Secure Blockchain Voting Technology

Baby D Dayana, S Nishanth, A D Krishna, R D Nitish

***Abstract:** The n paper-ballot voting system and Electronic voting machines (EVM's) has provided long term trust among the various places in the world for the purpose of voting. But each of the systems have their own flaw. Introduction of Blockchain for the purpose of Voting can be a remarkable change in the voting system which will be trusted globally. This Paper discusses about casting vote on a blockchain which improves the efficiency of the voting process and also the security of the vote which has been cast by the citizen.*

***Index Terms:** Blockchain, Electronic voting, Hashing, Ethereum*

I. INTRODUCTION

Trust of the people plays an important role in our democracy. The voting system has helped in increasing the trust of the people for the government. Since the trust of the people plays a major role it is important that they don't lose their trust on voting system. Voting is a platform where people get to elect their representatives to form the government. This helps the people with a trust that the government is in safe hands that shall take care of issues like health and education. Institutions like 'Election Commission' came into existence to make the voting process more effective. It is important to make sure that the trust on voting is not decreased. In the recent past there have been several incidents where the voting system faced several issues based on transparency and fairness. To prevent these mistakes, blockchain can be great trusted alternative for casting vote. Since this task is very serious task which is going to decide who will be ruling the country for the next five years it is necessary to make sure that the task is give to a trustworthy agency. The election commission of India plays an important role in this system.

There are 543 constituencies in India which are placed by the elected representatives in each constituency. There is each officer appointed to each region for the purpose of verification and to ensure proper polling is taking place in that particular region. It is the responsibility of the assigned officer of the region to make sure that each and everyone who comes to cast their vote are able to cast their vote without any problem and help each one of the if they have any problem regarding this. They must also make sure that the polling machines are brought at proper time to the respective area without any problem.

The voter's list is prepared by the Election Commission of India prior to the election date and the list is cross checked with the vote id to whomsoever comes to cast their vote. The list is prepared by taking in account of the people who have crossed the age of 18. Once the voter enters the polling booth, he/she will be asked to show the voterId. The details of the voterId will be copied on to the Election commission's database where they have the separate list with all the voters who have casted their vote with the help of the QR code present in the voterId. and also, the biometric scans which take place after that. Once these processes are done the voter is allowed near the voting machine which contains all the candidates and their respective party symbols displayed on a screen. The voter can choose whom he wishes to vote for the displayed information present on the screen. Once the voter has selected the candidate which he wishes to vote he will be asked for confirmation on the same screen for double confirmation whether he/she has chosen the correct option. This polling process continues till the given time frame by the Indian Election Commission. After the elections are over the result from each polling station is sent to the headquarters for the announcement of final results.

II. LITERATURE REVIEW

[1] Ryan Osgood gives an example of the mistrust in e-voting systems by mentioning the Switzerland incident in March 2017, which is during the time of election

the voters did not receive the postal ballots on time, once the ballots were issued, the issued ballots were already voted without any concern from the voters.

The system also insists on needing a more secure, private and a completely reliable system of voting where there is full transparency to the citizens.

[2] Baocheng Wang describes how blockchain based voting is applied only to small scale voting which should be enhanced and used for much bigger storage units and data analysis. The system introduces an anonymous voting scheme. The concept behind this is that block chains are publicly visible, and any transitions can be traced back to its origin and the final recipient. The main advantage of this technique is that each recipient address is unique, thereby won't result in and address rouse and also, no observer can determine whether the transitions are sent to a particular address or two addresses are associated with it. A sophisticated form of cryptographic calculations is used in the voting scheme, where even the time consumed by a single mode is counted. The proposed voting method which is completely based on an onetime ring signature and homographic encryption where it is completely non interactive and non-receipt form of voting method. For a large scale voting in the blockchain, they use DPOS for distributed consensus and miner node to randomize the votes and count the ballots Since DPOS is used, there is a high chance of vulnerability in the E-voting system.

Revised Manuscript Received on October 30, 2019.
* Correspondence Author

Mrs. Baby D. Dayana, assistant professor at the Department of Computer Science, SRM Institute of Science and Technology, Ramapuram
S.Nishanth, student at the Department of Computer Science, SRM Institute of Science and Technology, Ramapuram .
A.D.krishna, student at the Department of Computer Science, SRM Institute of Science and Technology, Ramapuram .
R.D.Nitish, student at the Department of Computer Science, SRM Institute of Science and Technology, Ramapuram .

Retrieval Number: A1441109119/2019©BEIESP
DOI: 10.35940/ijeat.A1441.109119
Journal Website: www.ijeat.org

Published By:
Blue Eyes Intelligence Engineering
& Sciences Publication

[3] Gunnlaugar K , Mohammed Hamdaqa talks about introducing electronic voting systems to minimize the cost of running an election and also ensuring the security , privacy and compliance requirements, since it has the potential to limit fraud, while making the voting process traceable and verifiable. The proposed method in is to use smart contracts, they are programmable contracts that automatically execute when pre-defined conditions are met. They automate transactions and allow parties to reach agreements directly and automatically. They also redefine trust, as contracts are visible to all the users of the block chain. These are the advantages of this paper. The conclusion of this paper is that by using a private blockchain, it is possible to send hundreds of transactions per second onto the blockchain, utilizing every aspect of the smart contract to ease the load on the block chain.

[4] Basit Shahzad and Jon Crowcroft introduces proof of completeness algorithm which introduces random number along with the hash value in the blockchain so that the blocks are sealed and the entire blockchain is sealed in order to make sure further security to the system. The merkle tree formation of the blocks are also introduced here. This proposal is quite complicated and this cannot be used for voting in areas with high population.

[5] Ahmed Ben Ayed proposes a longest chain rule for the purpose to overcome concusses in blockchain . This system divides the ‘n’ number of votes casted at the same time to the same blockchain in order to prevent ddos attacks to the blockchain in the system. This system will work fine with few populated areas. Largely populated areas there must be powerful resources in order to make sure that the systems work properly. More maintenance is required for this system to function properly.

III. BLOCK INITIATION

The number of blockchains created is dependent upon the number of candidates taking part in the election.

1. Genesis block

This block is created with the details of the candidate who is taking part in the election with a hash value.

2. Second block

This block contains the hash value of the first block and also contain the verification from the election commission about the details present in the genesis block are legit. If not the entire blockchain will be destroyed.

3. Voting blocks

The blocks which are added by the voters will be added to the respective blockchain of the candidate whom they have casted their vote.

4. Block numbering

The blocks are numbered staring from the block which has been considered as the vote, which makes easy to count the votes which the candidate has obtained.

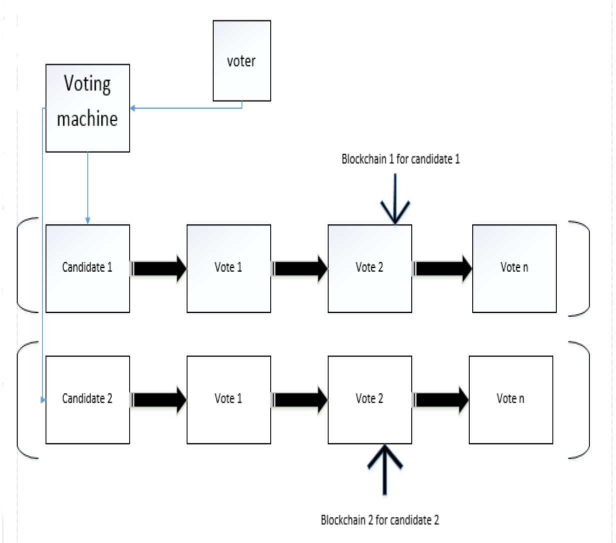
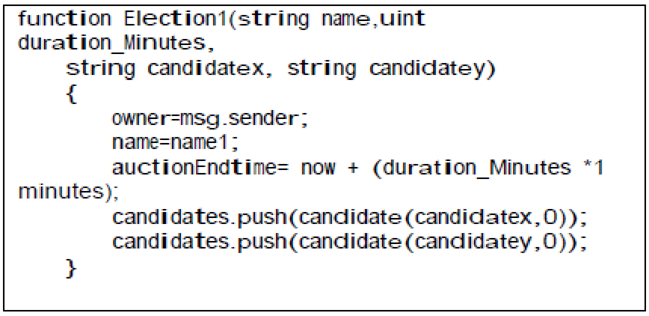


Fig. 1. Individual blockchain for each candidate

5. Hashing

The hash value generated by the system will be added to each block and hash value of the previous block will be copied on to the next block. The process continues till the nth block.

Code snippets from Ethereum blockchain is used and coded in solidity for example.



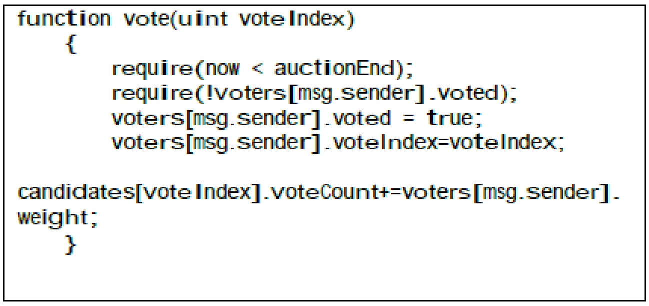
```
function Election1(string name,uint
duration_Minutes,
    string candidatex, string candidatey)
    {
        owner=msg.sender;
        name=name1;
        auctionEndtime= now + (duration_Minutes *1
minutes);
        candidates.push(candidate(candidatex,0));
        candidates.push(candidate(candidatey,0));
    }
```

Code.1: Code block of election function

[6] Election function is created which is used to add the genesis block into the blockchain. The candidate details are pushed into the blockchain once verified.Ddos can lead to a major seatback in the entire blockchain and thus makes the total voting system to collapse.

More than one block addition the same time will also cause the blockchain to be disturbed and does not offer fair election results.

Creation the blockchain is easy but division of them according to the candidates is a difficult job and also to observe and maintain the blockchain.



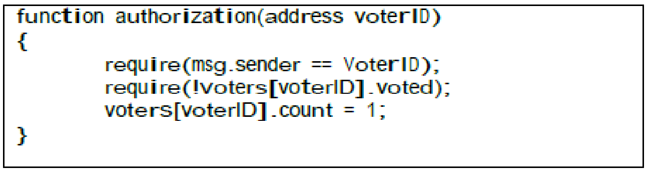
```
function vote(uint voteIndex)
    {
        require(now < auctionEnd);
        require(!voters[msg.sender].voted);
        voters[msg.sender].voted = true;
        voters[msg.sender].voteIndex=voteIndex;

candidates[voteIndex].voteCount+=voters[msg.sender].
weight;
    }
```

Code.2: Code block of vote function

[6]Vote() function adds the vote which is casted by the voter.The function checks whether the auction duration has ended or not.

If not then it allows to add the block into the blockchain as vote.



```
function authorization(address voterID)
{
        require(msg.sender == VoterID);
        require(!voters[voterID].voted);
        voters[voterID].count = 1;
}
```

Code.3: Code block of authorize function

Authorization function prevention the duplication of votes as it keeps track of the persons who have voted already using the VoterID.

IV. PERFORMANCE ANALYSIS

Using a same blockchain for multiple candidates uses less resources since it does not require many database and server or the creation and maintenance of the blockchain.

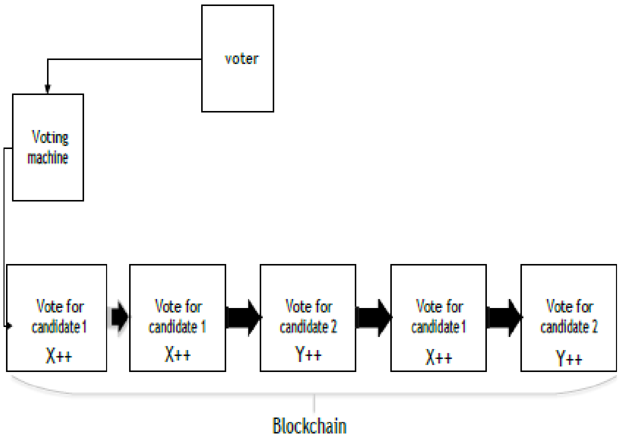


Fig. 2. Same blockchain for all candidates

The system Having only one blockchain does not provide more security and is not more time efficient. This is more vulnerable to Distributed denial of service (Ddos)attack.

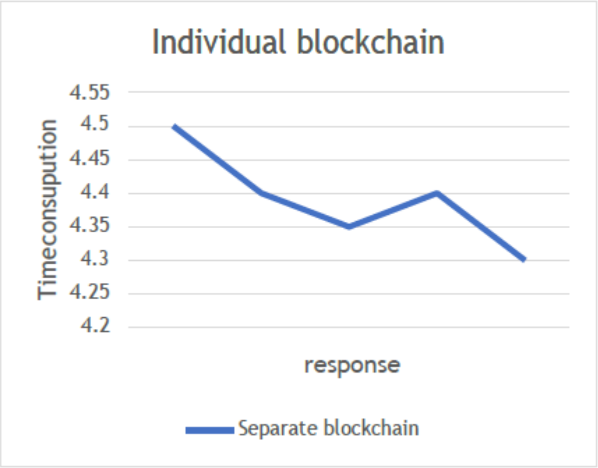


Fig. 3. Expected performance of Individual blockchain

The typical analysis of the blockchain which is having all the candidates in the single blockchain is taken according to the time taken to add the block and the response time for the block to reflect on the blockchain .The analysis is just a demo not real one, They just show the expected output in the particular situation.

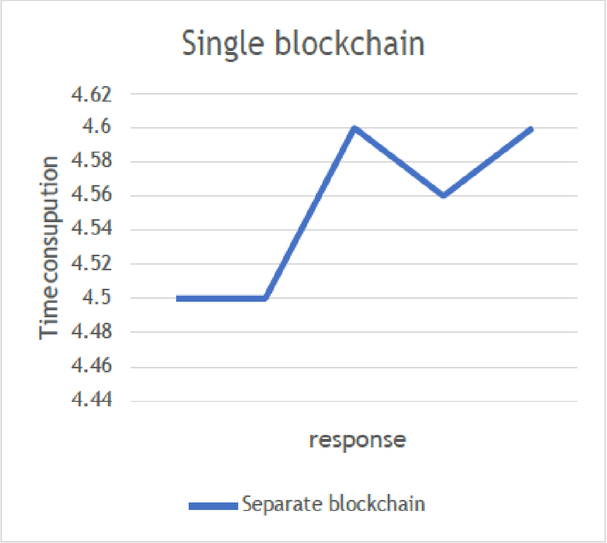


Fig. 4. Expected outcome for single blockchain

The graph shows that usage of individual blockchain for each candidate will lead to increased performance and also more efficiency to the voting process.

The single blockchain also have problem in identification of votes(blocks) that has been added to the blockchain to as which candidate the block belongs to and increases the time for the announcement of results. Since there are more technical advancements in a single blockchain, it also requires a lot of human resource who could understand the working of the blockchain so that the blocks can be distinguished easily. The inclusion of more blockchains may seem to be more hardware resource consuming and expensive but it will bring a drastic change in the performance of the voting systems. (The graphs have been plotted by assumed values and not the originally tested outcomes).

V. CONCLUSION

The blockchain technology provides the best alternative to the existing system which has many flaws and trust issues today. The application of blockchain for voting provides more secure voting system. Even though the system is more expensive and skilled human resources as well as more powerful computer hardware and lot of coordination among the election conducting bodies are required, it still provides the perfect transparent voting system which improves and encourages the quality of democracy.

FUTURE ENHANCEMENTS

Voters can be allowed to voting using their mobile phones by creating a mobile application which connects to the blockchain by making sure necessary security steps are taken and verification are done. This increases the number of voters participating in the polling system as it prevents the time waiting in queue whereas here it can be done from anywhere provided necessary security steps are taken. This may seem complicated but if this complicated task is achieved it can be a great solution for everyone who is complaining about the quality and the trust of the elections which are being conducting presently.

REFERENCES

1. 1.http://www.cs.tufts.edu/comp/116/archive/fall2016/rosgo od.pdf
2. 2.https://doi.org/10.1016/j.procs.2018.03.063
3. 3.https://ieeexplore.ieee.org/abstract/document/8457919

4.https://ieeexplore.ieee.org/abstract/document/8651451/
5.http://aircconline.com/ijnsa/V9N3/9317ijnsa01.pdf
6.https://ieeexplore.ieee.org/abstract/document/8355340

AUTHORS PROFILE

Mrs. Baby D. Dayana is an assistant professor at the Department of Computer Science, SRM Institute of Science and Technology, Ramapuram

S.Nishanth is a student at the Department of Computer Science, SRM Institute of Science and Technology, Ramapuram .

A.D.krishna is a student at the Department of Computer Science, SRM Institute of Science and Technology, Ramapuram .

R.D.Nitish is a student at the Department of Computer Science, SRM Institute of Science and Technology, Ramapuram .