Securing E-Voting System using Blockchain

Abhit Roy[1] , Sarthak Verma[2] , Golda Dilip[3]
Department of Computer Science and Engineering[1 ,2]
Associate Professor, SRM Institute of Science and Technology, Chennai, India[3]
SRM Institute of Science and Technology, Vadapalani, Chennai.

Abstract*— E lections in a Western democracy are a very important case, but vast parts of citizens across the globe have no confidence in their democratic systems, this is a massive problem for democracy. Also the biggest economies in the world, such as India, the United States and Japan, are also struggling from a faulty democratic structure. Poll fraud, the theft of the EVM (electronic voting machine), the bribery of polls and the seizure of polling stations are the main problems with the new electoral method. In this research, we are researching the issues with the voting processes and attempting to develop the e-voting model that can fix certain issues. This research also attempts to analyze the use of blockchain to incorporate automated online voting systems as a software. The paper segment would illustrate several of the common blockchain systems that provide blockchain as a utility and related electronic e-voting mechanism that is focused on blockchain that fixes all shortcomings respectively, thus preserving the privacy of the user and still accessible to public inspection.

Keywords*— Blockchain, SHA256, E-Voting.

I- INTRODUCTION

Blockchain technology that came in 2009 was the underlying concept of the bitcoin ,the first cryptocurrency , has become a fashionable subject in today's package world[2]. Blockchain was originally used primarily for money exchanges and trading, although experiments have started to indicate that, as a consequence of a strong degree of anonymity during this period, With time this may be seen in other ways. T hrough Bitcoin, for example, the entire amount of coins and simultaneous collective action in the world can be checked for momentarily and simply[2]. In this P2P-based network, there is no need for a central authority to sanction or complete the operations.

As a consequence, however, not just the money transactions will be unbroken throughout this distributed chain, and the network will be held securely with the aid of certain cryptographic means. Like the assets of people, wedding certificates, checking account books, medical info, and so on, tons of data will be recorded with relevant modifications using this method. Ethereum coin (Ether)[3], another cryptocurrency with valuable creation conditions, which appeared many years after Bitcoin, defines the blockchain in an incredibly specific way, disclosing that this system can generate package that will contain knowledge that is organized as higher than delineate.

The package programs enforced by sensible contracts (explained later) area unit written into the blockchain and area unit changeless. If published, they can not be (illegally) deleted nor manipulated. Therefore, with no external stimulus, they can function perfectly, autonomously and transparently for ever. As already reported, aside from digital trading, the blockchain network with its distinctive centralized and secured framework could address many issues. It would be fully appropriate answer for e-voting comes.

E-voting is being studied extensively, and lots of implementations area unit tested and even used for a minute. However, only a few versions of the area units are relatively successful, so the area unit is still in usage. There are many popular Internet voting polls and questionnaires. This is mainly due to official elections area unit essential parts of democracy and democratic administrations, this area unites the most popular methodology of the body in time[6]. More, what's most valued in democratic societies may be a sturdy electoral method that has transparency and privacy[6]. Today, lots of area selection units produced by individuals (and representatives of organizations) indicates the area unit utilized of loads of fields originating from the region of selection systems.

Obvious advantages of e-voting using blockchains include:

i)Greater openness thanks to transparent and distributed ledgers[5]. ii) Inherent confidentiality[5].

iii) Protection and efficiency (especially against Denial of Service Attacks)[5].

iv) Immutability (strong voting integrity and individual votes)[5].

II. EXISTING SYSTEM

In modern democracy, voting for a specific candidate is done using Electronic Voting Machine (EVM), and voting for each and every candidate and their parties is done separately in each district. Also the result is announced later once the counting is done.

1) Architecture Description: -

Electronic Voting is the voting system where electronic devices are used to cast and count the votes. In this system, standalone Electronic Voting Machines (EVM).

2) Methodology:-

Electronic Voting is the voting system where electronic devices are used to cast and count the votes. In this system, standalone Electronic Voting Machines. A n EVM is composed of two units: (i)the control unit and (ii) the ballot unit. Those units are connected by a wire. The EVM's control unit is maintained alongside the presiding officer or polling officer. The balloting unit is kept within the voting compartment for electors to cast their votes. This is done to ensure that the polling officer verifies your identity.With the EVM the polling officer must click the ballot button instead of issuing a ballot paper, which allows the elector to cast their vote. A list of noms and/or symbols of candidates will be available on the screen next to it with a blue button.

3) Challenges of existing system:-

- The existing system is not transparent. There is no surefire way of checking if a voters' votes were registered in or not in the central database.
- It is not secure as there have been many instances where the confidential information of the voters was leaked.
- The present voting environment is no open process. Its internal workings are only available to certain individuals, as opposed to being open to the public.
- A power-hungry organization can easily manipulate the system.
- The current election process is a very expensive affair that requires heavy prior planning, organization of police officials and other election officials.
- For the results of the election, the public have to wait for a certain duration. Thus, it is easy to forge the votes during this period.
- For casting the vote to the candidate the voter has to go to the voting booth to cast their vote. Thus, there is no online portal to cast the vote.

III. PROPOSED SYSTEM

The primary aim behind the implementation of blockchain into the current democratic system is to open up the whole voting process to citizens. Some of the extra goals that can be achieved are like removal of forgery from the parties' end, hacking of EVM and fake voter Id's. Thus, this will make the whole system more secure and tamper-proof.

1) Participants:

- *Miner:-* To ensure that only eligible voters can vote, the e-voting protocol was deemed necessary for the establishment of a central authority. The miner is responsible for having contacts to the voters to vote their ballot online and for offering the consent of the election committee to accept the parties and candidates and also to upload the election results to the ledger. The miner will be the first block of the blockchain i.e genesis block. When the miner has approved the order, it generates the new block and the key hash
- *Voter:-* A elector known by one's public key is deemed to be an person authorized to cast a ballot against one of the candidates. A elector still has the right to register an Invalid ballot as a means of dissent, which would not be counted against the final result but will be entered into the system, however.
- *Election Commission:-* The election commission is responsible for registering the parties and the candidate as per their district.

2) Modules:

- *Requesting to vote:-* Using his identity, the individual would have to sign in to the voting program-in this situation, the e-voting system would use his Social Security Number, his address and the vote validation number sent to registered voters by local authorities. Any details received would be verified by the algorithm and, if matched to an eligible elector, the individual will cast it. a ballot. Our e-voting system requires electors to establish their own identities and to register for voting. Systems for generating arbitrary identity are typically susceptible to the attack at Sybil, where attackers assert a large number of false identities and fill the ballot box with illegitimate votes.
- *Casting a vote:-* Voters would either have to opt for one of the parties, or cast a dissenting ballot. Voting may be performed through a user-friendly interface. For each elector, a token known as Ethereum is created, with the initial Boolean value one and after a vote is a cast, it becomes 0[1]. If and only if the sum of the ethereum is 1. Voting can be taken by an elector It solves the question of revoking.
- *Encrypting vote:-* After the user casts his vote, the system will generate an input that contains the voter After the consumer casts his ballot, the program would produce an input containing the voter ID number accompanied by the elector's full name as well as the previous ballot hash. That would be a different way of feedback and the authenticated performance would be unique too. Every vote cast will record the cryptographic details in the block header. The details connected with each vote will be authenticated using a one-way hash function of SHA that has no established reverse. The only way to reverse the hash potentially is to guess the seed data and the form of encryption, and then hash it to see if the tests correlate. The process of coding votes makes it almost impossible to reverse

engineer, so no means would be available to obtain information from the electorate.

- *Adding the vote to the Blockchain:-* Once the voting is done the super admin will add the result to the ledger.

3) SHA-256 Algorithm:-

In this we are using the SHA-256 algorithm to encrypt the casted vote thus this makes the whole system verifiable and more transparent. SHA-256 is the cryptographic algorithm that is newer and more efficient. The SHA-256 algorithm generates a 256-bit hash value from packed 512-bit message fragments, with an initial message length of up to 264-1 bytes. SHA-256 often dynamically measures a 256-bit hash for verification, but that can be truncated to either 196 or 128 bits printing and storage. Thus a truncated SHA-256 in written quotes provides a major advantage to human accessibility and dramatically increases protection at the cost of a minor output loss relevant to SHA-1. In order to scale the e-voting platform it is necessary to use the most efficient algorithm in order to do the operations faster, securely and give the results immediately.

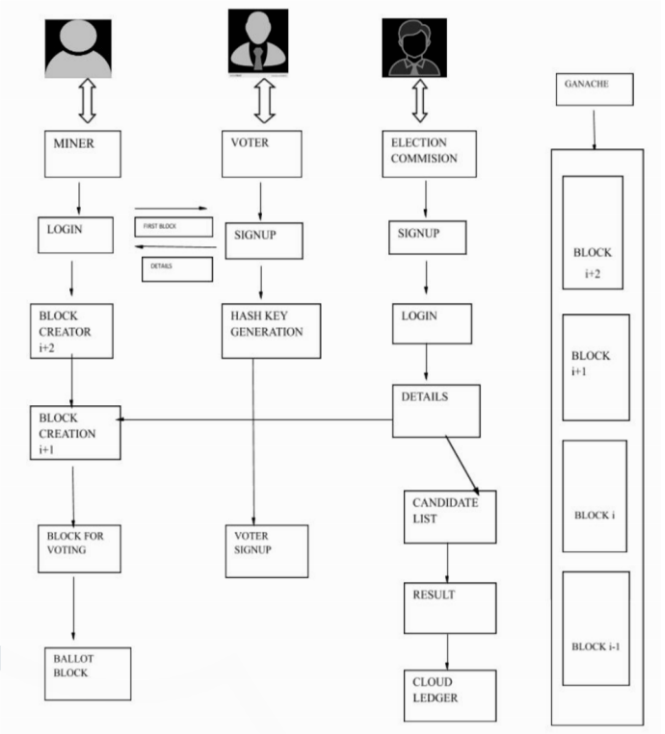

Fig 1: Architecture of blockchain-based e-voting system

IV. SYSTEM ARCHITECTURE

The system architecture is used to explain the working of the software or module according to its principles, concepts, and characteristics which are logically related and consistent with each other. The design of the approach has the attributes, properties, and functions that solve as many challenges as possible or the potential provided by the job method and the definition of the life cycle and applied by the technologies.

This is an abstract, conceptual-based, regional, and program-oriented word to attain the goal and work-life span of the method. System architecture also concentrates on the high-end structure in the system and system elements. One architecture can be used for representing the common structures, pattern and set of requirements for similar classes and families.

Referring to Fig. 1, We can see that the framework mentioned in this paper is about the committee of miners, voters, and the election commission. Initially, the miner will log in. As soon as he logs in, genesis block will be created. A hash will be generated for the first block. This will not have any previous hash. Then the voters will sign up. The voters will not be able to log in till the miner verifies their account. Once the miner verifies their account each voter will be assigned with a new hash and their previous hash will be the same as the miner's hash. Then the election commission will sign up. Even he will not be able to log in till his account is verified by the miner. Once the miner verifies the election commission a new hash will be assigned to him with the previous hash same as the miner's hash. Then the election commission has the role to register parties. Parties will be registered using the candidate's name, photo, symbol, and district. Every elector will only vote once, then he will not be allowed to change his / her vote. Voting will be done separately for each region. Even the miner is not allowed to change the votes. Voting will be conducted for each district separately. Even the miner is not

allowed to change the votes. At last, when the voting is over, the result will be uploaded to the cloud by the miner and the result will be displayed similar to Table I a nd Table
II.

TABLE I

S.No	Category	Data
1.	Candidate Name	xyz
2.	Candidate District	abc
3.	Candidate Hash	5c7953c85845f9ce0929c5b236aa57d66dbca8ca15ae665121c6981b3cf0362b
4.	Vote Count	434

```
{
  "hash": "84940be38352452f3298bffc279aa0dfcac9e90d117caff525e3fe8a0a17f040",
  "previousHash": "0",
  "data": "Admin",
  "timeStamp": 1582523939632
},
{
  "hash": "0e9824e6f61bbbb8e9ef51ba92d30277d1a6eea5b7a2b2de70dd89f93ad500de",
  "previousHash": "84940be38352452f3298bffc279aa0dfcac9e90d117caff525e3fe8a0a17f040",
  "data": "abhit",
  "timeStamp": 1582524030551
},
{
  "hash": "8887b788872fde495963e9ab5f9301e274143cc20f4ccf423d1da903bcb1325f",
  "previousHash": "0e9824e6f61bbbb8e9ef51ba92d30277d1a6eea5b7a2b2de70dd89f93ad500de",
  "data": "sarthak",
  "timeStamp": 1582524100737
},
{
  "hash": "aaa56eb54b85ed7ad4fa25e05be08e45dbd3e629ded05bc23b5a08617da6f964",
  "previousHash": "8887b788872fde495963e9ab5f9301e274143cc20f4ccf423d1da903bcb1325f",
  "data": "Aakash",
  "timeStamp": 1582524126380
},
{
  "hash": "341defea36bb964199e2fcffb79850dd478625d8a94887b90b1c3c6255e23be9",
  "previousHash": "aaa56eb54b85ed7ad4fa25e05be08e45dbd3e629ded05bc23b5a08617da6f964",
  "data": "jerome",
  "timeStamp": 1582524168468
},
{
  "hash": "91f9b5326f3dbd9265538c496df96ba1a7edf99cae4fbb54215c8553815d7542",
  "previousHash": "341defea36bb964199e2fcffb79850dd478625d8a94887b90b1c3c6255e23be9",
  "data": "Government",
  "timeStamp": 1582524205691
},
```


TABLE II

Fig. 2: Output with block information

S.No	Category	Data
1.	Candidate Name	pqr
2.	Candidate District	lkz
3.	Candidate Hash	40c494706007c42dcc74c73ac048469bcce66dba5b0d0ffb46c6c87d3e159b1e
4.	Vote Count	337

V. IMPLEMENTATION

For the implementation, we have used NetBeans as a platform to run Java codes along with Ganache and Metamask. We are using a solidity programming language to write the smart contract for e-voting on ethereum platform. To integrate the web-based application with the blockchain we are using web3js. The NetBeans output has been shown in Fig. 2. The code snippets can be seen in Fig.
3.

```
window.App = {
    start: function () {
        var self = this;
$.getJSON('public/js/MetaCoin.json', function (data) {
          var AdoptionArtifact = data;
         console.log("AdoptionArtifact",AdoptionArtifact);
          MetaCoin = TruffleContract(AdoptionArtifact);
        console.log("MetaCoin 1",MetaCoin);
          MetaCoin.setProvider(new Web3.providers.HttpProvider("http://localhost:7545"));
        });
    console.log("web3.eth",web3.eth);
    web31 =web3;
        web3.eth.getAccounts(function (err, accs) {
            if (err != null) {
                return;
            }

            if (accs.length === 0) {
                  return;
            }
            accounts = accs;
            account = accounts[0];
            console.log("Maccount :: ",account);
            fromAccount = accounts[0];
            toAccount = accounts[0];

             alert("fromAccount :: "+fromAccount);
             alert("toAccount :: "+toAccount);
            self.refreshBalance();
           self.sendCoin(fromAccount,toAccount);
        });
},
    setStatus: function (message) {
        var status = document.getElementById("status");
        status.innerHTML = message;
},
    refreshBalance: function () {
        var self = this;
var meta;
         console.log("meta1",meta);
         console.log("MetaCoin",MetaCoin);
          web3.eth.getBalance(account,function(error,result){

    if(error){
       console.log(error)
    }
```

Fig. 3 Code Snippets

VI. FUTURE ENHANCEMENTS

Considering the current situation of modern democracies it is very important for the application to be scalable so that it can be used by large number of people efficiently. Since there is a tradeoff between transaction throughput and scalability. The same can be seen in the existing framework because the implementation of blockchain technologies would render the framework of better efficiency and scalability far simpler.

VII. REFERENCES

[1] Ali KaanKoc, EmreYavuz,Umut Can Cabuk,GokhanDalkoloc "Towards Secure E-Voting Using EthereumBlockchain", 978-1-5386-3449- 3/18/$31.00 ©2018 IEEE.

[2] S. Nakamoto, “Bitcoin: a peer-to-peer electronic cash system”, [Online]. Available: https://bitcoin.org/bitcoin.pdf.

[3] G. Wood, "Ethereum: a secure decentralised generalised transaction ledger", Ethereum Project Yellow Paper, vol. 151, pp. 1-32, 2014.

[4] C.D. Clack, V.A. Bakshi, and L. Braine, “Smart contract templates: foundations, design landscape and research directions”, Mar 2017, arXiv:1608.00771. [5] Freya Sheer

Hardwick, Apostolos Gioulis, Raja Naeem Akram, and Konstantinos Markantonakis, “
E-Voting with Blockchain: An E-Voting Protocol with Decentralisation and Voter Privacy”, arXiv:1805.10258v2 [cs.CR] 3 Jul 2018
[6] N. Braun, S. F. Chancellery, and B. West. "E-Voting: Switzerland's projects and their legal framework–In a European context", Electronic Voting in Europe:
Technology, Law, Politics and Society.
GesellschaftfürInformatik, Bonn, pp.43-52, 2004. [7] Y. Takabatake, D. Kotani, and Y. Okabe, “An anonymous distributed electronic voting system using
Zerocoin“, IEICE Technical Report, pp. 127-131, 2016.