Software Requirement Specification SEDA 1, (2022)
IEEE Std 1074-1991

Decetralized Voting System

Bhavin Patil
Dept. of Computer Engineering
Vishwakarma Institude of Technology
Pune, India
bhavin.patil21@vit.edu

Chaitanya Patil
Dept. of Computer Engineering
Vishwakarma Institude of Technology
Pune, India
chaitanya.patil21@vit.edu

Manasi Patil
Dept. of Computer Engineering
Vishwakarma Institude of Technology
Pune, India
manasi.patil21@vit.edu

Uma Thakur
Dept. of Computer Engineering
Vishwakarma Institude of Technology
Pune, India
uma.thakur21@vit.edu

***Abstract*— The voting method is the mechanism for implementing the people's view to better administer the system. Throughout recent years, but the electoral system in India also as in some countries abroad is flawed and may be easily manipulated and hampered by those with power to suit their personal benefits. They are not entirely safe since ballots are simple to strike. It also challenges voter safety and transparency. Additionally, counting the votes takes too long. To solve these problems Digital technology is used in the voting phase for citizens in many nations. Digitalization alone cannot fix the issues fully. There are also many ways of manipulating or modifying digital technology. We are using blockchain technology because the backbone of our product. By analyzing the aforementioned problems, this research work combines the digitalization with the blockchain technology to provide a voting mechanism. The main goals of our voting mechanism are to provide integrity, anonymity, privacy, and security of voters. The system can highlight a number of the popular blockchain frameworks that provide blockchain as a service and associated electronic E-voting system. In this paper, based on the blockchain technology, we propose a decentralized e-voting protocol, without the existence of a trusted third party.**

Keywords*— Blockchain Technology, Distributed System, End to End Transactions, Smart Contract, Mining, Electronic Voting System and E-voting.*

I. INTRODUCTION

This document describes the structural properties and software requirements of Decentralized Voting System

A. Vision

The vision of this document is to make the Decentralized Voting System's functional and non-functional requirements understandable. It also assists to make the functionality of the system evident to end users.

B. Scope of the Project

The Decentralized Voting System is made for the people of the country residing around the world and wants to vote for their representative. The election can be conducted in two ways the paper ballot election and the automated ballot elections.

The automated ballot elections called the electronic voting The Decentralized Voting System is highly developed and the online polling system can be replaced by accurately and directly voting online and immediate results The Decentralized Voting System is done by the internet so it can be called the Internet Voting.

C. Goals and Objectives

Goal:
Our project's major goal is to create a set of protocols that allows voter to vote at any field areas by using if they prefer online voting. We are using blockchain technology which allow digital information to be recorded and distributed, but not edited and we are using this concept in our project.

Objective:
The major objectives of our project are:

- To assess the ability of election systems to appropriately conduct safe, useful, and accessible elections in order to provide voters confidence that the election is a true expression of their will.
- To facilitate the interoperability of election systems
- To enable voters and election jurisdictions to examine the performance and capability of election systems in an open and transparent manner.

II. LITERATURE SURVEY

A variety of approaches have been developed to introduce differences in electronic and online voting systems, using various strategies and methodologies. While some of them provide some level of confidentiality and security to the system, the voting information and process must be managed and controlled by modern technologies that secure and guarantee the security and privacy of voters and voter information.

A. Basic E-voting approach/architecture:

The systems that are developed to caste the vote by means of digital approach using online portals and electronic devices use various encryption and decryption techniques to guarantee the secure data transaction

B. Homomorphic Encryption Technique:

Homomorphic encryption is a powerful technology with a wide range of applications. It has recently been used in the construction of an online voting system. The exponential ElGamal cryptosystem is used in the voting system based on

this encryption. The contents of each cast ballot are encrypted using the exponential ElGamal encryption before being sent. This crypto system's additive homomorphism characteristic allows for immediate tallying of encrypted ballots without the need to decrypt them.

C. Centralized architecture:

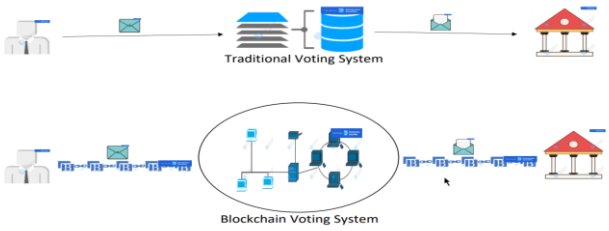
However, there are a variety of approaches for converting data into a coded format to prevent manipulation when transmitting over the network. One disadvantage that might be highlighted here is that when the correct data has been stored in the database, a high level of trust and security is necessary. If the data is valuable, centralized storage is unpleasant since illegal access and hacker attacks will put the system's reliability in jeopardy.

The centralized architecture approach is used to apply previous concepts and designs. This could lead to ethical and security issues. We put the data at danger by collecting it in a centralized location. It is possible to control it in an inequitable manner. As a result, the fair framework uses blockchain to solve the challenge of storing information in a distributed fashion. Blockchain is a decentralized ledger that keeps track of all completed transactions in chronological order.

Traditional databases are maintained by a single organization, and that organization has complete control of the database, including the ability to manipulate with the stored data, to censor otherwise valid changes to the data, or to add data fraudulently. For most use cases, this is not a problem since the organization which maintains the database does so for its own benefit, and therefore has no motive to falsify the database's contents; however, there are other use cases, such as a financial network, where the data being stored is too sensitive and the motive to manipulate it is too enticing to allow any single organization to have total control over the database. Even if it could be guaranteed that the responsible organization would never enact a fraudulent change to the database (an assumption which, for many people, is already too much to ask), there is still the possibility that a hacker could break in and manipulate the database to their own ends.

D. Blockchain (Decentralized) Architecture:

Blockchain technology solves these problems by creating a network of computers (called nodes) which each store a copy of the database, and a set of rules (called the consensus protocol) which define the order in which nodes may take turns adding new changes to the database. In this way, all of the nodes agree as to the state of the database at any time, and no one node has the power to falsify the data or to censor changes. The blockchain further requires that an audit trail of all changes to the database is preserved, which allows anyone to audit that the database is correct at any time. This audit trail is composed to the individual changes to the database, which are called transactions. A group of transactions which were all added by a single node on its turn is called a block. Each block contains a reference to the block which preceded it, which establishes an ordering of the blocks. This is the origin of the term "blockchain": it is a chain of blocks, each one containing a link to the previous block and a list of new transactions since that previous block. When a new node joins the network, it starts with an empty database, and downloads all of the blocks, applying the transactions within them to the database, to fast forward this database to the same state as all the other nodes have. In essence, a blockchain establishes the order in which transactions were applied to the database so that anyone can verify that the database is accurate by rebuilding it from scratch and verifying that at no point was any improper change made.



Architecture of Decentralized Voting System

III. SPECIFIC REQUIREMENTS

A. Interface Requirements

1) User Interfaces: The system must have a user interface that is accessible via all Web browsers for all sorts of users. For Election Mode and Normal Interactive Mode, the voter interface must be distinct.

2) Hardware Interfaces: This software system does not have any physical interfaces. The only way to communicate is through a computer system.

3) Software Interfaces: The poll server is powered by a http server that can handle server pages. It keeps track of the polls in a relational database, which it connects to using normal database connectivity APIs. The environment must have a Java Virtual Machine running in order to run the setup software.

B. Functional Requirements

1) Data Management of the System: During the election process, massive amounts of data are generated. As a result, data should be captured in a methodical manner.

2) Blockchain Storage: In the voting blockchain, a hash value derived from voter information is saved on the genesis block as a list of voters, and each vote is stored as a block in the chain. Another sort of blockchain is utilized to hold the metadata of the Election Commission's database.

3)Registration of Voters: The following are the steps in the voter registration process:

- In order to be a legitimate voter, each person must go to their local voter registration office and fill out the necessary paperwork.
- A key generation algorithm will be utilized to generate a public and private key pair.

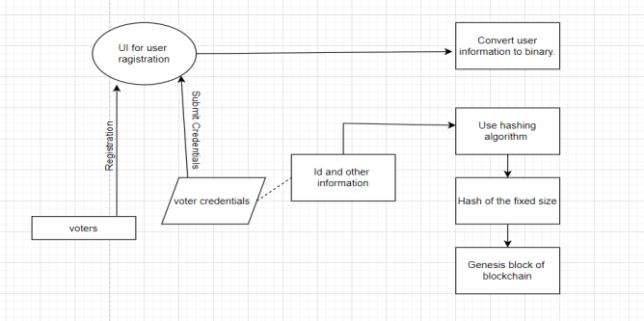
- In the blockchain network, the public key is used to identify voters. The private key is transmitted to the voters' mobile phone numbers. They can vote and participate in the voting process using this private key.

- A hash is generated from a voter's provided fingerprint using a fingerprint hash generation technique. The entire process of hash generation from voter-submitted data.

- The generated hash will be merged with the additional information provided by the voters to generate a new hash value.

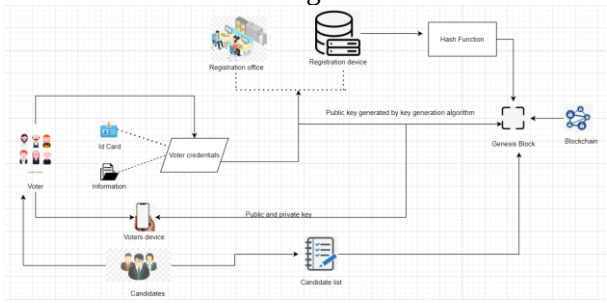
- The final hash value will be placed as a voter list in the blockchain's genesis block.

Where the hash value equals the proof-of-membership value.



4)Registration of Voters:

Because the candidate is also a voter, candidate registration is comparable to voter registration. The candidate number, party symbol, and public key will be stored in the blockchain's genesis block.



5) Vote Casting using smart contract: The following are the functions of smart contracts running on the blockchain:

- A voter's identity must be verified:
  - A voter uses an internet-connected device to log into the voting system using a private key.
  - Provide your NID, fingerprints, and other personal information.
  - On the blockchain, smart contracts compare the legitimate voters' information in the genesis block to the information submitted.
  - If the information is correct, the voter is given a candidate list.

- Create a Block for Casted Vote:
  - The voter selects one of the candidates from the list and votes.
  - Use a digital signature to sign the vote and send a transaction to the SC.
  - For that voter's vote, SC generates a VID (Vote ID).
  - Increase the number of votes cast for the chosen candidate.
  - Create a block with the voter's transactions, including the VID and Candidate Vote number.

- Miner Selection:
  - The SC uses a Miner Selection Algorithm to choose a miner to generate the block's target hash.

- Generate Hash:
  - The SC-nominated Miner modifies the block by inserting the current mined block's hash and into the Block, increasing the nonce.
  - The miner starts generating the hash that is desired a large number of noticeable zeros (also known as Proof of work) Increase the value of a variable known as nonce which identifies the verified hash.
  - The Miner generates the desired hash of the block which will be added to the network and the miners will get monitory as reward.
  - Proof of Work Any digital currency, such as Bitcoin, necessitates massive computational resources as miners compete to be the first to produce the block's objective hash in order to avoid record interference. It has been proposed that a Miner be chosen in the proposed voting architecture based on a heuristic generated from a Miner's achievements. such as latency, energy utilization, and node capacity.

- Verify Block:
  - After adding the vote to the chain, Sc will remove the hash value from the

voter list and add it to another list called Already voted to prevent double voting.
    - Return the voter's VID so that their vote may be verified in the blockchain.

- Counting of Votes:
    - The number of votes in each block will be counted by the smart contract. The vote is counted immediately as it is submitted, therefore there is no danger of voting manipulation or fraud.

C. Non-Functional Requirements

- Public Verifiability: All participants in the election process (including those who observe the voting process) can independently verify the election's whole method and outcome.
- Individual Verifiability: Each voter can check to see if his or her vote was correctly recorded and counted.
- Dependability and Reliability: To protect against assaults, asymmetric-key encryption and various blockchain methods are used. To ensure that only genuine and confirmed votes are added to the blockchain network, digital signatures (blind signatures or short-linkable ring signatures) are employed to validate votes.
- Consistency: All nodes have the same copy of records (same copy of blockchain) at any given time, and all of them will have the same end result after the election process is through, thanks to blockchain's consensus mechanisms.
- Auditability: If necessary, the entire operation can be audited after the election.
- Anonymity: There is no link between voters and their votes. Cryptography and the use of zero-knowledge proofing to validate ballots assure complete voter anonymity.
- Openness: The entire procedure is open to the public. It is both secure and transparent.
- Scalability: The digital signature process is based on a short-linkable ring signature, which may handle a large number of voters.
- Eligibility: Ensuring that only those who are eligible have access to the system.
- Authentication: Using a unique voter ID and other credentials, users desiring to use the e-voting system are authenticated.
- Objectivity: The election results are not yet available. Due to the lack of a centralized authority, votes can only be counted when the full election process has been completed, which can only be done by decrypting the encrypted blocks in the blockchain network.

D. Software Requirements

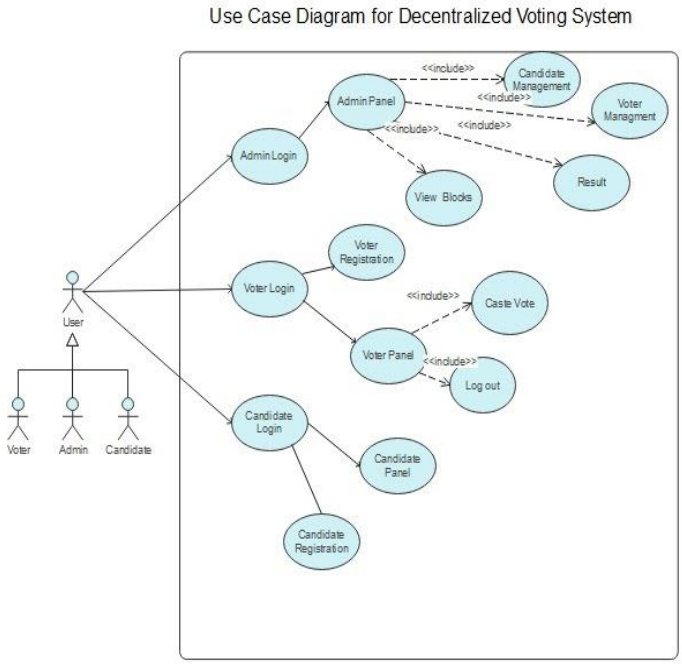
- Operating System: Windows 10.
- Framework: Visual Studio, Remix, Solidity, Truffle, Ganache, NodeJS
- Server: Localhost
- Database: MS-SQL Server 2012/14 or SQLite

E. Hardware Requirements

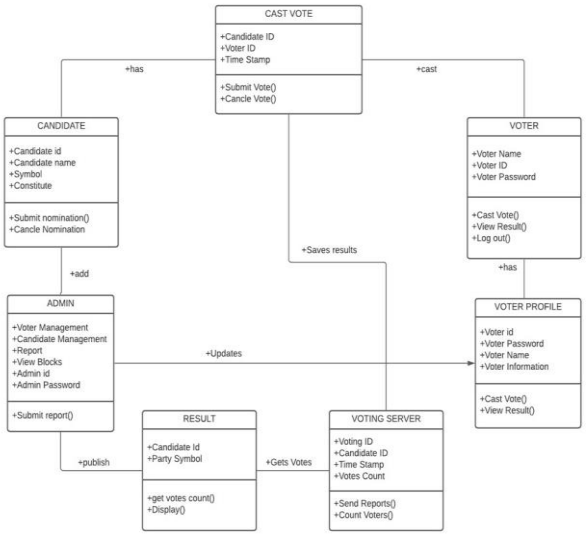
- Processor: Intel Quad core 1.7 GHZ Processor or above.
- Storage: Minimum 10GB of Hard Disk Drive or Solid-State Drive.
- Memory: Minimum 8GB of RAM.

IV. DIAGRAMS

A. Use Case Diagram:

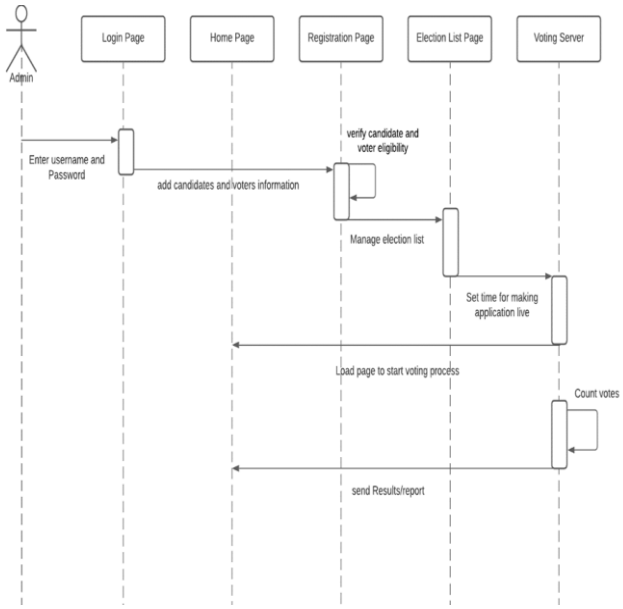


B. Class Diagram:

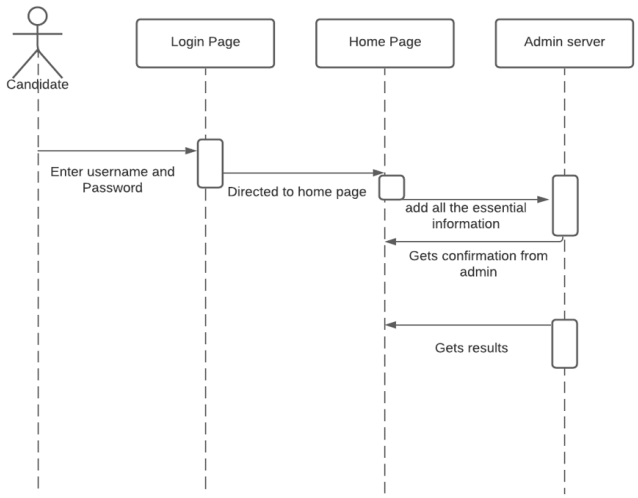


C. Sequence Diagram:

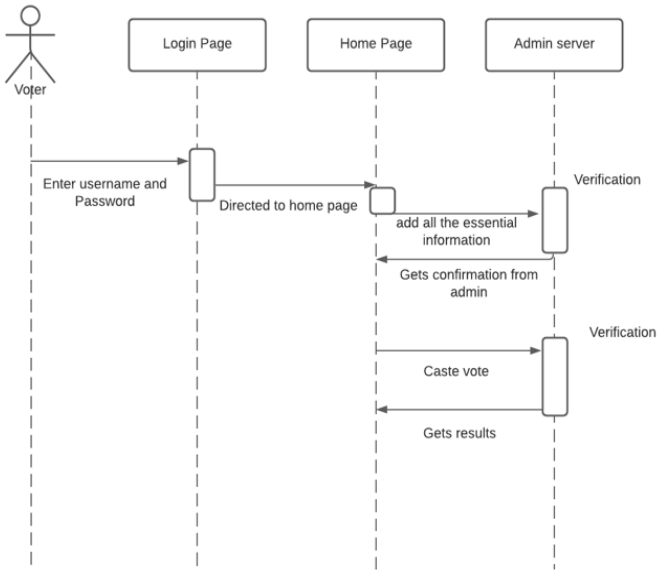
- Admin



- Candidate

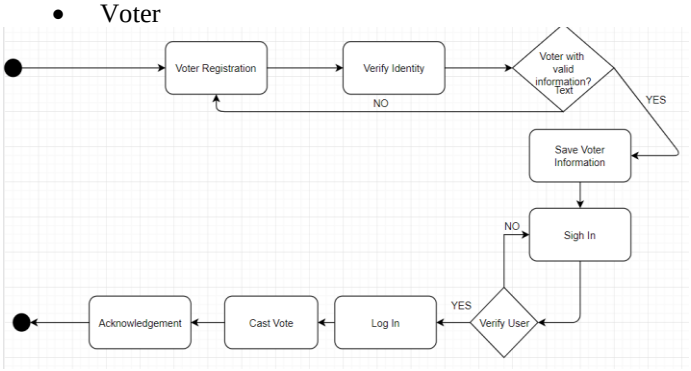


- Voter

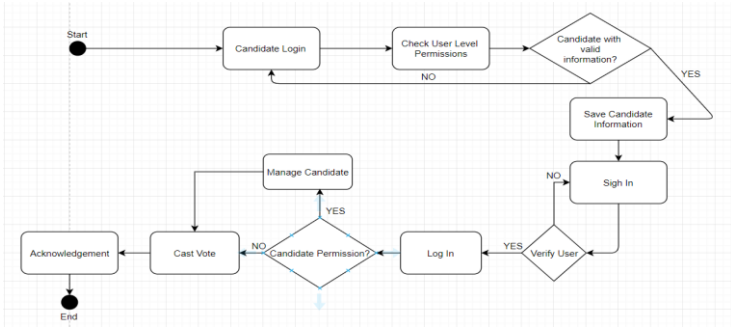


D. Activity Diagram:

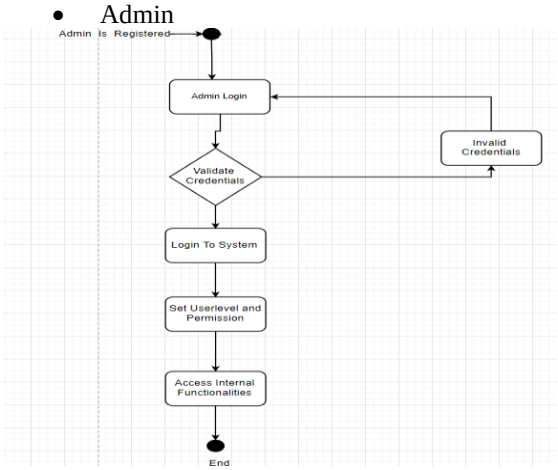
- Voter



- Candidate



- Admin



V. USER STORIES

Here are some user stories (Epics, Features and User Stories)

ID	EPICS
E1	As a candidate I must be able to cast vote.
E2	As voting administrator I must be able to access the voting system.
E3	As a voter I must be able to vote in proper secure environment.

ID	FEATURES
E1F1	As a candidate, I want access to the candidate dashboard.
E2F2	As a candidate, I must select the areas to register myself.
E3F3	AS a voter, I want my voting information must to store secure.
E4F4	As an administrator I must be able to monitor all the activities.

ID	USER STORIES
E1F1U1	As a candidate I want to access the result of the election.
E2F2U2	As a voter I want to see the list of candidates listed in the area, so that I can choose between the options.
E3F3U3	As a voter I want an option not to vote any of the candidate listed in the system.
E4F4U4	As an administrator I want the privilege to block the user if the user trying to break the code of conduct.
E5F5U5	As an administrator I must able to announce the result at the end of the election process.

VI. BACKLOG

DECENTRALISED VOTING SYSTEM				
As a…	I want to be able to….	So that…	Priority	Status
Admin	sign in	I can monitor system	Must	Done
Admin	view candidate database	I can verify Candidate eligibility	Must	Work in Progress
Admin	view voter database	I can verify voter eligibility	Must	Work in Progress
Admin	manage election list	I can set time for making application live	Must	Work in Progress
Admin	make changes in the system	Load page to start voting process	Must	Work in Progress
Candidate	Login	I can make my profile	Must	Done
Candidate	Update profile	I can improve profile	could	To be Started
Candidate	View result	I can see whether I won nor not and the number of votes I received	Must	Work in Progress
Voter	Login	I can make my profile	Must	Done
Voter	Update profile	I can improve profile	Could	To be started
Voter	Register vote	I can vote for my favourite candidate to win	Must	To be started
Voter	View result	I can see who is won and with how many votes	Must	To be started

VII. CONCLUSIONS AND FUTURE WORK

Many countries face significant difficulties in protecting security in the voting framework. To ensure the participation and legitimacy of the voter, the integrity of the vote data and the counting of votes without manipulation, a blockchain based voting system using smart contract has been proposed. The transparency of the blockchain enables more auditing and understanding of elections. This mechanism where the SC performs the authentication process of voter and plays a role in selecting a Miner in the Blockchain to reduce the computational cost. It also counts the vote immediately which reduce the time consumption of election process. This mechanism provides the environment to the citizens to cast their vote using smart devices from anywhere. This will help to improve the amount voters in order to achieve any country's democracy. The blockchain are going to be publicly verifiable and distributed during a way that nobody is going to be ready to corrupt it.

REFERENCES

[1] Liu, Y.; Wang, Q. An E-voting Protocol Based on Blockchain. IACR Cryptol. Eprint Arch. 2017, 2017, 1043

[2] Syada Tasmia Alvi, Mohammed Nasir Uddin and Linta Islam. Digital Voting: A Blockchain-based E-Voting System using Biohash and Smart Contract.

[3] Uzma Jafar * , Mohd Juzaiddin Ab Aziz and Zarina Shukur. Blockchain for Electronic Voting System—Review and Open Research Challenges.

[4] Prof. Anita A. Lahane1,∗, Junaid Patel1,∗∗ , Talif Pathan1,∗∗∗ and Prathmesh Potdar1,∗∗∗∗. Blockchain technology based e-voting system.

[5] Friðrik Þ. Hjálmarsson, Gunnlaugur K. Hreiðarsson School of Computer Science. Blockchain-Based E-Voting System

[6] Mrs M.Kamala1 , Dharmikesh Kalakonda 2 , Abiram Muppaneni 3 ,Mahesh Pala 4. Decentralised Voting System.

[7] Andrew Barnes, Christopher Brake and Thomas Perry. Digital Voting with the use of Blockchain Technology.

[8] Emilbek Joldoshev, Hassan Salahe Matar, Mehmet Barış Özkan and Hüseyin Lutin. Software Requirement Specification For Online National Election Voting.