ELECTRONIC VOTING SYSTEM USING BLOCKCHAIN

Prof Chaithra S[1], JK Hima[2], Rakshita Amaresh[3]

[1]*Prof. Chaitra S, Dept. of Information Science Engineering, RRCE, Karnataka, India*
[2, 3]*Student, Dept. of Information Science and Engineering, RRCE, Karnataka, India*
---***---

Abstract - *E-voting is a web-based voting software solution based on security. There were many ways voting practiced over years which had raising hands for voting, using ballot papers. This proposed paper overcomes the above problems by using blockchain technology. "Blockchain is used to create secure and scalable distributed systems that show several edges over centralized systems. The presented paper is suitable for small scale elections [4]". A smart contract is built for voting purpose using ether as the security tokens. Truffle framework is used for implementation, testing and deployment. Ganache would be used as an Ethereum client. For additional security purpose facial detection has been implemented at the time of registration.*

Key Words: **Blockchain, Ethereum, E-voting, Facial Detection, Smart Contracts.**

1. INTRODUCTION

Nowadays, in India there are two methods of voting. E-Voting is principally different than online polls that are currently in use, since it involves %100 accuracy on real physical level (not account level) identity authentication for attending persons.In the paper proposed, this paper discusses the security measures for electronic voting machine using blockchain technology and to add additional security a technology has been included, the concept of face detection and recognition to identify the voter [2]. "Blockchain eliminates the need of a central server to manage network and a centralized database thus ensuring trust. It is a complete decentralized open ledger system. Public ledger records all the votes casted and is permanent and immutable. It ensures that no vote can be changed once casted [3]".

Blockchain has two main features:

(i) Immutability: A given "new block" to the ledger should refere the previous form of the ledger. This generates the fixed chain, from which the blockchain gets its name from, and prevents obstructing with the honesty of the previous entries.

(ii) Verifiability: The register can be decentralized, cloned and assigned over many locations. This ensures high opportunity and provides mediator verifiability as all nodes support the consensus version of the ledger.

(iii) Decentralized System: A Decentralized System is a System where lesser level parts can work on nearby data to accomplish objectives.

Blockchain-enabled e-voting could reduce voter fraud and increases voter access. Eligible voters can cast a ballot anonymously using a computer or a laptop. Blockchain enabled voting uses encrypted key and tamper-proof personal IDs. Blockchain is said to be one in all of the technologies that will stay for a long run, and researchers have had a dispute that this technology is going to derange several industries in the up-coming years, and democratic elections are one of the main areas where blockchain can go to rework [10].

There are few instances where votes are documented at the voting booths are changed at the constituencies either purposely or accidently. The projected design addresses the problems of vote tempering as a result of transactions added to the block are safe with a cryptographic hash function that makes tempering of the votes placed in the blockchain are nearly unobtainable and make it immutable. This design permits the encrypted votes, the proofs, and therefore the algorithm to be hosted independent of the election services, eliminating the danger of tampering or denial of service whereas still maintaining voter verifiability.
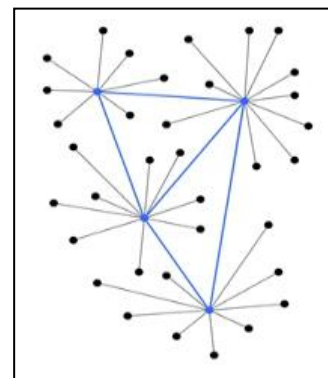

Fig -1: Decentralized System

2. LITERATURE REVIEW

The creation of blockchain process right now is in the voting system in the constituent structure. Members are clear and cannot vote more than once, the new progression ensures that all center points. This is authentically related are in one place. Likewise ensures all hubs that have enrolled the outcomes are incorporated into the figuring procedure. As far as expense can likewise be more effective on the grounds that it does not need hardware that's dependably modified in every race did. Considering the structure and the results it may be assumed that the system has a positive value of account, the voting system subjected to Blockchain advancement [1].

A blockchain is a typical, appropriated, and lasting record. The blockchain has delivered genuine eagerness for use in a combination of endeavours and zones, going from setting aside cash, back, and insurance to restorative administrations, government, retailing, and gathering. Affiliations are using blockchains to develop new applications that are more strong and capable. Right now explore the blockchain development for building PC information structures. First direct an efficient examination of employments and issues related to blockchain development, and after that recognize a scarcely any issues that require moreover investigate with the ultimate objective to be really tended to. Also analyzes the potential utilization of blockchain in guidance, and how preparing structures can benefit by the happening to blockchain advancement [2].

3. RELATED WORK

Election is a traditional decision making process by which people elects the leaders. Elections are conducted to elect a party to rule. The question of who is allowed vote is an issue of the government. The electorate generally does not include the entire population. For example, people aged above 18 years can only vote. In many cases, nomination for office is selected through pre-election process. Election plays a vital role in modern day world. Electronic voting systems are democratic arrangements and these convert the vote into an important result [4].

In the traditional voting system, the initial step was to count votes, in which many vote count systems and ballots were used. There are various electoral reform voting methods such as approval voting, single transferable vote, instant runoff voting or a Condorcet method; these are acquiring demand for lesser elections in some countries where more dominant countries conduct elections in long-established counting methods.

When elections are conducted, political leaders and the supporters conceive to get a hold on to the general public by participating for votes in what are referred to as campaigns. Partisans for a campaign can be normally acquainted or loosely associated with and often use campaign announcements.

There are many problems with elections which includes weak rule of law. Authoritarians may use the potential of executives to always abide in power in spite of the results obtained after counting the votes obtained at elections.
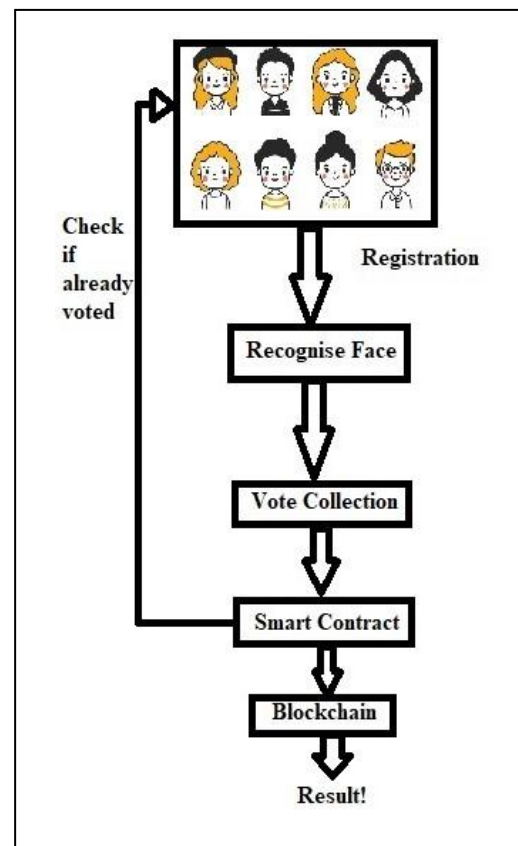
4. PROPOSED SYSTEM

Fig -2: Electronic voting system using blockchain

Utilizing traditional paper method to vote can decelerate the complete process of determining the vote, due to the time and strength required in tallying the final votes. The proposed system solves this problem; it includes an Online voting systems that have added security where each user registers with a unique Id along with an added picture only after the users have verified using face detection can proceed to cast the vote using ones crypto wallet key (Ethereum). Each transaction is given within the smart contracts. This process starts when the voting procedure at each end is finished [5]. Prior the voting process starts, every node creates a private key and a public key. Public key of every node will be dispatched to all nodes aligned in the procedure [6]. When an election takes place, each node collects the voting outcome from each and every voter. When the procedure is finished, the nodes will hold back until it's the

turn to create a block. If the node catches a spin, it will generate and give-in the block that has been filling up and completed in digital signature to transmit to each and every node by applying turn rules in block-chain formation to steer clear of crashed and make sure that all nodes are into the blockchain [7]. The blockchain with smart contracts comes out as an honest process to utilize in progression of shielded, in-expensive, more firm, more transpicuous and easier-to-use electronic voting systems. Since each vote is taken as an individual block it is not possible to tamper any votes.

5. METHODOLOGY

This system can be used for a small scale organisation. The blockchain technology and Face Detection is executed in web3.js and Python using the Flask framework respectovely. The web page to caste vote is developed using HTML, CSS, and javascript along with the nodejs.

A. Web Portal

A web page is utilized for casting voting and reviewing vote outcomes. The web page gives unquestionable visions for both nominees and voters [8].

1) Registration: Voters information is entered prior the voting procedure starts, by empowering the sign-up feature along with face recognition for voters.

2) Cast Vote: Voter information is accumulated and validated ahead of casting a vote. A voter logins to crypowallet and uses ethereum crptocurrency on a metamask to cast vote.

B. Blockchain

The blockchain technology might abode several problems with reference to e-voting process stated in electronic voting and create e-voting affordable, simpler, and a lot more secure to make. It's a significant new model that will be able to help establish dispersed systems, which guarentee the data probity, accessibility, and desensitized [9]. The blockchain technology is presenting everyone the Internet of value: a new, diffused program that may ease the development in the high society of trade and alter the previous order of human relations for the betterment. This technology intends to transform the processes.

Every time an individual votes the transaction will be stored and therefore the blockchain will be refurbished. To make sure that the model is safe, the block contains the antecedeant voter's details. On the off chance that any of the blocks were undermined, at that point it may be anything but difficult to look out since all blocks are associated with each other. The blockchain is decentralized and can't be defiled; no single point of failure exists. The blockchain is the area where specific voting happens [15]. The voters vote gets dispatched to atleast one among the nodes on the framework, therefore the node then appends the vote to the

blockchain. The electoral framework will have a node in every region to ensure that the system is decentralised.
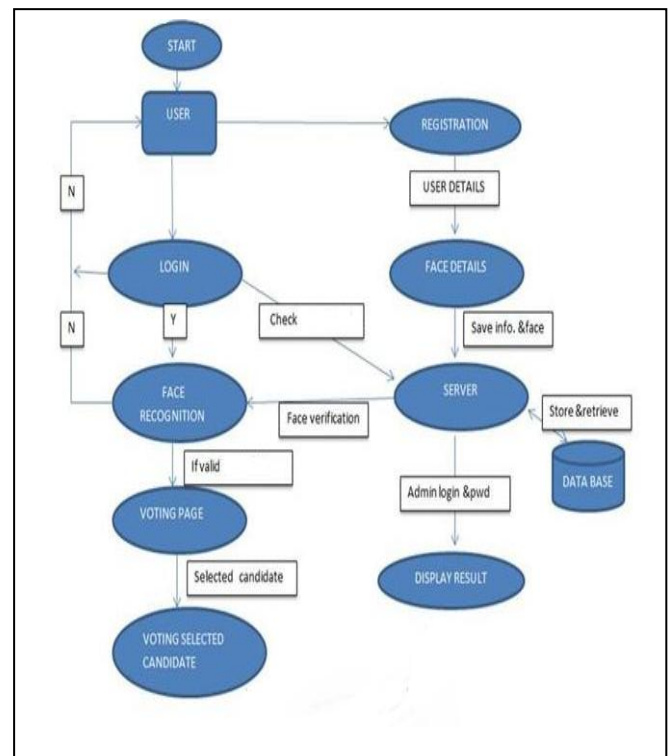

Fig -3: The voting process

1) *Ganache:*

Truffle Framework is utilized to check the smart contracts and dispatch them to the blockchain. Truffle framework encourages making, testing and conveying decentralized applications. It offers progress to blockchain network. Truffle development framework can be used to fabricate Smart contracts and compile inherent contracts.

Ganache is a piece of Truffle environment. It gives a private blockchain to Ethereum improvement. It will in general be seen as an Ethereum customer. It is used to test the decentralized application based on truffle. It tends to be utilized to convey contracts while creating decentralized applications. It similarly empowers running tests on blockchain and smart contracts. When the application is tried on ganache, it tends to be deployed on Ethereum consumer like Geth. Ganache gives a local and virtual blockchain for testing. It gives ten external customer accounts. Each record in Ganache has been distributed a stand-out Ethereum address and a private key related with it. All the records come preloaded with 100 'counterfeit' ethers. Ganache comes in two variations, CLI and UI. This utilization has used UI for straightforwardness. Running ganache resembles running an Ethereum node. It looks like a virtual hub. Ganache can be related with wallets for trades. For this utilization, Meta-mask is utilized. Meta-mask is a chrome extension.
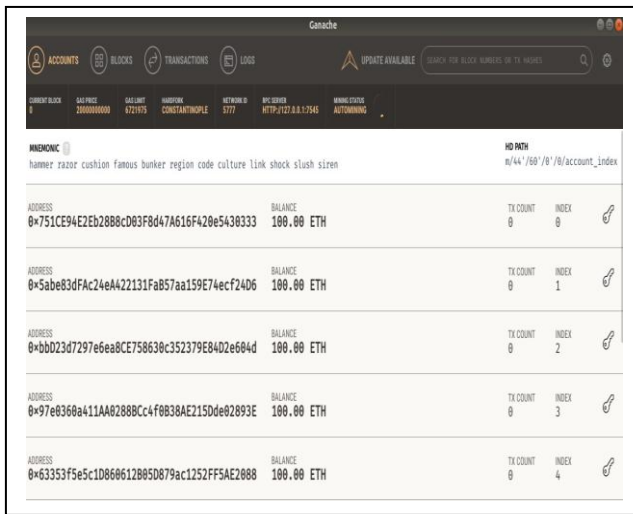
Fig -4: Ganache

2) *Meta-mask:*

MetaMask is an association that permits the client to visit the circulated web of tomorrow in the browser today. It permits running ethereum decentralized applications directly in the program without running the whole ethereum node. MetaMask is a self-facilitated wallet to stock, dispatch and acknowledge ETH and ERC20. It allows to control money as it is an HD wallet that provides a mnemonic phrase that can be kept as backup. MetaMask stores private keys using browser's data store. MetaMask is constructed to live in browser in its default use. A basic transaction in MetaMask has at least a requirement of 21,000 gas. Gas alludes to the evaluating value required to perform an exchange or to execute a smart contract on the ethereum blockchain stage. The demand price of gas is decided by the network's miners.

MetaMask uses a crypto-community standard to generate seed phrase, which is similar to those applied across software and hardware. When a vault is created with MetaMask, a randomly generated 12-word seed phrase will be given. These phrases could be used to generate accounts and private keys. In MetaMask there are two kinds of accounts. The one is when a MetaMask wallet is created and the other is the ones where the account is imported. The imported accounts are the ones that will be generated using the seed phrase outside of MetaMask.
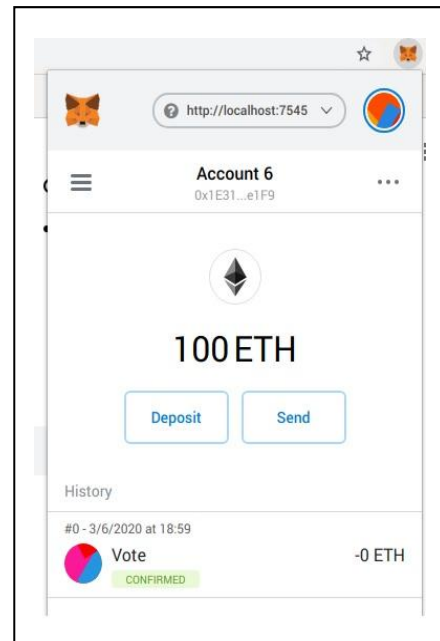

Fig -5: Meta Mask account

6. SAMPLE CODE

A. Smart Contract

```solidity
pragma solidity 0.5.0;

contract election{

struct Candidate{

        uint id;

        string name;

        uint voteCount;

        }

mapping(address => bool) public voters;

mapping(uint => Candidate) public candidates;

uint public candidatesCount;

event votedEvent (

        uint indexed _candidateId

        );

constructor () public {

        addCandidate("1");

        }

function addCandidate(string memory_name) private{
```

```
        candidatesCount++;

candidates[candidatesCount]=Candidate(name,0);

        }

function vote( uint_candidateId) public{

        require(_candidateId>0 && _candidateId <=
Count);

        voters[msg.sender] = true;

        emit votedEvent(_candidateId);

        }

}
```

B. Face Detection

```
import face_recognition

import cv2

import numpy as np

from flask import Flask, render_template

app = Flask(__name__)

@app.route('/')

def index():

  return render_template('webs.html')

def facefun():

  ver_flag = False

  name_count = 0

  view_count = 0

  unknown_count = 0

  print("imported")
```

C. Algorithm

This paper uses some of the state of the art technologies for this purpose like opencv, cascade filters, flask etc. OpenCV is the most popular library for pc vision. Initially written in C/C++, it at present gives ties to Python. OpenCV utilizes AI calculations to go searching for faces inside an image.

Since faces are so confounded, there isn't one simple test that will tell on the off chance that it found a face or not.

Rather, there are a huge number of little examples and highlights that must be associated. The algorithms break the assignment of perceiving the face into a huge number of littler, bite-sized undertakings, every one of that is easy to unwind. These assignments are additionally called classifiers.

This paper uses haar cascades which are xml files that help in detecting the face by using the facial features.

Face detection utilizing Haar cascades is an AI based methodology where a course work is prepared with an assortment of information. OpenCV as of now contains a few pre-defined classifiers for face, eyes, grins, and so forth. All the above mentioned methods are readily available in the python library called face_recognition.

1. Upload images of various actors

2. Create facial encodings; this is the process of extracting features.

        face_recognition.face_encodings (image1)

3. Facial detection using cascade filters and encode the features of the frame

4. Detection of facial distances between the current frame and all the other user images.

5. Match the correct image according to the face distance.

        The web framework is used for linking the face recognition module with the blockchain module that is implemented in nodejs.

7. RESULTS

At first, registration needs to be done by providing a name. Once the registration is done face-authentication takes place. Where it verifies the user, once the voter is verified the voter must login/sign-up to the meta mask account. After the credentials are entered and the voter is logged into the meta mask account, the voter must import respective crypto wallet. Then the voter can vote preferred candidate.

Fig -6: Result

The above figure displays the result after the voter has cast vote. By using blockchain technology, it can be made sure that a voter cannot vote more than once. The technology ensures that a voter uses only one account per vote. By using this technology it is an assurance that the votes cannot be tampered. While voting it uses ether gas for the confirmation of the vote.

8. CONCLUSION

As seen that current voting system within organisation has numerous disadvantages, for example, long procedure, time taking, not secure however now it can be seen that the methodology using blockchain is progressively helpful from the current framework. Since, this paper utilizes two degree of security right now the false voters can be effectively distinguished. The facial validation method is particularly useful in perceiving the flaw voters, with the goal that the misuse of the democratic countings can be diminished. The voters can cast vote from anyplace by logging with basic details on a local blockhain network through web and cast vote using a crypto wallet. As each activity is performed through web on each block it becomes impossible to change or modify a particular block.

REFERENCES

[1] Archit Pandey, Mohit Bhasi and K.Chandrasekaran, "Votechain: A Blockchain Based E-Voting System", 2019 Global Conference for Advancement in Technology (GCAT), INSPEC Accession Number: 19319487, doi: 10.1109/GCAT47503.2019.8978295.

[2] S.Gopi, B.Giridharan, R.Mohamed Rifoy, S. Sivachidambaram and S.Yuvaraja, "Effective In-house Voting and Implementation Using Blockchain Verification", e-ISSN: 2395-0056, vol. 6 Issue: 03 | Mar 2019.

[3] Venkata Naga Rani, Akshay S, Arun Kumar and Ishwar Kumar MA, "Decentralized E-voting System", p-ISSN: 2395-0072, vol. 6 Issue: 03 | Mar 2019.

[4] Kriti Patidar and Swapnil Jain, "Decentralized E-voting Portal Using Blockchain", 2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT), INSPEC Accession Number: 19277744.

[5] Yash G Gupta, Arun Kushwaha, Amar S Rajeevan, Govind Mhala and Bhagyashree Dhakulkar, "Survey on E-voting Using Blockchain Technology", CiiT International Journal of Software Engineering and Technology, vol.11, January 2019.

[6] Rashadur Rahman "A Secured Electronic Voting System Using Blockchain", ID: 1404073, Chittagong University of Engineering and Technology, Oct 26, 2018.

[7] Ali Kaan Koç, Emre Yavuz, Umut Can Çabuk and Gökhan Dalkılıç "Towards Secure E-voting Using Ethereum Blockchain", International Symposium on Digital Forensic and Security (ISDFS), Vol. 6 , March 2018.

[8] Mrs. Harsha V Patil, Mrs. Kanchan G Rathi and Mrs. Malathi V Tribhuwan, "A Study on Decentralized E-Voting System Using Blockchain Technology", p-ISSN: 2395-0072, vol. 5 Issue: 11 | Nov 2018.

[9] Umut Can Cabuk, Eylül Adıgüzel and Enis Karaarslan, "A Survey on Feasibilty and Suitability of Blockchain Techniques for the E-Voting Systems", IJARCCE, Vol.7, Issue 3, March 2018.

[10] Samuel Agbesi, George Asante, "Electronic Voting Recording System Based on Blockchain Technology", 12th CMI Conference on Cybersecurity and Privacy (CMI), 29 Nov, 2019.

[11] P Apoorva, H.C Impana, S.L Siri, M.R Varshitha and B B Ramesh, "Automated Criminal Identification by Face Recognition Using Open Computer Vision Classifiers", 2019 3rd International Conference on Computing Methodologies and Communication (ICCMC), 27-29 Mar 2019, INSPEC Accession Number: 18958309.

[12] Umut Can Cabuk, Eylül Adıgüzel and Enis Karaarslan, " A Survey on Feasibilty and Suitability of Blockchain Techniques for the E-Voting Systems", IJARCCE, Vol.7, Issue 3, March 2018.

[13] Umut Can Cabuk, Eylül Adıgüzel and Enis Karaarslan, " A Survey on Feasibilty and Suitability of Blockchain Techniques for the E-Voting Systems", IJARCCE, Vol.7, Issue 3, March 2018.

[14] Umut Can Cabuk, Eylül Adıgüzel and Enis Karaarslan, " A Survey on Feasibilty and Suitability of Blockchain Techniques for the E-Voting Systems", IJARCCE, Vol.7, Issue 3, March 2018.

[15] Ahmed Ben Ayed, "A Conceptual Secure Blockchain-based Electronic Voting System", IJNSA, Vol.9, No.3, May 2017.

BIOGRAPHIES

Chaithra.S received her Bachelor in Engineering (BE) degree in Information Science and Engineering (ISE) from Visveswaraya Technological University (VTU), Karnataka, India in 2011 and the M.Tech degree in Computer Science and Engineering from, Visveswaraya Technological University (VTU), Karnataka, India in 2016 and is currently working as a Assistant professor in the department Information Science and Engineering, Rajarajeswari College of Engineering, Karnataka, India. Her research interest includes Internet of Things and Artificial Intelligence.

JK Hima completed her Bachelor of Engineering in Information Science and Engineering from Visvesvaraya Technological University, Belagavi in 2020. She has undergone industry internship at Castleton technology working as a web developer. She participated in Block-athon held by PES, Mandya. She attended "IETE -PANTECH Technical Training on blockchain" held in June, 2020. She also attended 2 day National Level Programme "Blockchain technology" organized by Madanapalle Institute of Technology and Science. She was one of the organising members of Internaltional Women's Day celebration on March 8 2019 organized by Rajarajeswari Groups of Institutions, Bangalore. It is recorded in the Limca Book of Records for the largest human image of Karnataka map in 2 colors, most women taking Oath on women Empowerment and most women displaying messages on women Empowerment.

Rakshita Amaresh completed her Bachelor of Engineering in Information Science and Engineering from Visvesvaraya Technological University, Belagavi in 2020. She has undergone industry internship at Castleton technology working as a web developer. She participated in Block-athon held by PES, Mandya. She attended "IETE -PANTECH Technical Training on blockchain" held in June, 2020. She also attended a core Java course conducted by Rooman Technologies. She was one of the organising members of Internaltional Women's Day celebration on March 8 2019 organized by Rajarajeswari Groups of Institutions, Bangalore. It is recorded in the Limca Book of Records for the largest human image of Karnataka map in 2 colors, most women taking Oath on women Empowerment and most women displaying messages on women Empowerment.