

## Blockchain based E-Voting System

Adarsh.G.Vernekar<sup>1</sup>, Mahesh Phutane<sup>2</sup>, Rohit Godase<sup>3</sup>, Vinayak Waghmode<sup>4</sup>, Mr.S.M.Shinde<sup>5</sup>

<sup>1-4</sup>Student of Graduation at Department of Computer Science and Engineering, SVERI's College of Engineering, Pandharpur, Maharashtra, India

<sup>5</sup>Assistant Professor, Department of Computer Science and Engineering, SVERI's College of Engineering, Pandharpur, Maharashtra, India

\*\*\*

**Abstract** - Election is the basic building block for any democracy. Any threat to election process can be a threat to national security. It's been a great challenge to create to create a secured E-Voting system that satisfies all the essential requirements. Blockchain technology has wide applications as it offers distributed ledger technologies. This paper reviews a study of blockchain technology in electronic voting systems.

Moreover the paper focuses on multiple technical, legal, and security issues for a blockchain based electronic voting system. It also focuses on need to set up a secured E-voting system and thereby requirements for its successful establishment. The paper also evaluates the potential of blockchain technology to build a secure, cost efficient, transparent Blockchain based E-voting system that can be established throughout the nation.

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

### 1. INTRODUCTION

According to the current social environment a good and transparent election has become intense need for current society. The present election system does not offer transparency in counting votes. There are several threats in current voting system like fake voters, malpractices on polling booths etc. So a need to establish a secured voting system came into existence. Blockchain based electronic voting system can overcome all the issues which are in the current election systems. Blockchain technology can provide multiple properties due to its distributed ledger technology. Blockchain is a decentralized computational and information sharing platform which enables multiple authorities who do not have trust among them but they cooperate and collaborate in certain decision making procedure. Blockchain technology was firstly introduced by Satoshi Nakamoto in the year 2008 and implemented in a crypto currency called Bitcoin. The basic property of blockchain technology is that it uses add and append only strategy for data related operations. Hence in the blockchain we cannot delete the existing data. Blockchain technology uses peer to peer network systems. Blockchain is a chain of interconnected blocks that includes all the information of the user through distributed ledger technology. The concept of block interconnection was evaluated from the Merkle tree by Ralph Merkle. Every node is labeled with a cryptographic hash function of a block data. Hence a non leaf node is labeled with a cryptographic hash of labels of child nodes. As

all the block in a blockchain are interconnected any change in blockchain can be easily detected.

### 2. NEED OF BLOCKCHAIN IN E-VOTING

To perform a national election voting system should ensure many security requirements. They can be stated as:

- 1) Voting system shouldn't be traceable
- 2) The voting system should provide proof of vote to the voter and should ensure whether the vote was counted and counted correctly.
- 3) Voting system should perform eligibility check such that only eligible voters could perform voting.
- 4) The election system should be cost efficient
- 5) Limited access should be provided by the voting system depending upon their roles.
- 6) Hence use of Blockchain technology in E-voting system can meet up to the all the needs for an ideal voting system a blockchain is tamperproof and non – alterable.

### 3. PRELIMINARIES IN E-VOTING

Before the implementation of an Blockchain based Electronic voting system we must consider the type of blockchain that we are implementing in our model. The blockchain must be categorized onto three types like private, public, consortium blockchains. A public blockchain grants access to read and create data to any user in the network. Eg. Bitcoin. In a private blockchain there are certain limitations over read and write access to the participants. While consortium blockchain can be called as partially decentralized blockchain in which consensus procedure is controlled by the selected set of nodes in the network called as Validators. In our scenario we use a permissioned blockchain with a variation of consortium based chain as it is more efficient. The first implementation of the blockchain technology was Bitcoin. The Bitcoin uses proof of work consensus algorithm. Consensus is stated as a common agreement in a certain decentralized platform. There are consensus algorithms as per their applications. Another consensus algorithm Proof of stake was in the Peercoin crypto currency. It provided increased protection and overcome the problem of the high power consumption of the servers. In our case we use proof of Authority consensus

algorithm where transactions are validated by the approved users called as Validators. The process of validating is automated hence there is no need of any constant monitoring. These selected nodes on the network perform validation and certification of the transaction on the blockchain. Validation process was previously done by the miners in the proof of work consensus in public blockchain. But in our case other than mining fees Validators are paid for their service. Hence proof of authority is the best for the implementation of the Blockchain based Voting system. Smart contract is a term of agreement between the nodes in networks which is directly written in the form of code. These are irreversible, non-trackable applications that execute in the decentralized platform. Once the smart contract is defined it cannot be altered or no any individual can edit the code. Hence the smart contract creates a trusted relationship which is not dependent on single entity. Hence the participants totally trust on the network. Smart contracts enable self verification and self administration. So we consider in our case Election as a smart contract.

#### 4. METHODOLOGY

While implementing a blockchain based E-voting system, the existing and previous voting system must be taken under consideration. Various processes of defining roles evaluating frameworks, security and legal issues must be considered.

##### A. Election as a smart Contract

In our blockchain based election system we have defined an election as a smart contract. So in our network election is considered as an agreement between the participating nodes. Once the smart contract is defined it includes data for defining the roles of each participant, process of the election and terms and conditions within the election procedure. This election smart contract can be deployed on multiple platforms like Geth(Go-Ethereum) framework. It supports smooth running of the smart contract without any discrepancy or third party involvement. The transaction rate is also desirable. Hence we consider this platform in our case.

##### 1) Defining Roles in the Network

A certain role must be defined to every participant in the network. Multiple individuals can be assigned the same role or different roles in the network.

##### i) Admin

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

##### ii) Voters

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

##### iii) Constituency Nodes

Administrators create the election procedure and smart contracts deploy the respective constituency nodes representing each constituency. These nodes verify the voters by accessing the smart contracts. If voter is verified by all the constituency nodes then and then the voter's casted vote will be considered as valid and added into the blockchain.

##### iv) Boot nodes.

A boot node will help the constituency nodes to reach each other and communicate. Boot nodes play vital role in establishing network among the constituency nodes. Below figure gives a transparent idea about the roles and the respective tasks of the participant in the network.

##### B. Election process

The election process is administered by the smart contracts that are enabled into the blockchain. The smart contracts are defined accordingly with reference to roles defined to the participants within the network. The election process consists of multiple procedures to be carried out in it. The administrators can create the election ballots by using of DApps. An admin can define the candidates and voting constituencies through him. The smart contract creates the ballot and deploys into the blockchain network. The voter registration is additionally a crucial factor about the election process. The administrators perform the registration process. As only eligible voters should be given opportunity to cast a vote therefore the admins need to display the list of eligible voter before conducting election process. For verification of voter every voter are often assigned certain voter ID and a code with his respective information that's which constituency voter belongs and other details. Voter can cast his vote by re-entering the Voter ID and Voter code during voting. When an individual voter votes he interacts with the ballot and election system. 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 of voter is to be casted. Every voter are going to be designed with a certain wallet. Once the vote is casted by voter then weight will decrease by 1. Hence his may easily make sure that either a voter casts his vote just one occasion. Voter can use any computer in any voting constituency for voting. This is often because for successful authentication a legitimate voter ID

and voting code are to be presented by the voter. It doesn't deal with the actual physical location of the voter. Once the election is completed the airing of the result's very important task to be performed. Every ballot smart contract counts their votes at their own level. Every participant within the blockchain network should update their ledger copy for ease in counting of the votes. The smart contracts publish the final count of votes after the election is over & thereby it's displayed by the administrators. The verification of vote is additionally a crucial factor. When an individual voter casts his vote to any individual 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 voting system. The transaction provide to the voter are often given within the sort of a QR code for security purposes. Hence a voter can verify that whether his vote was counted and voted correctly.

## 5. SECURITY ISSUES

In any electoral system security is the basic requirement. The blockchain enabled E-voting system ensures maximum security than the normal voting systems.

1) The DoS attacks aren't possible as we use Proof of authority consensus algorithm in our case. If such attack occurs an individual would be easily caught and tracked. We can also ensure use of Byzantine fault tolerance algorithm to locate failed nodes if such condition occurs.

2) Every node is authenticated by the constituency nodes to verify whether the vote is eligible or not. Also if a voter tries to cast a vote multiple times his wallet value is already reduced by 1 so once he casts a vote automatically the individual cannot cast a vote multiple times and therefore the system shows maximum security.

3) Limited access to ledger provided to the participants depending upon their roles within the network provides high security to the network.

4) The Proof of Authority consensus is against the Sybil attack hence there are no chances of Sybil attacks.

## 6. ADVANTAGES

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

1) This E-Voting system is cost efficient than the traditional electoral system.

2) Maximum security is provided by the network to all or any the participants within the election.

3) Within the Blockchain enabled E- electoral system no single authority can control the network.

4) 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 electoral system a voter can verify whether his vote was counted correctly to the proper candidate.

5) In the traditional electoral system directly the results are displayed. There was no transparency whether the vote was counted and no related information related to it had been provided to the voter. But in our voting system voter can verify his vote and there's clear transparency regarding the election process.

6) Within the traditional electoral system malpractices are often performed on the booth. Coerced voting can be administered. But during this electoral system voter can cast his vote with total privacy. There's no need for the voter to travel to the booth to cast his vote.

## 7. CONCLUSIONS

The primary motive of initiating the decentralized electronic voting system is to form election process cheaper, secured, faster and easier for the society. During this paper we've focused on the blockchain based E-voting system that guarantees cost efficiency, privacy and security to the election procedure. We've outlined the use of election process as a sensible contract. We've assigned specific role to every participant within the network. We've also focused in the security issues within the E-voting system. This election system will provide a verification to voter and transparency is maintained throughout the system about his casted vote. Blockchain based Electronic Voting system is 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-connection774e221308aa>
- [4] <https://apla.readthedocs.io/en/latest/concepts/consensus.html>
- [5] <https://www.binance.vision/blockchain/proof-of-authority-explained>
- [6] <https://mlsdev.com/blog/156-how-to-build-your-own-blockchain-architecture>
- [7] <https://en.bitcoinwiki.org/wiki/Block>

- [8] <https://docs.microsoft.com/enus/azure/blockchain/templates/ethereum-poa-deployment>
- [9] Friðrik Þ. Hjálmarsson, Gunnlaugur K. Hreiðarsson "Blockchain-Based E-Voting System"
- [10] <https://azure.microsoft.com/enin/blog/ethereumproof-ofauthority-on-azure/>
- [11] <https://ethereum.stackexchange.com/questions/55244/its-logical-to-use-proof-of-authority-for-a-public-blockchain/>
- [12] <https://hackernoon.com/setup-your-own-privateproof-of-authority-ethereum-network-with-geth-9a0a3750cda8>
- [13] Mrs Harsha V. Patil<sup>1</sup>, Mrs. Kanchan G. Rathi<sup>2</sup>, Mrs. Malati V. Tribhuwan<sup>3</sup> "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.html>
- [15] Manoj Shrinivas<sup>1</sup>, Chandan S<sup>2</sup>, Mohammed Shamail Farhan<sup>3</sup>, Ramyashree K<sup>4</sup> "A Decentralized Voting Application using Blockchain Technology" International Research Journal of Engineering and Technology (IRJET) Volume: 06 Issue: 04 | Apr 2019 BIOGRAPHIES



Name: Vinayak Hanumant Waghmode  
Student at Department of CSE, SVERI's College of Engineering, Pandharpur, Maharashtra, India.



Name: Mr. S.M. Shinde  
Assistant Professor at Department of CSE, SVERI's College of Engineering, Pandharpur, Maharashtra, India.

## BIOGRAPHIES



Name: Adarsh Gurudas Vernekar  
Student at Department of CSE, SVERI's College of Engineering, Pandharpur, Maharashtra, India.



Name: Mahesh Dilip Phutane  
Student at Department of CSE, SVERI's College of Engineering, Pandharpur, Maharashtra, India.



Name: Rohit Laxman Godase  
Student at Department of CSE, SVERI's College of Engineering, Pandharpur, Maharashtra, India.