

# Secure Online Voting System Using Blockchain

P Saichand, Nlolesh, P Srinivasa Reddy, R Amar Vinay Surya

Department of CSE, Vasireddy Venkatadri Institute of Technology, Guntur, Andhra Pradesh, India

## ABSTRACT

ONLINE VOTING SYSTEM is an online voting technique. In this system people who has right to vote in any place and whose age is above 18 years of any gender can cast his her vote online without going to any physical polling station. The main goal of voting is to come up with leaders of the people's choice. Elections in democratic countries have many issues affecting the fairness of election results. Firstly, some people do not care to vote for a variety of reasons, including lack of faith in the system and believing that the effort is not worth it. Secondly, troublesome voter-ID laws prevent citizens from voting if their ID fails to meet the requirements at the polling booth. Thirdly, voter fraud exists, where dishonest voters manage to vote multiple times for the same candidate, skewing the results. Fourthly, voting machines could be outdated and its accuracy cannot be guaranteed. Lastly, long voting lines at polling booths can discourage people from voting. Recently, much discussion and controversy arose on the missing votes of citizens in elections. Conducting elections through a DApp on the Ethereum platform can provide transparency, security and credibility to the process. This would prevent voter fraud as one voter can only have one ID and all polling systems are on the blockchain, which can identify duplicate attempts to vote . Governments can also save the logistics costs of holding physical polling booths and counting votes.

**Keywords :** Blockchain, Ethereum, Smart contract, Solidity, Truffle, DApp

## I. INTRODUCTION

The main goal of of voting is to comeup with leaders of the people's choice. A worthy e-voting system must perform most of this tasks while complying with a set of standards established by regulatory bodies and must also be capable to deal successfully with strong requirements associated with security, accuracy, integrity, swiftness, privacy.

The problems associated with elections can be avoided if the vote counting process was transparent, verifiable, and fair. The current system provides anonymity to the voted but it is not considered to be transparent. People are expected to trust the results

that is announced by the government when it comes to elections. There are many frauds involved in voting like ballot stuffing, booth capturing and voter fraud. All this is making the process of voting really hard. Another problem involved when considering indian elections is that the voting centres are far an the voter has to physically go to voting centres inorder to vote so the ratio of the amount of people who caste their vote and people who are eligible to vote an is reducing drastically. Blockchain uses encryption and hashing to make every vote secure. In this case, one vote is considered as a transaction. A peer to peer network is created to create a private blockchain that share this distributed ledger having voting transaction.

## II. METHODS AND MATERIAL

Ethereum has a huge opensource community having large varieties of softwares that can be used together to build secure distributed application. Considering the underlying security that ethereum provides ranging from digital signatures to hashing, it is difficult to change the source code of the given software.



Fig 1 : System Design

### A. Methodology

Ethers is the currency that is used to fuel ethereum network, in some terms it is also referred to as gas. All operations that you perform on this network requires some amount of gas to get it running. In our infrastructure, each vote is taken as one transaction, so whenever one vote is casted, a transaction is submitted to the blockchain network. To submit transactions the voter need, provide some amount of gas. In blockchain terminologies, you have a peer and a user which is the voter of our application. Peers are the miners that mine blocks or transactions that are submitted. A block is a set of transactions. These blocks are continuously mined by these peers. In our infrastructure, we have set up a private blockchain network so that we can decide as to what peers we want to connect to the network. Any peer that is routable and can be reached can be added to the peer. This is one distinction between a private and a public blockchain. All miners that are present in the network

should have high computational power and memory because mining is a compute intensive process that involves all the miners to solve a puzzle inorder to win a reward in the form of ethers or bitcoin in bitcoin networks.

### B. Contents of a block

The block contents can be seen by using its hash as the identifier as a hash of one block is unique in a blockchain. The contents of one block consists of the following information:

1. Block hash: This is the hash generated using the information about the hash of the previous block, the timestamp, the version of the software used, the Merkel root or the binary hashing of all the transactions that are present inside the blocks of the blockchain, the difficulty value that is specified in the genesis file and the nonce or the random number that is generated in the mining process.
2. Block number: This is the next consecutive number in the blockchain.
3. From: This refers to public key of the voter who has performed the which is the vote in this case. As discussed, every voter is associated with set of public, private keys.
4. Gas used: This refers to the amount of gas or ethers used to complete this transaction. This is supplied by the voter who has performed transaction.
5. Status: This field gives information about whether the transaction is successful or not, status 1 stands for a successful transaction and 0 if unsuccessful
6. To: This is the public address of the smartcontract to which the transaction is submitted to.
7. Transaction hash: It is an identifier that identifies a particular transaction.

### C. Genesis Block

This is the primary block in a network. Following are the contents of the genesis block:

1. Difficulty: Measure of the toughness of mining.
2. Gas Limit: Maximum amount of gas that is spent on one transaction.

- 3. Gas Used: Blockchain network is brought up by using few amounts of gas/heaters.
- 4. Mix Hash and Nonce: These terms infer if mining is completed successfully.
- 5. Parent Hash: This is the Keccak 256-bit hash of the previous blocks header. Although it is meaningless to have this field in the genesis block since it is the first block in the block chain. This field is used so that this block is similar to other blocks in the blockchain.
- 6. Time Stamp: It is the time when the block is created as per the system time.
- 7. Uncle: These are the blocks that are orphaned and provides security.
- 8. Size: This is the size of the blockchain in bytes.

#### D. Pseudo Code for smart contract

The pseudo code for our smart contract is as follows:

Contract voting:

```
hashMap votesReceived[candidateName=>votesReceived]
candidateList[]
```

getter function to return the number of votes a candidate #receives

```
function totalVotesFor(candidateName):
```

Input: Candidate Name

Output: Votes Received

```
return votesReceived[candidateName]
```

increments vote for a candidate

```
function voteForCandidate(candidateName):
```

Input: Candidate Name

```
votesReceived[candidateName]++
```

#checks if the candidate is valid

```
Function validCandidate(candidateName)
```

Input: Candidate Name

Output: Boolean Value

```
if candidateName is in candidateList
```

```
return True
```

```
else
return False
```

### III. RESULTS AND DISCUSSION

Voting application has served its purpose by incrementing the vote upon casting and keeping track of the number of votes a candidate has received.

In comparison to the existing methods, our proposed method is better in a way that it is simple, scalable and reliable. In the sense that it doesn't require any third-party resources like testrpc and ganache that is used to generate test ethers. In our topology we generate our own ethers by mining. The blockchain employed is private in the sense that only permissioned peers can access the blockchain. The application is easy to use and user friendly. Scalability is offered using MongoDB and the blockchain file system that is used to store the information of the blocks. Only valid users are allowed to vote and accordingly using the national identities each voter is authorized. In that way the logic is made simple and modular.

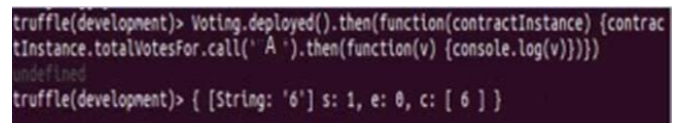


Fig 2 : Output on querying number of votes

### IV. CONCLUSION

This app addresses security factors like :

1. verification
2. transparency of counting votes
3. integrity
4. non-repudiation of votes

With the ethereum blockchain, any group can sort out a free, secure electronic voting. Ethereum and the smart contracts are the progressive achievements since the blockchain itself, precluded the restricted impression of blockchain as a digital currency (coin),

and transformed it into a versatile answer for some Internet-related issues of the present world, and may empower the wide utilization of blockchain.

## V. REFERENCES

- [1]. Shalini Shukla, Thasmiya, Shashank, Mamatha. Online Voting Application Using Ethereum Blockchain. 2018 International Conference on Advances in Computing, Communications and Informatics (ICACCI).
- [2]. Emre Yavuz, Ali Kaan Koc, Umut Can Cabuk, Gokhan Dalkilic. Towards secure e-voting using ethereum blockchain. 2018 6th International Symposium on Digital Forensic and Security (ISDFS)
- [3]. Jia Kan, Shangzhe Chen, Xin Huang. Improve Blockchain Performance using Graph Data Structure and Parallel Mining. 2018 1st IEEE International Conference on Hot Information-Centric Networking (HotICN)
- [4]. Ethereum Homestead Documentation. [Online], Available: [www.ethdocs.org/en/latest/](http://www.ethdocs.org/en/latest/)
- [5]. Ali Kaan Koç, Emre Yavuz, Towards Secure E-Voting Using Ethereum Blockchain, 1st ed, vol 1, 2018 IEEE
- [6]. Solidity Ethereum Virtual Machine, <https://www.bitdegree.org/learn/solidity-ethereum-virtual-machine>
- [7]. G. Wood, "Ethereum: a secure decentralised generalised transaction ledger", Ethereum Project Yellow Paper, vol. 151, pp. 1-32, 2014.

## Cite this article as :

P Saichand, N lokesh, P Srinivasa Reddy, R Amar Vinay Surya, "Secure Online Voting System Using Blockchain", International Journal of Scientific Research in Computer Science, Engineering and Information Technology (IJSRCSEIT), ISSN : 2456-3307, Volume 5 Issue 2, pp. 586-589, March-April 2019. Available at doi :

<https://doi.org/10.32628/CSEIT1952162>

Journal URL : <http://ijsrcseit.com/CSEIT1952162>