**A SEMINAR REPORT ON**

# Blockchain in E-Voting System

SUBMITTED BY

**Shubhangi Dhobale (71828231M)**

UNDER THE GUIDANCE OF

**Prof.Shrikant Dhamdhere**

**T.E. (COMPUTER ENGINEERING)**
**2019-20 (Semester II)**


**Department Of Computer Engineering**
**Genba Sopanrao Moze Trusts**
**Parvatibai Genba Moze College of Engineering,Wagholi,**
**Pune - 412207**


**Parvatibai Genba moze College of Engineering**
**Wagholi, Pune-412207**

**DEPARTMENT OF COMPUTER ENGINEERING**

**Certificate**

This is to certify that the seminar report entitled

# Blockchain in E-Voting System

SUBMITTED BY

**Shubhangi Dhobale (71828231M)**

Prof.Shrikant Dhamdhere.
(Seminar Guide)

Prof.Shrikant Dhamdhere.
(Head of Department)

Place: Pune
Date:

## CERTIFICATE

This is to certify that seminar entitled “Blockchain in E-Voting System” has been carried out by Shubhangi Dhobal, Exam No. 71828231M under guidance in partial fulfillment of the requirements for the degree of BACHELOR OF ENGINEERING of Pune University,during the academic year 2019-20. To the best of my knowledge and belief this work has not been submitted elsewhere for the award of any other degree.

Prof.Shrikant Dhamdhere.
(Seminar Guide)

Prof.Shrikant Dhamdhere.
(Head of Department)

Place: Pune
Date:

## Seminar Approval Sheet

**Seminar Topic Name:** Blockchain in E-Voting Sysytem
**Exam No:** 71828231M
**Class:** TE(COMP)

## Abstarct

Technology has positive impacts on various aspects of our social life. Designing a globally connected architecture enables ease of access to a variety of resources and services. Furthermore, technology like the Internet has been a fertile ground for innovation and creativity. One such innovation is blockchain – a keystone of cryptocurrencies. The blockchain technology is presented as a game-changer for many existing and emerging technologies. With its immutability property and decentralized architecture, it is taking centre stage in many services as an equalization factor to the current parity between consumers and large corporations/governments. One future application of the blockchain is in e-voting. The objective of such a scheme would be to provide a decentralized architecture to run and support a voting scheme that is open, fair, and independently verifiable. In this paper, we propose a potential new e-voting protocol that utilises the blockchain as a transparent ballot box. The protocol has been designed to achieve fundamental e-voting properties as well as offer a degree of decentralization and allow for the voter to change/update their vote (within the permissible voting period). This paper highlights the pros and cons of using block chain for such a proposal from a practical point view in both development/deployment and usage contexts.

**Keywords:** Block chain, Hashing, Decentralization

**Guide By:** Prof. Shrikant Dhamdhere.

**Sign :**

**Acknowledgement**

With immemse pleasure, I am presenting the seminar report as a part of curriculum of the B.E Computer Engineering. I wish to thank all the people who gave me an unending support right from the idea was conceived. I express my sincere and profound thanks to our Guide Prof. Shrikant Dhamdhere. I am also thankful to all my classmates who helped me in the preaparation of this seminar.

Shubhangi Dhobale
(TE COMP)

# Contents

# List of Figures

# List of Tables

# Chapter 1

# Abstract

Technology has positive impacts on various aspects of our social life. Designing a globally connected architecture enables ease of access to a variety of resources and services. Furthermore, technology like the Internet has been a fertile ground for innovation and creativity. One such innovation is blockchain – a keystone of cryptocurrencies. The blockchain technology is presented as a game-changer for many existing and emerging technologies. With its immutability property and decentralized architecture, it is taking centre stage in many services as an equalization factor to the current parity between consumers and large corporations/governments. One future application of the blockchain is in e-voting. The objective of such a scheme would be to provide a decentralized architecture to run and support a voting scheme that is open, fair, and independently verifiable. In this paper, we propose a potential new e-voting protocol that utilises the blockchain as a transparent ballot box. The protocol has been designed to achieve fundamental e-voting properties as well as offer a degree of decentralization and allow for the voter to change/update their vote (within the permissible voting period). This paper highlights the pros and cons of using blockchain for such a proposal from a practical point view in both development/deployment and usage contexts.

# Chapter 2

# Introduction

## 2.1 What is Blockchain?

Blockchain technology was first used within Bitcoin and is a public ledger of all transactions. A blockchain stores these transactions in a block, the block eventually becomes completed as more transactions are carried out. Once complete it is then added in a linear, chronological order to the blockchain. The initial block in a blockchain is known as the Genesis block or Block 0. The genesis block is usually hardcoded into the software; it is special in that it doesnt contain a reference to a previous block. Once the genesis block has been initialised Block 1 is created and when complete is attached to the genesis block. Each block has a transaction data part, copies of each transaction are hashed, and then the hashes are paired and hashed again, this continues until a single hash remains; also known as a merkle root. The block header is where the merkle root is stored. To ensure that a transaction cannot be modified each block also keeps a record of the previous blocks header, this means to change data you would have to modify the block that records the transaction. Blockchain is a chain of blocks. In this context, “block” means digital information and “chain” means public database. So “Blockchain is secure, decentralize, a distributed database managed by a cluster of computers.” It is a shared and immutable ledger.The information in blockchain is open for anyone and everyone to see. Blockchain is a technology that does not use third parties in data exchange. Third-party cannot temper blockchain data as it is stored on thousands of machines. Blockchain is public and private type, A public blockchain is readable and writable for everyone where private blockchain sets restrictions on who can read or interact with it. Blockchain is the backbone technology of Digital Cryptocurrency Bitcoin. Blockchain technology was first used in Bitcoin.It is a public ledger of all transactions. A blockchain stores these transactions in a block, when more transactions are carried out the block eventually becomes completed. For example, in Bitcoin, since the wallets are in a distributed structure, the total amount of coins and transactions followed clearly. There is no need for a central authority to approve or complete the operations on

this P2P system.

## 2.2 Features of Blockchain

- Immutability: Data can only be appended and cannot subsequently be changed or deleted.
- Privacy: Data is encrypted such that only authorised participants can access the data against which they have permissions
- Large capacity: The network capacity can be increased limitlessely by increasing the number of computers.
- Security: Every transaction is highly secure by the nodes on the network.
- Transparency: Every transaction on the blockchain is visible.
- Decentralization: There is no governing authority or a single person looking after the network.
- Distributed ledgers: The ledger on the network is maintained by all other users on the system. This distributes the computational power across the computers to ensure a better outcome.
- Cannot be Corrupted: Every node on the networkhas a copy of digital ledger. To add transaction every node needs to check its validity. If the majority thinks its valid,then its added to the ledger. This promotes transparency and makes it corruption-proof.

## 2.3 Process of Blockchain Creation

Every block has data, hash of the block and hash of previous block. When new block is created then hash of previous block is stored in this block and then hash of new block is calculated and store in it. In this way blockchain is created.

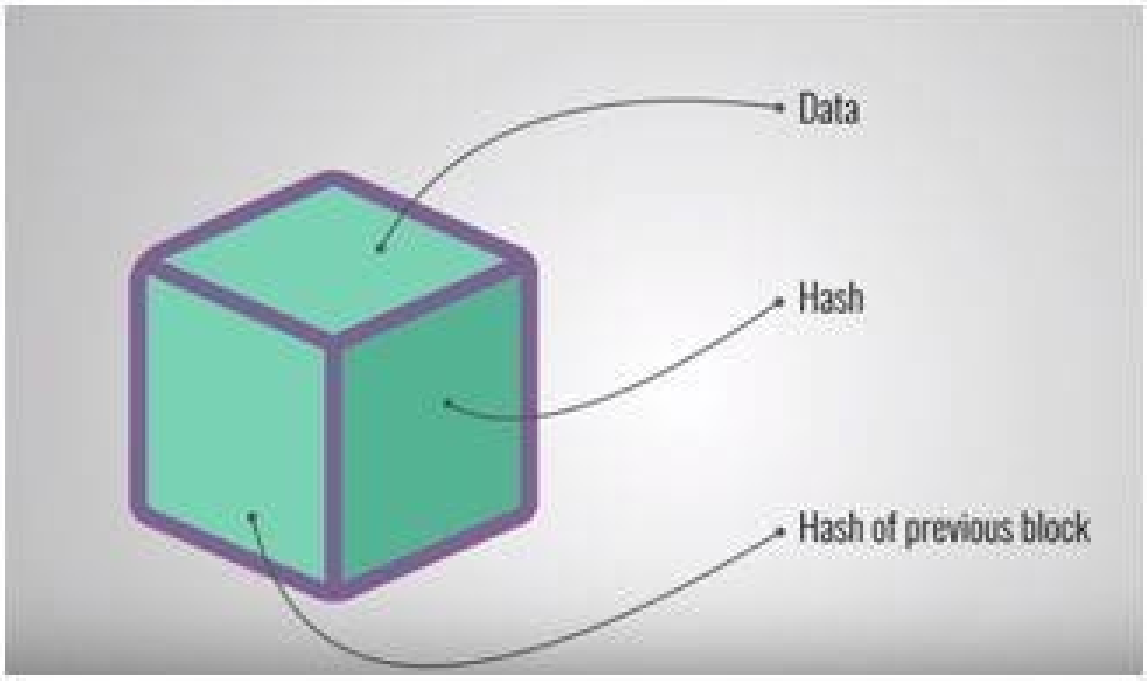


**Figure 2.1:** Block Representation

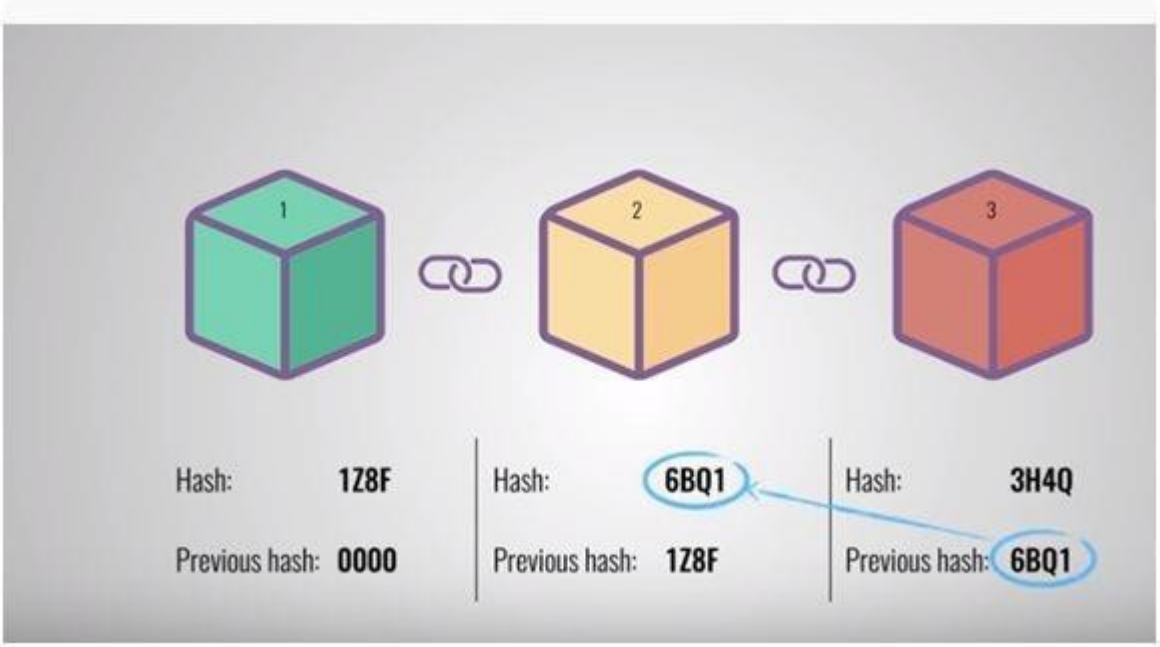


**Figure 2.2:** : Blockchain Creation

## 2.4 Working of Blockchain

Blockchain technology was first used within Bitcoin and is a public ledger of all transactions. A blockchain stores these transactions in a block, the block eventually becomes completed as more transactions are carried out. Once complete it is then added in a linear, chronological order to the blockchain. The initial block in a blockchain is known as the Genesis block or Block 0. The genesis block is usually hardcoded into the software; it is special in that it doesnt contain a reference to a previous block. (Genesis Block, 2015) Once the genesis block has been initialised Block 1 is created and when complete is attached to the genesis block. Each block has a transaction data part, copies of each transaction are hashed, and then the hashes are paired and hashed again, this continues until a single hash remains; also known as a merkle root.

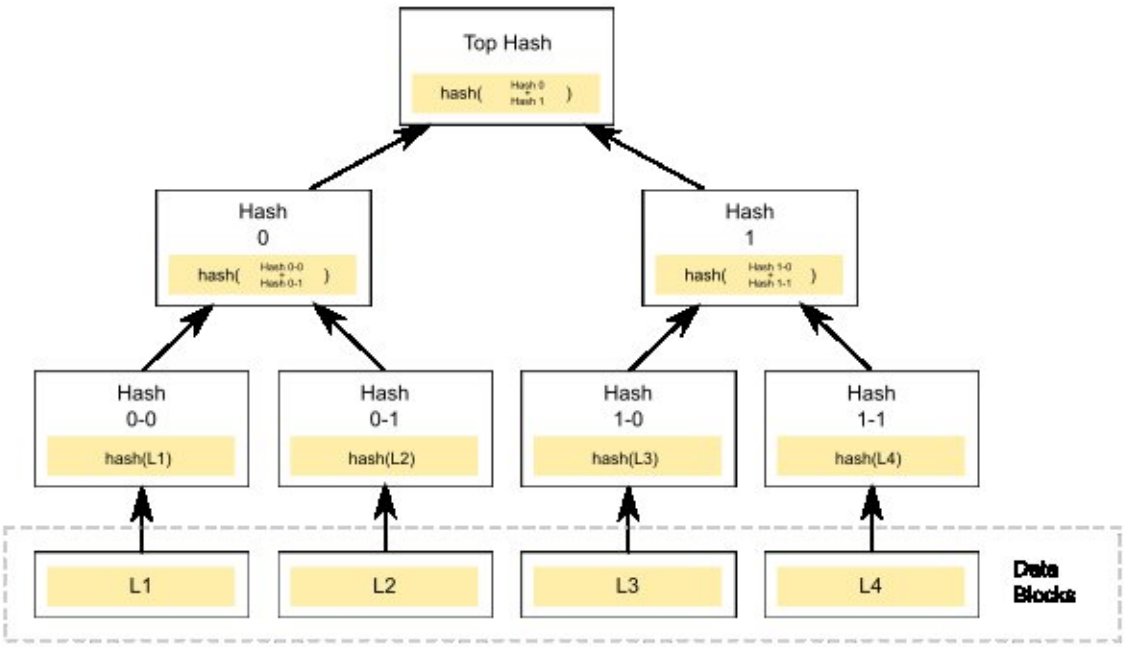


**Figure 2.3:** : Merkle Tree

# Chapter 3

# Literature Survey

| INDEX | TITLE | AUTHOR | PROPOSED THEORY | REMARK |
|---|---|---|---|---|
| 1. | Blockchain Based E-Voting system. IEEE International Conference on Cloud Computing Iceland, 2018. | Fridrik P. Hjalmarsson, Gunnlangur. | Blockchain based e-voting system taht uses ”Permissioned Blockchain”. | Cost efficient election while guaranteeing voters privacy. |
| 2. | A Proposal of Blockchain Based E-Voting syatem. IEEE,Japan, 2018. | Cosmas krisna, Adiputra Rikard Hjort. | combine the idea of double envelop encryption and blockchain technology. | Use Blockchain for e-voting system. |
| 3. | Blockchain Enabled E-Voting. IEEE,Korea, 2018e. | Nir Kshetri,Jeffrey voas. | Used digital currency analogy for casting a vote. | Address voter tampering,promote more voter participation,greater transparency and security. |
| 4. | Blockchain Technology for Innovations. IEEE, USA,2017. | Tareq Ahram, Arman Sargolzaei. | Application of Blockchain in various fields. | Identified blockchain as acatalyst for emerging use cases in financial and non-financial industries. |

**Table 3.1:** Summary

# Chapter 4

# Problem Statement

## 4.1 Problem Statement

There are many problems in current voting system like:

1. Vulnerability to hacking.
2. Susceptibility to fraud
3. Malicious programming.
4. The time gap between the voting and counting of votes is large which leads to tampering.
5. Due to the physical accessibility to the EVM, the third party can interrupt and change the count of votes.

   Due to this,voting system do not work properly. It facing main issue like security. That's why we built a secure voting system using blockchain to overcome challenges of current EVM based voting system and offers fairness,transparency as well as flexibility.

## 4.2 Goals and Objectives

- To Achieve high security using Blockchain.
- To develop trust factor in voting system.
- To achieve transparency in system by tracking all activities.
- To implement decentralized system so that data is stored in multiple systems.

## 4.3 Statement of Scope

Using blockchain technology, we can make sure that those who are voting are who they say they are and are legally allowed to vote. Plus, by using blockchain technology, anyone who knows how to use a cell phone can understand the technology required for voting. Using the blockchain for voting ensures a necessary level of transparency.The chief benefit of switching our voting systems over to the blockchain is the enhanced level of transparency the blockchain allows for. The blockchain would definitively preclude bad actors from cheating the system. It would make sure people do not vote twice, since we have an immutable record of their vote and their identity. And no one would ever be able to delete votes, because, again, the blockchain is immutable. Those charged with counting votes would have a final record of every vote counted that could be checked by regulators or auditors at any time.

# Chapter 5

# Existing System

## 5.1 Current Voting System

Voting Machines (quot;EVMquot;) are being used in Indian General and state elections to implement electronic voting in part from 1999 elections and recently in 2019 Vidhan Sabha Elections. Before EVM, vote counting was done by paper ballot but with the advancement in technology, electronic voting machines came into the picture. EVMs have replaced paper ballots in local, state and general elections in India.


**Figure 5.1:** EVM Machine

There are two units in EVM : the control unit and the balloting unit. These units are joined together with the help of cable. The control unit of the EVM is kept with the presiding officer or the polling officer. The balloting unit is kept within the voting compartment for electors to cast their votes. This helps polling officer to verify your identity. With the EVM, instead of issuing a ballot paper, the polling officer will press the Ballot Button which enables the voter to cast their vote. A list of candidates names and/or symbols will be available on the machine with a blue button next to it. The voter can press the button next to the candidates name they wish tovote for. No part of the EVM is "networked" is the most important thing .EVM machines are extremely simple machines, like pocket calculators, with no connection to the internet, no operating system and no way of being altered without physical access to the machines.There were earlier claims regarding EVMs39; temper ability and security which have not been proved.

## 5.2 Disadvantages of Current Voting System

- Vulnerability to hacking.
- Susceptibility to fraud
- Malicious programming.
- The time gap between the voting and counting of votes is large which leads to tampering.
- Due to the physical accessibility to the EVM, the third party can interrupt and change the count of votes.

# Chapter 6

# Proposed System

## 6.1 Proposed Voting System

Proposed system is an internet voting system . We provide an online platform for voting i.e a website. Propose system three parts as Voter, Election Administrator and Election Process.
Voter : Voter is the main part of the system which participate in the election process. He register himself in system by giving his personal information.

Election Administrator : To manage all the data coming from voter during registration. and election process, election administrator has worked. Also it generate public and private keys for voters. It is nothing but python packages.
Election Process : In this process voter select the candidate to vote and give his vote for selected candidate.

## 6.2 Working of Proposed System

In proposed system as told earlier voter register himself. During registration system takes voter's unique identity number. Unique identity is for generating unique public and private key for every voter. So here problem of double voting is solved. After taking all required information from voter, if the voter is eligible for voting process then only system accept registration of voters. Then system i.e election administrator generate public and private keys for voter.

### 6.2.1 Public and Private Key

Private key and public key are the hash value data which is unreadable. During election process for login purpose and giving vote to candidate public key and private key is required. It acts like login id and password in this voting process. But voter cannot always remember

it as it is large value. After successful registration this keys send to the registered email or mobile number. Also during voting process for data encryption and decryption purpose it is used.
After successful authentication and generating public and private key pair, voter login himself in system using keys. When voters enter in system he gets a list of all candidates.Voter chooses candidate for voting and give him vote. That vote is a block which is added in blockchain and broadcast to every system in the network. Every voter follow this process and every block is added in blockchain and hash value of each block is calculated. Every block contains previous block's hash value. So every block is connected with each other by hash value of previous block. As blockchain is decentralized then blockchain is created on every computer systems in network.

## 6.3 Preliminaries of E-Voting And Blockchain

In this section, we first elaborate on the design considerations when constructing an electronic voting system. Then, we provide an overview of blockchain and smart contract technology and its respective feasibility as a service for implementing an evoting system.

### 6.3.1 Design considerations

After evaluating both existing e-voting systems and the requirements for suchsystems to be effectively used in a national election, we constructed the following list of requirements for a viable e-voting system: (i) An election system should not enable coerced voting. (ii) An election system should allow a method of secure authentication via an identity verification service. (iii) An election system should not allow traceability from votes to respective voters. (iv) An election system should provide transparency, in the form of a verifyable assurance to each voter that their vote was counted, correctly, and without risking the voters privacy. (v) An election system should prevent any third party from tampering with any vote. (vi) An election system should not afford any single entity control over tallying votes and determining the result of an election. (vii) An election system should only allow eligible individuals to vote in an election.

### 6.3.2 Blockchain as a service

The blockchain is an append-only data structure, where data is stored in a distributed ledger that cannot be tampered with or deleted. This makes the ledger immutable. The blocks are chained in such a way that each block has a hash that is a function of the previous block, and thus by induction the complete prior chain, thereby providing assurance of immutability. There are two different types of blockchains, with different levels of restrictions based

on who can read and write blocks. A public blockchain is readable and writeable for everyone in the world. This type is popular for cryptocurrencies. A private blockchain sets restrictions on who can read or interact with the blockchain. Private blockchains are also known as being permissioned, where access can be granted to specific nodes that may interact with the blockchain . In addition to cryptocurrency, blockchain provides a platform for building distributed and immutable applications or smart contracts. Smart contracts are programmable contracts that automatically execute when predefined conditions are met. Similar to conventional written contracts, smart contracts are used as a legally binding agreement between parties. Smart contracts automate transactions and allow parties to reach agreements directly and automatically, without the need for a middleman. Key benefits of smart contracts compared to conventional written contracts are cost saving, enhanced efficiency and risk reduction. Smart contracts redefine trust, as contracts are visible to all the users of the blockchain and can, therefore, be easily verified. In this work, we define our e-voting system based on smart contracts.

## 6.4 Blockchain Based E-Voting System

We propose a blockchain based e-voting system ,which meets the essential requirements of e-voting system.

- The blockchain based e-voting system is public, distributed, and decentralized. It can records votes from voters across many mobile devices and computers,
- The blockchain based e-voting system allows the voters to audit and verify the votes inexpensively.
- The database of votes is managed autonomously and is using a distributed server of timestamp on a peer-to-peer network.
- Voting on blockchain is a workflow where voters regarding data security is marginal, which removes the characteristics of infinite reproducibility from e-voting.

Based on above illustration, thescheme id depicted in below figure(5.4.1) and is designed as follows:

- **Voting Blockchain:** It is growing list of voting blocks.
- **Voters:** The person who casts a ballot for his/her chosen candidate is voter. The voter can vote or withdraw a vote.
- **Voting office:** It is organization of voting. It can query the public key of voter, verify the votes and query the votes.

- **Public Key Infrastructure(PKI):** It is set of procedures that manage public key encryption.
- **Vote Database:** It is a database according to the statistics of votes updated by voting office.
- **Miners:** The responsibility of miners is to deal with accepted votes andadding them to the public voting blockchain.

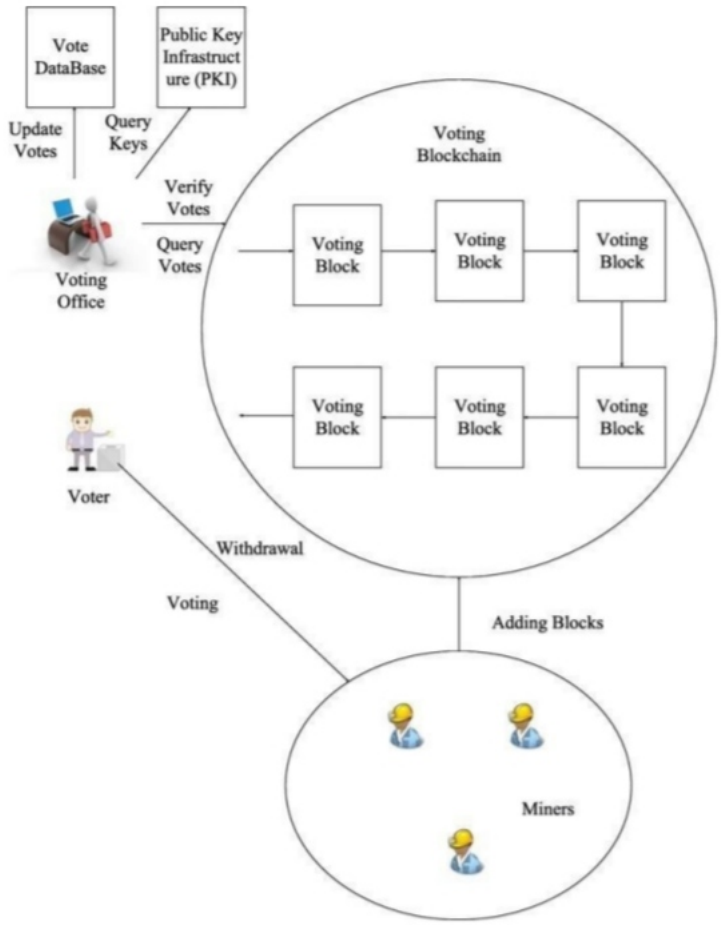


**Figure 6.1:** Blockchain based E-Voting System

## 6.5 Election Roles and Process

### 6.5.1 Election Roles:

As can be seen in Figure(6.2), elections in our proposal enable participation of individuals or institutions in the following roles. Where multiple institutions and individuals can be enrolled to the same role.

1. Election administrators: Manage the lifecycle of an election. Multiple trusted institutions and companies are enrolled with this role. The election administrators specify the election type and create aforementioned election, configurate ballots, register voters, decide the lifetime of the election and assign permissioned nodes.

2. Voters: For elections to which they are eligible for, voters can authenticate themselves, load election ballots, cast their vote and verify their vote after election is over. Voters can be rewarded for voting with tokens when they case their vote in an election in the near future, which could be integrated with a smart city project.

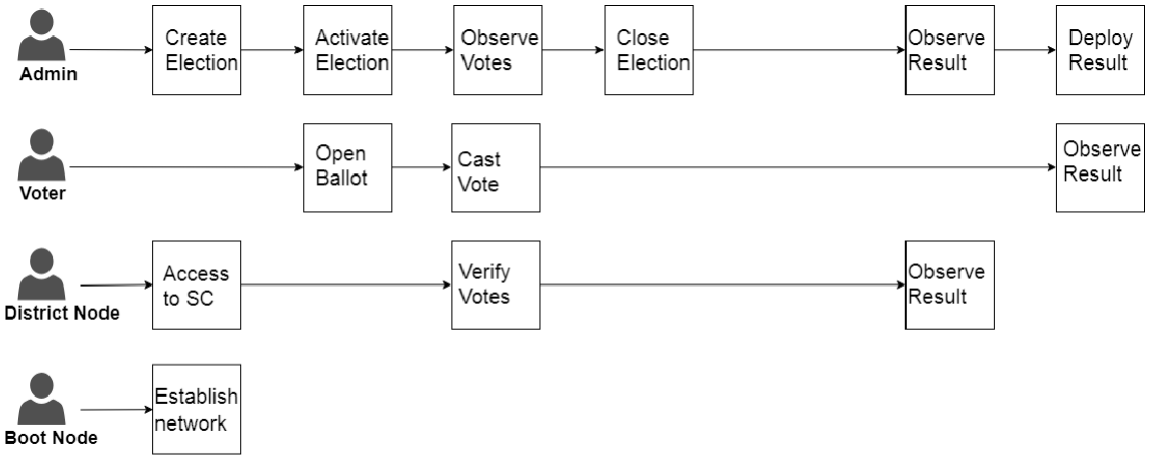


**Figure 6.2:** Election roles and Process

3. District nodes: When the election administrators create anelection, each ballot smart contracts, representing each voting district, are deployed onto the blockchain. When the ballot smart contracts are created, each of the corresponding district nodes are given permission to interact with their corresponding ballot smart contract. When an individual voter casts his vote from his corresponding smart contract, the vote data is verified by all of the corresponding district nodes and every vote they agree on are appended onto the blockchain when block time has been reached.

4. Bootnodes: Each institution, with permissioned access to the network, host bootnode. A bootnode helps the district nodes to discover each other and communicate. The bootnodes do not keep any state of the blockchain and is ran on a static IP so that district nodes find its peers faster.

### 6.5.2 Election Process:

In our work, each election process is represented by a set of smart contracts, which are instantiated on the blockchain by the election administrators. A smart contract is defined for each of the voting districts of the election so multiple smart contracts are involved in an election. For each voter with its corresponding voting district location, defined in the voters registration phase, the smart contract with the corresponding location will be prompted to the voter after the user authenticates himself when voting.

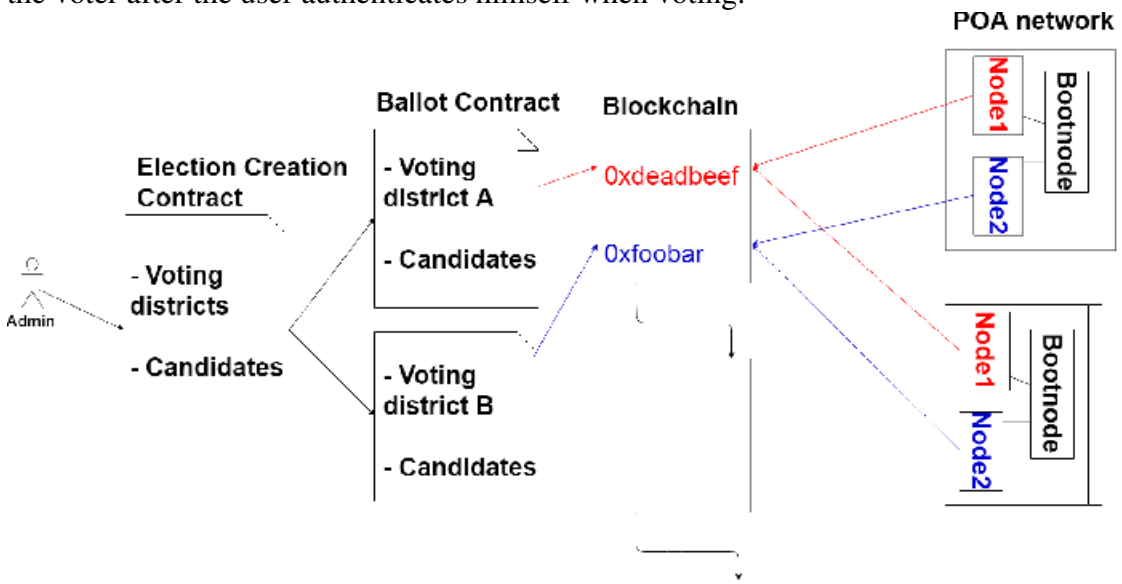


**Figure 6.3:** Election as a Smart Contract

## 6.6 Design and Implementation

To introduce a method of secure authentication, our proposed system is designed to use electronic ID authentication via Aukenni[25], which is an Icelandic service provider for identity verification. Aukenni utilizes the Nexus software and RFID scanners. When a user registers for an electronic ID, a user chooses a PIN number for its corresponding ID consisting of 6 numbers. A user will therefore identify himself in the voting booth by scanning his ID and providing his corresponding PIN number to authenticate himself to the system.

1. Any computer in any voting district can be used by any eligible voter to vote, since the wallet for the corresponding voter has information on which voting district the voter is supposed to vote from. For a user to successfully authenticate, a valid ID and PIN number needs to be presented at a voting district using a card reader and the nexus software.

2. If the authentication is successful, the corresponding smart contract is prompted for the ongoing election. The ballot for the aforementioned election is a smart contract which has a list of the candidates a voter can choose from.

3. When a voter has selected a candidate and casts his vote, the voter proceeds to sign his vote by re-entering the corresponding PIN number for his electronic ID.

4. After the voter has signed his vote, the vote data proceeds to be verified by the corresponding district node, which the voter is interacting with the smart contract through. If the aforementioned district node accepts the vote data, the vote data must be agreed upon by the majority corresponding district node.

5. If the majority of district nodes agree upon the vote data, consensus for the particular vote has been reached. The user then receives the transaction ID for the corresponding transaction of his vote in the form of a QR-code and the option to print the transaction ID. When the vote is casted and has been verified, a function in the smart contract adds one vote to the party which was voted for. This functionality of the smart contract structure is utilized to determine the election result in each of the voting districts. Figure(5.6.1) is a visual representation of the steps we just ellaborated.

6. All transactions which were received and verified in the ongoing block time are deployed onto the blockchain after the block time has reached its time limit. With each new block added to the blockchain, each district node updates his copy of the ledger.

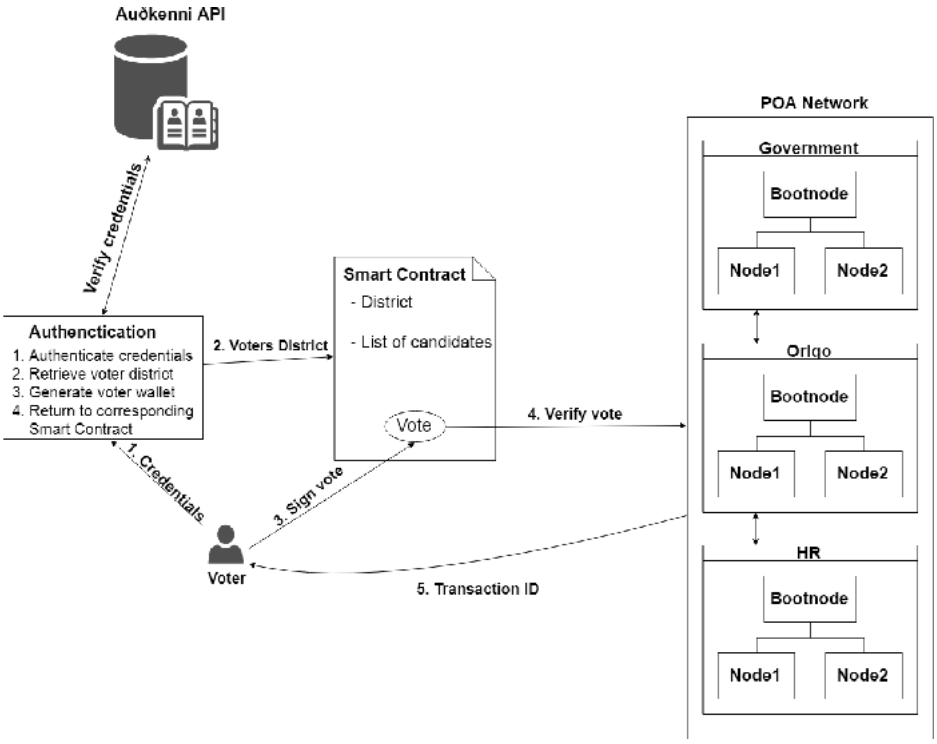


**Figure 6.4:** Voter authentication Process

# Chapter 7

# Architecture of E-Voting System with Blockchain

## 7.1 Architecture of Voting System

When determining on the architecture we took powerful inspiration from both the distributed and acquirability of the Bitcoin network and the gathering process of traditional voting. The network is a multi-tiered, decentralised infrastructure which having the two definite blockchains, the net- work is split into three abstract tiers, National, Constituency and Local. The local tier contains all the digital polling stations all over the country, each of which is connected to a constituency node. A local node is setup to only be in contact with the other local nodes under the connected constituency node and the constituency node itself.

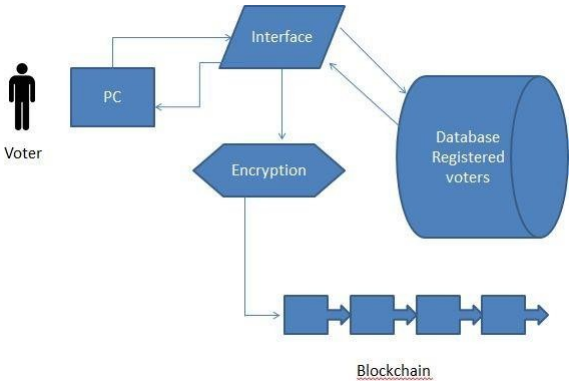


**Figure 7.1:** : E-Voting System Architecture

## 7.2 Use Case Diagram:

### 7.2.1 User Profile

- **Voter:** User register itself in the system. If user registered successfully he has right to vote.
- **Administrator:** It is python packages which help to generate public and private key
- **Candidate:** He stand for election.

### 7.2.2 Use Case view

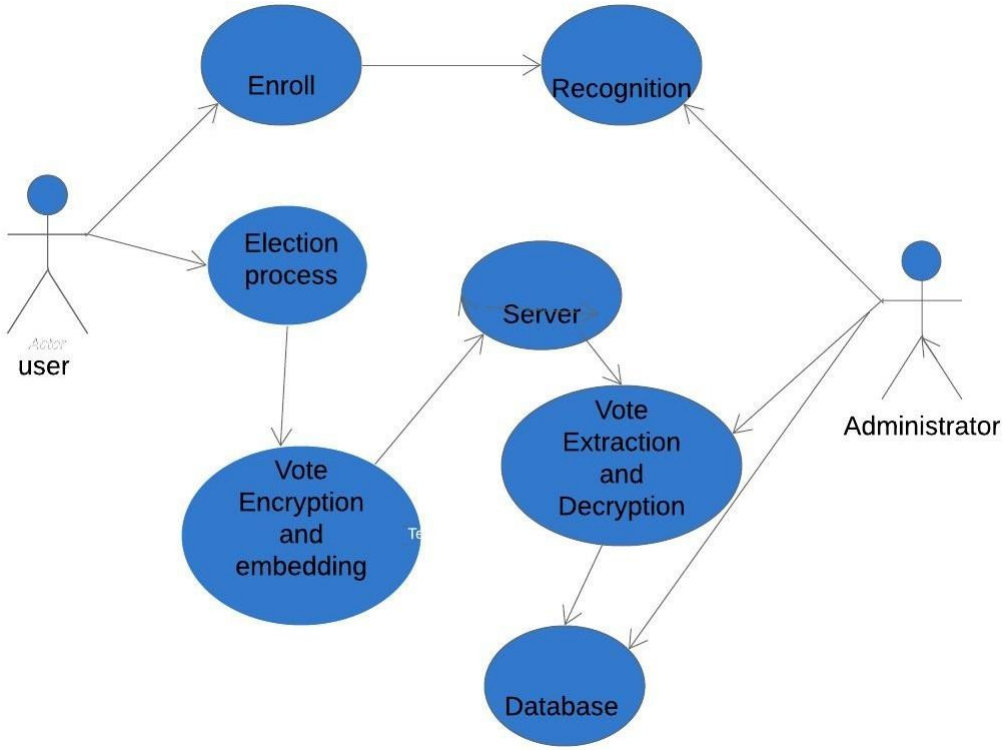


**Figure 7.2:** : Use Case Diagram

## 7.3 Activity Diagram :

Activity diagrams are graphical representations of workflows of stepwise activities and actions with support for choice, iteration and concurrency. In the Unified Modeling Language, activity diagrams are intended to model both computational and organizational processes (i.e.,workflows), as well as the data flows intersecting with the related activities. Although activity diagrams primarily show the overall flow of control, they can also include elements showing the flow of data between activities through one or more data stores.

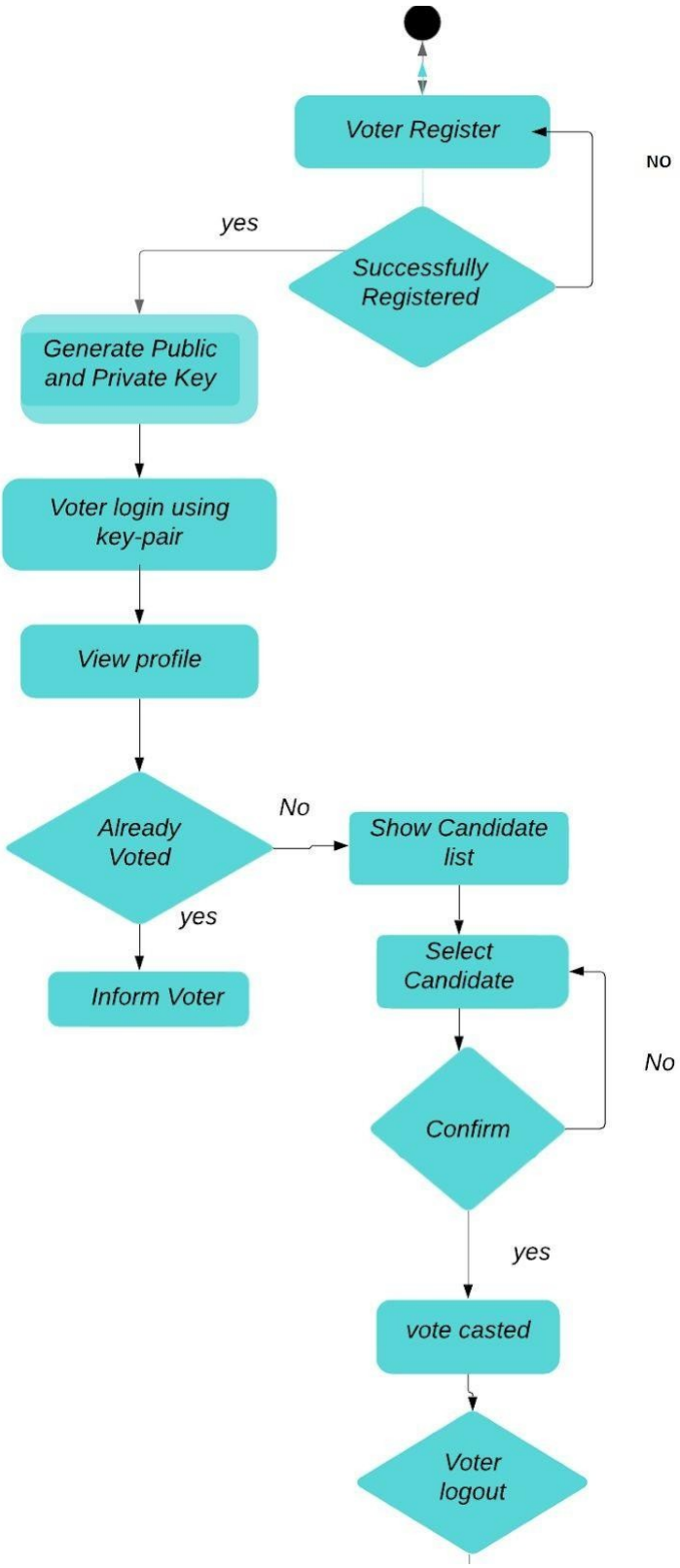


**Figure 7.3:** : Activity Diagram

# Chapter 8

# Conclusion

Blockchain Technology is gaining popularity day by day. Using blockchain in voting system will help to achieve secure and cost-efficient election while guaranteeing voter's privacy. Also, due to the encryption mechanism, it is impossible for any person to gain access to all the votes without first taking control of the entire service network.

The idea of adapting digital voting systems to make the public electoral process cheaper, faster and easier, is a compelling one in modern society. Making the electoral process cheap and quick, normalizes it in the eyes of the voters, removes a certain power barrier between the voter and the elected official and puts a certain amount of pressure on the elected official. It also opens the door for a more direct form of democracy, allowing voters to express their will on individual bills and propositions.

# Bibliography


[1] sos.ca.gov.(2007).Top-to-BottomReview—CaliforniaSecretaryofState. Available at: http://www.sos.ca.gov/elections/voting-systems/oversight/ topbottom-review/.

[2] Nicholas Weaver. (2016). Secure the Vote Today. Available at:https:// www.lawfareblog.com/secure-vote-today.

[3] TechCrunch, (2018). Liquid democracy uses blockchain to fix politics, and now you can vote for it [Online]. Available at: https://techcrunch. com/2018/02/24/liquid-democracy-uses-blockchain.

[4] Geth.ethereum.org. (2018). Go Ethereum. Available at: https://geth. ethereum.org

[5] Vitalik Buterin. (2015). Ethereum White Paper. Available at: https:// github.com/ethereum/wiki/wiki/White-Paper.

[6] Nca.tandfonline.com. (2015). Pirates on the Liquid Shores of Liberal Democracy: Movement Frames of European Pirate Parties. [Online]. Available at: https://nca.tandfonline.com/doi/abs/10.1080/13183222.2015.1017264.Wr0zCnVl8YR

[7] Feng Hao, P.Y.A. Ryan and Piotr Zielinski. (2008). Anonymous voting by two-round public discussion. Available at: http://homepages.cs.ncl.ac.uk/feng.hao/files/OpenVote$_{I}ET.pdf$

[8] Feng Hao and Piotr Zielinski. A 2-Round Anonymous Veto Protocol Available at: http://homepages.cs.ncl.ac.uk/feng.hao/files/av$_{n}et.pdf$.

[9] The Dining Cryptographers Problem: Unconditional Sender and Recipient Untraceability. Available at: https://users.ece.cmu.edu/ adrian/ 731- sp04/readings/dcnets.html.