A PROJECT REPORT

ON

Decentralized Voting System Using Blockchain Technology

Submitted in partial fulfillment of the requirements for the award of degree of

BACHELOR OF TECHNOLOGY

IN

COMPUTER SCIENCE & ENGINEERING

GALGOTIAS
UNIVERSITY
(Established under Galgotias University Uttar Pradesh Act No. 14 of 2011)

Under The Supervision of
Dr. T. Poongodi
Associate Professor
Department of Computer Science and Engineering

Submitted By:

SHAMBHAVI BHARDWAJ-18021011623

ASHUTOSH DIXIT-18021011692

SCHOOL OF COMPUTING SCIENCE AND ENGINEERING
DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
GALGOTIAS UNIVERSITY,GREATER NOIDA
INDIA DECEMBER,2021

DECLARATION

We hereby declare that the project entitled - “Decentralized Voting system using BlockChain Technology”, which is being submitted as a project of 7th semester in Computer Science & Engineering to Galgotias University, Greater Noida (U.P) is an authentic record of our genuine work done under the guidance of Associate Professor **Dr. T. Poongodi**, Dept.
Computer Science & Engineering, Galgotias University.

Date:- 20-12-2021

SHAMBHAVI BHARDWAJ

ASHUTOSH DIXIT

CERTIFICATE

The Final Thesis/Project/ Dissertation Viva-Voce examination of

“SHAMBHAVI BHARDWAJ(18SCSE1010392) & ASHUTOSH DIXIT (18SCSE1010464) ” has been held on ________________ and their work is recommended for the award of B.Tech(CSE).

Signature of Examiner(s) **Signature ofSupervisor(s)**

Signature of Project Coordinator **Signature of Dean**

Date: December, 2021
Place: Greater Noida

ACKNOWLEDGEMENT

We would like to express our sincere gratitude to **Dr. T. Poongodi**, Associate Professor of the department of Computer Science & Engineering, whose role as project guide was invaluable for the project. We are extremely thankful for the keen interest she took in advising us, for the books and reference materials provided for the moral support extended to us.

Last but not the least we convey our gratitude to all the teachers for providing us the technical skill that will always remain as our asset and to all non-teaching staff for the gracious hospitality they offered us.

SHAMBHAVI BHARDWAJ
ASHUTOSH DIXIT

ABSTRACT

Voting is the backbone of democracy and the fundamental right of every citizen. BlockChain based Election is like a boon for every nation through which the election can be conducted digitally, Unlike those old (paper based) and traditional (EVM) voting systems it makes the whole process of election safe, smooth and easy. In this era of Covid-19 this Block chain enabled election is the need of the hour, People can cast votes from their own space just with the help of a mobile phone or a computer, Security would get enhanced and threats like EVM hacking, Chaos at election booth would reduce drastically just by the implementation of this advanced voting system.

This project revolves around the idea of developing an electronic voting system using blockchain technology. Personal ID’s and unique keys would be provided to each and every eligible voter which can’t be tampered at any cost. It has two modules to make the entire project look consolidated and unified. First module is the Election Commission who will be responsible for conducting elections, appending concerned parties and candidates contesting for the election attached under Smart contracts. The user end will be the voter's module where each and every eligible voter can cast a vote according to their respective Constituent Assembly and the votes would get registered on the blockchain to make it tamperproof.

Table of Contents

List of Figures

INTRODUCTION

The advancement of blockchain technology has led to the core concept of decentralization which has continuously drawn attention. Keeping this factor in mind , the main objective of this research is to realize new convenient and secure applications through the use of blockchain technology. At present, the service industry, for example the financial and banking industry, transmits private information with use of a trusted third party. Having said that, they are facing many difficult and complicated procedures. Since blockchain technology has these characteristics of decentralization, the researchers surveyed the architecture of the existing E-voting systems and discovered the integration of blockchain into the application, this would strengthen data verifiability and lower the cost by still managing to maintain the accessibility and transparency of the voting. The anonymities of voters, the security of ballot communication and the verifiability of votes at the billing phase are the most fundamental requirements of voting. The anonymity and security can be attained with the help of a secret sharing scheme with Paillier's public-key cryptosystem at the time the verifiability of votes can be achieved by help of the transparency and non-repudiation of blockchain. Thus, using this practice voters themselves can calculate the ballots and confirm the election results on their own without a trusted third party. This project will integrate the advantages and properties of three level system names as blockchain and secret sharing scheme, Paillier's homomorphic encryption and unaware or unsecured transfer to construct a decentralized e-voting system.

This application is to provide a web-based decentralized voting application where each and every voter has a fair role to play. It uses a blockchain mechanism and prevents double-voting and fraudulent voting. In this application, each voter registers with valid details and then votes for the corresponding party. Each registered voter has a unique voter ID. A set of authentication keys is generated against each voter. When a user votes, it is checked whether it is the first time or it is already done before. And it is ensured that there can be only one vote casted from each voter. After passing through this verification, the vote is then recorded as done. All votes that are accepted require consensus across the network. No single node controls it and every node is an owner and each vote is peer-peer verified.

Given that every recorded vote on the blockchain needs consensus on the network and the fact that it is merely impossible to manipulate too many systems at the time, the chances of fraudulent votes are very low. The voting system is 100% transparent, no central authority owns it and the voters identification remains confidential. Also, people don't have to leave their sofa to cast their votes but they can do it online at their own convenience. Since this application is decentralized, it ensures high availability and data security.

It provides:

1. Anonymity of voters: ensures that whoever is casting a vote, they are authorized to do so.
2. Only one vote per person: No one would be able to vote more than once in the same election.
3. Data integrity: Ensures that once voted, it cannot be manipulated.

Existing Problem-

We are facing a lot of problems in our day to day life for example, Democratic voting is a crucial and serious event in any country. The most common way in which a country votes is through a paper based system.But with the use of blockchains a secure and robust system for 4 digital voting can be devised. This report outlines our idea of how blockchain technology could be used to implement a secure digital voting system. 2.After the first point that refers to ideality of problem statement we should now see its reality so nowadays blockchain is used Blockchain has often been described as a solution in search of problem, but the technology is slowly moving out of research labs and into real-world applications to creating a growing global market that Research and Markets expects to rise from $80 million this year to more than $2.3 billion by 2023. 3.As Blockchain is helping the voting system to be digital and make it useful for us .Moreover ,Blockchain can readily be applied to real estate information and Blockchain can improve health care services. With patient health records in a blockchain environment, all the healthcare providers in a person's network can receive permission, once verified, to access, view and update the same, single record of that person's history. So if block chains are not used, we have to face consequences about these day to day functions . 4.For our design we tried to create a system that doesn't entirely replace the current voting but rather integrates within a current system. We decided to do this to allow for as many different ways to vote as possible, this is so voting can be accessed by the majority of the population.

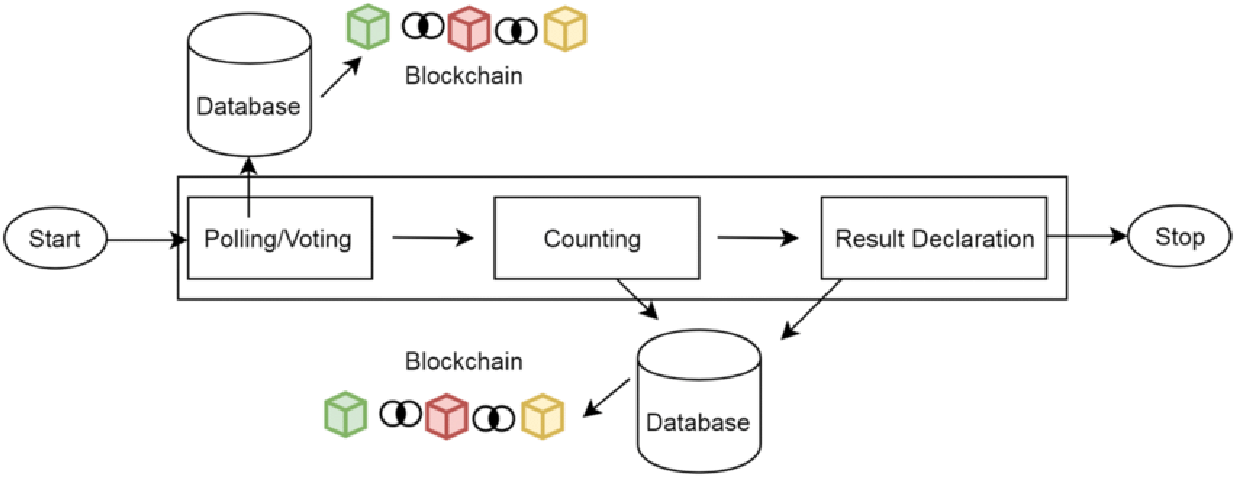
Domain Knowledge:

Domain knowledge is knowledge about the environment in which the target system operates.In this we are talking about blockchain so,we should know in what fields this system works---Blockchains permit to store information in a tamper-resistant and irrevocable manner by reverting to distributed computing and cryptographic technologies. The primary purpose is to keep track of the ownership of tangible and intangible assets.

Technical Excerpts:

Blockchain-enabled e-voting (BEV) could reduce voter fraud and increase voter access. Eligible voters cast a ballot anonymously using a computer or smartphone. BEV uses an encrypted key and tamper-proof personal IDs.
E-voting is among the key public sectors that can be disrupted by blockchain technology.1 The idea in blockchain-enabled e-voting (BEV) is simple. To use a digital-currency analogy, BEV issues each voter a "wallet" containing a user credential. Each voter gets a single "coin" representing one opportunity to vote. Casting a vote transfers the voter's coin to a candidate's wallet. A voter can spend his or her coin only once. However, voters can change their vote before a preset deadline.
A blockchain is simply a cryptographically verifiable list of data. One of the reasons for the enthusiasm around the blockchain is that databases do not have any cryptographic guarantees of integrity, guarantees that are necessary for any database operating in an adversarial environment.
With Bitcoin and variants being developed by practitioners rather than cryptographers, the trust tends to be put not in formal proofs and properties but in

practical resistance to attacks based on common knowledge and experience by practitioners



Methodology to implement E-voting using blockchain:

This method has 5 main requirements

1. Authentication
2. Anomility
3. Accuracy
4. Verifiability
5. Flexibility and Mobility

BACKGROUND AND RELATED WORK

Blockchain is a stable ledger. Smart contract is a blockchain-based application that responds to and processes incoming information.

The idea of secret sharing was first proposed by Shamir [3] in 1979 effective protection against server side attacks.

The Paillier cryptosystem for public keys was proposed by Paillier [5] in 1999.

additive homomorphic encryption is widely used in many applications, such as electronic voting, maintaining confidentiality of original information.

The negligent transfer proposed by Rabin [4] is a law to protect privacy

sender and recipient when the sender sends a few messages to the recipient, however does not know what message the recipient received. In addition, the recipient can get only one but you do not know anything about the other message.

The first things that come to mind about the blockchain are cryptocurrencies and smart contracts because of the well-known initiatives in Bitcoin and Ethereum. Bitcoin was the first crypto-currency solution that used a blockchain data structure. Ethereum introduced smart contracts that leverage the power of blockchain immutability and distributed consensus while offering a crypto-currency solution comparable to Bitcoin. The concept of smart contracts was introduced much earlier by Nick Szabo in the 1990s and is described as “a set of promises, specified in digital form, including protocols within which the parties perform on these promises”. In Ethereum, a smart contract is a piece of code deployed to the network so that everyone has access to it. The result of executing this code is verified by a consensus mechanism and by every member of the network as a whole. Today, we call a blockchain a set of technologies combining the blockchain data structure itself, distributed consensus algorithm, public key cryptography, and smart contracts [18]. Below we describe these technologies in more detail. Blockchain creates a series of blocks replicated on a peer-to-peer network. Any block in blockchain has a cryptographic hash and timestamp added to the previous block, as shown in Figure 1. A block contains the Merkle tree block header and several transactions. It is a secure networking method that combines computer science and mathematics to hide data and information from others that is called cryptography. It allows the data to be transmitted securely across the insecure network, in encrypted and decrypted forms

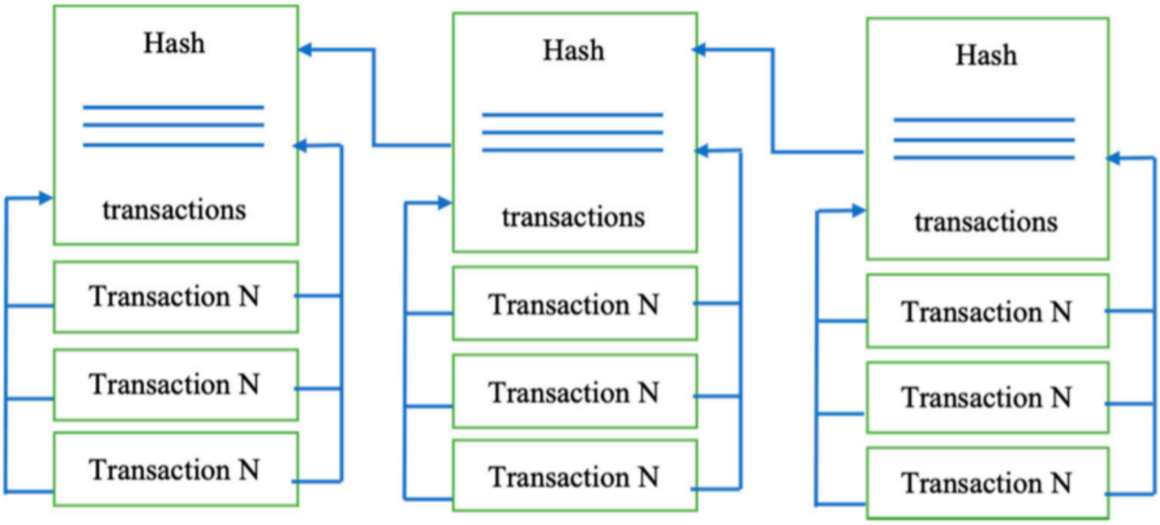


Fig: The Blockchain Structure

Smart contracts breathed new life into blockchain solutions. They stimulated the application of blockchain technology in efforts to improve numerous spheres. A smart contract itself is nothing more than a piece of logic written in code. Still, it can act as an unconditionally trusted third party in conjunction with the immutability provided by a blockchain data structure and distributed consensus. Once written, it cannot be altered, and all the network participants verify all steps. The great thing about smart contracts is that anybody who can set up a blockchain node can verify its outcome.

As is the case with any other technology, blockchain technology has its drawbacks. Unlike other distributed solutions, a blockchain is hard to scale: An increasing number of nodes does not improve network performance because, by definition, every node needs to execute all transactions, and this process is not shared among the nodes. Moreover, increasing the number of validators impacts performance because it implies a more intensive exchange of messages during consensus. For the same reason, blockchain solutions are vulnerable to various denial-of-service attacks. If a blockchain allows anyone to publish smart contracts in a network, then the operation of the entire network can be disabled by simply putting an infinite loop in a smart contract.

A network can also be attacked by merely sending a considerable number of transactions: At some point, the system will refuse to receive anything else. In cryptocurrency solutions, all transactions have an execution cost: the more resources a transaction utilizes, the more expensive it will be, and there is a cost threshold, with transactions exceeding the threshold being discarded. In private blockchain networks, this problem is solved depending on how the network is implemented via the exact mechanism of transaction cost, access control, or something more suited to the specific context.

Core Components of Blockchain Architecture These are the main architectural components of Blockchain:-

- Node: Users or computers in blockchain layout (every device has a different copy of a complete ledger from the blockchain);

- Transaction: It is the blockchain system’s smallest building block (records and details), which blockchain uses;

- Block: A block is a collection of data structures used to process transactions over the network distributed to all nodes.

- Chain: A series of blocks in a particular order;

- Miners: Correspondent nodes to validate the transaction and add that block into the blockchain system;

- Consensus: A collection of commands and organizations to carry out blockchain processes

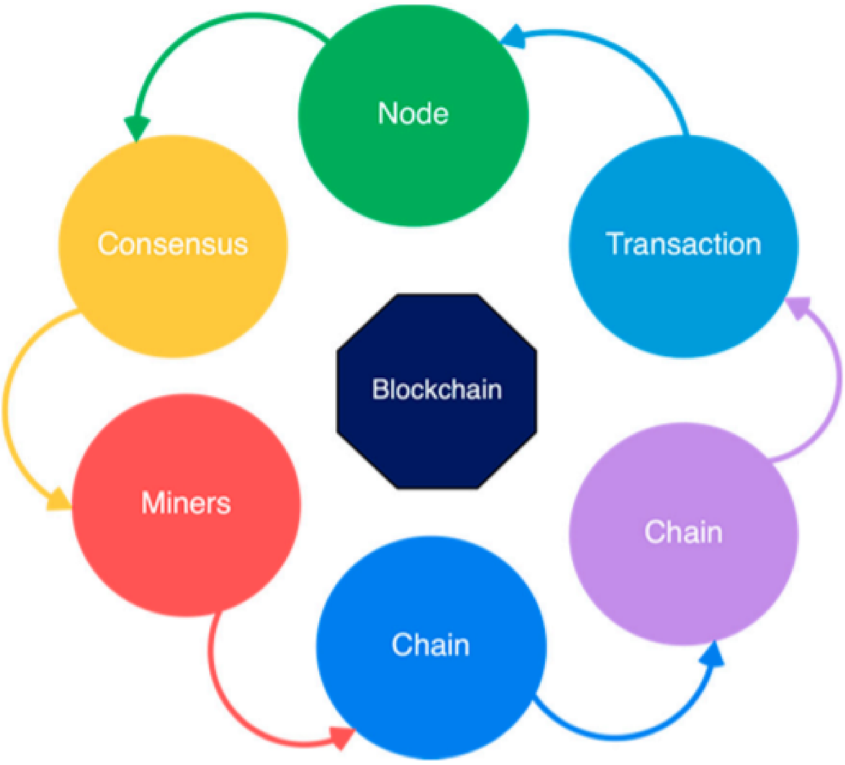


Fig:Core components of blockchain architecture

LITERATURE SURVEY

Advancements in information technology are too controlling the election processes and methods. Researchers are actively working to donate to the procedure and to improve the allowance of such structure to voting systems. Electronic voting is assessed from contrasting angles to traditional voting systems, for example convenience, reducing any point of error, and getting results faster and accurately.Election commissions possibly face numerous difficulties in the course of election. The most frequent problems are unfitted approval to the voting, replication , or illegal voting. Secure authentication is very crucial to confirm that the eligible voter literally casts the vote which is their right.

E-voting can in general be partitioned into two departments. One is the ballots, Ballots can operate remotely, together with closed systems placed in election offices. In pool locality E-voting, the voters can still take part physically, but at this point the ballots are removed and counted electronically. In the process of remote online voting, votes summed remotely, generally using a personal device through the Internet. For example Such alternative devices can be your own voting kiosks, computers, mobile devices, paper-based E-systems, and over televisions.Such applications and systems must be accepted by society. A practical secure e-voting plan should be structured to provide the following features:

Eligibility: making the practice such that only registered and authorized voters can cast a vote.

Uniqueness: to ensure no one can vote again in a given one set.

Noncoercibility: its is a practice by which system predicts value that no one is allowed to follow up the person for which voter he voted for

Reliability: ensured votes are well recorded securely even in case of system malfunctions

Integrity: integrity being that crucial point ensures no one can practice to change the votes

Verifiability: make sure that the votes are summed appropriately.

The first block is the foundation block which contains the candidate's name. This block will not be counted as a vote . In this system a candidate may return a blank vote indicating dissatisfaction. Whenever a voter votes transaction is recorded and blockchain is updated. The block may as well contain previous voters information to ensure security. The user’s vote is sent to one of the nodes of the system and node adds vote to blockchain.

Representation Of E-Voting

1. The voter will login to the system using his/her credentials provided by the government.

2. Our system will check the data ,if matched with a valid voter ,vote can be casted
3. There are two options given (I) Vote for candidate (II) Vote NOTA

4. After the user casts his vote, the system will generate an input that contains the voter identification and the hash of the previous vote. This way each input will be unique and ensure that the encrypted output will be unique as well. The encrypted information will be recorded in the block header of each vote cast. It can be encrypted using SHA-256 in which reverse string cannot be generated. Therefore there is no way to retrieve voter’s information.

5. Once the block is created the information is recorded in corresponding blockchain and gets linked with previously cast vote

Solidity is one of the most popular languages used by Blockchain Developers. Influenced by C++, Python, and JavaScript, it was designed to target the Ethereum Virtual Machine(EVM). Solidity is statically typed, supports inheritance, libraries, and complex user-defined types. By using Solidity a user can do the following

1. Mine ether token
2. Transfer tokens between addresses
3. Create smart contracts and execute it on the Ethereum Virtual Machine
4. Explore the block history

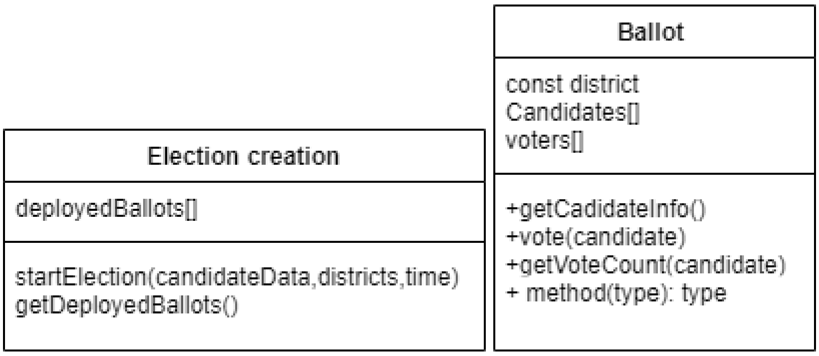
Solidity supports the OOP paradigm and is most commonly used for writing smart contracts. With Solidity, Blockchain Developers can write applications that can execute self-enforcing business logic embodied in smart contracts, thereby leaving a non-repudiable, and authoritative record of transactions. This comes in handy for creating contracts for voting, crowdfunding, multi-signature wallets, and blind auctions.

Smart Contracts:-

The system includes two Smart contract:

Ballot smart contract. The Ballot smart contract is where the votes are recorded. Each district or constituency would have a Ballot instance deployed on the blockchain; and it consists of a list of candidate data for each district. The Ballot consists of a vote function which can be called by the client to increment the vote count of a candidate. Since this function changes the state of the contract, its function is payable, and thus recorded on the blockchain. Each ballot has a time parameter which specifies the duration till which the vote function would be valid. This contract will be accessed by the voting machine for voting and the ECI portal for monitoring and counting process.

Election creation smart contract. the election creation smart contract is what is used to deploy the ballots on the blockchain. Only the ECI representative, operating the ECI portal client can connect to this contract. This contract takes input as the database of all candidates of respective districts and deploys ballots for every district onto the blockchain. This contract also has a function which returns the addresses of the deployed ballots, so they can be used by the voting machines later.



There are two web clients in this project viz the ECI portal and the voting machine. Both of these clients require communication using both http and rpc protocols, hence make use of api/libraries such as XMLHttpRequest and web3.js

1. Web Portal

The ECI portal has several functions. First, it has to register eligible voters. For this, a table consisting of required voter data is created using this functionality. This data includes a hash of voter id and fingerprint and the voters' district. For each registered voter, this data is collected and maintained in a database. Secondly, to create a database of candidates of respective districts, another functionality is added. This would create a table of candidate data which will be used to load the ballots later. Third, this portal allows the ECI official to start the election, by specifying the candidates and the time duration. This would make use of election creation smart which would intern deploy the Ballots. The Addresses of these deployed ballots are maintained in a separate table for future use. Lastly, the portal makes use of the address stored in the table, to access the ballots to monitor the votes; thereby declaring the winner of the election.

2.Election Interface:

The voting machine interface would first verify the voters' eligibility. For this, the machine would input the voter id and fingerprint signature from the voter. This data is hashed and compared with the voter database for authentication. Eligible voters are given access to the ballot, where the can cast their vote. The interface is simple and provides instructions in several languages. The interaction with the ballot is done by using web3 ipc protocol which would connect to the node on the machine. The web app interacts with the ballot smart contract using web3js and thus sends vote as a transaction.

3. Voter Module:
In this module, voters who have been provided with the personal ETH wallet will import onto the voting portal using the Metamask extension and cast their vote.

COLLECTING INFORMATION

Observation and collecting statistics constitute techniques. Observations spotlight what's needed. On the opposite hand, collecting statistics highlights the techniques had to execute the proposed project. Both observations and the real collecting of statistics need to consist of remarks from the organization that in the end will enjoy the finished project.

A . Objective and Opportunities

Once the employer has analyzed the desires and recognized the objectives, the employer desires to allocate finances to capitalize the project. By efficiently figuring out the desires, an employer can start to allocate sources to pay for the project. Additionally, a commercial enterprise desires to don't forget the capability destiny coins float of the project. This lets the commercial enterprise investigate capability value financial savings to reduce expenses and maximize the performance of the project.

B. Existing System

In India, earlier than 2004 there has been a paper-primarily based totally balloting structure. It is known as the ballot paper system. Electors need to come upon polling sales space & forge their vote via means of marking on seal in the front of the image of an elector for which they want to forge their respective votes on ballot paper. Total results have been introduced via means of calculating the votes. The most voted party will be declared as the winner. India a country has populace extra than one hundred twenty crores the ballot paper balloting isn't a lot reliable, time ingesting and really hard to rely the votes & there also are troubles like substitute of ballot paper bins with identical, harm of ballot paper, stamp marking seal for multiple candidates as a result there's a robust want to triumph over those troubles. In order to triumph over those troubles Electronic Voting Machines Were introduced. Electronic Voting Machine (EVM's) [4] specifically includes components:

1. Control Unit: It shops and assembles votes, utilized by ballot workers.

2. Ballot Unit: It is positioned withinside the election sales space and is used by the voters. Both the devices are related thru 5m cable and one give up of the cable is completely constant to the ballot unit. The manipulated unit has a battery % inside, which motorizes the system. The ballot unit has sixteen candidate buttons and the unused buttons are included with a plastic overlaying tab withinside the unit. An extra ballot unit may be related while there are extra than sixteen candidates. The extra ballot unit may be related to a port on the bottom of the primary ballot unit. EVM's are across the world called DRE's (Direct recording Electronic) EVM's are universally utilized in India for the reason that the overall elections of 2004, while ballots have been absolutely out of trend. They were utilized in all of the meeting polls and preferred elections of 2009. By the use of EVM's, Votes are effectively recorded and there's no trouble in counting, scalability [5], Accuracy, rapid announcement of outcomes and robustness of the system. Main Problem lies in authentication, the individual that is balloting might not be the valid individual. Other troubles like taking pictures of sales space via the means of political parties, casting of votes via the means of underage human beings and fraud balloting might also additionally occur. An individual is supplied with the voter identity identification card as an evidence of identity, issued via way of means of the Indian government. Lot of troubles are visible in voter identity identification playing cards like call misprinting, lack of call, no clean image on image identity identification card, etc.

C. Proposed System

Several research was finished on the usage of pc technology to enhance elections . These researches inform approximately the dangers of adopting digital vote casting devices, due to the software program demanding situations, insider threats, community vulnerabilities, and the demanding situations of auditing. We've proposed to lay out the present online vote casting device that's included with the Blockchain technology. The proposed device has the subsequent benefits in comparison to the present device: • Users' can vote from everywhere withinside the international community till they own a citizenship of the country. • The vote casting is saved withinside the Blockchain which makes it tamper proof. • As there's no status queue for casting votes it's going to take a whole lot of time and decrease the workload.

PRELIMINARY INVESTIGATION

The primary purpose of initial research is to discover the hassle. First, the brand new or improved machine is established. Only after the popularity of want, then the proposed machine is in comparison after which in addition evaluation is feasible. At this stage, we needed to understand the hassle and opportunities. The present machine is studied and observed that there have been few regions wherein we will combine with different generations to make the machine higher than the present machine. It became analyzed that such a proposed machine might be feasible to broaden with given and it'd come to be the viable solution.

In this project, the largest project was to combine the present online vote casting machine with the designed blockchain framework and in addition improvement degrees we encountered numerous unit stage issues which includes the version for the Election Commission to create votes and keep the important info of applicants in conjunction with the election info. In the later part of this document, we've raised the capabilities which may be introduced to our software program to make it higher than the preliminary deployment.

A. Feasibility Study A feasibility observation is a high-degree pill model of the whole machine evaluation and layout process. The observer starts off evolved via a way of classifying the trouble definition. The motive of feasibility observation isn't to clear up the trouble, however to decide whether or not the trouble is really well worth solving. It is an initial observation that's performed earlier than the actual improvement of the mission commences now no longer maintaining the aspect of mission’s success. It creates a roadmap of what are the feasible answers if we pick a sure path.

B. Technical Feasibility Evaluating [8] the technical feasibility look at is the trickiest part of a feasibility look at. This is because, at this time, there are no longer too many precise designs of the device, making it tough to get entry to troubles like performance, expenses (as a consequence of the type of era to be deployed) etc. A quantity of troubles ought to be taken into consideration even as doing a technical analysis. Understanding the one-of-a-kind technology concerned withinside the proposed device earlier than taking off the assignment we ought to be very clean approximately what is the technology which might be required for the improvement of the brand new device. Overall, this look at wishes to illustrate that the proposed device that wants to be advanced is technically feasible. This requires:

- An define of the requirements,
- A viable device design

C. Economic Feasibility The monetary feasibility look at evaluates the value of the software program improvement in opposition to the closing profits or advantages received from the advanced system. There should be scopes for earnings after the successful Completion of the undertaking. The existence cycle of an engineering undertaking or product consists of of numerous stages, namely :

(i) Planning and design;

(ii) Development;

(iii) Operation and maintenance. It must be achieved to discover the monetary danger related to the undertaking. Various strategies like net present value (NPV), pay-back interval, return on investment (ROI) are employed. Techno-Economic Assessment (TEA) is a value-advantage assessment of the usage of distinctive methods. These exams are used for obligations such as:

- Evaluate the monetary feasibility of an undertaking.
- Investigate coins flowing over the life of the undertaking.
- Evaluate the probability of various generation scales and applications.
- Compare the monetary best of various generation utilities imparting the identical service.

D. Operational Feasibility The operational feasibility look at specializes in the diploma to which the proposed improvement undertaking suits in with the present commercial enterprise surroundings and goals in regards to improvement schedule, transport date, company culture, and current commercial enterprise processes. It is likewise the degree of ways properly the answer will be painted withinside the corporation after it's miles deployed. As we're coping with the blockchain balloting system, which in a roundabout way goals the country's or state's election method protocol, there can be a detailed evaluation among those to test which one dominates the other. It is likewise the degree to which human beings will sense the undertaking as in will human beings be conversant in use this in a right manner or it will likely be too complicated to deal with. There are factors of operational feasibility to be considered: • Is the trouble really well worth solving? • How do the quit users (citizens in this case) and management (Election Commission) sense this case?

E. Schedule Feasibility It way that the challenge may be carried out in a suitable time frame. When assessing time table feasibility, a structures analyst have to do not forget the interplay among time and costs. For example, rushing up a challenge time table may make a challenge feasible, however a great deal greater expensive. Other troubles that relate to time table feasibility encompass the following: • Can the business enterprise manage the elements that have an effect on time table feasibility? • Has control mounted an organization timetable for the challenge? • What situations have to be glad all through the improvement of the system? • Will an extended time table pose any dangers? If so, are the dangers acceptable?\ • Will challenge control strategies be to be had to coordinate and manage the challenge? • Will a challenge supervisor be appointed? It is likewise the chance that timeframes may be met and that that is good enough to meet organization’s needs.

F. Legal Feasibility It determines whether or not the proposed gadget conflicts with the felony necessities, in this situation as we didn’t attempt to execute something on the general public domain, consequently this task is felony feasible. It is critical that the task is following the necessities to begin a task which include certificates, copyrights, enterprise insurance, tax number, fitness and protection measures and lots of more. There are a few matters to bear in mind in felony feasibility have a look at which include moral problems and a few social problems. These problems are privateness and accountability. In this task, the whole lot is designed retaining in thoughts all of the felony phrases and no real-international facts or privateness has been breached of any character of this to apply it as a pattern voter to put in force this application.

SOFTWARE REQUIREMENTS

Project Planning is the most essential thing in developing a project. It sets out the phases, activities and tasks needed to deliver a project. The timeframes required to deliver the project, along with the resources and milestones are also shown on the project plan. Initially, the project scope is defined and the appropriate methods for completing the project are determined. Following this step, the durations for the various tasks necessary to complete the work are listed and grouped into a work breakdown structure.

Project planning is often used to organize different areas of a project, including project plans, workloads and the management of teams and individuals. The logical dependencies between tasks are defined using an activity network diagram that enables identification of the critical path. Project planning is inherently uncertain as it must be done before the project is actually started.

Therefore, the duration of the tasks is often estimated through a weighted average of optimistic, normal, and pessimistic cases. The critical chain method adds “buffers”; in the planning to anticipate potential delays in project execution. Float or slack time in the schedule can be calculated using project management software.

Then the necessary resources can be estimated and costs for each activity can be allocated to each resource, giving the total project cost. At this stage, the project schedule may be optimized to achieve the appropriate balance between resource usage and project duration to comply with the project objectives. Once established and agreed, the project schedule becomes what is known as the baseline schedule. Progress will be measured against the baseline schedule throughout the life of the project. Analyzing progress compared to the baseline schedule is known as earned value management.

A project plan is a model of the process that the project team intends to follow to realize the project objectives. It brings together a number of important aspects of this process including its scope, timing and associated risks. The project plan can be viewed as a type of “contract” between the project team members and the reviewers. It defines the process by which objectives will be achieved, and the responsibilities in carrying out this process. It also underpins a number of other key project management functions including estimating and forecasting, options analysis and decision-making, and performance monitoring and control.

The essential elements of a project plan are:

- Scope statement
- Schedule

- Requirements
- Quality criteria
- Project resources
- Communications Plan

Software Requirement Specification

Introduction: This document describes the structural properties and software requirements of the Online Election System using Blockchain Technology.

Problem Definition: Manual voting system has been deployed for many years in our country. However, in many parts of our country people cannot attend the voting because of several reasons. To illustrate, sometimes people may not be in their own registration region and due to this fact, they cannot fulfill their voting duties. In order to solve these problems, there is a need of online election voting system with this keeping in mind that EVM votes tampering issues are also encountered, so this online election system will be integrated with Blockchain Technology to make it tamper proof.

Purpose: The purpose of this document is to make the functional and non-functional requirements of the Online Election System using Blockchain Technology easy to comprehend. It also serves the purpose of making the functionality clear to end users.

Scope: This SRS document applies to the initial version (release 1.0) of the "Online Election System using Blockchain Technology" software package. This document describes the modeling and the requirement analysis of the system. The main aim of the system is to provide a set of protocols that allow voters to cast votes while the election commission is responsible for creating elections and adding candidates.

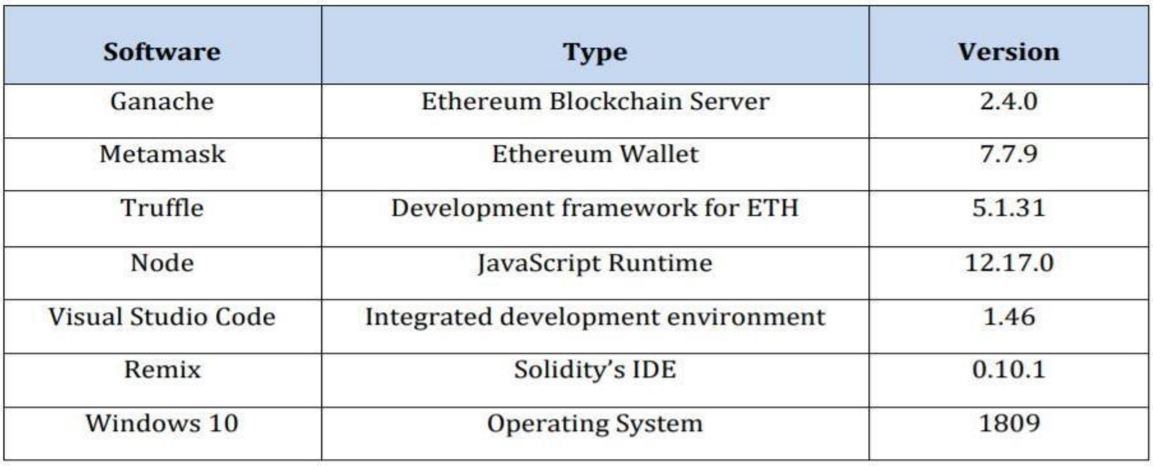
Definitions and Abbreviations: The following is a list of terms, acronyms and abbreviations used by the Online Election System using Blockchain software package and related documentation.

For the proper working of the system we can list our assumptions and dependencies as follows:

- Metamask Browser Extension: Metamask allows users to manage accounts and their keys in a variety of ways, including hardware wallets, while isolating them from the site context.

- Ganache: It is a personal blockchain for rapid Ethereum and Corda distributed application development.

- Truffle: A world class development environment, testing framework and asset pipeline for blockchains using the Ethereum Virtual Machine (EVM), aiming to make life as a developer easier.
- NodeJS: It is a JavaScript runtime built on Chrome's V8 JavaScript engine.



Software	Type	Version
Ganache	Ethereum Blockchain Server	2.4.0
Metamask	Ethereum Wallet	7.7.9
Truffle	Development framework for ETH	5.1.31
Node	JavaScript Runtime	12.17.0
Visual Studio Code	Integrated development environment	1.46
Remix	Solidity's IDE	0.10.1
Windows 10	Operating System	1809

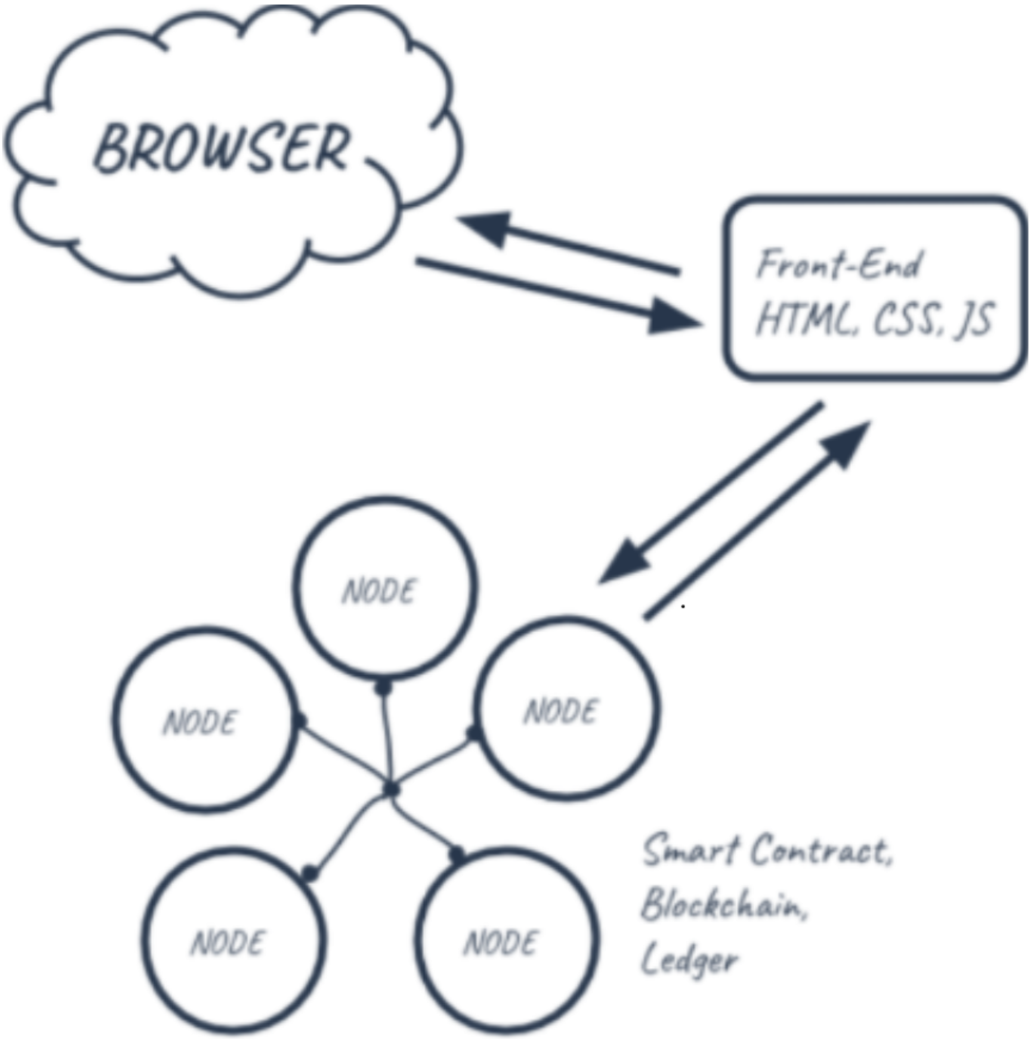
Overview: The remainder of this document identifies the actors, use-cases, use-case scenarios, activity diagrams, assumptions and dependencies needed for the analysis and design of the Online Election software package. The rest of the document contains the overall description of the system, requirements, data model and behavioral description of the system and project planning.

Overall Description: The Online Election System is a web-based system so fundamental features related with web-based technologies such as client-server and database properties determine the software requirements of that project along with the addition of a blockchain framework.

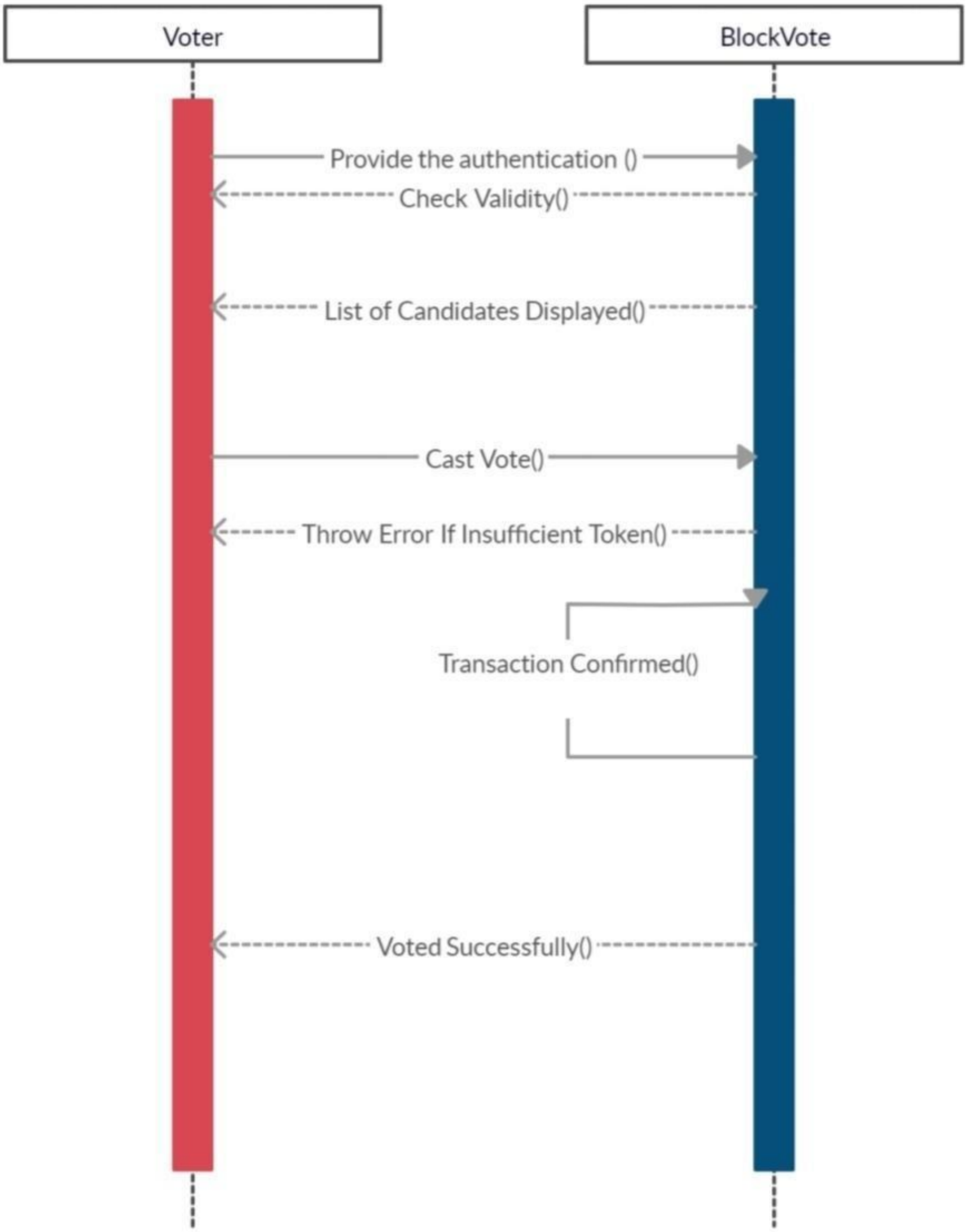
Product Perspective: The software product is a standalone system and not a part of a larger system. The system will be made up of two parts. One will be used for general purposes by the EC, such as viewing candidates, registered parties and past years' election results. The voters will reach the system connected to another module through web pages by using web-browsers such as Mozilla, Internet Explorer and Google Chrome. On the election day, the voter needs to import his/her Ethereum's wallet and get authenticated accordingly. The voters cast their votes using the interface that is provided. These votes are accepted by the blockchain and then thrown into the server. The EC configures the whole system according to its needs on the server

DATA MODELS

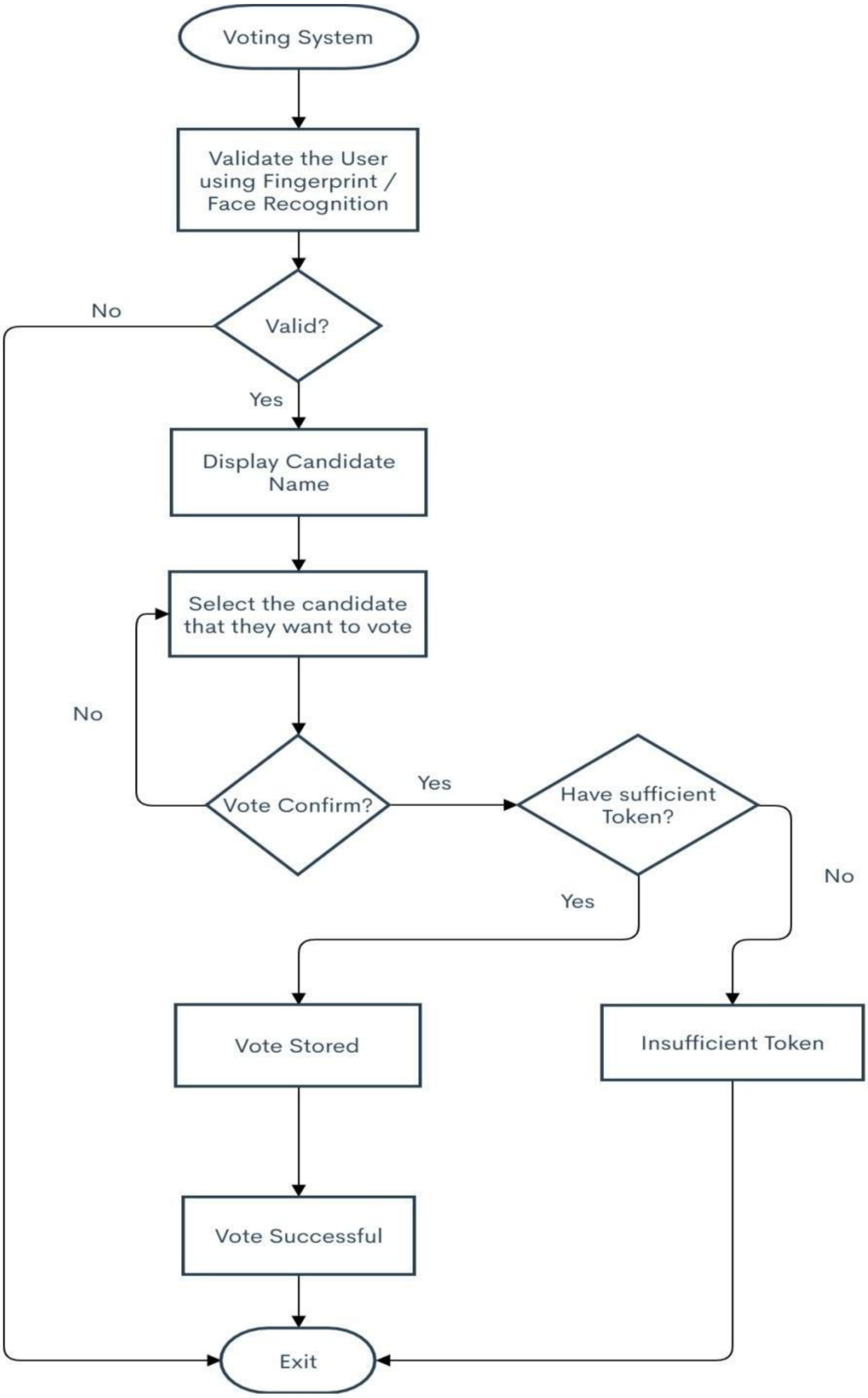
Flow Representation:



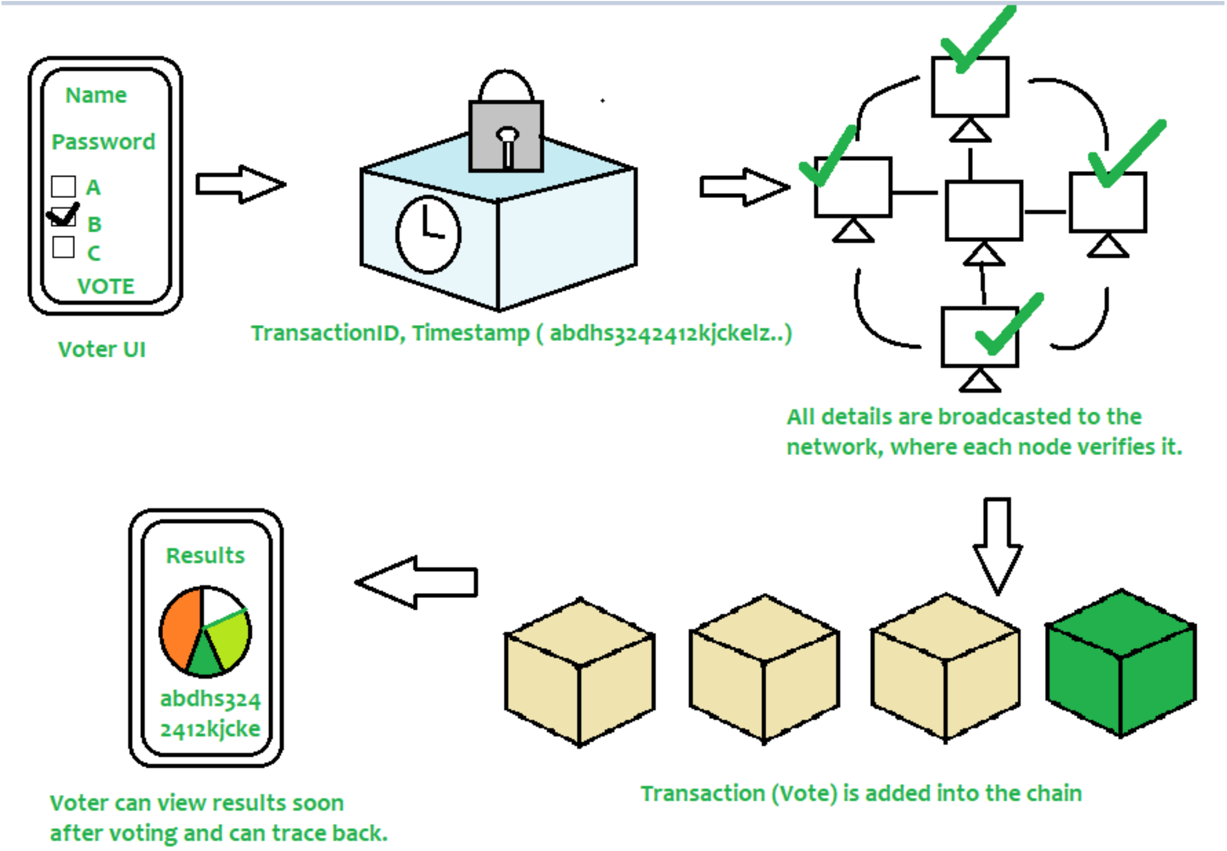
SEQUENCE DIAGRAM:


Voter
BlockVote
Provide the authentication ()
Check Validity()
List of Candidates Displayed()
Cast Vote()
Throw Error If Insufficient Token()
Transaction Confirmed()
Voted Successfully()

FLOW CHART DIAGRAM:



WORKING FLOW DIAGRAM


Name
Password
□ A
☑ B
□ C
VOTE
Voter UI
TransactionID, Timestamp (abdhs3242412kjckelz..)
All details are broadcasted to the network, where each node verifies it.
Results
abdhs324 2412kjcke
Voter can view results soon after voting and can trace back.
Transaction (Vote) is added into the chain

According to the diagram above, the voter needs to enter his or her details in order to vote. All data is then encrypted and saved as per operation. The work is then broadcast to all nodes in the network, which are then verified. When the network allows action, it is kept in the block and added to the chain. Note that once a block is added to the chain, it stays there permanently and cannot be updated. Users can now see results and track activity if they want.

Since the current voting system does not meet the security requirements of the current generation, there is a need to build a system that uses the security, comfort, and trust involved in the voting process. Voting systems therefore use Blockchain technology to add an extra layer of security and encourage people to vote anytime, anywhere without a problem and make the voting process more economical and time-saving.

PROBLEMS AND SOLUTIONS OF DEVELOPING ONLINE VOTING SYSTEM

Whether talking about traditional paper-based voting, voting via digital voting machines,
or an online voting system, several conditions need to be satisfied:

- Eligibility: Only legitimate voters should be able to take part in voting
- Reusability: Each voter can vote only once
- Privacy: No one except the voter can obtain information about the voter's choice
- Fairness: No one can obtain intermediate voting results
- Soundness: Invalid ballots should be detected and not taken into account during Tallying.
- Completeness: All valid ballots should be tallied correctly.

Below is a brief overview of the solutions to satisfy these properties online voting systems.

Eligibility:

The solution to the issue of eligibility is obvious. To participate online
To vote, voters must identify themselves using a known identification system. I the identities of all legitimate voters need to be added to the list of participants. But there
Threats: First, all changes made to the participation list need to be evaluated that no illegal voters can be added, and secondly, the screening process should be both reliable and secure so that the voter's account can not be stolen or misused. Creating such a system of identification is a complex task in itself . However, because this type of system is required for a variety of other situations, especially related ones digital government services, researchers believe it is best to use existing diagnostics systems, and the question of creating one is beyond the scope of the task.

Reusability:

At first glance, the use of non-invasion may seem straightforward — when the voter their vote, all that must be done is to mark the list of participants and not let them vote a second time. But privacy needs to be considered; so, providing both redundancy and voter anonymity is complex. In addition, it may be necessary to allow the voter to vote again, making the task even more difficult. A brief overview non-reusable strategies will be provided below in accordance with the framework to use privacy.

Privacy:

Privacy in the context of online voting means that no one knows except the voter how the participant voted. The achievement of this structure depends largely on one (or more) of the following techniques: blind signatures, homomorphic encryption, and mix-networks.
A blind signature is a way to sign data when the signatory does not know what it is they sign. It is accomplished by using the blinding function for blinding and signing functions vary – Blind (Sign) = Sign (Blind (message)). Requester blinds (blinding function) message and sends it to be signed. After receiving the signature of the blind message, they use their knowledge to blind the boundaries in order to get the signature of the blinded message. Blind signatures block mathematically anyone other than the applicant in linking the blind message and the corresponding signature mix with the blind.
The voting system proposed by Fujioka, Okamoto, and Ohta in 1992 uses a blind man signature: The eligible voter closes his or her vote and sends it to the guarantor. Confirmation ensures that the voter is allowed to participate, sign the blind vote, and return it to the voter. The voter then receives an open ballot signature and sends it to tall, and tall confirms the signature of the author before accepting the vote.Many online voting agreements have emerged from this

program, which improves usability (in the first case, the voter had to wait until the end of the election and send a vote key encryption key), which allows for re-voting, or the use of coercion resistance. The biggest threat here is the signature strength: There must be a verified log for all signed signatures;
This information is reasonably consistent with the voter's acceptance of the vote, so it should ensure that only eligible voters receive signatures from the signatory. It should too it should be ensured that voter accounts are not allowed to vote but did not participate voting is not used by a criminal. To really break the link between the voter and the voter, The vote and signature must be posted on an anonymous channel.

Fairness:
Justice about no one getting the middle results is directly achieved:
Voters cast their ballots before submitting, and those options are excluded from the text at the end of the voting process. The important thing to remember here is that if a person has a key to remove encryption by accessing encrypted resolutions, they can get intermediate results.
This problem is solved by distributing the key among a few key holders.
System when all the key holders are needed to remove the encryption encryption — if one of the top executives does not participate, encryption can not be performed. Therefore, threshold schemes are used where a certain number of senior executives are required to perform encryption.
There are two main ways to distribute a key: confidential sharing, where the person is trusted the vendor divides the generated key into parts and distributes it among senior executives (e.g.,Shamir's privacy sharing protocol); and spread the key generation, when there is no reliable seller is required, and all stakeholders contribute to key accounting (for example, Pedersen's
Distributed Key Generation Distributed).

Soundness and Completeness
On its surface, the perfection and sound of the buildings seems straightforward, but self-awareness can be a problem depending on the protocol. If votes are available decrypted one by one, it is easy to distinguish between the permissible and the non-permissible, but objects become more difficult when it comes to homomorphic encryption. As one vote is
No encryption has ever been removed, the effect of encryption will not be displayed if more than one option is selected
or if a vote is constituted to be considered as ten (or million) elections at a time.
So,we need to verify that encrypted data meets the external valid balloon features to interfere with any information that may be helpful in determining how a vote is cast. This work is resolved by unconventional evidence . By definition, this is a way of hiding words confirming a statement about the value without disclosing the value itself. Specifically, general evidence indicates that a certain number belongs to a particular set in such cases.

SYSTEM DESIGN

Design Goals: Design goals are important properties of the system to be optimized, and which may affect the overall design of the system. There is a fine line between system design and requirements. Requirements include specific values that must be met in order for the product to be acceptable to the client, whereas design goals are properties that the designers strive to make "as good as possible", without specific criteria for acceptability.

System Design:
At a very high level, a simple voting system comprises an organizing authority, a voting machine and a vote. In the case of our system, we add an ethereum based blockchain, which establishes the network between the three mentioned entities.

Main concern of the system:
Who-
Any user that requires a democratic voting/polling system.

What-
A decentralized voting system to ensure a fair voting process is followed i.e., no vote tampering occurs by using a blockchain mechanism to validate the votes and log the voters' picks.

Wow Factor-
Assuring that the vote cast remains influence free and untampered so as to preserve the integrity of the process.

Ultimately our project converges to a Decentralised Web application(). The components of this application are:
Smart Contracts
Front-end Software for Election Commision (ECI) and for Voting Machine
Voter Authentication Service

A. Identification of want:
Identification of want is a technique of figuring out what and the way an end-consumer could assume a product to carry out after the deployment at manufacturing level. There's additionally non- technical desires of an end-consumer or a commercial enterprise customer which displays the users' belief of the product and now no longer the real technical workaround, however they're intently associated with the technical want at times. By enforcing a want identity system, the agency is able to ensure the right allocation of belongings to special challenges in the agency.

B. Identification of problem:
Identifying ability issues earlier than the begin of a mission can keep the corporation considerable quantities of time and money. Problem evaluation is one

of the maximum essential tiers of mission making plans due to the fact this level facilitates to manual all next evaluation and decision-making. If the mission does now no longer strengthen beyond this level with answers that the corporation can implement, the mission needs to now no longer cross ahead in its cutting-edge form.

C. Observation:

The wishes for a venture are diagnosed after the agency makes observations about the venture. Observations are frequently subjective and consequently a person with information approximately the proposed venture must assist to make observations. A suitable observer can discover the wishes of the venture through answering key questions on the venture. If the observations think about the venture itself and the final results of the venture, the observations must meet all the wishes of the venture.

Modularization Details: The project has been divided into many modules in which for every functionality we have designated modules. Any software comprises many systems which contain several sub-systems and those sub-systems further contain their sub-systems. So, designing a complete system in one go consisting of each and every required functionality is a hectic work and the process can have many errors because of its vast size.

Effective modular design can be achieved if the partitioned modules are separately solvable, modifiable as well as compilable.

Following are the project modules:

(i) Election Commission: In this module, an entity named Election Commission will be responsible to set up the smart contract and register candidates, parties and start off an election.

(ii) Election Test: This is the module to test our smart contract where we use Mocha Framework to perform unit tests on our application.

(iii) Voter Module: In this module, voters who have been provided with the personal ETH wallet will import onto the voting portal using the Metamask extension and cast their vote.

Implementations: The tiers given below alludes to different levels or layers where activities occur.

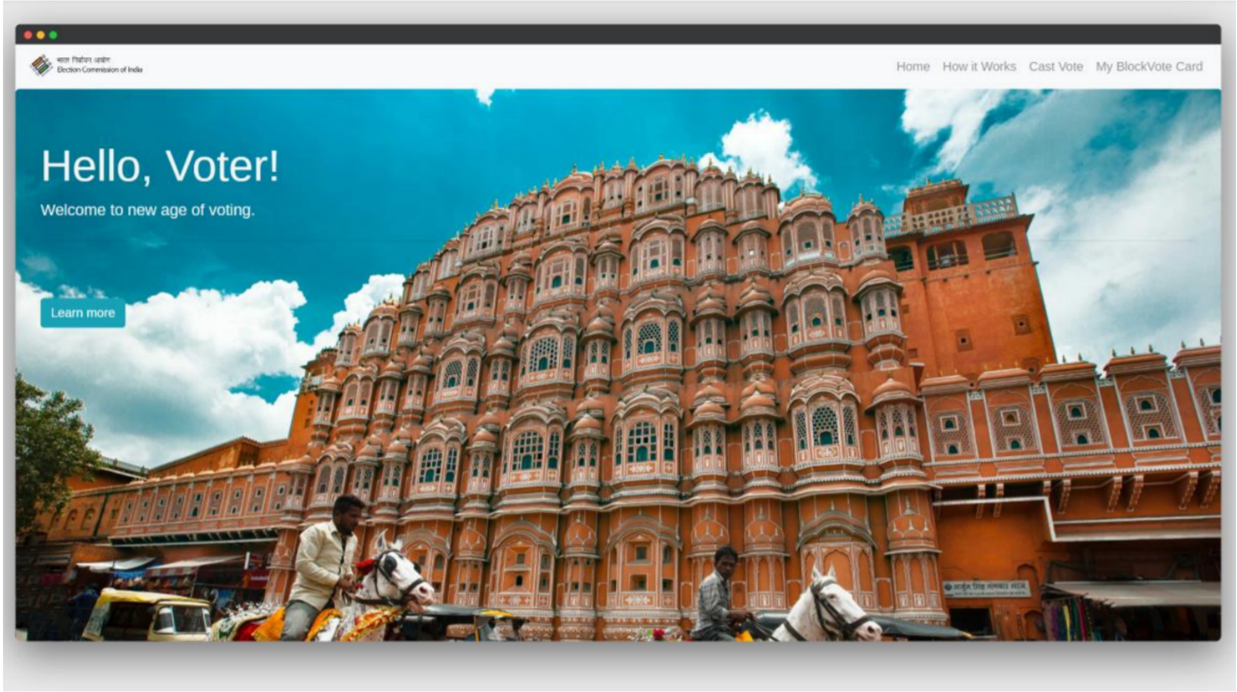
Client: Client is any user or program that wants to perform an operation over the system. Clients interact with the system through a presentation layer.

Presentation Layer: This layer is responsible for the presentation of data at the client side, i.e., it provides an interface for the end-user into the application to cast the votes.

Resource manager: The resource manager deals with the organization (storage, indexing and retrieval) of the data necessary to support the application logic. This resource manager here is the Local Blockchain server maintained by Ganache.

Application logic: The application logic figures out what the system actually does. It takes care of implementing the business rules and establishing the business processes. Blockchain voting system is designed and implemented according to the three tier architecture.

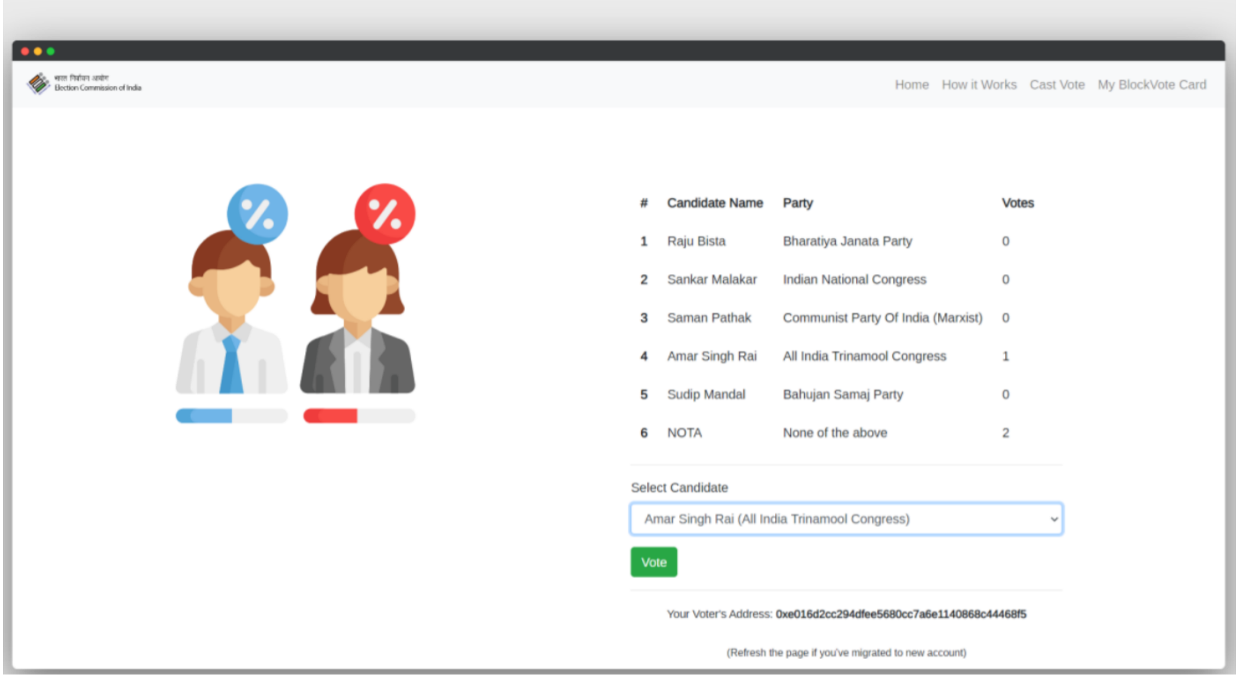
User Interface Design



Hello, Voter!

Welcome to new age of voting.

Homepage



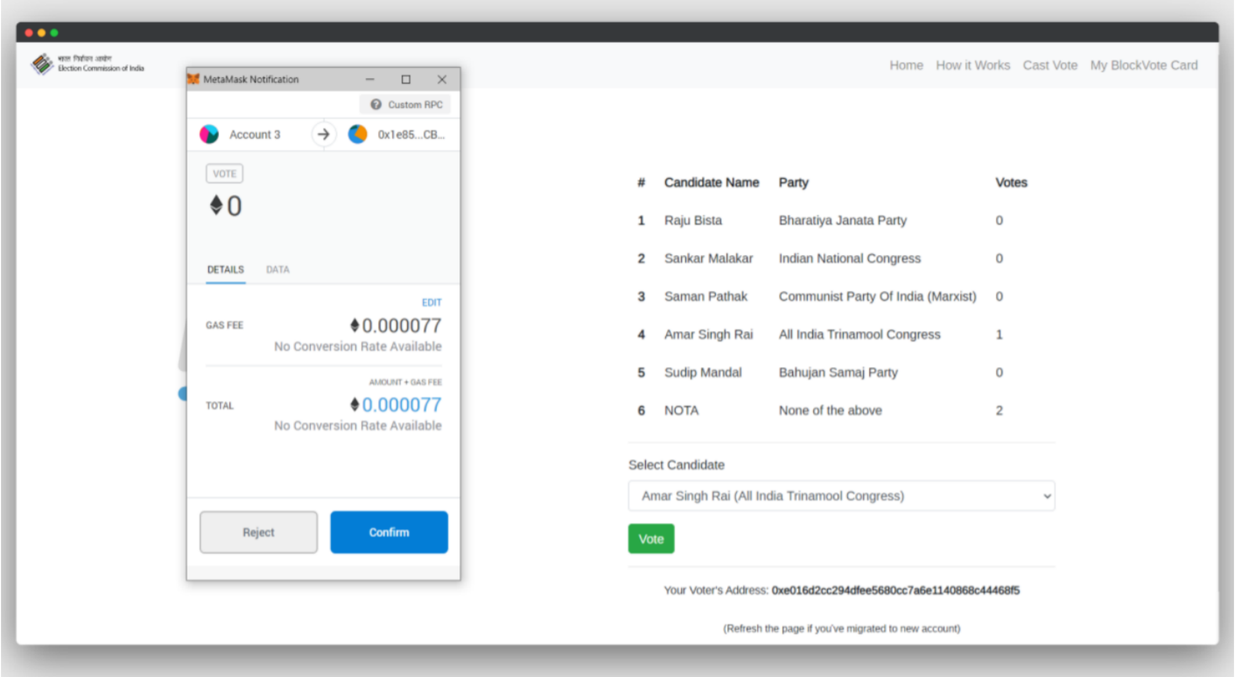
#	Candidate Name	Party	Votes
1	Raju Bista	Bharatiya Janata Party	0
2	Sankar Malakar	Indian National Congress	0
3	Saman Pathak	Communist Party Of India (Marxist)	0
4	Amar Singh Rai	All India Trinamool Congress	1
5	Sudip Mandal	Bahujan Samaj Party	0
6	NOTA	None of the above	2

Select Candidate: Amar Singh Rai (All India Trinamool Congress)

Your Voter's Address: 0xe016d2cc294dfee5680cc7a6e1140868c44468f5

(Refresh the page if you've migrated to new account)

Casting the Vote



0

GAS FEE 0.000077
No Conversion Rate Available

AMOUNT + GAS FEE
TOTAL 0.000077
No Conversion Rate Available

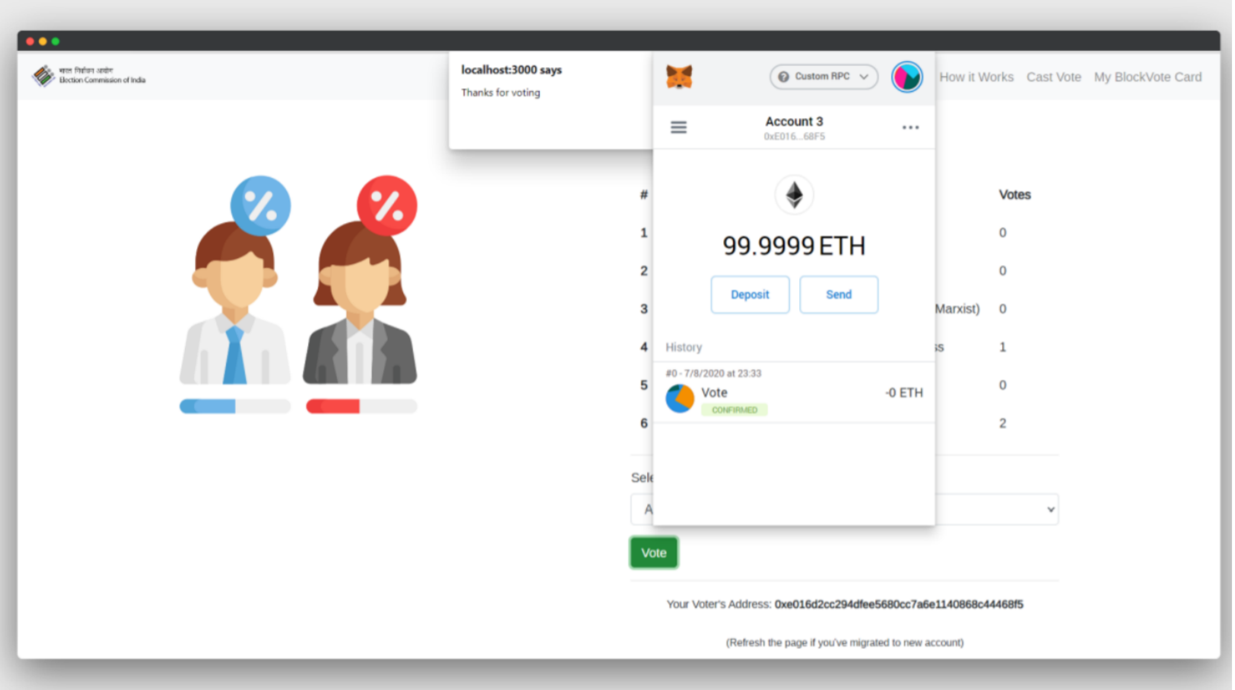
#	Candidate Name	Party	Votes
1	Raju Bista	Bharatiya Janata Party	0
2	Sankar Malakar	Indian National Congress	0
3	Saman Pathak	Communist Party Of India (Marxist)	0
4	Amar Singh Rai	All India Trinamool Congress	1
5	Sudip Mandal	Bahujan Samaj Party	0
6	NOTA	None of the above	2

Select Candidate: Amar Singh Rai (All India Trinamool Congress)

Your Voter's Address: 0xe016d2cc294dfee5680cc7a6e1140868c44468f5

(Refresh the page if you've migrated to new account)

Confirming the transaction to cast vote



localhost:3000 says

Thanks for voting

Account 3

0xE016...68F5

99.9999 ETH

Deposit Send

History

#0 - 7/8/2020 at 23:33

Vote -0 ETH

CONFIRMED

#		Votes
1		0
2		0
3	Marxist)	0
4	s	1
5		0
6		2

Sele

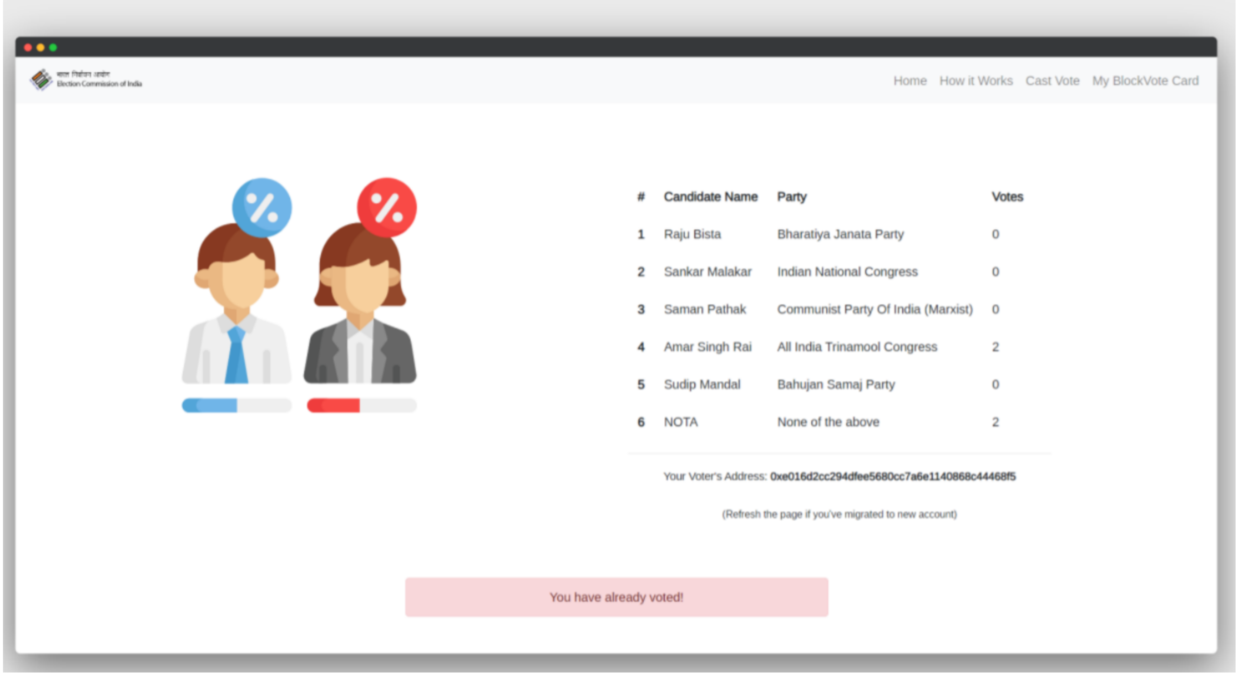
A

Vote

Your Voter's Address: 0xe016d2cc294dfee5680cc7a6e1140868c44468f5

(Refresh the page if you've migrated to new account)

Transaction confirmed by miners



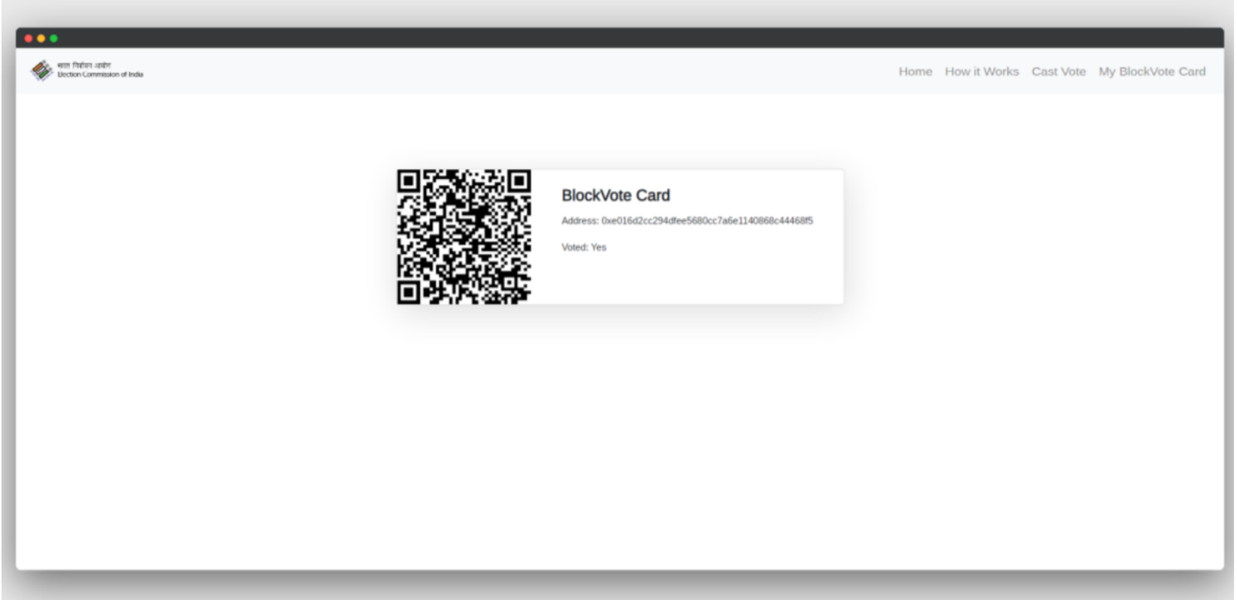
#	Candidate Name	Party	Votes
1	Raju Bista	Bharatiya Janata Party	0
2	Sankar Malakar	Indian National Congress	0
3	Saman Pathak	Communist Party Of India (Marxist)	0
4	Amar Singh Rai	All India Trinamool Congress	2
5	Sudip Mandal	Bahujan Samaj Party	0
6	NOTA	None of the above	2

Your Voter's Address: 0xe016d2cc294dfee5680cc7a6e1140868c44468f5

(Refresh the page if you've migrated to new account)

You have already voted!

Already Voted Prompt

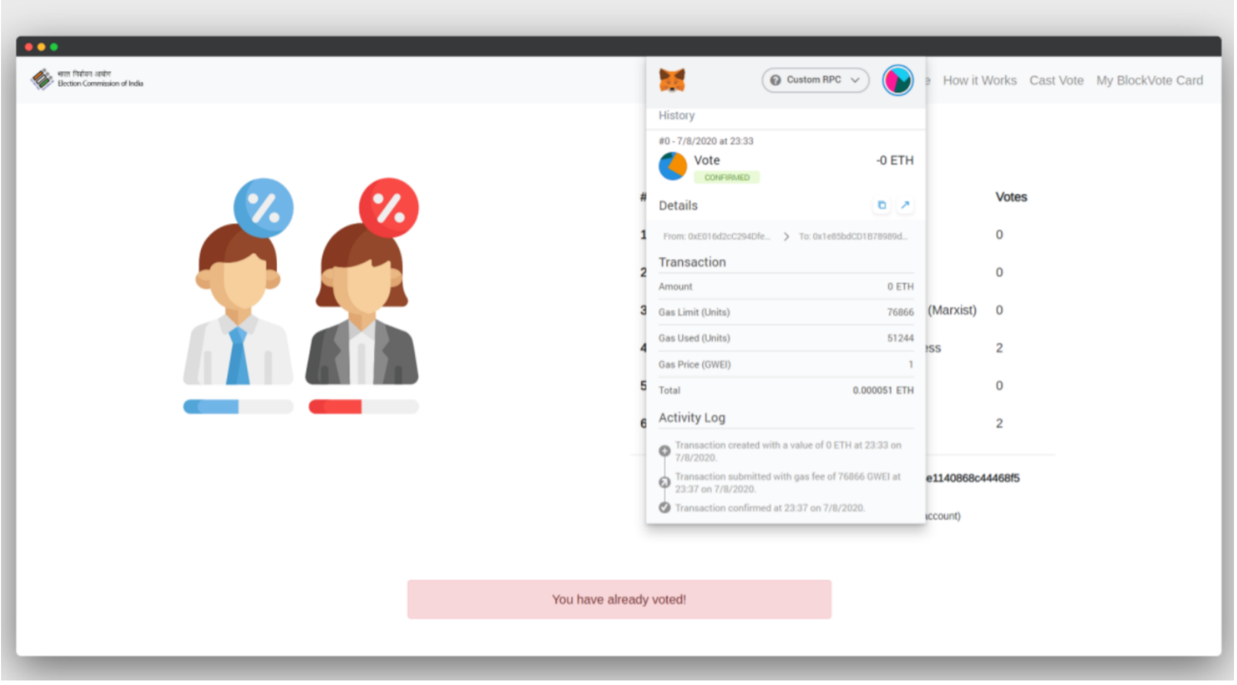


BlockVote Card

Address: 0xe016d2cc294dfee5680cc7a6e1140868c44468f5

Voted: Yes

Customized BlockVote Card



History

#0 - 7/8/2020 at 23:33

Vote -0 ETH

CONFIRMED

Details

From: 0xE016d2cC294Dfe... > To: 0x1e85bdCD1B78989d...

Transaction

Amount	0 ETH
Gas Limit (Units)	76866
Gas Used (Units)	51244
Gas Price (GWEI)	1
Total	0.000051 ETH

Activity Log

Transaction created with a value of 0 ETH at 23:33 on 7/8/2020.

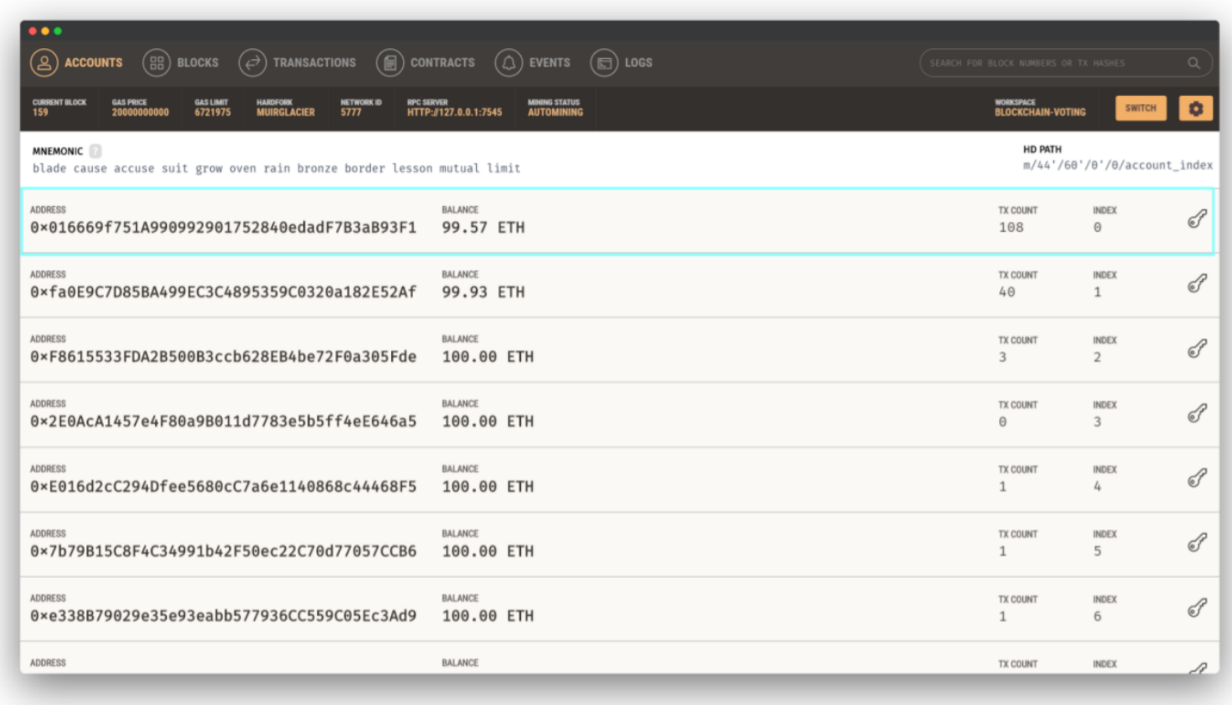
Transaction submitted with gas fee of 76866 GWEI at 23:37 on 7/8/2020.

Transaction confirmed at 23:37 on 7/8/2020.

You have already voted!

Transaction Confirmed Log

The user interface of the application is already discussed under the System Design. Let us have a look at the back-end blockchain server.



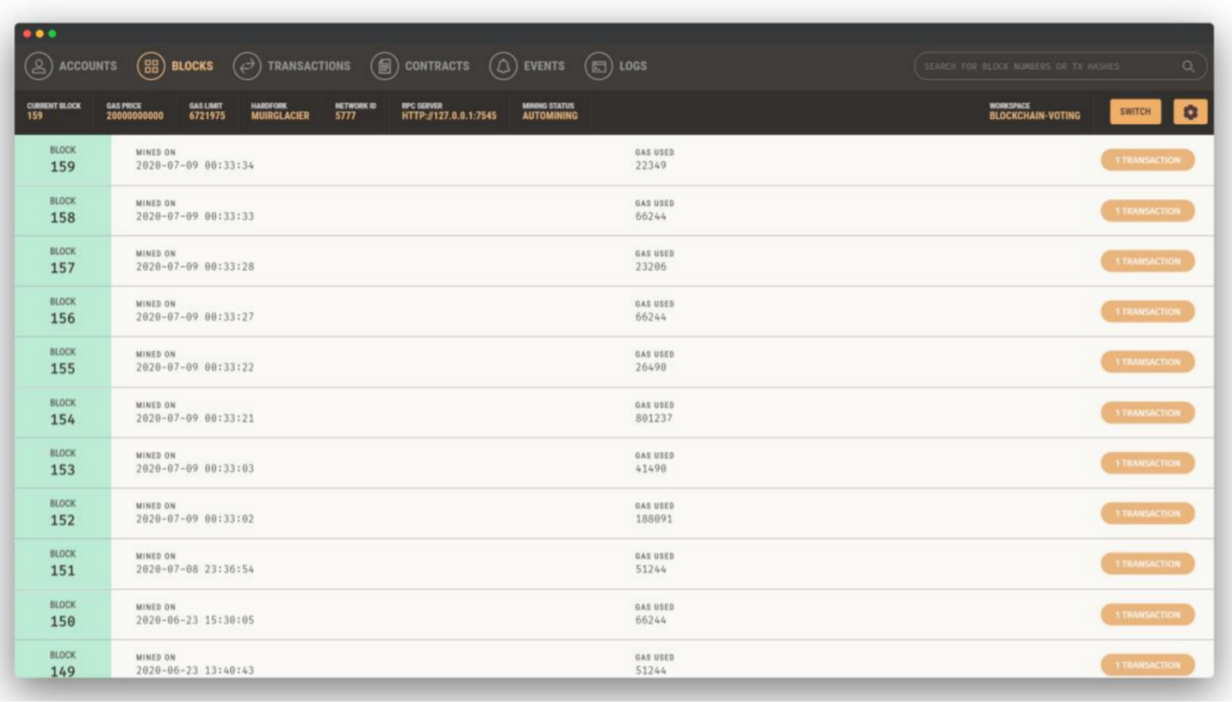
CURRENT BLOCK	GAS PRICE	GAS LIMIT	HARDFORK	NETWORK ID	RPC SERVER	MINING STATUS	WORKSPACE
159	20000000000	6721975	MUIRGLACIER	5777	HTTP://127.0.0.1:7545	AUTOMINING	BLOCKCHAIN-VOTING

MNEMONIC
blade cause accuse suit grow oven rain bronze border lesson mutual limit

HD PATH
m/44'/60'/0'/0/account_index

ADDRESS	BALANCE	TX COUNT	INDEX
0×016669f751A990992901752840edadF7B3aB93F1	99.57 ETH	108	0
0×fa0E9C7D85BA499EC3C4895359C0320a182E52Af	99.93 ETH	40	1
0×F8615533FDA2B500B3ccb628EB4be72F0a305Fde	100.00 ETH	3	2
0×2E0AcA1457e4F80a9B011d7783e5b5ff4eE646a5	100.00 ETH	0	3
0×E016d2cC294Dfee5680cC7a6e1140868c44468F5	100.00 ETH	1	4
0×7b79B15C8F4C34991b42F50ec22C70d77057CCB6	100.00 ETH	1	5
0×e338B79029e35e93eabb577936CC559C05Ec3Ad9	100.00 ETH	1	6

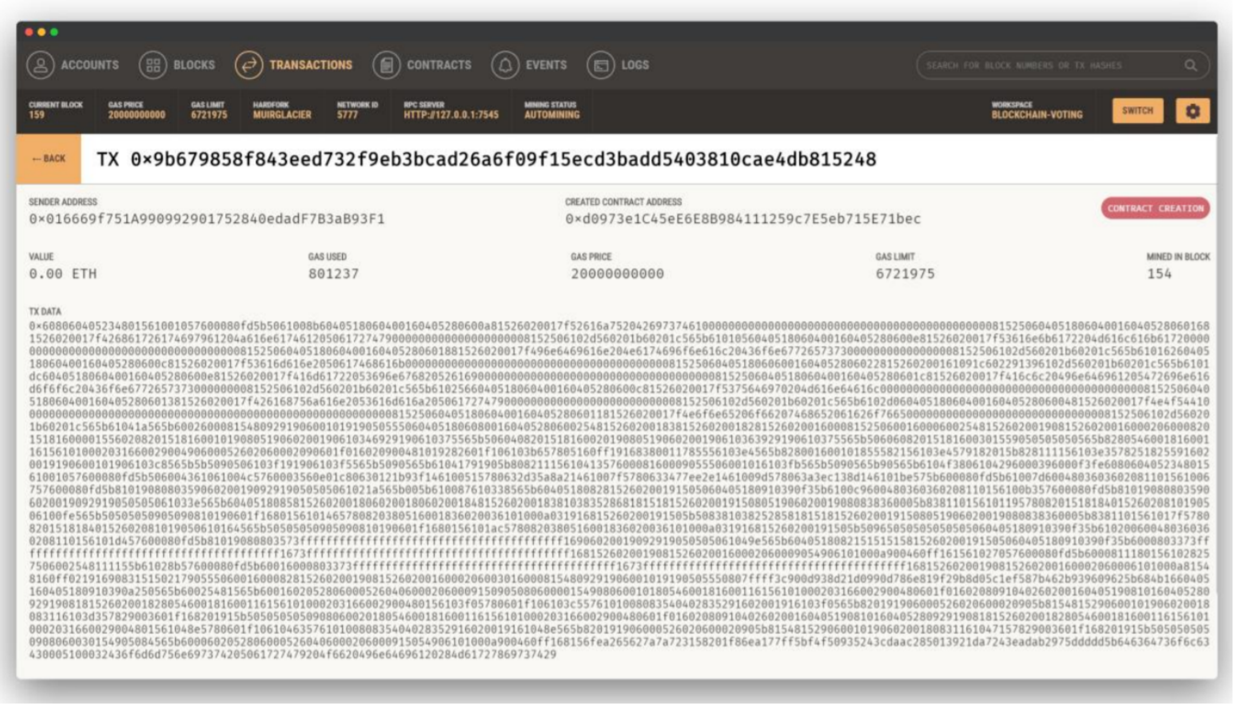
Smart Contract Owner Account



CURRENT BLOCK	GAS PRICE	GAS LIMIT	HARDFORK	NETWORK ID	RPC SERVER	MINING STATUS	WORKSPACE
159	20000000000	6721975	MUIRGLACIER	5777	HTTP://127.0.0.1:7545	AUTOMINING	BLOCKCHAIN-VOTING

BLOCK	MINED ON	GAS USED	
159	2020-07-09 00:33:34	22349	1 TRANSACTION
158	2020-07-09 00:33:33	66244	1 TRANSACTION
157	2020-07-09 00:33:28	23206	1 TRANSACTION
156	2020-07-09 00:33:27	66244	1 TRANSACTION
155	2020-07-09 00:33:22	26490	1 TRANSACTION
154	2020-07-09 00:33:21	801237	1 TRANSACTION
153	2020-07-09 00:33:03	41490	1 TRANSACTION
152	2020-07-09 00:33:02	188091	1 TRANSACTION
151	2020-07-08 23:36:54	51244	1 TRANSACTION
150	2020-06-23 15:30:05	66244	1 TRANSACTION
149	2020-06-23 13:40:43	51244	1 TRANSACTION

Blocks Mined after Transactions



CURRENT BLOCK 159 | GAS PRICE 20000000000 | GAS LIMIT 6721975 | HARDFORK MUIRGLACIER | NETWORK ID 5777 | RPC SERVER HTTP://127.0.0.1:7545 | MINING STATUS AUTOMINING | WORKSPACE BLOCKCHAIN-VOTING

TX 0×9b679858f843eed732f9eb3bcad26a6f09f15ecd3badd5403810cae4db815248

SENDER ADDRESS
0×016669f751A990992901752840edadF7B3aB93F1

CREATED CONTRACT ADDRESS
0×d0973e1C45eE6E8B984111259c7E5eb715E71bec

VALUE
0.00 ETH

GAS USED
801237

GAS PRICE
20000000000

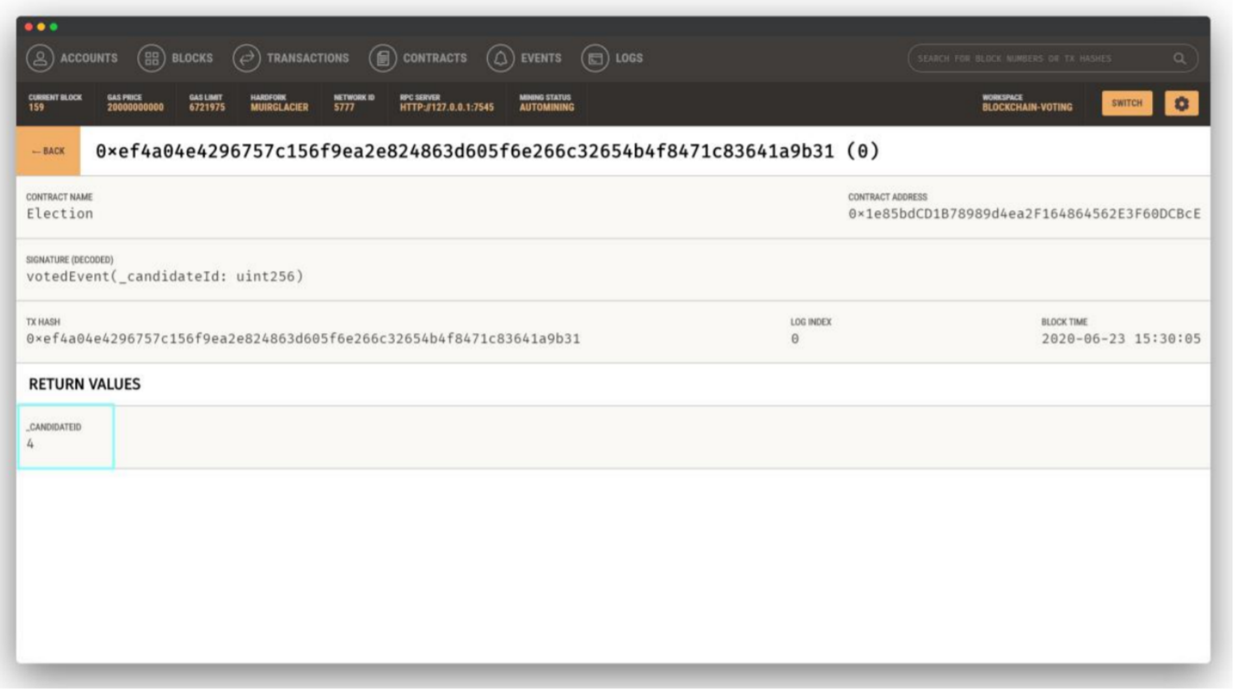
GAS LIMIT
6721975

MINED IN BLOCK
154

TX DATA

```
0×6080604052348015610010576000080fd5b5061008b6040518060400160405280600a81526020017f52616a752042697374610000000000000000000000000000000000000000000008152506040518060400160405280601681
1526020017f426861726174697961204a616e61746120506172747900000000000000000000008152506102d560201b60201c565b6101056040518060400160405280600e81526020017f53616e6b6172204d616c616b61720000
000000000000000000000000000000008152506040518060400160405280601881526020017f496e6469616e204e6174696f6e616c20436f6e677265737300000000000000008152506102d560201b60201c565b61016260405
18060400160405280600c81526020017f53616d616e2050617468616b00000000000000000000000000000000000000008152506040518060600160405280602281526020016109 1c602291396102d560201b60201c565b6101
dc6040518060400160405280600e81526020017f416d61722053696e67682052616900000000000000000000000000000000000008152506040518060400160405280601c81526020017f416c6c20496e646961205472696e616
d6f6f6c20436f6e6772657373000000008152506102d560201b60201c565b6102566040518060400160405280600c81526020017f5375646970204d616e64616c00000000000000000000000000000000000000008152506040
518060400160405280601381526020017f426168756a616e2053616d616a2050617274790000000000000000000000000008152506102d560201b60201c565b6102d06040518060400160405280600481526020017f4e4f54410
00000000000000000000000000000000000000000000000000000008152506040518060400160405280601181526020017f4e6f6e65206f66207468652061626f76650000000000000000000000000000008152506102d56020
1b60201c565b61041a565b6002600081548092919060010191905055506040518060800160405280600254815260200183815260200182815260200160008152506001600060025481526020019081526020016000206000820
151816000015560208201518160010190805190602001906103469291906103755 65b506040820151816002019080519060200190610363929190610375565b50606082015181600301559050505050565b8280546001816001
16156101000203166002900490600052602060002090601f016020900481019282601f106103b657805160ff19168380011785556103e4565b828001600101855582156103e4579182015b828111156103e3578251825591602
0019190600101906103c8565b5b5090506103f191906103f5565b5090565b61041791905b808211156104135760008160009055506001016103fb565b5090565b90565b6104f3806104296000396000f3fe6080604052348015
61001057600080fd5b506004361061004c5760003560e01c80630121b93f146100515780632d35a8a21461007f5780633477ee2e1461009d578063a3ec138d146101be575b600080fd5b61007d6004803603602081101561006
757600080fd5b810190808035906020019092919050505061021a565b005b610087610338565b6040518082815260200191505060405180910390f35b6100c9600480360360208110156100b357600080fd5b81019080803590
6020019092919050505061033e565b604051808581526020018060200180602001848152602001838103835286818151815260200191508051906020019080838360005b8381101561011957808201518184015260208101905
06100fe565b50505050905090810190601f1680156101465780820380516001836020036101000a031916815260200191505b50838103825285818151815260200191508051906020019080838360005b8381101561017f5780
82015181840152602081019050610164565b50505050905090810190601f1680156101ac5780820380516001836020036101000a031916815260200191505b509650505050505050604051809103 90f35b61020060048036036
0208110156101d457600080fd5b81019080803573ffffffffffffffffffffffffffffffffffffffff169060200190929190505050610 49e565b6040518082151515158152602001915050604051809103 90f35b6000803373ff
ffffffffffffffffffffffffffffffffffffff1673ffffffffffffffffffffffffffffffffffffffff16815260200190815260200160002060009054906101000a900460ff161561027057600080fd5b6000811180156102825
7506002548111155b61028b57600080fd5b60016000803373ffffffffffffffffffffffffffffffffffffffff1673ffffffffffffffffffffffffffffffffffffffff16815260200190815260200160002060006101000a8154
8160ff02191690831515021790555060016000828152602001908152602001600020600301600081548092919060010191905055508 07ffff3c900d938d21d0990d786e819f29b8d05c1ef587b462b939609625b684b1660405
160405180910390a250565b60025481565b6001602052806000526040600020600091509050806000015490806001018054600181600116156101000203166002900480601f0160208091040260200160405190810160405280
929190818152602001828054600181600116156101000203166002900480156103f05780601f106103c5576101008083540402835291602001916103f0565b820191906000526020600020905b8154815290600101906020018
083116103d357829003601f168201915b50505050509080600201805460018160011615610100020316600290048060 1f0160208091040260200160405190810160405280929190818152602001828054600181600116156101
0002031660029004801561048e5780601f106104635761010080835404028352916020019161048e565b820191906000526020600020905b8154815290600101906020018083116104715782900 3601f168201915b5050505050505
0908060030154905084565b6000602052806000526040600020600091505490610 1000a900460ff168156fea265627a7a723158201f86ea177ff5bf4f50935243cdaac285013921da7243eadab2975ddddd5b646364736f6c63
430005100032436f6d6d756e697374205061727479204f6620496e64696120284d61727869737429
```

Contract Creation Transaction



CURRENT BLOCK 159 | GAS PRICE 20000000000 | GAS LIMIT 6721975 | HARDFORK MUIRGLACIER | NETWORK ID 5777 | RPC SERVER HTTP://127.0.0.1:7545 | MINING STATUS AUTOMINING | WORKSPACE BLOCKCHAIN-VOTING

0×ef4a04e4296757c156f9ea2e824863d605f6e266c32654b4f8471c83641a9b31 (0)

CONTRACT NAME
Election

CONTRACT ADDRESS
0×1e85bdCD1B78989d4ea2F164864562E3F60DCBcE

SIGNATURE (DECODED)
votedEvent(_candidateId: uint256)

TX HASH
0×ef4a04e4296757c156f9ea2e824863d605f6e266c32654b4f8471c83641a9b31

LOG INDEX
0

BLOCK TIME
2020-06-23 15:30:05

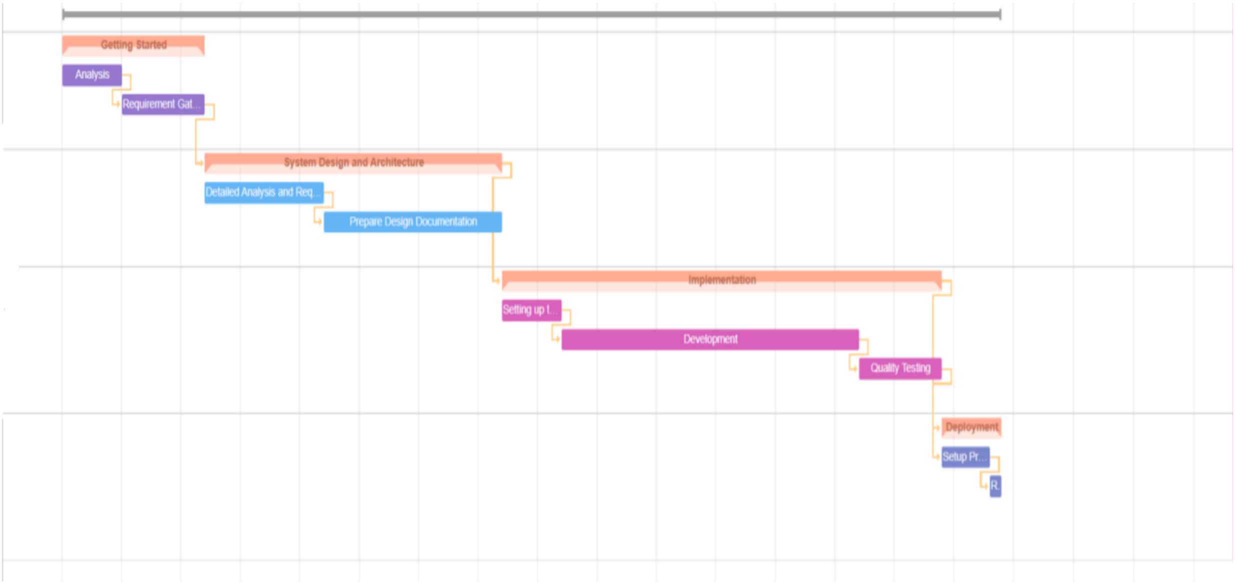
RETURN VALUES

_CANDIDATEID
4

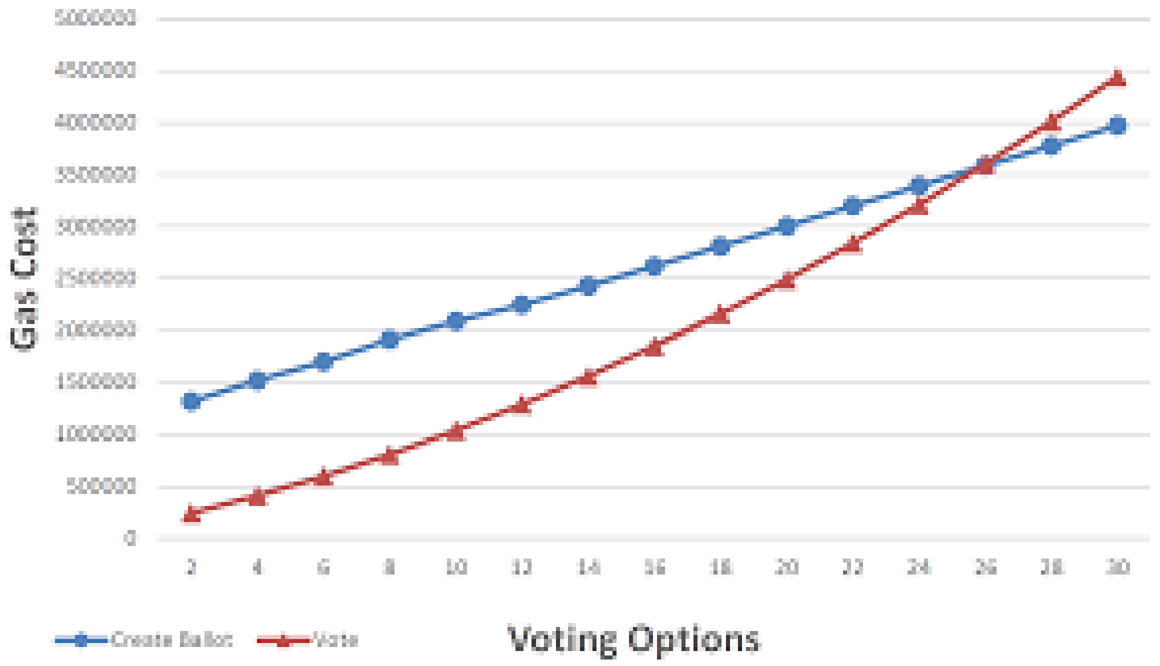
Voted Event Transaction

CHARTS

- **Gantt Chart :**Gantt chart is a type of a bar chart that is used for illustrating project schedules. Gantt charts can be used in any projects that involve effort, resources, milestones and deliveries. At present, Gantt charts have become the popular choice of project managers in every field. Gantt charts allow project managers to track the progress of the entire project. Through Gantt charts, the project manager can keep a track of the individual tasks as well as of the overall project progression.



- **PERT :** Project Evaluation and Review Technique (PERT) depicts the activities and schedule of the activities or tasks through a network diagram. PERT is used to estimate the complete time of the project. PERT Planning comprises the following steps: 1. Identification of definite activities and breakthroughs 2. Determining the proper sequence of the activities 3. Construction of network diagram 4. Estimation of the time required for each activity 5. Determination of Critical Path 6. Updation of PERT chart Critical path is the path which gives us or helps us to estimate the earliest time in which the whole project can be completed. Any delay to an activity on this critical path will lead to a delay in the completion of the whole project. In order to identify the critical path, we need to calculate the activity float for each activity. Activity float is actually the difference between an activity's Earliest start and its latest start date or the difference between the activity's Earliest finish and its latest finish date and it indicates how much the activity can be delayed without delaying the completion of the whole project. If the float of an activity is zero, then the activity is a critical activity and must be added to the critical path of the project network. In this example, activity F and G have zero float and hence, are critical activities.



Advantages

Advantages of e-voting system using blockchain below:

1. You can vote anytime/anywhere (During Pandemics like COVID-19 where it’s impossible to hold elections physically
2. Secure
3. Immutable
4. Faster
5. Transparent

SYSTEM SECURITY MEASURES

Data Security

Security is about risk management, so it is important to start with an understanding of the risk associated with the blockchain solutions. The specific risks of a blockchain solution depends on the type of blockchain being used. Let’s take a look at the various types of blockchains with decreasing level of risks and increasing levels of security:

• Public Blockchains are public and anyone can join them and validate transactions. They are generally riskier (for example, cryptocurrencies). This includes risks where anyone can be part of the blockchain without any level of control or restrictions.

• Private blockchains are restricted and usually limited to business networks; membership is controlled by a single entity (regulator) or consortium.

• Permissionless blockchains have no restrictions on processors.

• Permissioned blockchains allow the ledger to be encrypted so that only relevant participants can see it, and only those who meet a need-to-know criterion can decrypt it.

There are a number of other risks with blockchain solutions, and they can be broadly categorized into three areas:

• Business and governance: Business risks include financial implications, reputational factors, and compliance risks. Governance risks emanate primarily from the decentralized nature of blockchain solutions, and require strong controls on decision criteria, governing policies, identity, and access management.

- Process: These risks are associated with the various processes that a blockchain solution requires in its architecture and operations.

- Technology: The underlying technology used to implement various processes and business needs may not always be the best choice, and this can ultimately lead to security risks.

Blockchain Security Threat Models The security of a solution should also be evaluated in the context of its threat model. Blockchain, by nature, has robust record integrity guarantees, however a number of things can go wrong in other parts of a blockchain-based application that can lead to compromise and loss. Some examples include weak access controls, loose key and certificate management protections, and insufficient communication security. The key to properly securing such an application is to develop a comprehensive threat model for it and mitigate identified weaknesses.

One well-known model is the Spoofing, Tampering, Repudiation, Information disclosure, Denial of service attacks, and Elevation of privilege (STRIDE) model that is used to study relationships between the actors and assets, review threats and weaknesses related to these relationships, and propose appropriate mitigations.

Blockchain applications often incorporate external components — Identity and access management (IAM) systems, multi-factor authentication (MFA), public key infrastructure (PKI), and regulatory and audit systems — that are owned and managed by actors. These systems need to be carefully scrutinized before they can become part of the overall solution as they are developed or controlled by third parties. These should be taken into consideration for the threat model in a blockchain solution.

Security controls unique to blockchain

- API security best practices are used to safeguard API-based transactions.

- Data classification are adopted for the approach to safeguard data/information.

- The appropriate endorsement policies are defined and endorsed based on business contracts.

- Secrets-store for both application and privileged access is leveraged.

LIMITATIONS AND FUTURE SCOPE

1) Efficient energy

It provides energy-intensive process such as peer to peer communication , asymmetric encryption etc

2) Time Efficient System

Reduces time consumption in the voting process with the use of blockchain.

3) Helps to resolve the conflict between political parties due to abstract voting policies.

CONCLUSION

Democracies depend on trusted elections and citizens should trust the election system for a strong democracy. However traditional paper-based elections do not provide trustworthiness. 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. This project has been developed into a blockchain-based electronic voting system that utilizes smart contracts to enable secure and cost-efficient elections while guaranteeing voters privacy. It outlines the systems architecture, the design, and a security analysis of the system. In the next build of this application, it has been proposed to create separate client designs for various roles such as one for election commission and one for candidates registered to a certain party with the existing voting client design. Also, the current versions lack authentication as we don’t have access to the current Aadhar or Voter SDK to integrate in our application. Also, it is planned that in the next build notification prompt will be given on the day of voting to all the voters to cast their vote so that the voter turnout is maximum for that election.

1) There is no way of tempering the votes due to this latest technology of blockchain where everything is stored by spending a definite quantity of token.

2) Minimization of duplicacy due to the transparency of the voting system.

3) It can save a lot of effort by narrowing down the time consumed in the elections and results .

Therefore it is safe to conclude that Blockchain has taken the world by storm and it is definitely proving to be a savior in election process by ensuring uncorrupted elections

REFERENCES

1. https://en.wikipedia.org/wiki/Blockchain
2. https://www.geeksforgeeks.org/decentralized-voting-system-using-blockchain/
3. https://www.apriorit.com/dev-blog/734-blockchain-for-e-voting-systems
4. Wolchok, Scott, et al. "Security analysis of India's electronic voting machines." Proceedings of the 17th ACM conference on Computer and communications security. ACM, 2020.
5. Ohlin, Jens David. "Did Russian cyber interference in the 2016 election violate international law." Tex. L. Rev. 95 (2020).
6. Ayed, Ahmed Ben. "A conceptual secure blockchain-based electronic voting system." International Journal of Network Security & Its Applications 9.3 (2019): 01-09.
7. Hanifa Tunisia, Rifa, and Budi Rahardjo. "Blockchain based e-voting recording system design." 2017 11th International Conference on Telecommunication Systems Services and Applications (TSSA). IEEE, 2020.
8. Yu, Bin, et al. "Platform-independent secure blockchain-based voting system." International Conference on Information Security. Springer, Cham, 2019