

DECENTRALISED VOTING SYSTEM USING ETHEREUM BLOCKCHAIN

¹K.Sumukh Bharadwaj, ²Tejas Kalburgi, ³Chandra Mouli, ⁴Dr.Vikram Palodia

¹U.G Student, ²U.G Student, ³U.G Student, ⁴Asst.Professor

^{1,2,3,4}Electronics and Communication Engineering,

^{1,2,3,4}Sreenidhi Institute of Science and Technology, Hyderabad, India

Abstract : We are investigating the troubles within-side the election balloting structures and seeking to suggest the e-voting version with the usage of blockchain which could solve the issues. Also, our attempts aim to assess the software of blockchain as provider to enforce dispensed digital voting structures. The phase of paper will spotlight a number of famous blockchain structures that provide blockchain as a provider and related digital e-balloting machine, that's primarily based totally on decentralised system that addresses all obstacles respectively, it additionally preserves participant's anonymity whilst nonetheless being open to public inspection.

IndexTerms – e-balloting, blockchain, anonymity, decentralised.

I. Introduction

Voting has always played a prominent role in democracy for expressing people's choice of leader . The process of electing the leader has changed from raising hands and filling out ballot paper at the voting centre to electronically casting votes . This method of voting has been changing to improve its efficiency and reduce the errors . Implementing a electronic voting for various voting events has reduced burden of counting votes manually and making it a easy process

Estonia followed by Switzerland and Norway were the first to implement electronic systems for state wide and council elections. Researchers and security experts have kept these systems under close scrutiny. The secrecy of the source code is one of the primary critiques. As an example the transparency of the Estonian Voting system is questionable as the script for posting votes has never been made public. Leaked source code of the now discontinued Swiss voting system analysed by the researchers and a statement was made saying that it was very much possible for someone to replace all valid ballot votes with fraudulent ones using a cryptographic backdoor.

Another critical risk of using these methods is they're centralisation . This means they are being controlled by a single organisation responsible to conduct these elections and have high security flaws, such as vulnerability to distributed denial-of-service (DDoS) attacks . A DDoS attack makes the system inaccessible by overloading it with requests . Given the computing power , there is a possibility to launch state level attack to analyse and alter the voting data of all the electronic voting machines

II. LITERATURE REVIEW

A. Votereum: An Ethereum-based E-voting system : It evaluations the requirement and proposed a gadget i.e Votereum , that is primarily based totally on crypto forex ethereum for E-voting .The proposed gadget is empowered through the Ethereum platform, which includes one server that manages the complete gadget and the alternative handles all blockchain-associated requests. The paper makes use of the Advanced Encryption System algorithm which creates a mystery key for the apparent textual content and makes it secure [1]

B. Survey on Blockchain Based E-Voting Recording System Design: By adopting blockchain within-side the distribution of databases on e-balloting structures can lessen one of the dishonest reasssets of database manipulation. For encrypting records fetched from fingerprint sensors we're going to use the AES set of rules. This studies discusses the recording of balloting end result the usage of blockchain set of rules from each location of election.[2]

C.Blockchain-Based E-Voting System:This paper evaluates the ability of disbursed ledger technology thru the outline of a case study, particularly the system of an election and enforcing a blockchain-primarily based totally software which improves the safety and reduces the price of web website hosting a national election. It makes use of quorum Geth model to put in force this model , that is a non-public patron service .[3]

D.Decentralised Voting Platform Based on Ethereum Blockchain: In this they've proposed a singular method for a decentralised trust-less vote casting platform that is based on Block-chain era to remedy the believe issues. The key capabilities of the device encompass making sure transparency and , and imposing one vote in line with cellular smartphone quantity for each ballot with ensured privacy. To accomplish this, the Ethereum Virtual Machine (EVM) is used because the Blockchain runtime environment.It makes use of HTML5 web-app compiled the use of Apache Cordova and Ethereum network [4]

E.Blockchain Based E-voting System : In this they have given a approach where they used solidity programming to create smart contract and a hash code for voter to enter while voting at voting stations [7]

F. Blockchain based E-Voting Recording System Design: This recording machine takes place while the vote is over. Blockchain era may be one method to remedy the troubles that regularly arise within-side the electoral machine. The use of hash values in recording the voting .It makes use of Elliptic Curve Digital Signature Algorithm and SHA-256 algorithm [9]

G. Online Voting: Voting System Using Blockchain: Article offers a brief overview on numerous methodologies which might be utilised in modern voting. The paper will assist to construct a gadget with a view to face the prevailing and upcoming demanding situations and could eliminate drawbacks from those preceding architectures . It makes use of Cryptographic verification and Homomorphic Encryption Technique: [10]

III.METHODOLOGY

In Our System we have designed an architecture where it is a complete website with better addition of a security layer using registration data and a one time email id password to vote for the desired candidate . We have taken this to complete the system with its previous flaws and make it ready to deploy for any kind of voting , keeping the traditional look of voting machines to avoid complications in the interface .

3.1System Architecture :

Architecture of the system is described below in this section

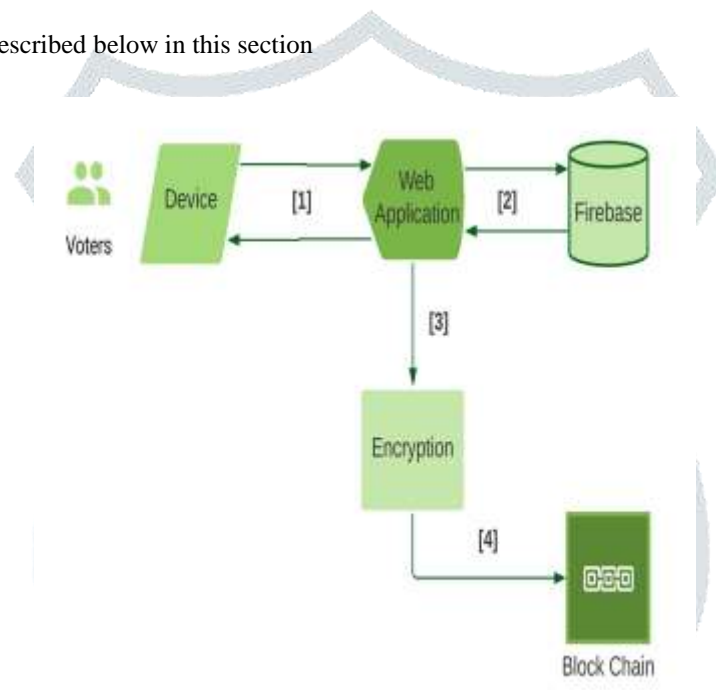


Figure IIII block diagram of voting system

First step of the system is to register for voting in the election . The process involves checking if the user is verified and is eligible to vote . Making sure if the details are genuine and not being used to fraudulent the Application . Voting is a key part of Democracy so it is important to protect the right of a person from being tampered and misused . After the user is verified and eligible, he/she will be given a one time login id and password which is filled with ethers , enough to vote one person .

On the voting day the user uses his id and password to vote and as soon as his vote has been registered he/she will be logged out of the system automatically . Results will also go live status as they vote .

3.2Analysis of Requirements :

The system is analysed and made into two parts for better implementation of it . The implementation of the system is described in this section where the whole system is divided into two phases :

1. Registration Phase and
2. Voting Phase

3.2.1 Registration phase :

In this process the user gives the details such as his Social Security Number or Aadhaar with his Mobile Number . If the user is eligible to vote as per the smart contract he will be checked with database if he is already registered the request will be denied or else he will registered and given a one time login id and password .This System used for registration is made using HTML/CSS front end and Firebase for backend which contains the user identity The details generated are invalid once voted and keeping it secure.

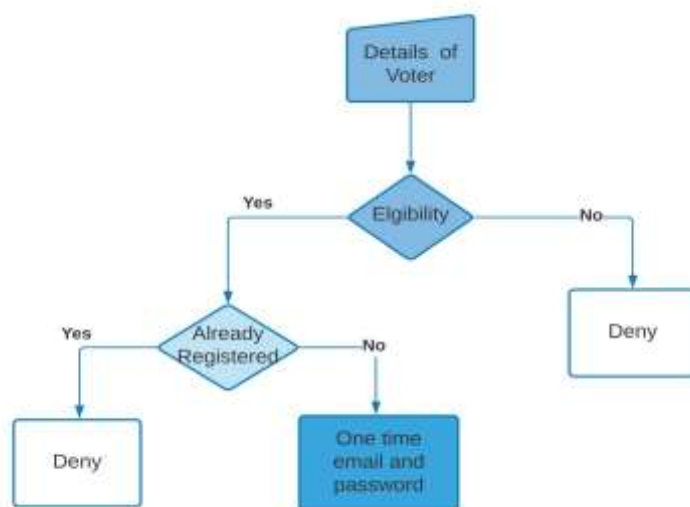


Figure III2 Process of registration

3.2.2 Voting Phase :

The System is a replacement of the traditional voting system i.e EVM which is made using HTML5 for front end and BlockChain for back end . A Smart Contract is written on how the elections should be conducted and votes to be counted , the contract is written using solidity language mentioning the names of candidates and their party symbols . Smart contract is the brain of the system which decides on how the things move in the back end .

Every Request and change in the block chain is taken as a transaction . Transaction is the interface for world and Ethereum networks . Every vote casted is noted as a transaction and added as a block to the ethereum network . Every transaction requires a service fee in the form of ethers or transaction fees in the form of a gas fee . We have used the Ganache-CLI which sets up a private network and initiates the ethereum which keeps track of the transactions of the system .Truffle is used as a pipeline for the ethereum virtual machine and tests our framework

Transaction ID	Gas Usage	Block Number	Date and Time
0x40aeaa9dead1c534edc680d70ccb1496 24d675f014bd2996528b5d2c6bdc9451	48613	1	Thu Jun 24 2021 11:16:26 GMT+0530

Every time a vote has been recorded it is taken as a transaction with id , amount of gas used the block which it is being added and the location and time stamp of the vote .

MetaMask bridges the system to the distributed web in our browser . It lets us run decentralised Applications made using ethereum without the need of a full ethereum node running in our system .

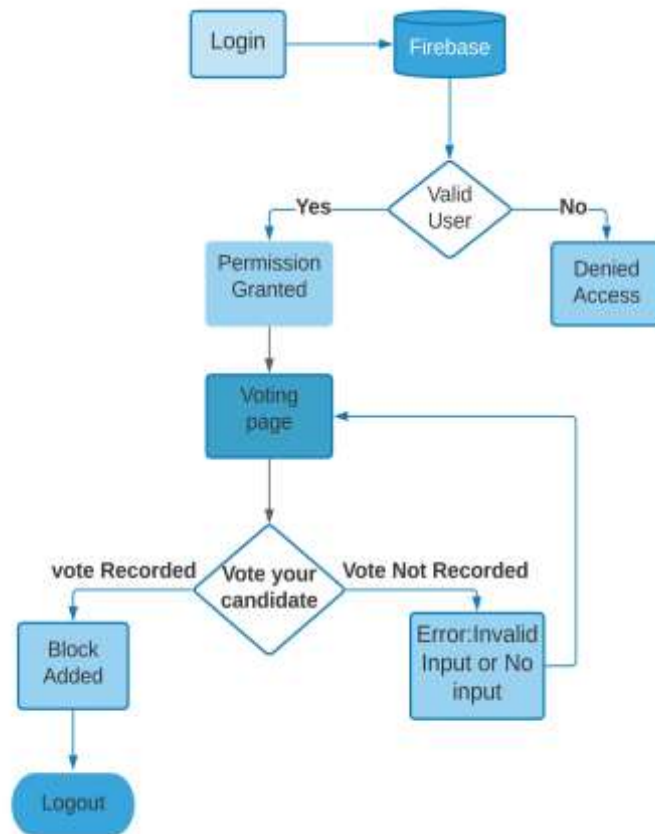


Figure III3 process of voting

In the voting phase as to avoid misclicks by the user , The Voter has to enter the name of the candidate name which he/she wants to vote and click the vote button to cast their right . The system is designed in a way that it does not record transactions unless the candidate is the same as mentioned in the smart contract and if the person tries to submit an empty field it alerts them .

3.3 Software:

The below are the softwares used for developing the system , VS code has been used to manage project and edit it

Operating System	Mac OS Big Sur
Programming Language	HTML5, JavaScript, Solidity
Database	Firebase

3.4 Hardware:

The basic version of hardware was used to check if the system works on lower end devices

Processor	Intel core i5
Storage	SSD 128gb
RAM	8gb

IV CONCLUSION:

In the project we have proposed a decentralised voting system using block chain that uses smart contracts to enable secure and efficient elections with people's privacy . It is shown that block chain offers technology to tackle the tampering of votes and fake results which keeps the integrity and transparency of the system . It can manage hundreds of transactions per second keeping the smart contract on the block chain . It requires more furnishing of current system to implement it in larger countries . Block chain keeps the transparency of the system which is required for our current voting system to enable better auditing and understanding of elections .Decentralised applications do not take any kind of influence as there is no specific center authority , it brings a more democratic approach of choosing a candidate . For DApp Voting to become more transparent and open ,the solution is based on block chain technology . This project tries to make a more practical version of the e voting system where the block chain verifies and distributes practically .

REFERENCES

- [1] M. Jamal, M. Tarik, Alexander Isar, "Precoding techniques in OFDM systems for PAPR reduction", 16th IEEE Mediterranean Electrotechnical Conference, 2012.
- [2] Baig and V. Jeoti, "PAPR Reduction in OFDM Systems : Zadoff-Chu Matrix Transform Based Pre/Post-Coding Techniques", IEEE Second Conference on Computational Intelligence, Communication Systems and Networks, pp505-510, Pahang, June 2010.
- [3] Yasir Rahmatallah and Seshadri Mohan, "Peak-To-Average Power Ratio Reduction in OFDM Systems: A Survey And Taxonomy", IEEE Communications Surveys & Tutorials, Vol. 15, No. 4, Fourth Quarter 2013.
- [4]T. Jiang and G. Zhu, "Nonlinear companding transform for reducing peak-to-average power ratio of OFDM signals," IEEE Trans. Broadcast.,vol. 50, no. 3, pp. 342–346, Sep. 2004.
- [5]X. Li and L. J. Cimini, Jr., "Effect of Clipping and Filtering on the Performance of OFDM," IEEE Commun. Lett., vol. 2, no.5, May 1998, pp. 131–33.
- [6] V. Sudha and Dr. D. Sriram Kumar, "PAPR Reduction of OFDM System using PTS method with different Modulation Techniques", 2014 International Conference on Electronics and Communication System (ICECS -2014).
- [7] Hem Dutt Joshi and Rajiv Saxena, "PAPR reduction in OFDM systems using precoding with clipping", 2011 International Conference on Communications, Computing and Control Applications (CCCA)