An Introduction to Blockchain Based E-Voting System

Adarsh Vernekar[1]

Department of Computer Science & Engineering, SVERI's College of Engineering, Pandharpur, Maharashtra, India

---***---

Abstract - *For any democracy election acts like a basic building block. Any threat to election process is a threat to national security. It has been a big challenge to build a secure E-voting system that satisfies all the basic requirements. Blockchain has wide applications as it offers distributed ledger technologies .This paper reviews a study of blockchain technology in distributed electronic voting systems. Moreover the paper focuses on legal technical and security issues. It also focuses on the requirements to establish a decentralized E-voting system. Also the paper evaluates potential of blockchain technology to establish a secure, cost efficient, transparent fraud less and improved E- voting system. The paper outlines the potential of the blockchain technology to establish a secure, cost efficient, transparent fraud less and improved E-voting system that can be established throughout a nation.*

***Key Words*: Blockchain, e-voting, smart contract.**

1. INTRODUCTION

According to the today's social environment a fair and Transparent election has become an intense need for today's society. The current ballot system does not offer transparency in counting of votes. There are several threats of voting frauds, like fake voters, frauds in the polling booths etc. So, an intense need for establishment of secure decentralized fraud less, voting system came into existence.

Electronic decentralized voting system using blockchain can overcome all the issues in traditional voting systems. Blockchain provides various properties due to its decentralized ledger technology. Blockchain is a decentralized computational & information sharing platform which enables multiple authority domain who do not trust on each other but they cooperate and collaborate in certain decision making process. Blockchain was firstly introduced in 2008 by Satoshi Nakamoto & implemented in 2009. The basic property of blockchain is that it uses add and append only strategy. In Blockchain we cannot delete the existing data. Blockchain uses peer to peer network systems. Blockchain is a chain of blocks that includes all the information of user through distributed ledger technology. The concept of block interconnection was evaluated from Merkle tree by Ralph Merkle. Every node is labeled with a cryptographic hash of a block data. Thereby a non-leaf node is labeled with a cryptographic hash of labels of child nodes. Hence all the blocks are interconnected any change in blockchain can be easily detected.

2. NEED OF BLOCKCHAIN IN E-VOTING

To carry out a national election certain e voting system should ensure many of the security requirements. They can be listed as

- Voting system should not be traceable
- The voting system should ensure whether the voter's vote was counted & proof of vote should be provided.
- Election system should not enable single entity to control systems.
- Election system should allow only eligible individuals to participate in voting.
- The Election system should not be expensive.
- The election system should provide limited access to participants depending on their roles.

The use of blockchain Technology in E-Voting system can meet all the above needs as a blockchain is tamperproof and non-alterable.

3. PRELIMINARIES IN E-VOTING

Before implementation of an E-Voting system using blockchain the type of blockchain used into the system must be considered. The blockchain can be categorized into basic three types, Private, Public and consortium blockchain. A public blockchain grants access to read and create to any user in the network e.g. Bitcoin in a private blockchain there are certain limitations over read and write access to participants. While a consortium Blockchain is a partially decentralized Blockchain in which consensus process is controlled by selected set of nodes called as validators. In our case we use a permissioned blockchain with variation in consortium based chain as it is more efficient.

The first implementation of blockchain was bitcoin. The bitcoin uses Proof of Work consensus algorithm .Consensus is a procedure to reach a common agreement in a certain decentralized platform. There are various consensus algorithms according to the applications. Another consensus algorithm Proof of stake was implemented in Peercoin crypto currency. It provided increased protection and prevented the problem of high power consumption of servers. In our case we use Proof of Authority consensus algorithm. Here the transactions are validated by the approved users called as validators. The process of validation is automated such that there is no need of constant monitoring. These selected nodes on the network validate and certify the transactions on the blockchain.

Validation was previously done by the miners in Proof of Work consensus in public blockchain .Here other than mining fees validators are paid for their service. Below table displays how use of Proof of authority consensus can be useful and efficient.

Property	Proof of Work	Proof of Stake	Proof of Authority
Energy Usage	High	Low	None
Hardware Need	High	Low	None
Block generation speed	Low	High	High
Transaction speed	Slow	Fast	Fast
Attacks	DoS, Sybil attack possible	DoS possible	DoS and Sybil attacks not possible
Scalability	Less	More than PoW	Most scalable
Application	Bitcoin	Peercoin	Private institutions
Leader selection	Hash rate	Stake	Authority based

Fig.1 Comparison of Consensus Algorithm

Smart contract is a term of agreement between the nodes of networks which is directly written in code. These are irreversible, non- track able applications that execute in decentralized platform. Once a smart contract is defined it cannot be altered or no one can edit the code. Hence a smart contract creates a trusted relationship which is not dependent on any single entity. Hence the participants totally trust on the network. Smart contracts enable self-verification and self –administration. So, we consider election as a smart contract in our case.

4. METHODOLOGY

While implementing a blockchain enabled electronic voting system we consider existing and previous e voting systems. Various processes of defining roles evaluating frameworks, security and legal issues should be considered.

4.1. Election as a smart contract

In our election system we have defined an election as a smart contract. So in our network the election is the agreement between the participating nodes. Once the smart contract is defined it includes defining the roles of each participant, process of election and terms & conditions within the election process.

This election smart contract can be deployed on the Geth (Go-Ethereum) framework. It supports smooth running of smart contract without any fraud or any third party involvement. The transaction rate is also desirable. Hence we consider this platform in our case.

4.1.1 Defining roles

Every participant must be defined a certain role. Multiple individuals can be assigned the same role or different role.

a) Administrators

The administrators will manage all the execution of the election. They can be assigned the tasks of creation of election its activation, observe the votes decide the time to close the election and tallying & displaying of the results.

b) Voters

Voter is a basic participant who casts a vote in the election. Voter can verify their eligibility & authenticate themselves and load election ballots .They can cast their vote and verify the vote that they had casted.

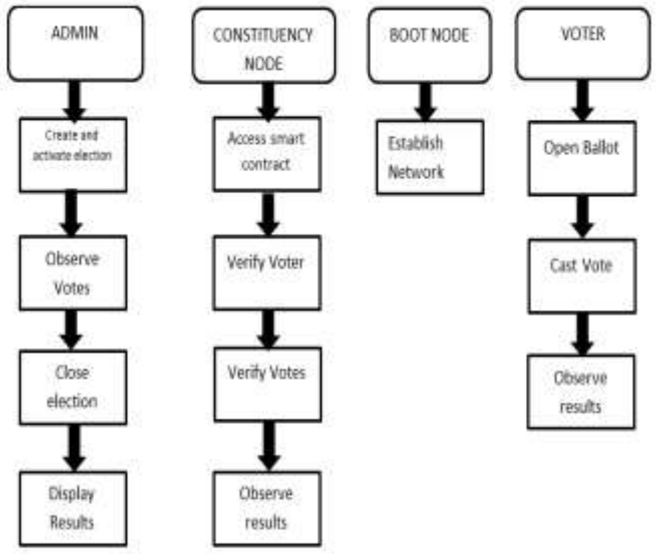
c) Constituency Nodes

Administrators create the election process the smart contracts deploy the respective constituency nodes representing each constituency. These nodes verify the voters by means of accessing smart contracts. If the voter is verified by all the constituency nodes then and then the voter's vote will be considered and appended into the blockchain.

d) Boot Nodes

A boot node will help the constituency nodes reach each other and communicate with each other. Boot nodes play a vital role in establishing network between the constituency nodes.

Below figure 2 displays a clear idea of the roles and the respective tasks to be performed.



4.1.2 Election process

The election process is carried out by the set of smart contracts that are enabled into the blockchain .The smart contracts are defined accordingly with respect to roles defined to the participants in the network.

The election process consists of multiple procedures in it. The administrators can create the election ballots by means of DApps. An admin can define the candidates and voting constituencies. The smart contract creates the ballot and deploys into the blockchain.

The voter registration is also an important factor in the election process. The administrators carry out the registration process. As only eligible voters should be able to cast a vote so the admins have to display the list of eligible voter before conducting election process. For verification of voter every voter can be assigned certain voter ID and a code with his respective information that is which constituency he belongs voter can cast his vote by re-entering the Voter ID and Voter code.

When an individual voter votes he interacts with the ballot. The smart contract interacts with blockchain and if the consensus is reached only then the vote is added to the blockchain by means of constituency nodes. The consensus is reached between the majorities of the constituency district nodes. If corresponding constituency nodes agree only then the vote is to be casted. Every voter will be designed with a certain wallet. Once the vote is casted then weight will decrease by 1. Hence this will easily ensure that either a voter casts his vote only once. Voter can use any computer in any voting constituency for casting vote. This is because for successful authentication a valid voter ID and voting code are to be presented by the voter. It doesn't matter with the actual physical location of the voter.

Once the election is done the displaying of the result is very important task to be performed. Every ballot smart contract counts their vote at their own level. Every participant in the blockchain should update their ledger copy for ease in counting of the votes. The smart contracts publish the final count after the election is over & thereby it's displayed by the administrators.

The verification of vote is also an important factor. When an individual voter casts his vote he gets a transaction ID of the vote he casted. Hence the voter can get verify his vote by submitting their transaction ID after authenticating himself to the system. The transaction provide to the voter can be given in the form of a QR code for security purposes. Hence a voter can verify that whether his vote was counted correctly.

5. SECURITY ISSUES

In any voting system security is the basic requirement. The blockchain enabled E-voting system will ensure maximum security than the traditional voting systems.

- The DoS attacks are not possible as we use Proof of authority consensus algorithm. If such attack occurs an individual would be easily caught. We can also ensure Byzantine fault tolerance algorithm to locate failed nodes if such condition occurs.
- Every node is authenticated by the constituency nodes whether the vote is eligible or not. Also if a certain voter tries to cast a vote multiple times his wallet value will reduce by 1 once he casts a vote hence automatically the individual cannot cast a vote multiple times and the system shows that the voter that the voter had already casted his vote.
- Limited access to ledger provided to the participants depending upon their roles in the network can ensure high security.
- The Proof of Authority consensus is against the Sybil attack hence there are no chances of Sybil attack.

6. ADVANTAGES

This decentralized E-voting system provides many advantages over the traditional E-voting system

- This E-Voting system is cost efficient than the traditional voting system.
- Maximum security is provided by the network to all the participants in the election
- In the Blockchain enabled E- voting system no single authority can control the network.
- This E-voting provides proof to voter and provides transparency to the voter. In traditional voting system there was no guarantee that whether the vote casted by the voter is counted correctly. But in this voting system a voter can verify whether his vote was counted correctly to the right candidate.

- In the traditional voting system directly the results are displayed. There was no transparency whether the vote was counted and no related information related to it was provided to the voter. But in our voting system voter can verify his vote and there is clear transparency regarding the election process.
- In the traditional voting system malpractices can be performed on the polling booth. Coerced voting can be carried out. But in this voting system voter can cast his vote with total privacy. There is no need for the voter to go to the polling booth to cast his vote.

7. CONCLUSIONS

The main motive of initiating the decentralized electronic voting system is to make election process cheaper, secured, faster and easier for the society. In this paper we have focused on the blockchain based E-voting system that guarantees cost efficiency, privacy and security to the election process. We have outlined the utilization of election process as a smart contract. We have assigned specific role to every participant in the network. We have also focused in the security issues in the E-voting system. This election system will provide a verification and transparency to voter about his vote. Blockchain based Electronic voting system proves to be a boon to the modern society of a nation.

REFERENCES

[1] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008.

[2]https://medium.com/smart-city-moscow/proof-of-authority-in-active-citizen-e-voting-platform-cf7d1553d55d

[3]https://medium.com/poa-network/poa-network-preserving-the-human-blockchain-connection-774e221308aa

[4]https://apla.readthedocs.io/en/latest/concepts/consensus.html

[5]https://www.binance.vision/blockchain/proof-of-authority-explained

[6]https://azure.microsoft.com/en-in/blog/ethereum-proof-of-authority-on-azure/

[7]https://ethereum.stackexchange.com/questions/55244/is-it-logical-to-use-proof-of-authority-for-a-public-blockchain

[8] https://hackernoon.com/setup-your-own-private-proof-of-authority-ethereum-network-with-geth-9a0a3750cda8

[9] https://mlsdev.com/blog/156-how-to-build-your-own-blockchain-architecture

[10]https://en.bitcoinwiki.org/wiki/Block

[11]https://docs.microsoft.com/en-us/azure/blockchain/templates/ethereum-poa-deployment

[12] Friðrik Þ. Hjálmarsson, Gunnlaugur K. Hreiðarsson "Blockchain-Based E-Voting System"

[13] Mrs Harsha V. Patil1, Mrs. Kanchan G. Rathi2, Mrs. Malati V.Tribhuwan3 *"A Study on Decentralized E-Voting System Using Blockchain Technology"* International Research Journal of Engineering and Technology (IRJET) Volume: 05 Issue: 11 | Nov 2018

[14]https://how.bitshares.works/en/master/technology/dpos.hml

[15] Manoj Shrinivas1, Chandan S2, Mohammed Shamail Farhan3, Ramyashree K4 "*A Decentralized Voting Application using Blockchain Technology*" International Research Journal of Engineering and Technology (IRJET) Volume: 06 Issue: 04 | Apr 2019

BIOGRAPHIES

Name: Adarsh Gurudas Vernekar, Student at Department of Computer Science ,SVERI's College of Engineering, Pandharpur