e-ISSN: 2582-5208

International Research Journal of Modernization in Engineering Technology and Science

(Peer-Reviewed, Open Access, Fully Refereed International Journal)

Volume:04/Issue:04/April-2022 Impact Factor- 6.752 www.irjmets.com

ONLINE VOTING USING ETHEREUM BLOCKCHAIN

Ashish Yoel[*1], Mrs. S. Kiruthika Devi[*2]

[*1]Student, Computer Science And Engineering, SRM Institute Of Science And Technology, Lucknow, India.

[*2]Professor, Computer Science And Technology, SRM Institute Of Science And Technology, Chennai, India.

ABSTRACT

The voting process is an important thing in every country. It is ever evolving as the government tries to provide the best possible way to conduct elections. The electronic voting or e-voting revolutionized the voting process. But it has its own drawbacks. National elections still use a centralized system, with only one organization in charge. One of the possible problems with traditional electoral systems is the organization that fully controls the website and the system, potentially disrupting the database and also can change the rules of the election at any given time. Blockchain is the solution to the problem of online voting. In blockchain, whenever the data is added to the network its copy is given to all the other devices present in the network. Thus blockchain removes the chances of data manipulation.

Keywords: Online Voting, Government, Smart Contracts, Ethereum Blockchain, Solidity, Truffle, Metamask.

I. INTRODUCTION

Voting is a fundamental right of every citizen of the country that enables them to choose the leaders of tomorrow. Voting not only enables a citizen to vote for their favorite political party but it also helps them to realize the importance of citizenship. A nation's political foundation is built using elections. Government is always trying to improve the experience of elections so that more and more people participate in the elections. With the introduction of Electronic Voting Machine or EVM the voting experience has definitely improved considering where it started originally.

In the traditional way of voting in an election the voter has to go to the voting booth allotted to them, get their voter id checked, get the election slip and after the indelible ink applied to their finger only then they can vote in an Electronic Voting Machine or EVM. This method requires a lot of staff and not to forget that the election is conducted in many parts of the country simultaneously. The EVM can malfunction at any time requiring re-election. Adding to this, a lot of paper is in conducting offline elections. Online voting can be a way to conduct the elections but it has its own problem.

In the client-server architecture all the code, rules of the election and data is stored in a centralized server which has many drawbacks:

- Votes can be altered at any time.
- Rules of the election can be changed.

So making a centralized web application for online voting may not be a good idea.

So making the application using blockchain technology can result in something which we as a voter can rely on. Blockchain is making a big impact in today's world of technology. It has wide applications in different fields. Cryptocurrency is one of the real world examples which is based on blockchain. In the blockchain the data does not lie in a central server but instead the data is decentralized i.e. it's distributed across all the devices connected to it. Blockchain is a peer-to-peer network of nodes which communicates to one another. In blockchain data is contained in the bundle of records called blocks which are chained together to build the public ledger. All the nodes in the network work together to ensure that data in the public ledger remains secure and unchanged. This eliminates single-point of failure with groups working together to ensure the legitimacy of the transaction. The blockchain is both a network and a database since we can securely store data in it and connection of all the devices creates a network.

All the data in the blockchain is decentralized and secured. Similarly, the code on the blockchain is shared and unchangeable. The ethereum blockchain allows us to write the code that we can deploy to the blockchain and nodes on the network will execute this code.

All the features described above are important for our voting application because it means that the user will always know that their account has sent a particular transaction whenever we vote and the vote goes to the correct candidate and is recorded forever. And also the code which will contain the rules of the election which will be unchangeable forever.

The main things to focus here are the anonymity of the voter, verification of the vote and secrecy of the vote.

II. LITERATURE SURVEY

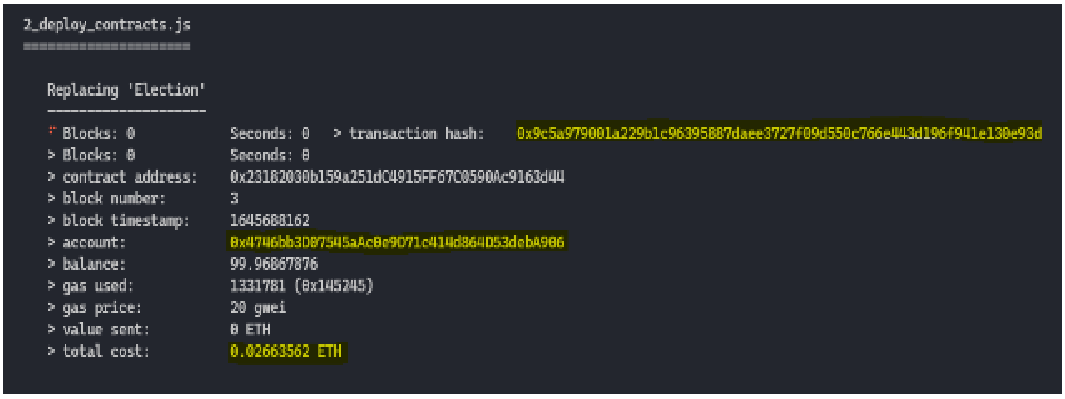
From the start elections are carried out in the offline mode. There was no feasible solution for conducting the elections online. But with the ever-increasing influence of technology on the world, the process of election can also be taken to a whole new level. Online voting is a new concept and with the help of emerging technology of blockchain it can be achieved.

The voter can participate in the elections in the comfort of their home. There will be an administrator which will be appointed to monitor and organize the elections and will be given the admin access for the application. The major thing that is assumed here is that the voter has access to the internet, owns a computer and knows how to operate it. The part of the entire proceedings,and not as an independent document. Please do not revise anyof the current designations.

III. PROPOSED WORK

Requirements for carrying out the voting process:

- Privacy: The privacy of the voter is of utmost importance. The vote of the voter should be accounted for in the final counting but the system should not record the details of the vote, mainly the name of the candidate the voter voted for.
- Eligibility: Only the eligible voter should be able to participate in the voting. The verification will be using Electors Photo Identity Card (EPIC) which contains the unique voter id number. The EPIC can be made only for the people who are eligible to vote i.e. citizens of the country above the age of 21. In the future, a solution can be found where the voter registers using their Aadhar Card. And only then the eligible and the registered user will be allowed to participate in the voting process.
- Convenience: The voting process should not be very complicated. The application should be with a very user-friendly interface. Although the process requires the meta-mask wallet in the web browser to communicate to the ethereum blockchain, the process should be simple enough so that people don't get frustrated.
- The voters should be unable to prove to other people/users that they voted to a particular candidate. There should be no information that relates the voter to the candidate he/she votes. The system should not extract information from the voter.
- With each transaction there is hash code generated with it, known as the transaction hash which is unique throughout the blockchain network. The voter upon the successful casting the vote will be given this transaction hash. Using this unique generated hash code, the voter can verify that their vote is counted in the final vote count. Although the user will not be able to see how they voted since the system will not record it while voting. The screenshot of the transaction hash (for the vote) is shown in Figure 1.



```
2_deploy_contracts.js
=====================

   Replacing 'Election'
   --------------------
   ⠋ Blocks: 0            Seconds: 0   > transaction hash:    0x9c5a979001a229b1c96395887daee3727f09d550c766e443d196f941e130e93d
   > Blocks: 0            Seconds: 0
   > contract address:    0x23182030b159a251dC4915FF67C0590Ac9163d44
   > block number:        3
   > block timestamp:     1645688162
   > account:             0x4746bb3D87545aAc8e9D71c414d864D53debA986
   > balance:             99.96867876
   > gas used:            1331781 (0x145245)
   > gas price:           20 gwei
   > value sent:          0 ETH
   > total cost:          0.02663562 ETH
```

Figure 1: Screenshot of the transaction hash generated when the code is deployed to the blockchain

- The eligible voter should be allowed to cast the voter only once. This can be by storing the voter id number and the address hash of the device which is unique for each device connected to the blockchain network.

The flow of user interaction in blockchain is shown in Figure 2.

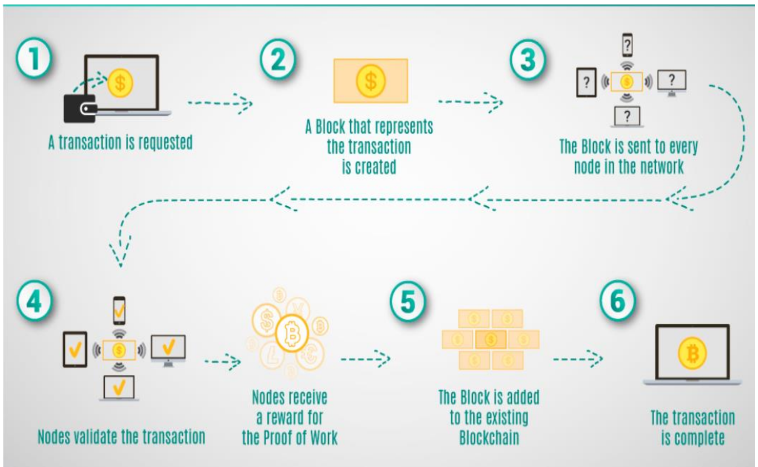

1
A transaction is requested
2
A Block that represents the transaction is created
3
The Block is sent to every node in the network
4
Nodes validate the transaction
Nodes receive a reward for the Proof of Work
5
The Block is added to the existing Blockchain
6
The transaction is complete

Figure 2: Example of the flow of interaction in a decentralized application.

At the first level there will be front-end security. This is responsible for interacting with the voter for voting functions and the administrators/executives for the function relating to managing the elections. The fingerprinting of the voter's device address is done at this stage. The user's browser should have a blockchain wallet such as Metamask installed in it, which is used to interact with the network. This is also checked at this level. After the transaction is sent from the user's device a block is created that represents the transaction. The block contains the current timestamp, current version of the block, transaction hash of the previous block and the cryptographic hash of the data which is to be added to the blockchain also known as merkle data. This block is then sent to every node in the network and it is validated by those nodes. The block is added to the blockchain and the transaction is complete.

So for now this is a fully decentralized application since all the rules of the election and the votes are to be kept secured. But it can be changed to semi-decentralized application according to our needs.

IV. IMPLEMENTATION

The voter:

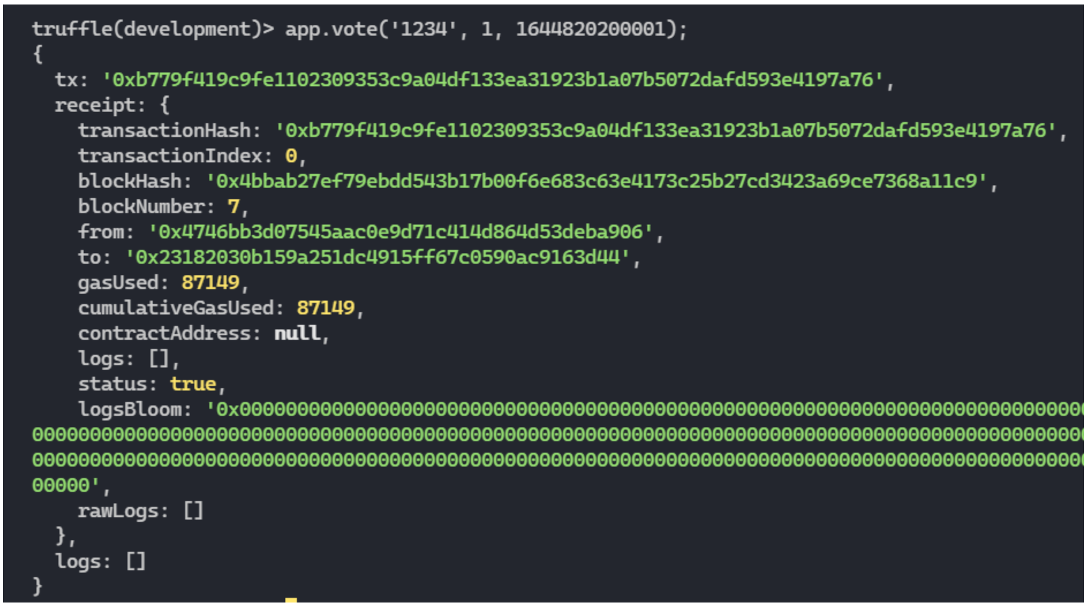
When a voter votes with their device, the voter id number and the device address is recorded as mentioned in the previous section. As per our proposed model, we allow one person, one machine, one vote.

Firstly, the voter will enter his/her voter id number from the EPIC. The entered voter id number will then be checked in the blockchain database. If the match is found, the application will show the message "The entered voter id is already present in the system, please retry with a different voter id number" and further access will be denied. If the voter id number is new but the device address is present in the database then the application will show the message "The device address is present, please try with the new device" and further access will be denied. The double authentication is an attempt to prevent biased votes. If the match for both the voter id number and the device address is not found, then the voter is shown the list of candidates he/she can vote for. The voter can choose the candidate from the list, pay and gas fees and complete the voting process.

After the successful casting of the vote, the data is mined by the miners of the blockchain. The miners will validate the data which is requested to be added to the public ledger. Once the block is validated, it is added to the blockchain and the voter is provided with the transaction hash which is a unique hash code which is generated with every transaction in the blockchain. With this transaction hash the voter can verify that the vote is counted in the final result. The sample transaction result is shown in Figure 3.

The administrator:

The responsibility of the election administrator is to organize the elections, monitor the elections and add the candidates participating in the elections. The administrator of the election can be a representative from the election commission or the other person appointed by the government.



```
truffle(development)> app.vote('1234', 1, 1644820200001);
{
  tx: '0xb779f419c9fe1102309353c9a04df133ea31923b1a07b5072dafd593e4197a76',
  receipt: {
    transactionHash: '0xb779f419c9fe1102309353c9a04df133ea31923b1a07b5072dafd593e4197a76',
    transactionIndex: 0,
    blockHash: '0x4bbab27ef79ebdd543b17b00f6e683c63e4173c25b27cd3423a69ce7368a11c9',
    blockNumber: 7,
    from: '0x4746bb3d07545aac0e9d71c414d864d53deba906',
    to: '0x23182030b159a251dc4915ff67c0590ac9163d44',
    gasUsed: 87149,
    cumulativeGasUsed: 87149,
    contractAddress: null,
    logs: [],
    status: true,
    logsBloom: '0x000000000000000000000000000000000000000000000000000000000000000000000000000
000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000000
00000',
    rawLogs: []
  },
  logs: []
}
```

Figure 3: Sample transaction for voting

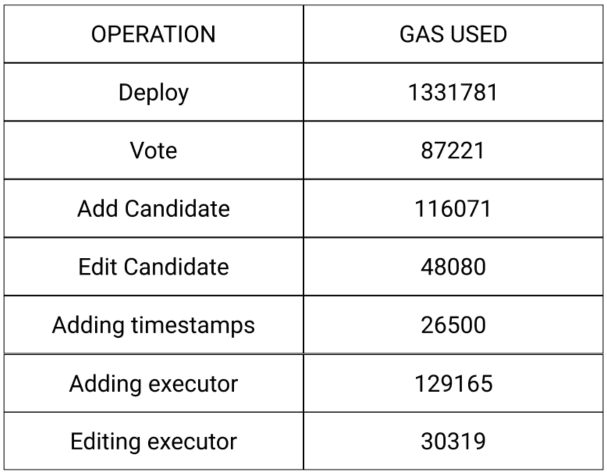
The admin has a lot of jobs. The most important of all is starting and ending the elections. The admin will enter start time and the end time which then will be converted into timestamp and stored in the blockchain. The elections will automatically start and end but this task has to be done by the admin.

The information of the political parties which are participating in the election are to be added by the administrator themselves. The facility of editing the information should also be available. The most important thing to note is that when the election is in process, the admin should not be able to add, edit or delete the information about any political party.

The elections are happening simultaneously at various places so it'll be difficult for one person to manage the process. So the facility to add more executors, working under the main administrator to manage the process of elections. The administrator has to give a unique username and a password and give it to an executor as login credentials. The executor can have any of the two roles: Viewer and Editor. The Viewer can see the progress of the ongoing elections. While the Editor can add and change the details of a political party as well as viewing the ongoing progress of the elections. The privilege of starting the elections remains with the main administrator.

V. ANALYSIS

On the ethereum blockchain there is a cost required to perform any change on the blockchain known as the gas cost. The cost is determined by the miners and it is based on supply and demand and the computational power needed to execute the code in the smart contract. Figure 4 shows the table with the operation and the resource used associated with execution of the smart contract code.



OPERATION	GAS USED
Deploy	1331781
Vote	87221
Add Candidate	116071
Edit Candidate	48080
Adding timestamps	26500
Adding executor	129165
Editing executor	30319

Figure 4: Gas used for various operations

VI. CONCLUSION

With the growth in technology the process of election is also getting better with increased efficiency and less errors. Blockchain technology enables us to make secure web applications and its use will increase in the coming future. If the online voting using blockchain is achieved keeping all the requirements in mind it will revolutionize the process of election and more people can participate in it, in the comfort of their home. For making the smart contract ethereum blockchain is used. But there are many other blockchains present which can be used to code smart contracts. Solana (another blockchain) launched in 2019 is gaining popularity in the blockchain market.

VII. REFERENCES

[1] Secure Digital Voting System based on Blockchain Technology by Kashif Mehboob, Khan Junaid Arshad, Muhammad Mubashir Khan.

[2] Blockchain Based E-Voting System by Prof. Mrunal Pathak, Amol Suradkar, Ajinkya Kadam, Akansha Ghodeswar, Prashant Parde.

[3] E-Voting on the Blockchain by Kevin Curran.

[4] Ethereum blockchain documentation: website

[5] Truffle documentation: website

[6] Metamask: website