International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 07 Issue: 05 | May 2020 www.irjet.net p-ISSN: 2395-0072

Voting System using Blockchain

Somya Sharma[1], Vibhor Garg[2], Shubham Kumar[3], Research Paper Guide - Ritin Behl[4]

[1,2,3]B.Tech (Final Year), Information Technology, ABES Engineering College, Uttar Pradesh, India
[4]Assistant Professor, Information Technology Department, ABES Engineering College, Uttar Pradesh, India

---

Abstract - *A general election cost too much with respect to money and time, but even after so many efforts cheating and fraud cannot be eliminated completely. So the solution can be searched through technology which is transparent, reliable, trustworthy and immutable. Blockchain has all these features and many more features provided so the process can be smoothened and all the malpractice can be removed from ground level. The general election required manpower such as security, management, and auditing along with a huge amount of money. But the features provided by blockchain would be cheap and more effective. The chances of malpractices can be eliminated as blockchain provides a reliable solution for the problem and maintains complete voter anonymity and prevents voter fraud. This solution not only required less amount of money but also saved a lot of manpower and time for the concerned authority. It is the best solution to solve the problem of all malpractice and cheating.*

Key Words: **Blockchain, Ethereum, Ganache, ABI, Wallet Address, JSON, EVM, ETH, Cryptocurrency, DAO**

1. INTRODUCTION

The present system for voting is not reliable and is difficult to manage. Elections of any type require a huge amount of money and people have been waiting up to 6 hours to vote in a primary election. An E-Voting system needs to have heightened security in order to make sure it is available to voters and should be protected against outside influences, changing votes from being cast, or keep the voter's ballot from being tampered with.

However, it is still a big challenge nowadays to prevent cheating in a voting mechanism. There are many incidences of malpractices in elections in various areas. So the need for an unbreachable system for voting is mandatory.

The system for voting using blockchain can provide a solution from a college election to the general elections of the country. The security concern can be reduced through blockchain and all the other challenges in elections can be coped via this technology.

To solve these problems, a system that is highly secure, transparent and convenient had to be chosen. Such a system should be able to provide the comfort and convenience that is much needed while maintaining trust and integrity. The best possible solution is given by blockchain technology which is the primary choice in trust-building applications. It is a cutting edge discipline that involves decentralized technology to provide highly secure transaction systems that are transparent too. The project we have created aims to provide an application that can be accessed by every voter at the convenience of their own premise and by using their own device. Thus, it eliminates the requirement of setting up voting areas that must be secured by armed personnel. It aims to maintain the democratic nature of elections that promote voter turnout and prevent double voting or vote modification. It is highly secure and private. The results that are traceable and verifiable at the end of the procedure.

The scenario of a small college election is different from the general election of the country, and blockchain provides various features to manage all scenarios. So it allows users to vote over a secure website through their home or from an election booth.

The credibility of a voter is checked through a secure database that is immutable provided by blockchain so cheating can be stopped from all places. Various functionalities will be provided to voters while voting alongwith and comfort.

The management will be to control all the features from anywhere and will also be able to see a live graph of the ratio of votes for each party or candidate. The basic functionality for authentication and confidentiality will be provided as well as complex functionalities can be also handled in a smooth manner. These methods save time and provide results faster and the election can be held in less time, as this process can be monitored without any limitation.

2. LITERATURE SURVEY

Following sources describe various principles and concepts about blockchain and online voting.

[1] - Bitcoin - A peer to peer electronic cash system

This was the first paper that described and conceptualized blockchain. Initially, blockchain was started as a method to directly send payments from peer to peer without the involvement of any third party such as governments or banks. It displays how many problems with a decentralized system can be solved with various systems and methods in place. It solves the imminent double-spending problem and provides byzantine fault tolerance to the system. It is, therefore, a commercial payment system that does not need government permissions and all transactions are cryptographically secured. Based on the systems laid out and described by Satoshi Nakamoto's paper, Ethereum was set up that uses the decentralized architecture to be able to run apps on it.

[2] - Internet voting from a comparative perspective- The case of Estonia

Estonia is a country in the European Union that has implemented an online voting system for major elections. The research paper describes the technical and political consequences, safety implementations and more. It considers data in both qualitative and quantitative manner, how it impacted the election process as well as cultural, legal and political factors.

[3] - A Review on Blockchain Technology and Blockchain Projects Fostering Open Science

The paper describes the various applications and uses of blockchain technology, its technical points and effects. It ventures through various applications such as financial transactions, cryptocurrencies, medicine, intellectual property protection and more. It performs analysis on the basis of technical requirements, industrial effects, practicality and future scope.

[4] - Security aspects of blockchain

The paper describes blockchain technology and its applications from a security point of view. It aims to understand the effects of blockchain as a powerful new technology but also it critically examines the security flaws that it might have and how to eradicate them if possible.

3. METHODOLOGY

We have called the designed system as EVOTE and will be addressed as such in the rest of the paper. EVOTE will follow all the software development guidelines as described by IEEE and will also implement blockchain in the most secure manner as advised in the above-described research guidelines. It aims to provide a realistic internet-based application that can be used to cast votes in an election of any size. It will aim to work with not only voting procedures that occur in organisations but also in village, city and national level elections. Also, we have tried to keep the application as simple as possible so that it may be able to run on primitive systems such as those in villages. The application will be able to run only with a running internet connection and the latest web browser. Further, we would like to develop a mobile-based application for EVOTE that will provide maximum portability. It aims to fulfil the following goals:

- Prevent ballot tampering and ensure voter security.
- Reduce election cost.
- Reduce the requirement of extensive human resources.
- Reduce logistical requirements that bug organising big elections.
- Increase transparency with elections thus increasing voter confidence.
- Ensure the CIA of security at all times.
- Increase accountability.
- Ensure the inherently democratic nature of elections.

Therefore, EVOTE will try to accomplish all the tasks that a conventional ballot based voting system ensures while providing a sense of comfort and security that one can get when he/she votes at their own premise.

3(a) - The following are the components used to create EVOTE:

1 - Ethereum:

Ethereum was launched in 2015 as the world's first programmable blockchain platform. Besides accomplishing the purpose of other blockchains being able to send money from one peer to another, Ethereum is able to host and run apps (to be called Dapps - Decentralized Apps) on its architecture. This was a revolutionary development in the field of blockchain as developers and people can now take advantage of the decentralized architecture and anonymity. It uses its own cryptocurrency known as ETH to be able to incentivize the mining and creation of new apps. These ETH (or Ether) can be sent from one entity on the web to any other entity without the interference of any other bridge such as banks or governments.

One of the main features of Ethereum based apps is the capability to run autonomously without the interference of any organisation (DAO). Thus, once an application has been launched on the Ethereum, it can keep on running without interference.

One thing that must be kept in mind while designing Ethereum based apps is that all transactions and processes must be deterministic. It means that all transactions must return the same result in all instances

since real money is involved. So applications must be developed intelligently.

2 - PHP:

PHP is a server-side scripting language that helps to form a backend for websites. It can be used to create static and dynamic websites or web applications. It earlier stood for Personal Home Pages but now it is changed to Hypertext Preprocessor. Scripts written in PHP can run on any server that is set up for PHP. It can generate data to be presented on the frontend, collect form data, read and write files and much more. PHP supports all operating systems and a wide range of databases.

3 - MySQL Database:

MySQL is a database system that is used to store records in a tabular format (RDBMS). It is open source under the GNU License. It provides a lot of utilities that make it a full-fledged database that can support websites. It provides cursors, triggers and views that can be used to automatically update the database and provide custom views to the users. It also supports full-indexing service that enables the fast search of data across the database which is a necessity for web applications. It can also be secured easily through high-quality encryption algorithms which is a necessity for web-based applications as well.

4. Solidity:

Solidity is a statistically typed programming language that is used to make applications that can run on the Ethereum platform. It is object-oriented and high-level language that enables writing smart contracts with ease. Solidity was created with properties of C++, Python and Javascript and can support the EVM completely. It supports functional programming, inheritance and is supported by various libraries that help to implement functionalities without writing them from scratch.

We can write self-sustaining business logic using Solidity known as a smart contract.

5. Ganache:

Ethereum smart contracts are programs executed within the context of transactions on the Ethereum blockchain. Ethereum Ganache forms part of the Truffle Suite, a set of developer tools that allows users to recreate blockchain environments locally and test smart contracts. Ethereum Ganache is a local in-memory blockchain designed for development and testing.

6. HTML, CSS, Javascript:

HTML, CSS and Javascript are the most basic building blocks of any web-based application.

- HTML - HTML stands for Hypertext Markup Language. It is used to create the scaffolding or body of a webpage. It uses special markup denotations known as tags. These tags are used to define properties of elements on the webpage such as text, images, links and more.
- CSS stands for Cascading Style Sheets. It is used to define styling for the webpage elements. It defines properties of how a web page will be displayed at user level.
- Javascript is a client-side scripting language that defines the behaviour of webpages. It is lightweight, just-in-time and compiled in nature. It provides dynamic nature to webpages by updating it in real-time.

3 (b) - Steps to create the application:

Step 1 - Create Smart Contracts :
Smart Contracts are like computer-generated agreements between parties involved in a transaction. They outline the rules of the transaction that both parties must obey. These rules of transactions are transmitted to all peers connected in the blockchain network. The voting smart contract ensures that no person can vote more than once, ensure correct vote casting and more.

Step 2 - ABI Extraction:

Extract ABI and contact address after deployment: Every contract has an ABI (Application Binary Interface) associated with it. This ABI provides the entire code in JSON format that can be understood and interacted with using javascript. It provides a programmatic summary of each variable and function, their return types and arguments. Contact address is the address at which the contract is deployed and can be communicated with. This is a hexadecimal address that provides recognition to the smart contract.

Step 3 - Database Setup:

Set up MySQL database for user authentication: MySQL database will provide an authentication mechanism so that only certain users can access the voting system

Step 4 - Creating a backend:

Create a PHP backend to join the frontend and database: A PHP backend system acts as an intermediary to connect the frontend to the backend. It takes requests from the frontend and processes it to extract required data from the database. It then modifies the received data to be able to be displayed by the web browser efficiently. In our application, the frontend receives the login credentials

(username and password) at the login page. The username and password are sent to the backend via a POST request and are verified from the database. If the result is correct, the voter is allowed to proceed with voting.

Step 5 - Create Frontend with HTML and CSS:

Create the HTML and CSS web pages: The HTML and CSS pages are what the user actually interacts with while on the software. They must be simple, responsive and intuitive in nature. They must be having appropriate methods to be able to interact with the backend.

Step 6 - Create Javascript Portion:

Create JavaScript portion: The javascript portion is the most important part of the non-blockchain side of the project. The javascript code uses the web3.js library to interact with the smart contract and perform the functions described in the ABI. It then transforms the data received from the blockchain and modifies the HTML/CSS elements to display the data retrieved from the Ethereum blockchain. Thus the javascript code performs the transactions on the blockchain.

Step 7 - Connect with Ganache-CLI:

Ganache-CLI provides a demo blockchain with 10 free accounts that can be used to perform actions on the software we have created. We can use the 10 accounts to perform voting in a local environment.

Step 8 - Connect the components:

Connect the components: The ABI and contract address is written in the javascript code. The HTML and CSS are interlinked The Javascript is then linked with the frontend. The PHP backend is referenced in the POST request in login. The Javascript interacts with the blockchain upon receiving requests from the frontend.

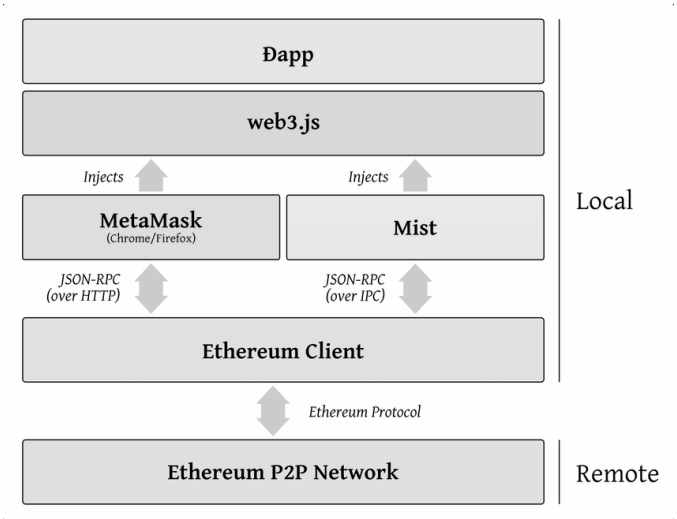

Fig 1 - Ethereum Architecture

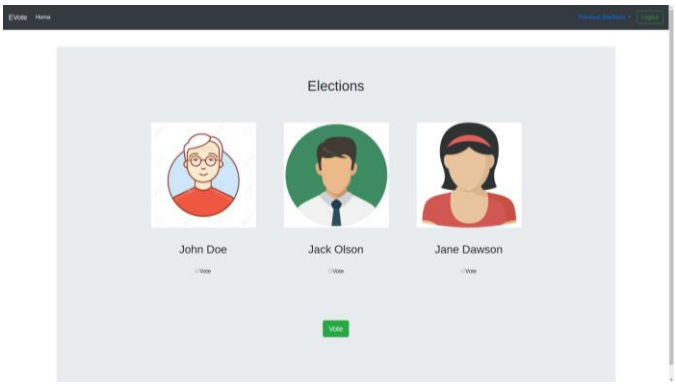

Fig 2- Snapshot of completed application

4. CONCLUSION

We proposed a simple mechanism to solve a complex scenario through simple, secure, robust, and decentralized technology. The main concept of this mechanism to stop fraud and cheating in all types of elections. The features provided by blockchain are simple but can manage different scenarios and complex situations. The motive of this system is to make voting safe and efficient. We hope that these techniques will handle different types of elections, such as college election, ward election, general election and more in the future with ease.

REFERENCES

[1] Satoshi Nakamoto “Bitcoin : A peer to peer electronic cash system ”, October 31, 2008.

[2] R. Michael Alvarez, Thad E. Hall, Alexander H. Trechsel “Internet Voting in Comparative Perspective: The Case of Estonia”, Volume 42, Issue 3, July 2009, pp. 497-505

[3] Stephen Leible, Steffen Schlager, Mortiz Schubotz, Bela Gipp, "A Review on Blockchain Technology and Blockchain Projects Fostering Open Science".

[4] Study Paper on Security Aspects of Blockchain https://www.tec.gov.in/pdf/Studypaper/Security%20aspects%20of%20blockchain.pdf