as a platform to attract and engage diverse groups of voters, including those who may face barriers to traditional voting methods.

II. LITERATURE SURVEY

To develop a comprehensive understanding and capture essential concepts relevant to this study, previous research and existing work in the field have been thoroughly reviewed and analyzed. While conducting a thorough literature review, we found a variety of terms that are commonly utilized in the development of blockchain applications. Presented below are a few examples of these terms:

A. Web3.js

Web3.js is a powerful JavaScript library that empowers developers to engage with the Ethereum blockchain and construct decentralized applications (dApps). This library offers a comprehensive range of functions and tools, enabling seamless communication with smart contracts, facilitating data retrieval and storage on the blockchain, and managing user accounts.

Acting as a crucial intermediary between web browsers and the Ethereum network, Web3.js enables the creation of user-centric and decentralized web applications that harness the potential of blockchain technology. By streamlining the integration of blockchain capabilities into web applications, it grants developers easy access to Ethereum's rich features and facilitates seamless interactions within the decentralized ecosystem.

B. Ethereum

Ethereum, an open-source and decentralized blockchain platform, plays a pivotal role in enabling the generation and execution of smart contracts. Ether (ETH), its native cryptocurrency, is employed within the network to facilitate transactions and incentivize participants. A prominent feature of Ethereum is its capacity to create and deploy self-executing smart contracts, which adhere to predetermined rules and conditions. These smart contracts empower the development of decentralized applications across diverse industries like finance, gaming, and supply chain management. In essence, Ethereum provides a robust foundation for developers to construct decentralized applications, execute secure transactions through smart contracts, and foster innovation within the blockchain ecosystem, all while promoting transparency and trust.

C. Truffle

Truffle, a well-known development framework, has gained popularity among Ethereum-based decentralized application (dApp) developers. It offers a comprehensive suite of tools, libraries, and utilities that streamline the entire dApp development process. Truffle simplifies various tasks including smart contract compilation, deployment, testing, and management. It seamlessly integrates with different blockchain networks, including Ethereum and its test networks. Leveraging Truffle, developers can write and compile smart contracts in Solidity, deploy them onto the blockchain, and automate testing procedures to ensure the reliability and functionality of their contracts. Moreover, Truffle provides a development console, a built-in build pipeline, and debugging capabilities to enhance the overall development experience. Its widespread adoption by blockchain developers attests to its effectiveness in accelerating the development and deployment of Ethereum-based dApps.

D. Ganache

Ganache, an integral component of the Truffle suite, serves as a personal blockchain development tool. It grants developers the ability to generate and oversee their own local Ethereum blockchain networks specifically designed for testing and development endeavors. By utilizing Ganache, developers can simulate blockchain environments featuring preloaded accounts, enabling them to thoroughly test their smart contracts and decentralized applications (dApps) in a controlled and predictable manner. Ganache is equipped with a user-friendly interface, an assortment of valuable tools, and adaptable customization options, rendering it a favored selection among Ethereum developers seeking to streamline their development and debugging processes.

E. Metamask

MetaMask is a popular browser extension and cryptocurrency wallet that allows users to interact with Ethereum-based decentralized applications (dApps) directly from their web browsers. It serves as a bridge between web browsers and the Ethereum blockchain, providing a secure and user-friendly interface for managing Ethereum accounts, storing cryptocurrencies, and interacting with smart contracts. MetaMask simplifies the process of accessing and utilizing dApps by eliminating the need for users to run their own Ethereum nodes or manage private keys manually.

III. METHODOLOGY

The proposed methodology for EVoting application consists of multiple phases. The first phase is adding all the voter details in the system. Every participant in the system has a specific role. The different roles are Administrator and Voter. Administrator is the one who takes care of everything related to conducting an election. The administrator will add all the information of voters along with information about the election like the name of the election, when it will start, when it will end, etc.

The next phase is the voting phase. During the voting phase, the user will enter his unique identification number. This identification number will be matched against the data that is stored by the administrator in the system. If the information is found, it will be fetched and displayed to the voter to confirm his identity. After confirmation by the voter, the system will generate an OTP and send that to the voter registration mobile number, which will be valid for 2 min. After the OTP verification, the voter will see a list of election candidates of his constituency. The voter can choose anyone among them and cast a vote for them. Once the vote has been verified, it will then be turned into a block and added to the blockchain.

The last phase is the Result declaration. On the day of result, every voter will receive a message from the system, stating that their vote has been successfully counted and included in the final result. Also the voter can enter his unique identification number on the system to verify the inclusion of their vote in the overall count.

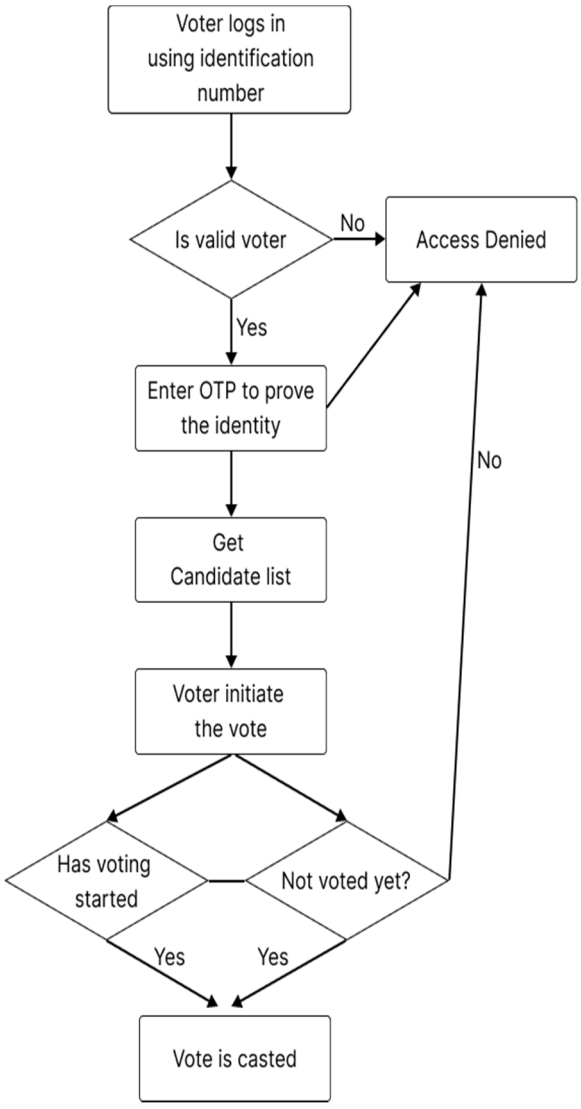
IV. PROCESS FLOW FOR A VOTER ON THE PROPOSED SYSTEM

A. Upon accessing the proposed system, the voter commences the process by logging in with their unique identification number. Subsequently, the system verifies the validity of the voter's registration. To be deemed a valid registered voter, the identification number provided must be present in the voter mapping, with the identification number serving as the key. Additionally, the system checks that the voter's age exceeds 18 and confirms their vital status as alive.

B. In the second step, once the voter's eligibility is confirmed, the system will display the voter's identification number specific to their constituency, along with the available list of candidates. Voters can then proceed to select their preferred candidate for voting.

C. During this step, the voter begins the voting process. Before the actual vote is recorded, the system verifies certain conditions. Firstly, it checks if the voting lines for the election are open. Additionally, it verifies several criteria such as the voter's age being above 18, ensuring that the voter has not already voted, and confirming that the candidate the voter initiated the vote for belongs to the same constituency as the voter. If all conditions are met, the vote is successfully recorded in the blockchain.

Flow Diagram



ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 11 Issue VII Jul 2023- Available at www.ijraset.com

V. IMPLEMENTATION

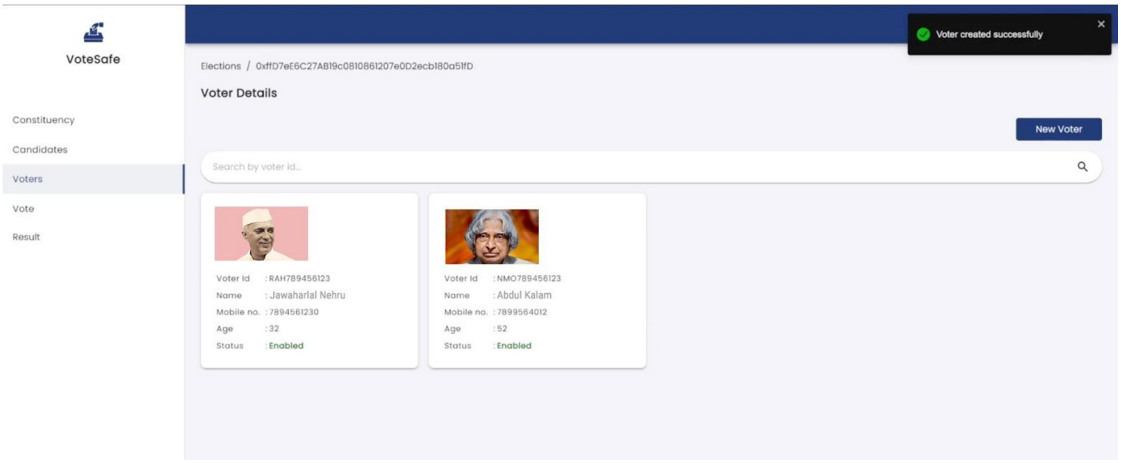
We have created a web portal using React for the frontend and Node.js for the backend. The election administrator can create and modify the voter and candidate lists, as well as determine the voting start and finish timings.

In the backend, we utilize MongoDB to store user information, such as names, emails, and passwords, for the election administrator. This data is used for authentication purposes within the system. All other data like who has voted to whom are stored in the Ethereum blockchain. We have used metamask wallet and web3.js library to interact with the Ethereum blockchain.

Also a smart contract for an election process is deployed on the Ethereum blockchain. It is written using solidity programming language. It automates and enforces the rules and conditions of an election, ensuring transparency, security, and immutability throughout the voting process. The smart contract consists of code that defines the parameters and logic of the election. It includes functionalities such as registering voters, casting votes, and tallying results. The contract ensures that each voter can only cast one vote and that their vote remains confidential. The smart contract also maintains an immutable record of all cast votes. It prevents tampering or manipulation of the voting data, as the blockchain's decentralized nature ensures that all participants can verify the integrity of the election results. After the voting period ends, the smart contract automatically counts and tallies the votes. The results are then made available to the participants, ensuring transparency and reducing the reliance on intermediaries or centralized authorities.

Client-side application consists of the various user interface screens like Create New Election, Add Voter, Update Voter, Add Candidate, Update Candidate, Vote, and Results. It is a simple system designed to be user friendly and easy to use. The user who wants to conduct the election needs to register in the system as an Election administrator. Then he can enter all the information like election details, voters and candidates participating in the election ,etc into the system.

Admin view of the application



On the day of election, when a voter provides their information, it undergoes verification through an authentication API. Upon successful authentication, a web token is generated to maintain the session, but its validity is limited to a duration of 5 minutes. To prove his/her identity the user is asked to enter the OTP that was generated for him after the authentication. As part of the authentication process, it is also verified whether the voter exists and has not already cast their vote. Example of authentication api request and response look like below:

```
# Request
{
  "identificationNumber": "ASDF7894561"
}
```

```
# Response
{
  token: "eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.
          eyJzdWIiOiIxMjM0NTY3ODkwIiwibmFtZSI6Ikp
          vaG4gRG9lIiwiaWF0IjoxNTE2MjM5MDIyfQ.Sf
          lKxwRJSMeKKF2QT4fwpMeJf36POk6yJV_adQssw5c",
  name: "vimal",
  age: 24
}
```

After successful authentication, the user will be redirected to the vote screen where he can see all the candidates enrolled in his constituency. The vote screen will look like below:

Voter view of the application

From the vote screen the user has the option to select any one candidate they wish to vote for. When the user clicks on the vote button the vote is casted and recorded in the blockchain.
After the voting period ends, the smart contract automatically counts and tallies the votes. The results are then made available to the participants, ensuring transparency and reducing the reliance on intermediaries or centralized authorities. The result screen will look like:

Result screen

VI. RESULTS AND DISCUSSION

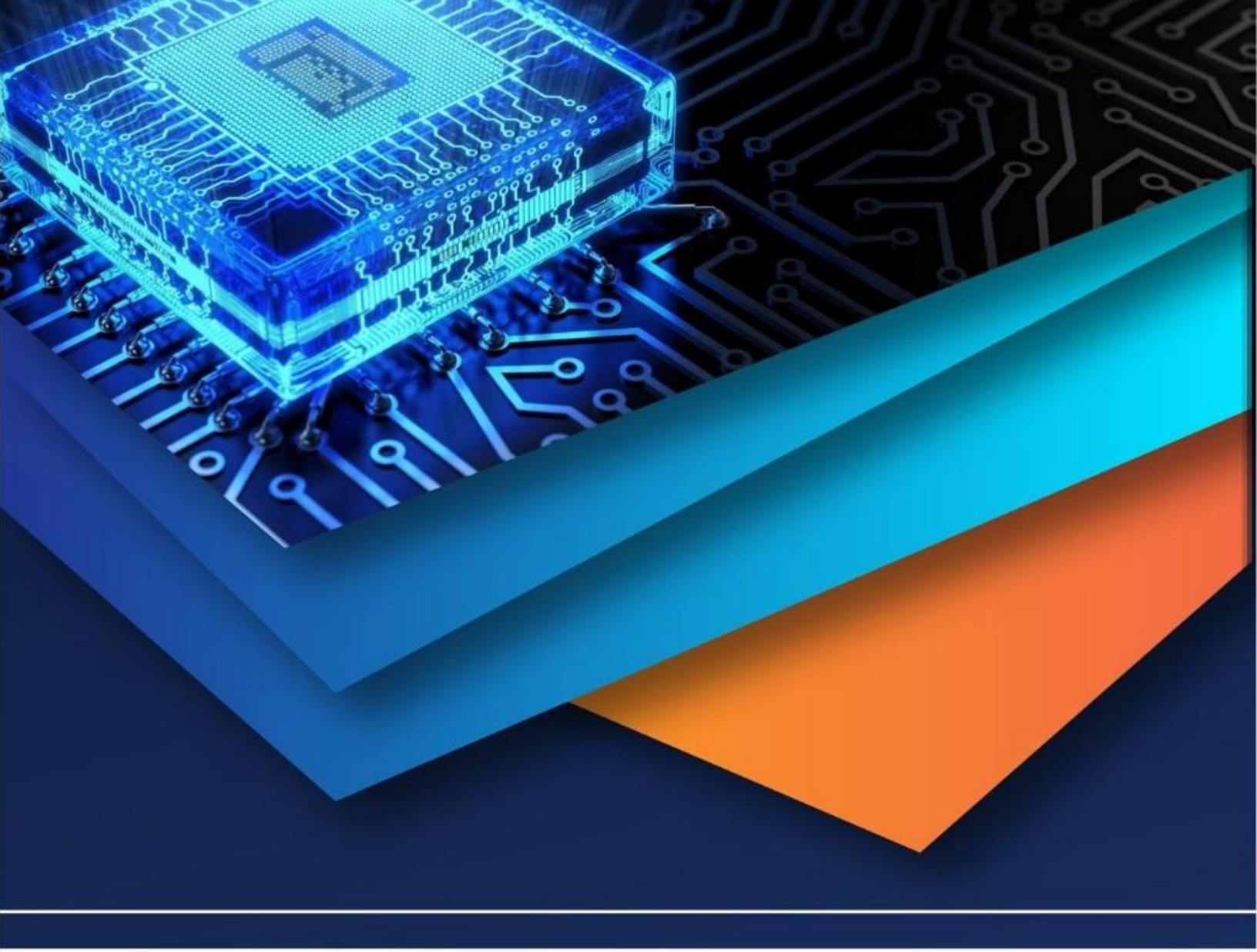
The results of the study indicate the feasibility and potential benefits of implementing e-voting systems using blockchain technology. Through the use of a blockchain-based platform, several key advantages were observed. Firstly, the transparency of the voting process was significantly enhanced. Each vote cast was recorded on the blockchain, allowing for easy auditing and verification of the results. This increased transparency instilled trust among the voters and minimized the potential for fraud or manipulation. Furthermore, the security of the e-voting system was greatly improved. The decentralized nature of blockchain technology made it extremely difficult for malicious actors to tamper with the voting data. The immutability of the blockchain ensured that once a vote was recorded, it could not be altered or deleted, providing a robust and tamper-resistant infrastructure for the electoral process. Additionally, the use of blockchain technology enabled greater accessibility and convenience for voters. With e-voting systems, voters could participate remotely, eliminating the need for physical polling stations and allowing individuals to vote from the comfort of their homes. This increased accessibility particularly benefited those with mobility issues, individuals living in remote areas, and voters who may be traveling during the election period.

VII. CONCLUSION

In conclusion, the development of a reliable and secure e-voting system using blockchain technology offers significant advantages over traditional voting methods. By leveraging blockchain's features of decentralization, transparency, immutability, and security, the system can address limitations such as geographical restrictions, security breaches, and time-consuming processes. It provides a decentralized and transparent platform for convenient voting, reduces costs, enhances accessibility, and ensures the integrity of the election process. For further advancements, with proper infrastructure and resources, it is possible to implement biometric authentication to verify the identity of the voter, which ultimately reduces fake identities.

REFERENCES

[1] E. Hubbers et al., ”RIES-Internet Voting in Action”, [inProceedings of the 29th Annual International Computer Software and Application Conference, IEEE Computer Society,Washington DC, USA, pp.417- 424,2005. http://dx.doi.org/10.1109/COMPSAC.2005.132].
[2] Ayed, A.B. (2017). A Conceptual Secure Blockchain Based Electronic Voting System. International Journal of Network Security Its Applications (IJNSA) Vol.9, No.3, May 2017.
[3] Votereum: An Ethereum-based E-voting system Linh Vo-Cao-Thuy, Khoi Cao-Minh, Chuong Dang-Le-Bao, Tuan A. Nguyen, IEEE.
[4] C. K. Adiputra, R. Hjort and H. Sato, "A Proposal of Blockchain-Based Electronic Voting System," 2018 Second World Conference on Smart Trends in Systems, Security and Sustainability (WorldS4), London, 2018, pp. 22-27, doi:10.1109/WorldS4.2018.8611593.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY