Implementation of Digital Voting System Using Blockchain

by

Naimul Hasan Sabbir
18301136
Md. Amirul Islam Chowdhury
18301254
Rishikesh Das
18301074
K.A. Mukit
18301043

A thesis submitted to the Department of Computer Science and Engineering
in partial fulfillment of the requirements for the degree of
B.Sc. in Computer Science and Engineering

Department of Computer Science and Engineering
School of Data and Sciences
Brac University
January 2023

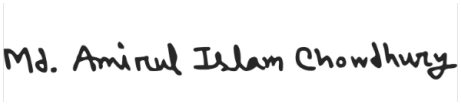
Declaration

It is hereby declared that

1. The thesis submitted is our own original work while completing degree at Brac University.
2. The thesis does not contain material previously published or written by a third party, except where this is appropriately cited through full and accurate referencing.
3. The thesis does not contain material which has been accepted, or submitted, for any other degree or diploma at a university or other institution.
4. We have acknowledged all main sources of help.

Student's Full Name & Signature:

Naimul Hasan Sabbir
18301136



Md. Amirul Islam Chowdhury
18301254

Rishikesh Das
18301074

K.A. Mukit
18301043

Approval

The thesis/project titled "Implementation Of Digital Voting System Using Blockchain" submitted by

1. Naimul Hasan Sabbir(18301136)
2. Md. Amirul Islam Chowdhury(18301254)
3. Rishikesh Das(18301074)
4. K.A. Mukit(18301043)

Of Fall, 2022 has been accepted as satisfactory in partial fulfillment of the requirement for the degree of B.Sc. in Computer Science on January 26, 2023.

Examining Committee:

Supervisor:
(Member)

Dr. Md. Khalilur Rahman
Professor
Department of Computer Science and Engineering
Brac University

Co-Supervisor:
(Member)

Mr. Mobashir Monim
Lecturer
Department of Computer Science and Engineering
Brac University

Thesis Coordinator:

Md.Golam Rabiul Alam
Associate Professor
Department of Computer Science and Engineering
Brac University

Head of Department:
(Chairperson)

Sadia Hamid Kazi, PhD
Chairperson and Associate Professor
Department of Computer Science and Engineering
Brac University

Abstract

Electronic voting has evolved over time as a viable alternative to traditional paper-based voting in order to decrease redundancies and anomalies. Traditional voting has not pleased the public or government officials in recent years. They are not completely secure because ballots are easy to tamper with. It also raises concerns about voter security and transparency. Blockchain technology can play an important role in overcoming these issues as it is based on a decentralized system with peer-to-peer network architecture. One of the most common causes of electoral fraud, vote manipulation, can be reduced by incorporating blockchain into e-voting systems. This study proposes a comprehensive design and implementation of an e-voting system that utilizes blockchain technology and validator nodes to ensure security and transparency. The system comprises a user-friendly frontend for voter registration and login, and to maintain the voter's anonymity, we utilized the Keccak-256 encryption method. The proposed system is structured in three layers, namely the district layer, the divisional layer, and the election commission layer, each of which is protected by its own set of validator nodes. It also utilizes a smart contract to register voters, facilitate the voting process, as well as assign them a unique voter ID. Validator nodes in each layer verify the authenticity of the votes based on their predefined set of conditions. The result aggregation process is safeguarded by a set of validator nodes that validate the integrity of the results. The proposed system is evaluated in terms of security, transparency, and scalability. The implementation of the system using the Ethereum blockchain platform is described, and the results of the evaluation are presented. The system is found to be secure against common attacks such as Sybil attacks and double-voting. The system is also found to be scalable, as it can handle a large number of voters and voting stations.

Keywords: E-voting; Blockchain; Peer-to-Peer network; Decentralized system; Ethereum; Smart Contract; Keccak-256

Acknowledgement

Firstly, all praise to the Great Allah for whom our thesis have been completed without any major interruption.
Secondly, to our supervisor Dr. Md. Khalilur Rahman sir for his kind support and advice in our work. He helped us whenever we needed help.
Thirdly, to our co-supervisor Mr. Mobashir Monim sir for his kind support and advice in our work. He also helped us whenever we needed help.
Last but not the least, we want to mention Dr. Sadek Ferdous Sir's name for his guidlines which helped us a lot.
And finally to our parents without their throughout support, it may not be possible. With their kind support and prayer we are now on the verge of our graduation.

Table of Contents

List of Figures

Nomenclature

The next list describes several symbols & abbreviation that will be later used within the body of the document

ABI Application Binary Interface

API Application Programming Interface

$DApps$ Decentralized Applications

EVM Electronic Voting Machine

EVM Ethereum virtual machine

GUI Graphical User Interface

IDE Integrated development environment

JVM Java virtual machine

KYC Know Your Customer

OCR Optical Character Recognition

POW Proof of Stake

POW Proof of Work

SHA Secure Hash Algorithms

Chapter 1

Introduction

Election is the process through which a country's democracy is established. It is also one of the most difficult tasks, with extremely severe limits. Many countries' constitutions stipulate that general elections must adhere to the principles of generality, freedom, equality, secrecy, and directness. The set of general constitutional voting requirements originates from the fundamental requirement of democracy, as well as the fundamental demand of democracy.
Blockchain has numerous characteristics in which decentralization, transparency, and immutability are some of the features which make blockchain suitable for implementing a decentralized electronic voting system. Participants can, for example, utilize blockchain addresses to represent their identities, resulting in pseudo anonymity. In traditional voting systems, all operations can be classified as transactions or transfers of virtual assets between voters and candidates. Furthermore, transaction contents can be encrypted to safeguard participants' privacy. The number of votes a candidate receives is determined by the number of transactions or virtual assets sent to the candidate's address. After the voting process is completed, all transactions linked to the voting event will be permanently and irrevocably saved in a distributed blockchain, assuring the voting process' integrity.[21]
Our research focuses on implementing the blockchain-based e-voting system that addresses the current flaws. Surprisingly, we observed that there has yet to be reported a consistent list of system requirements. This prompted us to re-examine the electronic voting system and offered a concept with a three-step vote casting process in a permissioned blockchain network. Our methodology includes voter registration, vote casting, and finally vote validation in three phases for completing remote e-voting. When it comes to implementing a digital voting system, the most important consideration is always vote casting section. We need to make sure the system is capable to secure data and protect against prospective assaults when such important decisions are at stake.
For vote casting we are going to use three stage stamping procedure where for each vote count it will be validated in local level, then in district level and finally in central level.
The technology of blockchain is one approach to potentially tackle the security challenges of casting of ballots [6]. In vote casting phase we have used cryptography method Keccak-256 for anonymity of voter's privacy and to create a digital signature from any other on the blockchain network expect the voter itself. Three step vote casting method for each single vote using existing consensus protocol and smart

contracts on each step of vote casting. As a result, it offers sophisticated permission and policy management.

1.1 Research Problem

The traditional paper-based voting systems had many limitations, such as integrity, accessibility of paper ballots, cost, transparency, and fairness. There were higher possibilities of biasness or chances of vote manipulation as there usually stands a central authority who is held responsible for the whole voting process, from voter verification and vote casting to vote count. As the world progresses day by day with technological advancement, electronic voting systems have been introduced, but the question of impartiality remains. Electronic voting systems usually depend on electronic virtual machines (EVM), and the physical security of those machines is questionable. Users who voted need proof whether their votes were casted properly to the right person they wanted to vote for without revealing their identity. Electronic voting systems alone cannot guarantee that there are no ties between the manufacturer and political parties. Moreover, it is vulnerable to hacking since hackers can manipulate the whole process through malicious programs. As a result, the system is vulnerable to fraud. Considering all the shortcomings of the existing voting models, we wanted to develop an online-based remote voting system that ensures the highest possible security along with preserving voters' anonymity to ensure a transparent and impartial election. Blockchain is a decentralized, distributed ledger technology that works on peer-to-peer networks to authorize and execute transactions keeping data records. Thus, we use blockchain technology to establish our model as this will not require any central authority as well as voters can vote without the intervention from a third party, and they can get assured of the fairness and transparency of elections due to the features of blockchain such as security, distributed, decentralized and immutability.

1.2 Research Objective

Our Blockchain-based digital voting system aims to implement an Ethereum-based decentralized electronic voting system where users can vote from wherever they want by verifying themselves as valid voters. Moreover, they can ensure whether their votes are appropriately casted or not, maintaining their identity hidden. The following is a description of our research's primary goal -

1. Make sure the system is properly authenticated. Online systems that deal with sensitive information or transactions must employ authentication, which is the process of determining whether a person or object is what it claims to be. In order to safely and confidently share private information, it is necessary to set up a network that guarantees the data's privacy, security, and authenticity during transit.

2. One person will be allowed to vote for up to one time [30]. Our research objective is to ensure that not more than one vote will be cast against one voter's account. Electoral fraud, such as voter impersonation, ballot stuffing, voter intimidation, and manipulation of voting machines, is questionable for

the fairness of an election. It is hypothesized that those who have experienced electoral success or failure are in a better position than those who have not to attenuate the negative effects of increased levels of observed electoral fraud on their judgments of the democratic process [8]. Thus, it has to be ensured that the election is fair.

3. To ensure the anonymity of voters, International law recognizes voter anonymity as a necessary requirement for a free and fair electoral process [4]. If it reveals that a person voted for whom, then it will not be beneficial for him/her, and voting rights will not be preserved.

4. Providing a scalable, widely applicable framework for electronic voting. By using Blockchain technology, people can be aware about whether the election is transparent or not. For instance, if any invalid transaction occurs, validators will declare that invalid and not add it to the Blockchain.

5. In spite of its widespread adoption, electronic voting machine (EVM) technology has not been proven to be totally secure against manipulation or fraud. Twenty or so nations throughout the world, including India, Australia, Norway, and Venezuela, have experimented with computerized voting systems in the last two decades, with varied degrees of acceptance and rejection [31]. So our motto is to overcome those shortcomings with the help of Blockchain technology.

6. In our architecture, consensus algorithms such as Proof-of-Work (PoW) and Proof-of-Stake (PoS) will help in preventing fraudulent voters and validating transactions. Security, preventing fraud, and establishing trust all rely heavily on Proof-of-Work (PoW), and Proof-of-Stake (PoS) choose validators randomly and process the transactions.

7. To build a decentralized voting system with no third party so that the risk of manipulation will get reduced and the fairness will get preserved.

1.3 Problem Statement

The winner of an election is usually measured by the results of that election, to be more specific, the number of votes the candidate gets. If a candidate gets higher votes than the opponents then he/she is considered the winner of that particular election.
From the perspective of the voters, they want to ensure that their votes are cast and counted properly or not. An election is considered to be fair if the result of that election is accurate enough to satisfy the mass people who voted along with the media and the press.
As the world progresses, many kinds of voting systems are introduced in different countries across all over the world. The most used system is the traditional ballot paper-based system where voters go to the designated polling station and cast their vote in the ballot paper. But the traditional paper-based voting system has certain drawbacks. For instance, it has some issues to deal with regarding voter integrity, confidentiality, as well as end-to-end verification. Moreover, the system

is very time-consuming, as well as there remains a high chance of electoral fraud. Someone can easily misinterpret the whole process with biasness. To make voting fair and secure, several research papers have been published, as well as implementation has been done on electronic voting systems. However, there is still a lack of voter identification and vote-casting process and this needs to be fixed to make the election more secure and fair. Without a thorough understanding of computer technology, the fundamental issues with electronic voting could be identified. After casting their ballots, voters will not have the opportunity to double-check the accuracy of the third party reporters' work until the results are made public. There would be no repercussions if the third party mistakenly or purposefully recorded the votes incorrectly. Without accountability, it is unclear whether or not this system is trustworthy, regardless of whether or not a computer is involved. Although computers have the ability to execute programs precisely and quickly, they are designed and programmed by humans, so there is still a chance of biasness. Developing foolproof computer hardware and software is one of the industry's biggest challenges. This problem is getting much more severe as computer systems get more complex. Moreover, there is a chance that the system can be taken over by hackers.

Political participation is indeed necessary to ensure a democratic regime's legitimacy [2]. The greater the number of citizens who do not vote, the less accountable elected authorities to become. To demonstrate the issue, consider elections in which the outcome is determined by a small part of the electorate. Indeed, where few people participate in decision-making, there is little democracy; conversely, the more people who participate in decision-making, the more democracy there is. [1]

So the purpose of our model is to develop a reliable, trustworthy, and authentic electronic voting system which ensures voter integrity, voting transparency including voters' confidentiality in a sensible way while upholding the system's overall security, time constraints, verification requirements, and financial constraints keeping in mind.

Chapter 2

Literature Review

2.1 Blockchain Mechanism

Back in 2008 Satoshi Nakamoto pseudonymous person or a group of people proposed a way for electronic transactions: "Bitcoin: A peer-to-peer Electronic Cash System" that does not rely on trust [3]. This system use a peer-to-peer network architecture which timestamps transactions using encrypted mechanisms to a continuing chain of hash based proof-of-work which is known as blockchain technology. Blockchain technology has been considered the next era of revolutionary core technologies after steam engines, electricity, and the Internet. If the steam engine increases productivity and economic growth, electricity meets their fundamental requirements, and the Internet revolutionizes the way information is shared, then Blockchain, as a trust-building mechanism, will revolutionize the way human values are conveyed. Blockchain is primarily used to address transactional trust and security issues [23]. Blockchain is revolutionary technology that has change how transaction works. It is a set of blocks that record information like who make the transaction to whom. It is a amount of digital line that distributed across the entire network making it more secure and impossible to hack and change any kind of information. It is verified and validated by every node in the blockchain network to proceed to the next step.

2.1.1 Genesis block

The Genesis Block, also known as Block 0 is the initial block in a blockchain and serves as the foundation for succeeding blocks. Because each block relates to the one before it, it serves as the ancestor from which all subsequent blocks may trace their lineage. A Genesis Block is the initial block of a cryptocurrency. On a block-chain network, a blockchain is a series of blocks that are used to record information about transactions. Each block has its own header, which is recognized by its block header hash. The Genesis Block serves as the foundation for these blocks, which are stacked on top of the others until the block-highest chain's point is reached, completing the sequence. The layers and extensive history of each sequence are among the features that make a blockchain-based crypto-currency so secure. Blocks can be considered as digital containers that retain network transaction information forever. A block is a series of unrecorded recent transactions. That is why a block resembles a ledger page . When a block is completed, control is passed to the next block in the chain. Because of being the very first block in a block-chain as well as act as a foundation

for succeeding blocks, the genesis block is also known as BLOCK 0. As each block relates to the one before it, it serves as the ancestor for all subsequent blocks. The technique of confirming bitcoin transactions and getting new bitcoins into the system began with this.

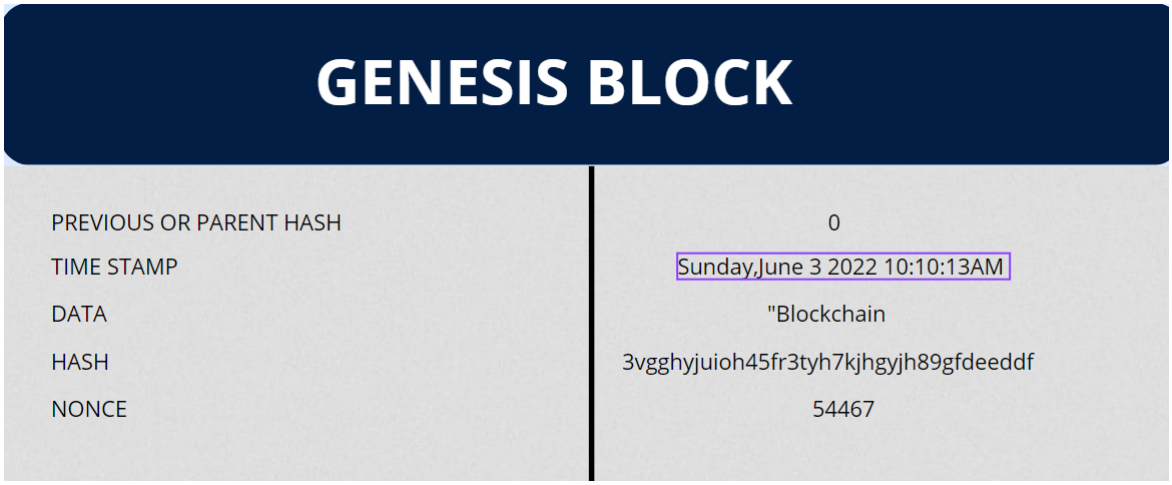


Figure 2.1: A Genesis Block

2.1.2 Block Data

All the blocks in a blockchain network are large data storage units except the genesis block. Every occurrence is documented as a sequence of data blocks, which are subsequently appended towards the block chain. As a result, block-chain refers to the process of connecting blocks via chains. Every block in a blockchain network is connected with its immediate next block by the hash value. The most significant aspect of the block-chain for information storage is the blocks or nodes. These blocks are posted to the blockchain and contain all commercial and non-transactional data. IOTA being the exception uses side chains or several threading chains. Like a linked list, the blocks in our design are added to the preceding hash in a chain.

2.1.3 Previous Hash

The prior hash connects every block in the blockchain, assuring the block-one-way chain's retrieval integrity. This system employs an immutable 64-bit SHA256 hash, which implies that we can not overwrite it. Every block in a blockchain network is linked with its previous block as well as the genesis block. During block traversal, we will never link to the genesis block since they are automatically formed and changed consistently. Because of this, blockchain is unchangeable as well as trustworthy.

2.1.4 Current Hash

All the blocks in the blockchain have a hash value which functions as a unique identifier for the block. These hashes are unchangeable and act as the blockchain's backbone since both of them symbolize and link the whole network. Every block links to the hash of its preceding block. The question is how to make these kinds of hashes unique. Timestamp, nonce, and ages are used to create these kinds of hashes.

We only create one hash from the 264 numbers because they are all unique,the hashes have 0 percent probability of matching.

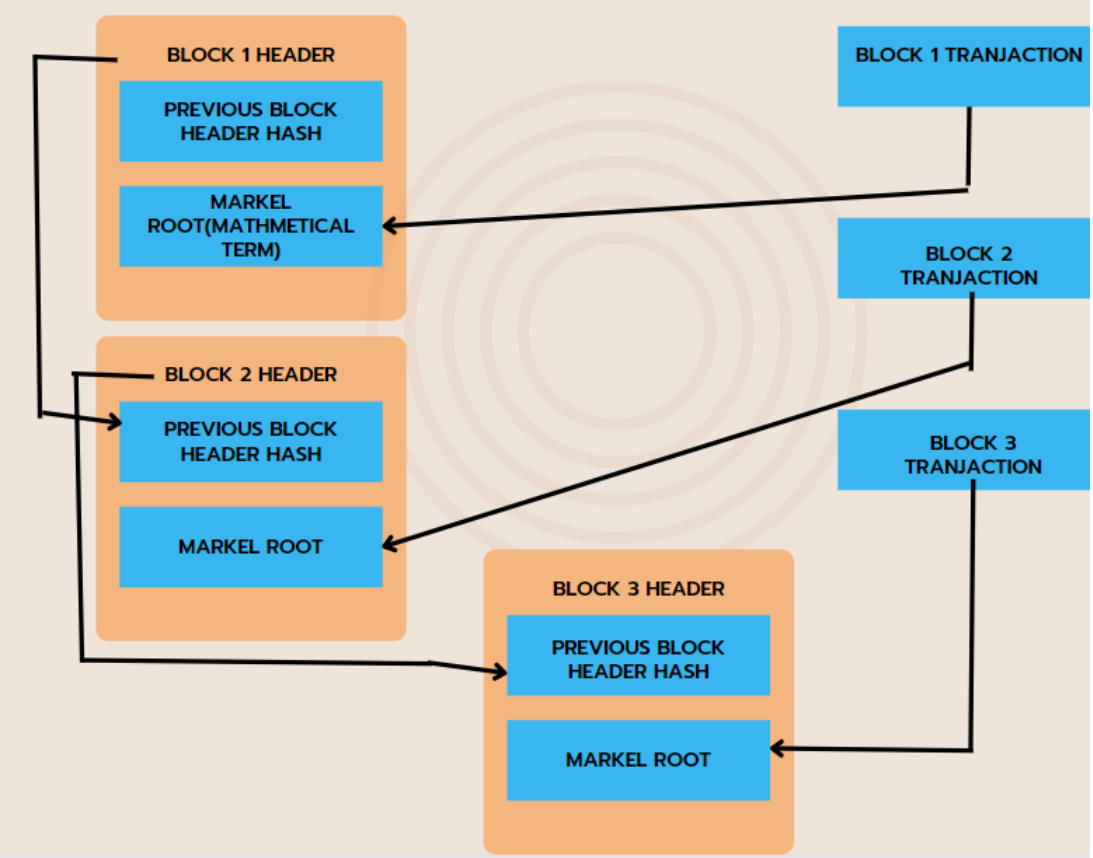


Figure 2.2: Current Hash

2.1.5 Timestamp

Every block contains a timestamp, a little amount of data that functions as a unique serial number. Its primary purpose is to determine the specific minute when each block was created, after mining and blockchain authentication. This is also used to generate a special hash that increases the block-transparency. Timestamps does not have to be based on an immutable understanding of time. The blocks are connected in chronological sequence as evidenced by the timestamps. On the blockchain, it logs the time with each transaction. It is temper evidence and it reveals when and what occurred in the blockchain. It serves as both a notary and is more trustworthy than a conventional one since the data in blockchain cannot be changed by anyone.

2.1.6 Nonce

A nonce is a random number used in cryptographic communication. Frequently, they are made up of sort of semi or random numbers. To ensure transmission on time, most nonce include a timestamp, which requires synchronization of workplace clocks. The use of a client nonce for access authentication to improves it's security in several ways. A nonce should be time-variant or include as many random bits

so that it can guarantee that the one previously produced value has a consistently negligible likelihood of being replicated.

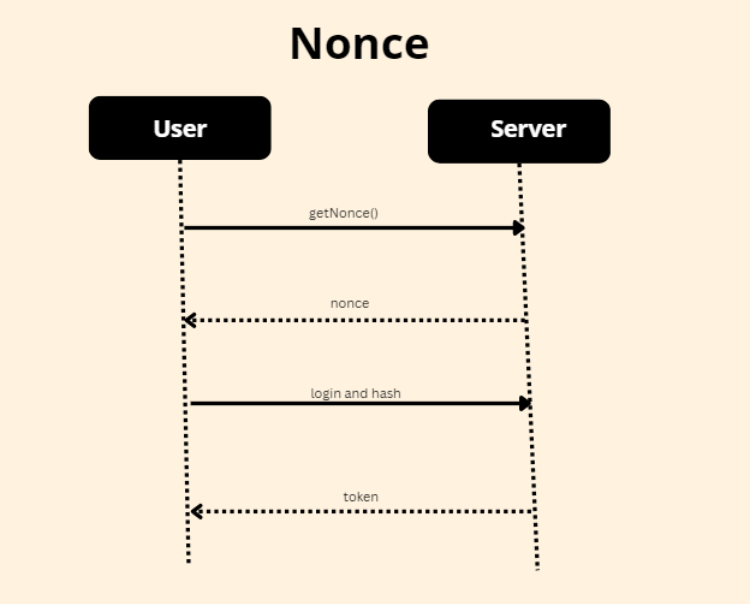


Figure 2.3: A Nonce

2.1.7 Consensus

Consensus defines a mechanism that valid whether a block is eligible or not as well as it is a way to determine which blockchain to choose as valid between two different blockchains [9]. Different blockchain platform uses different consensus mechanism. For instance, "Bitcoin" which is a popular cryptocurrency uses "Proof Of Work" consensus mechanism that require a complex calculation for solving a puzzle and it needs some significant time as well as computing power to finish the process.
Ethereum, a blockchain platform which is gaining popularity day-by-day uses "Proof Of Stake" consensus mechanism that require participants to own a fixed amount of currency for proving that they contribute a stake in the currency.

2.1.8 Proof Of Work

Proof of work is a well-known consensus protocol in which new blocks in the blockchain are created by solving computationally difficult puzzles. Mining is the term for this procedure, and miners are nodes that solve the puzzle. Because each block is linked to its neighbors via hash numbers, modifying a block (creating a new block with the same precedent) necessitates solving a difficult mathematical puzzle of the descendants and repeating the work for the entire chain, which would be extremely difficult. This prevents the blockchain from being overridden. There are numerous major concerns, such as the 51 percent hazard, consumption of time, and energy use.

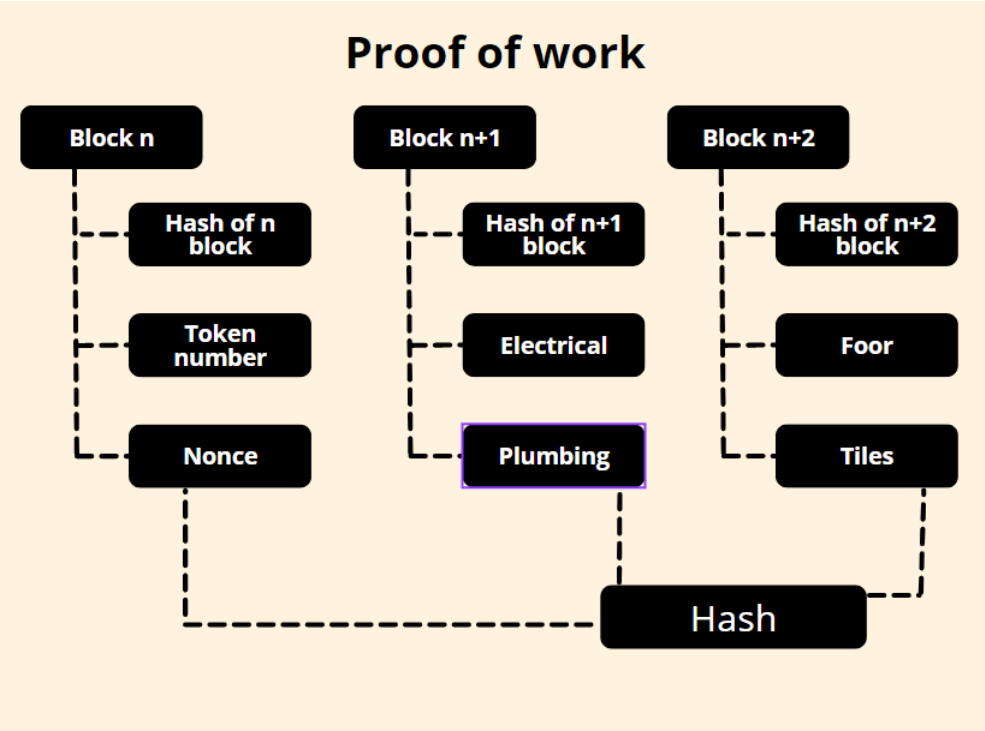


Figure 2.4: Proof Of Work

2.1.9 Proof of stake

Proof of stake is a consensus algorithm for verifying new transactions. A blockchain's record of transactions and data is managed by no central gatekeeper. This play a role on a large number of people to validate incoming transactions and add them to the chain as new blocks. Proof of stake is a compromise method for determining which contributors will be assigned to this attractive job since those who are picked will be compensated with additional crypto if they properly verify new data and do not trick the system.

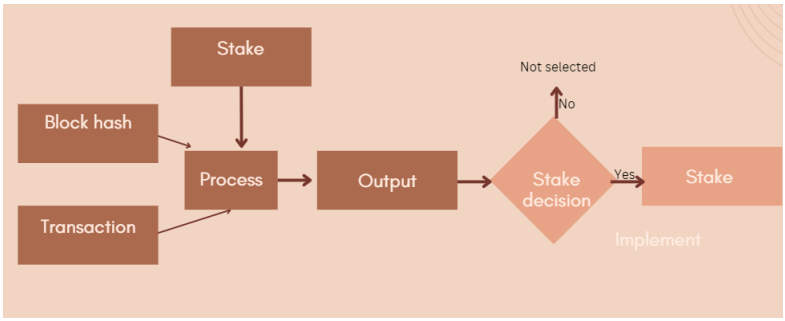


Figure 2.5: Proof Of Stake

2.1.10 Hybrid PoW & PoS

A hybrid PoW & PoS network can use both proof-of-stake and proof-of-work as consensus distribution mechanisms. When deciding transaction validation rights, hybrid Proof of Work/Proof of Stake consensus algorithms use aspects from both

PoW and PoS models. By doing so, they seek to minimize one other's shortcomings. This strategy tries to combine the security of PoW consensus with the governance and energy efficiency of PoS. PoW miners construct new blocks containing transactions to just be added to the blockchain as the first step in a hybrid consensus method. Following the creation of these blocks, PoS miners have to vote on whether or not to confirm them. PoS miners buy votes by staking a percentage of their tokens; larger stakeholders have more voting power. Instead than checking the entire vote count, the hybrid consensus process selects 5 votes at random to verify the authenticity of the newly formed block; if 3 of the 5 chosen votes are affirmative, the block is verified and added to the blockchain. In return for such operations, PoW miners earn 60% of the block reward, PoS miners 30%, and the other 10% is allocated to development activities.

2.1.11 Public Blockchain

Public blockchain is a permissionless decentralized blockchain architecture which does not have any restrictions. Everyone with an internet access can join the network and begin verifying blocks and sending transactions. To illustrate, all blockchain nodes have equal access to the blockchain, be able to produce new blocks of data, and validate existing blocks of data. Both Bitcoin and Ethereum are public blockchains.

2.1.12 Private Blockchain

Private blockchains are basically permissioned blockchain which are controlled by a single organization where the central authority will choose who can be a node to make transactions or verify it [29]. A private blockchain implementation can be used if one has to operate a private blockchain that permits only chosen entry of certified participants, such as those for a private business. A participant can have to go through a verification process to join such a private network.

2.1.13 Consortium Blockchain

Consortium blockchain is basically a type of permissioned blockchain which is controlled by a group of institutions instead of a single organization unlike private blockchain. Instead of starting from the very beginning, people share information among themselves in corsortium blockchain architecture. As a result, it helps to improve efficiency, transparency along with accountability. The remarkable feature of corsortium blockchain is basically it is comparatively faster, cost effective due to less energy consumption. It is scalable as it limits the nodes to enter into the network and verify the transactions. As a result, no one can suddenly join the network and verify themselves, some particular nodes have already been assigned to do these specific tasks. Corsortium blockchain ensures greater security along with monitoring the criminal activities. For this reason, there is no chance of 51 percent attack due to proper verification.

2.1.14 Permissioned Blockchain

In a blockchain network, the data which are saved on the blocks can be accessed and controlled by various nodes based on how the blockchain is configured. There are

four types of blockchain architecture which are public blockchain, private blockchain, Consortium blockchain and Hybrid blockchain. Permissioned blockchain has properties with the combination of Hybrid, Consortium and Private blockchain. One point to note out Which makes permissioned blockchain to be different from other two is that it handles an access control layer to allow specific tasks such as read, access and write etc. to be done only by specific verifiable participants. As our goal is to implement a secure voting system, we need to make sure the integrity, confidentiality and verifiability remain safe and that is why we prefer permissioned blockchain over public and private blockchain.

2.1.15 Markle Tree

Markle tree is basically a data structure which is used to encode Blockchain data in a more effective and secure way. In a Markle tree every leaf node is labeled with its corresponding cryptographic hash and every node which is not a leaf node is labeled with the cryptographic hash of the labels of its children nodes. It also decreases the quantity of memory required for verification. Merkle Tree is utilized in peer-to-peer networks for instance file-sharing programs, Bitcoin, and other decentralized blockchains.

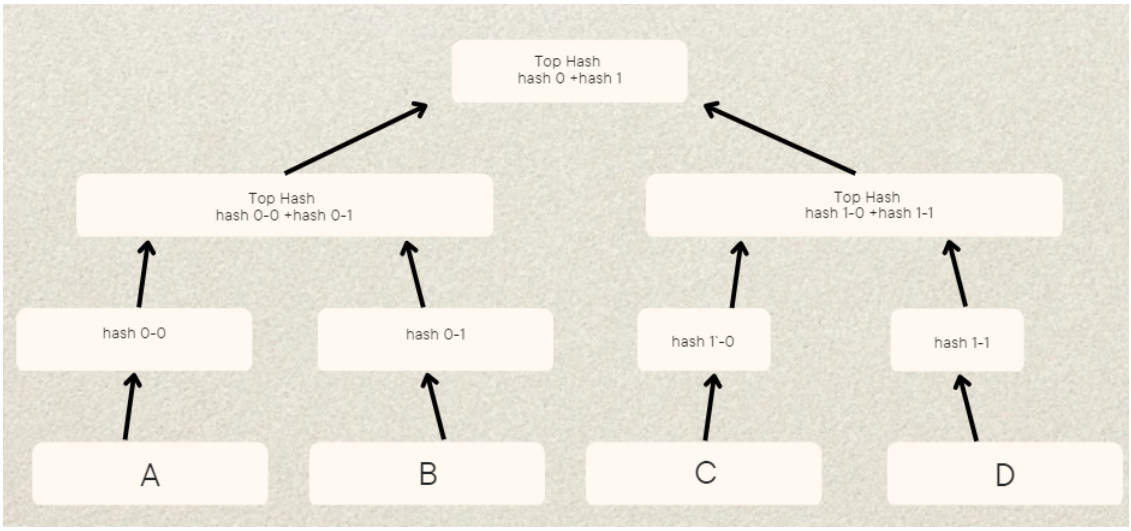


Figure 2.6: A Markle Tree

2.1.16 UTXO

An unspent transaction output or UTXO is considered one of the core components of Bitcoin, Etherium and many other cryptocurrencies which is used for the Account/Balance calculation. For instance, Inputs and outputs comprise bitcoin transactions. When a transaction is initiated, a user selects one or more UTXOs that serve as input or inputs. A user's wallet in UTXO keeps a record of a list of unspent transactions linked with all addresses maintained by the user, and the wallet balance is determined as the total of those unspent transactions.

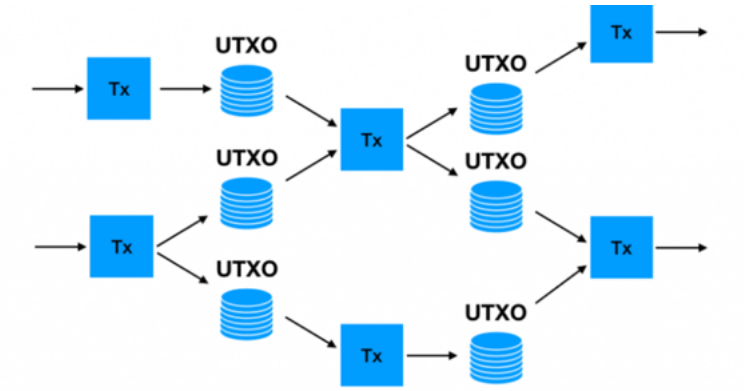


Figure 2.7: UTXO

2.2 Keccak-256

Figure 2.8: Keccak-256

It is important to note that Keccak-256, a cryptographic function, is included into Solidity (SHA-3 Family) [28]. This function takes an input and returns a hash of that input as a single 32-byte value, regardless of the number of inputs. Unlike several other hash functions, this one can only be utilized in one direction.
If we give the input string as “Dhaka, Bangladesh” then the output will be different from “Bangladesh, Dhaka”. A string’s hash value is quite sensitive to even minor changes. For its Ethash consensus engine, Ethereum employs Keccak-256.

2.3 Parliamentary Electoral Process

Bangladesh's unicameral parliament, known as the Jatiya Sangsad, has 350 members. A first-past-the-post system elects 300 of these MPs for a five-year term from single-member constituencies. The remaining 50 seats, which are allocated for women, are filled by assigning seats to each party in proportion to the number of MPs they were able to elect. The party or alliance with the most seats in Parliament is named Premier.

2.4 Election to the House of Commons: Qualifications and Disqualifications

If a person is a citizen of Bangladesh and has reached the age of twenty-five, he is eligible to be elected as a member of Parliament.
A person is disqualified from running for or being elected to the House of Commons if they-

- A competent court has ruled that the person is mentally ill.
- is a bankrupt who has not been dismissed.
- gains citizenship in a foreign country or declares or admits allegiance to a foreign country.
- has been condemned to a term of imprisonment of not less than two years for a criminal offense involving moral turpitude, unless five years have passed since his release.
- occupies any profit-making position in the service of the Republic that is not declared by law to disqualify its bearer.
- is barred from running for office by or under any law.

2.5 Related works

A paper with the title "Implementation of Auditable Blockchain Voting System with Hyperledger Fabric" showed a Auditable Blockchain Voting System implementation at a high-level in connection with numerous hyperledger fabric components [23]. The strategy outlined in this article, National Electoral Commission defines a group of private organizations to create Blockchain substructure to have a blockchain network. In the network there will be two channels, one is VITsDistribution channel and another one is Voting channel. Three main assets have been used which are Election, VIT, Vote. Also along with variables for each asset three smart contracts have been employed, each one for each asset. The National Electoral Commission distributes Voter Identification Tokens(VITs) from local offices to the voter after validation and records the data into blockchain for ensuring only verified voters attain their VIT tokens by VITsDistribution channel. During the voting process, a voting channel is utilized to run the election where voters select their desired candidate on an app which is certified by ABVS in polling places. After that, the ABVS

system shifts votes to the blockchain network. However, the proposed system gives the ability to cast votes as long as the voters have their VITs, since the most recent vote will be counted. Most importantly, votes remain encrypted until the election time is finished. Votes will be counted and second time validation is conducted in the verification and counting phase.

Yousif Abuidris and others in their paper "Secure large-scale E-voting system based on blockchain contract using a hybrid consensus model combined with sharding" proposed a hybrid consensus scheme made up of Proof of Credibility and Proof of Stake to solve scalability, latency and efficiency of the system to ensure the safety of electronic voting systems [20]. To ensure a secure computing environment and reliable public bulletin board a smart contract authors introduced. Moreover, authors compared and described how assaults were carried out between their claimed hybrid blockchain and traditional blockchain.

In a paper titled "A Secure and Optimally Efficient Multi-Authority Election Technique," researchers presented a multi-authority secret-ballot election scheme that would ensure robustness, universal verifiability, and privacy where voters will use a computer to participate, and the major consideration will be the voter's effort. Voters vote on a bulletin board under this approach. The bulletin board uses extended memory, which allows any component to read the data but not to modify it. The ballot does not contain any information regarding the vote, but it does have a statement stating that it is a legal vote. When the deadline has passed, the final tally is completed and can be checked against the sum of all submitted votes by anyone. Because of the encryption mechanism utilized, this assures that the data is verifiable.

In this proposed scheme, "Secure Digital Voting System based on Blockchain Technology" they have implemented an e-voting system with the help of blockchain to provide e-voting applications the ability to make sure voter anonymity, integrity and end-to-end verification [10]. For developing the system, they have used an open source blockchain platform known as "Multichain". The system is designed by using a web-based interface to facilitate user engagement with measures such as fingerprinting to protect against double voting. In this proposed system, it generates a strong cryptographic hash for each vote transaction including information related to a voter for protecting the anonymity and integrity of a voter. Moreover, to keep an individual's vote secret it generates a voter hash during the time of registration into the system. It is also called the unique identifier of a voter which will be used during the voter identification process. Additionally, the system has been implemented with a secure authentication mechanism by using finger printing technology as well as biometrics to make sure only authorized voters can access the system. For vote casting, the system used the "Multichain" platform of blockchain which is responsible to establish a fixed number of private blockchains which will be needed by the election committee for vote casting purposes. Furthermore, votes that are already casted are recorded in the data tables at the backend of the database where ledger synchronization technology is used and voters are given the access to view the table to be able to track their votes by using the unique identifier that was provided to them after being registered.

In the paper “A proposal to use elliptical curves to secure the block in E-voting based on blockchain mechanism”, the authors wanted to use digital signature instead of proof-of-work as it is difficult to implement because computers have to prove that they have done the work by solving a complex mathematical problem in order to add or mine a block of a transaction in the blockchain and to solve complex computational problems, it requires high computational power and resources [25]. Although proof-of-work is more secure, it is not impossible for the hackers to alter or manipulate the data, i.e if the hackers can get access to more than 50 % of computing power then they can launch a blockchain attack. Moreover, the system uses a distributed database which replicates the data to different servers, as a result, the possibility of manipulation still exists. Thus, digital signatures are implemented which uses public key cryptography to diminish the attempts of altering when it has been signed. In digital signature based blockchain, the signature validity and previous block's hash have to be scrutinized before creating a new block. In this research, they have implemented elliptical curve cryptography for signature purposes in order to validate the block along with securing the chain. They have used Node.js as their backend and MongoDB as their database and some modules i.e SHA-256, jsonwebtoken. Before casting a vote, users have to validate themselves as eligible users by checking the required inputs and then check the previous block, if there isn't any then the a genesis block will be created. After that, they have to check the prior block's hash by rehashing the existing information. The fourth validation is to check whether the previous block's signature is valid or not by using the public key, the hash and signature of the prior block. If it is valid then the private key of the user will be used to store the data to the blockchain.

”Mobile-Electronic voting machine (M-EVM) or Modified Electronic voting machine (MEVM)” was offered as the name for an E-Voting System that uses mobile SMS.It has 2 different ways. There are two modes to this system. The option for people who do not have mobile phones is an old traditional method, but there is another mode for those who do have mobile phones, which is a requirement for using M-EVM. The voter's name and mobile phone number must be registered in the EVM database for M-EVM voting to be successful. Voters can vote for a particular candidate by sending a message in the necessary format, and M-EVM will acknowledge the voter's vote. After voting, that person's name would be removed from the list, and that voter would be unable to vote again. After one hour of voting, all registered cellphone numbers will be notified of the election results through this system. On the other hand The Blockchain-based Electronic Voting System (EVS) eliminates the security risks associated with traditional EVS and ballot voting, ensuring transparency to the point where even the Election Commission is unable to see who the voter voted for. No one can amend or temper the vote once it has been cast since the blockchain is immutable. To protect data confidentiality, the idea of a Trusted Third Party (TTP) is used, which works as a middleman between a voter and the Election Commission to verify and validate voters so that they can vote anonymously without risking their security. The mechanism is multi-chained and can prevent repeated votes from being cast by the same voter. Before voting can begin, each voter must register, which requires the voter to give their NID card number. The Election Commission secures NID data using encryption to ensure that the voter is valid, and after validation, the voter is directed to the voting module.

After the voting is completed, various reports about candidate results, party results, constituency results, and so on can be generated. Users must log in using the same information they used to register, and after logging in, he would be routed to the voting portal to cast his vote after verification. He wouldn't be able to log in again after the first time because the information would be saved in the database.

Marianne Dengo outlines how blockchain technology may be used to provide secure electronic voting, which is the main research topic, in his work "Blockchain Voting: A Systematic Literature Review." An extensive review of the literature was done in order to accomplish this [27]. The use of blockchain voting for elections and elections at many levels was thus identified. Four main strategies—voting via smart contracts, Zcash, customised blockchains, and cryptographic signatures—were found to provide a fuller view of a blockchain-based voting process. The advantages and limitations of blockchain voting were also identified. A framework that provides a summary and reference for different blockchain-based solutions was developed as a result of the literature review.The first step is outlining the justification for the review, developing the study questions, and designing the review method. The second phase includes locating applicable papers, choosing major research, assessing their quality, and gathering and synthesising the necessary data. The final phase entails providing prepared and evaluated outcomes reporting. This section gives a description of the SLR's first phase. According to him, the resulting framework provides a way to locate relevant studies quickly and efficiently, which might be helpful for anybody preparing to design, construct, and regularly utilise voting systems.Moreover, this essay For the primary search, multiple electronic databases are searched using search strings. Following that, a second search is conducted by repeatedly reading the citations of the articles found during the original screening. A collection of articles found by searching libraries is chosen for relevance using entrance conditions.As the first step in the screening process, conduct a comprehensive search to identify an introductory gathering of applicable research. In order to search the chosen online media, it is crucial to build a search string linked to the issue.

Patrick Mccorry, Maryam Mehrnezhad and others in their paper "On Secure E-Voting over Blockchain" they proposed the viability of conducting an election using a blockchain in three different contexts, including decentralised voting, remote voting, and in-person voting [22]. For usage in decentralised voting, we offered a potential for improvement of OV-net well over E2E verifiable e-voting technique, namely DRE-ip over a secure message board. Also mentioned was the proof-of-concept implementation of decentralised voting. The Ethereum blockchain is displayed. Secure voting processes promote the legitimacy of democracies. Counting results is a crucial stage in publishing voting to determine the winner. Yet, this is also the stage where votes are most prone to being counted incorrectly or not entirely due to an absence of visibility. Digital voting systems could not be made available for public inspection.If the voting software has a bug or a hacker gains access to it, the automated count or vote might be covertly changed. The privacy of voters is likewise protected by E2E voting technology. The only criteria that can be satisfied by conventional paper voting is the first one, which asks that voters choose a party on an actual ballot. Votes cast may not be counted correctly or may be misplaced due to human error, maliciousness, or bad luck. Some of the most significant problems

with electronic voting are thought to be resolved in the database that underpins Bitcoin, according to many.

In the paper “E-Voting system using Blockchain technology “ where Aishwarya Indapwar , Manoj Chandak and Amit Jain highlight the topic of Blockchain is a type of hybrids technology that provides solutions for scenarios in which only users on a whitelist are permitted access, yet all transactions are open to the public [16]. There will be the transparency that democratic institutions demand. However, e-voting may bring up some new problems, such as privacy protection. Blockchain is a decentralised storage system that manages an ever-growing library of documents that are secure against modification. It has no single point of failure and is dispersed as opposed to centralised. A person’s past and accessible keys, which are personal to them, may be used to establish a secure digital signature. Blockchain technology uses hash cryptography, namely the Sha-256 hash algorithm, to secure data. Many bricks make up each chain. Each block contains a transaction that is hashed, placed in a Markle tree, and saved. The blockchain technology prohibits the possession of the chain by any computer; instead, it distributes the chain across network nodes. The difficult arithmetic problem of finding a separate dimwit and hash that produces hash requires the use of specialised software. To be effective on a large scale, polls must be flexible. Additionally, there should be no evidence that bribes or other types of fraud were used to influence the way the votes were cast. The technology needs to be reasonably priced, safe, and impenetrable to hacking.

Raj Kumar Bogati outlined how to use a secure electronic voting system utilising blockchain technology in his paper “Secure E-voting System using Blockchain Technology”. Blockchain technology may be used to secure elections if there are enough voters. By using the power of the Ethereum network and the blockchain structure, I was able to provide a model of blockchain technology for e-voting while also resolving some of the core problems that traditional e-voting systems face.Participants in the procedure utilise electronic voting machines to cast their ballots.Electronic voting machines are used to cast ballots by participants in the process. The major problem with voting machines is the possibility of tampering with the results to commit vote fraud. Voting machines are far more secure thanks to blockchain technology. An election system must provide safe authentication by utilising identity verification services. In an electoral system, votes shouldn’t be possible to be traced back to specific voters. A voting mechanism should only permit individuals who are qualified to vote to exercise their right. Researchers propose a hybrid paradigm that combines Proof of Stability and Proof-of-Stake to overcome issues with protecting electronic voting systems. Scientists have theoretically validated a remote vote-by-web system that allows people to cast ballots from their homes. Voters would benefit from the system’s dependability, security, and anonymity. The developed method eliminates the possibility of voter identity, vote consistent, or voting secrecy errors. Researchers discuss the issues that the emergence of computing power has created for current technologies. The authors suggested a secure web forum with an E2E verified e-voting.

In the paper ”Towards Secure E-Voting Using Blockchain,” Mishkaat Ansari, Mohammed Ahmed Shaikh, and Yasra Ansari described a novel electronic voting system

based on blockchain that makes use of smart contracts to ensure voters' anonymity while enabling secure and affordable elections. They have described the system's design, architecture, and security analysis [12]. The security of the acquired voter data will be enhanced by using External database server-based solutions and blockchain technology. In India, only electronic voting platforms (EVS) created in the last two decades by a few state-owned businesses are used. These tools' simple design, ease of use, and longevity have helped them become quite popular. They have been given since there have been multiple reports of complaints of irregular voting. Blockchain technology was established in 2008 by Satoshi Nakamoto to safeguard electronic money transfers. In order to construct a chain of links linking the earlier blocks, this system creates a hash when data is recorded and stores it in the following block.The hash changes anytime the data does since it is generated from the data. "Blockchain" refers to a web-based program for digital assets. It is composed of an ever-growing list of records that are linked and encrypted blocks. On every system, its database can be entirely recreated without jeopardising its security or dependability.

Dipali Pawar, Pooja Sarode and others in their paper named "Implementation of Secure Voting System using Blockchain" refers to the system's main goal is to demonstrate a blockchain voting system implementation proposal. By protecting the privacy of the voter, our program will provide a transparent and economical election. The system will have the ability to recognize manipulated votes and settle issues even if there are votes that have been altered.In today's culture, we require a safe voting process that provides equity, privacy, and security [17]. Systems controlled by a single entity should not be possible through voting. The voting process should guarantee that votes were cast and counted and should give evidence of cast ballots. As "Decentralised Voting Systems," certain voting procedures may be mentioned. The e-voting system must be impenetrable to tampering and unchangeable.Today's society requires a safe voting system that provides justice, privacy, and security. A single entity shouldn't be able to govern systems through a voting mechanism. Decentralised voting methods refer to a variety of voting procedures. The electronic voting method needs to be impenetrable and unchangeable.The key pairs consist of two components: a public key and a private key. The operation of these key pairings is shown in the diagram below. In this method, voting data is stored in the shape of blocks that are connected to one another to establish a path of voting history via a decentralised network. ECC cryptography is used to encrypt and decrypt messages utilising public and private encryption and decryption processes. Since it is a part of the open chain of activities on the Bitcoin network, once the data is saved in the databases, it cannot be altered.

Aditya Gaikwad , Mayur Jadhav and others in their paper "E-voting using block chain Technology" discuss the concept of Blockchain e-voting.In several nations, electronic voting has started to be utilised in elections. This project intends to implement vote results across all election sites using block chain technology [18]. This will be a technique that relies on a specific turn on the internet for each node, unlike Btc including its Proof of Work. Although it improves the lives of many people today, digital technology does not completely guarantee anonymity or honesty. A large number of intelligence services throughout the world have influence over portions

of the Internet, giving them the ability to track or intercept ballots.For electronic voting, we provide a novel consensus technique called Proof of Vote (POV). Block verification using the Proof of Stake protocol does not need a lot of computation. Proof-of-stake protocols divide stake blocks according to the present wealth of miners rather than according to the proportional hashing rates of miners (i.e., their mining power). The blockchain key of all operations in the Bitcoin system, which uses block chain technology, is presently available. The study of secure communication methods in the presence of outside parties is known as cryptography. Cryptosystems come in two flavours: symmetric and asymmetric. It is possible to locate nodes that can jointly control and change data using this block chain authorization mechanism.

The paper "Ethereum Blockchain-based voting system" the author highlighted the fact about e-voting based on the author's explanation, is comparable to JavaScript and features an addressID function. It just uses the Ethereum platform as a basis [15]. On the Ether network, "gas," which is needed to fuel the system, must be paid for each confirmation of a transaction. To maintain data as extensive as the entire number of voters registered for such a U.S. presidential election, however, may cost millions. Online voting has been a hotly debated subject for years. Because of the immutability feature of blockchain, online voting has always been absolutely safe. In this article, we will examine the problems with current online voting and offer a suggestion for a system that makes use of the Ethereum network. Hackers may use strategies like spoofing and DDoS to influence the online voting process (distributed denial-of-service). Assaults on the internet would have a far bigger impact than strikes on the actual voting mechanism. Phase 2 will provide it access to the current web voting system as well as any potential security holes. Electronic voting may replace the need to interact with voters and keep a record of them at the polls. Based upon how the voting process was especially constructed, the result is entirely public and may be independently verified by the appropriate parties. The administrative time and cost for voting would be little compared to the huge amounts of money the state borrows on voting. Using smart contracts, criminals may ensure that their favoured candidate will win the election then only will they pay that voter their money. This might be prevented by using a way to encrypt the voting choice that can only be decoded by the administrator.

In the paper "Online Voting System Using Blockchain Mechanism" Dr. N. Sundarajulu , Mr. J. Ilanthendral and Lavanya R proposed our suggestion for leveraging block chain technology to address the problems with digital voting. We conducted an online vote before some hackers targeted our network (SQL Injection Attacks). The block chain will finally fix the issue for further electronic voting installations [24]. In this research, we investigate the implementation of a voting machines (e-voting) system using blockchain as a service. It offers an original, block chain-based electronic voting system through a case study. Together with Volatiles & Essent, the team created the system's architecture, design, and analysis.Voting is one of the many uses for block chain technology. Everything in the block chain is encrypted, making it simple to prove that perhaps the data was also not altered. Furthermore, the encryption technology prevents anyone from accessing all votes before even acquiring control of the whole service network.Permission public blockchains provide better performance and governance than public block chains. Since it takes less

time to update the rules throughout the network, they also are more cost-effective. Permission networks successfully use blockchain and make use of its decentralised nature for storage. Each voter will be given a unique username and password, that they can utilize to cast their vote for each candidate in every election. The software system provides voters with access to a list of candidates.The administrator has complete control of the system and is able to censor and delete any information that is unrelated to election rules. With the help of block chains, individuals will be able to interact and vote in local and international elections in new ways.

In their article "Blockchain Enabled E-Voting System," SriRaksha S Arun, Shibani, and others claim that the BEV really employs tamper-proof ID verification, intelligent fingerprints, and an encrypted key. It safeguards Multi-Party Computation because of features like transparency, decentralisation, irreversibility, and nonrepudiation (MPC). The documents, or blocks, that make up a blockchain must be linked together via cryptography.[10] It has characteristics like network decentralisation, enhanced security, and resilience. The system is composed of a client-server architecture and a blockchain-based mechanism. Voting requires a computer or a phone at the absolute least. Each voter is given a "wallet" with personal login details and a "virtual currency" that stands in for a chance to vote. Through the e-voting service, anyone may register to vote and take part in the elections. The e-voting technology uses a number of different blockchain nodes to carry out the vote. Every node contributes an activity to the system based on the correct contracts already in place.

Chapter 3

Methodolgy and Requirement Analysis

Our proposed model's prime concern is on the vote validation process. To make the validation fair, we have added multiple layers of validation as an extra security measure. Each set of the validator nodes will be assigned different roles to make the validation process efficient on a big margin.

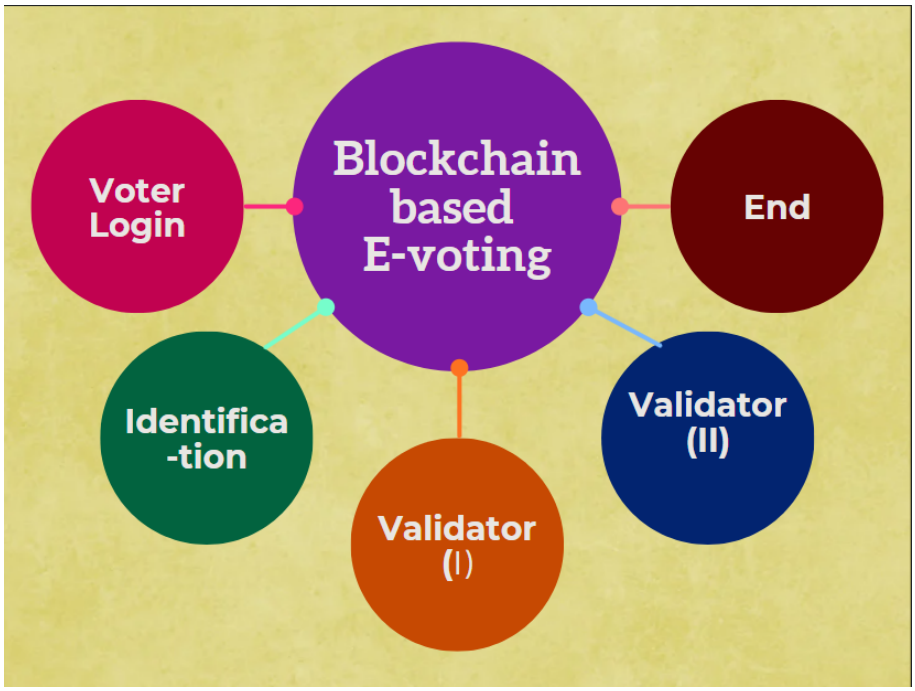


Figure 3.1: Basic map of Blockchain based E-voting

3.1 Smart Contract

Smart contracts are often used to automate the implementation of an agreement so that all parties can be certain of the result right away, without the need for any third parties. We can compare smart contracts with a simple computer program that is written in a language familiar by a computer and acts like a business logic among

the parties of an agreement and they are only executable when specific conditions are met.

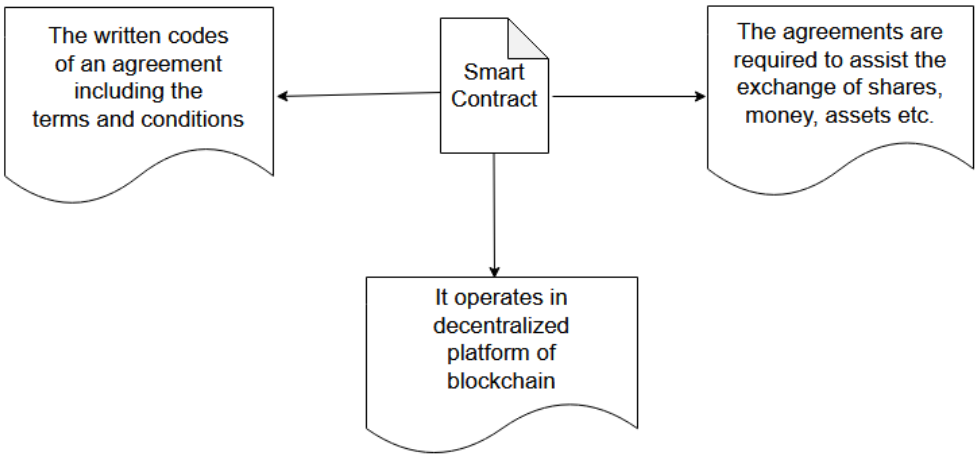


Figure 3.2: What a smart contract is

Smart contracts are gaining popularity day-by-day unlike traditional contracts. In traditional contracts, parties have to rely on a third party whom they need to trust and get the contract executed and to eliminate the dependency on such third parties (i.e Government, lawyers etc), smart contracts assists to do so. Moreover, full transparency is not available in traditional contracts whereas smart contracts provides it fully so that anyone among the parties can review the transactions executed by these.
For implementing our proposed model, we have designed a smart contract using blockchain which can make the validation process fair. In centralised voting system, it confronts a lot of problems at the time of tracking votes such as manipulation of identity as well as vote counting, biased decision-making and so on. That is why we have designed a smart contract to eliminate these issues. In this contract, specific terms and conditions are set such as no voter can vote with other voter's id, each vote should registered in a blockchain network, voter's age should be eligible etc. The validation will be done by the validators on the blockchain network in decentralized manner. Finally, each voter's vote will be recorded on the distributed ledger so that it cannot be manipulated.

3.2 Decentralization in Blockchain

Decentralization defines the method of distributing the power and authority to the participants of a network instead of one central authority. Blockchain offers this facility by which a company or platform that does not require the involvement of any third party as well as run with various decision-makers selected by using "Consensus" mechanism.

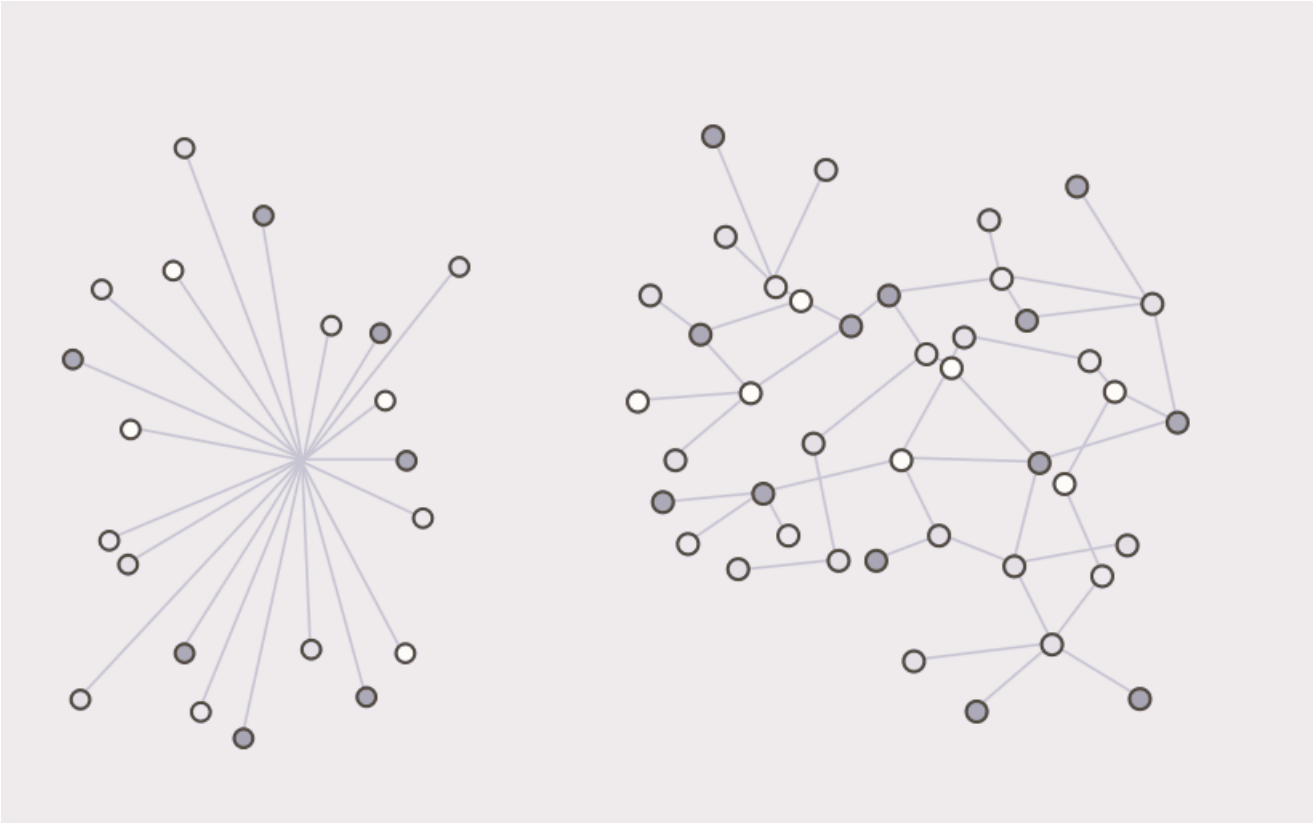


Figure 3.3: Centralized & Decentralized System

Decentralized systems are not controlled by a single leader unlike centralized systems where every user has to rely on a central authority who are in charge of all the operations on the system. Since control is divided in many nodes in distributed systems, so there exists no central server and that established the novel generation of ”DApps” (Decentralized Applications).

3.3 Decentralized Applications

Decentralized Applications are also known as ”DApps” are software programs which illustrates the newest progress of decentralization and these applications are designed on top of a blockchain platform and works in a peer-to-peer network. These applications need to fullfil some criteria as follows:

An open-source platform: First of all, the application need to be autonomous and no particular node should be in charge of its operations. Also, each alterations of the app has to be consensus-driven depending on the update provided by the participants [7].
Operations need to be secured: Secondly, to mitigate any kind of central-point-of -failure, the details of the operations by the application has to be stored in a decentralized blockchain to make it cryptographically secured [7].
Consensus driven: The application has to use some cryptographic algorithm, also known as consensus algorithm to generate crytographic token that can be considered as a proof-work of those who contributes to the applications (i.e miners) [7].

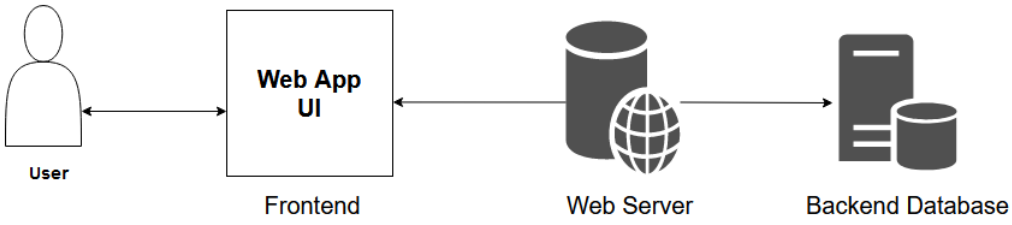


Figure 3.4: Workflow of a Centralized Application

Decentralized applications are more promising than centralized applications in terms of security, data integrity as well as efficient control on the app.

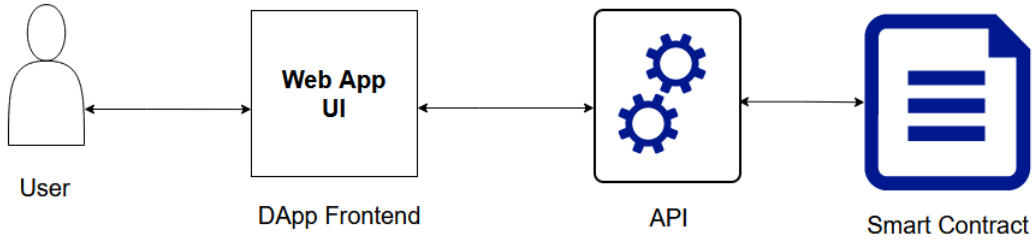


Figure 3.5: Workflow of a Decentralized Application

3.4 Distributed Ledger

To define the distributed ledger, we can compare it with a ledger that is expand across the network including all peers on the network where every peer takes a copy of the whole ledger. It is a type of database that is shared among all the participants of blockchain network so that they can keep track of transaction records. Distributed ledgers are secure and not tend to data manipulation and cyber attacks unlike central ledgers that has single point of failing.
For instance, "Bitcoin" is an example of highly famous distributed ledger that is implemented for paying via online with less trasaction cost to eliminate traditional online payment method. This technology is showing so much potential that it can make peopl's life easier in a matter of time. Similarly, "Ethereum" which is a famous distributed ledger that can assist the developers to build applications by introducing smart contracts. So, we can claim that "Distributed Ledger Technology" (DLT) will play a vital role in blockchain technology.

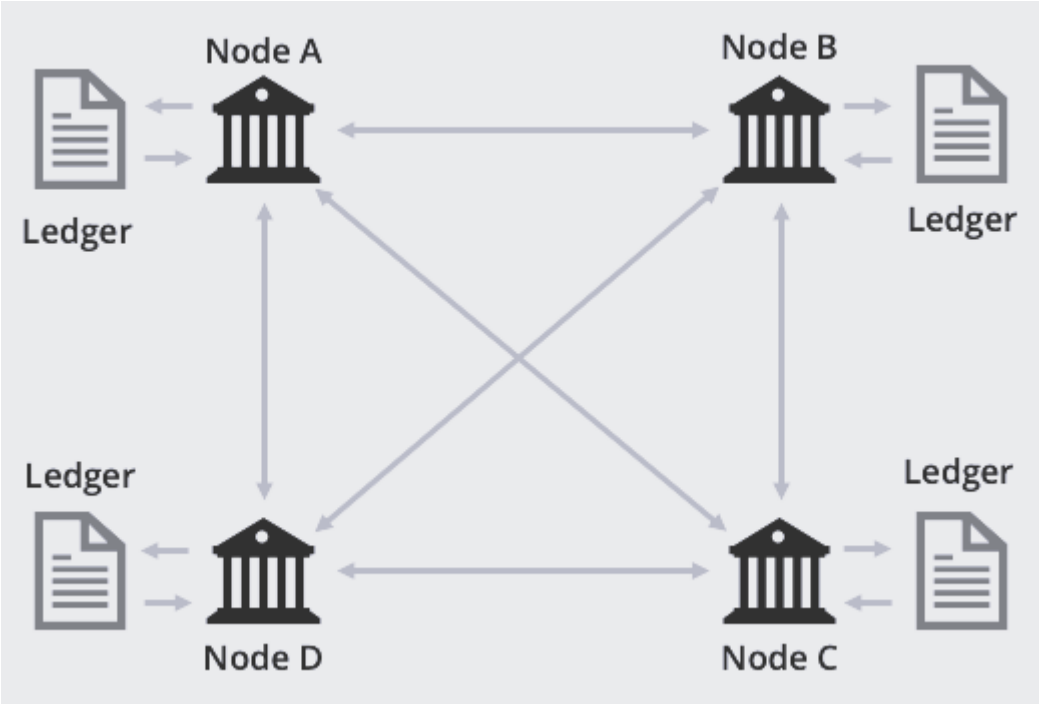


Figure 3.6: A Distributed Ledger

3.5 Ethereum & Ethereum virtual machine mechanism

Ethereum is a technology that is mainly based on blockchain. Blockchain makes the network decentralized. If we want to make a decentralized system, then we need a network which can run an application that is decentralized and that is where we need "Ethereum". Vitalik Buterin is the inventor of Ethereum. In Ethereum, we have an amazing concept which is EVM (Ethereum virtual machine). EVM is needed to run an application on ehtereum platform. To explain, when we want to run any software in java we need JVM (java virtual machine). In the same way, if we want to write software and want to run them on the Ethereum network, then we need that virtual machine. We often think that bitcoin and Ethereum are the same things but they are not. Both are different concepts. For instance, Bitcoin, which is more of cryptocurrencies. On the other hand, Ethereum is more for decentralized applications. We often have a question about the cryptocurrency in Ethereum because we have bitcoin. But Ethereum is not a cryptocurrency, it is a platform. In this platform, if we want to use cryptocurrency, we have ether. And to run a decentralized application we do need ether.
We have probably heard the term EVM everywhere now. In fact, way more projects use it other than just Ethereum even though it was built for Ethereum. Avalanche, polygon, binance smart chain and many other chains use this highly specialized blockchain platform. Technically, EVM is a cloud computer that is operated by all the nodes that contribute to it. This means that it is not a single computer somewhere. It is the accumulation of thousands of computers around the world. In reality, these computers are made up and operated by people like us. Each computer on the ethereum network runs a piece of software that is basically just computing

the output of a smart contract. This cloud computer EVM has many similar parts to a real computer such as memory and parts specialized for computing numbers. It is different though from a real computer because it does not need a monitor or keyboard. Smart contract codes written by developers is what the EVM process succeeds. The most common programming language in EVM is "Solidity". This language allows developers to write code they can understand and make predictions on how the code will work.
Solidity is not the code that the EVM reads and processes though. EVM reads something called byte-code which is basically just a bunch of ones and zeros. We already know that computers do math in binary. When a developer writes a smart contract they must compile it. This is a term meaning they turn the solidity language code which is human readable and understandable into byte code, so that the EVM can understand it and read it and this is mostly because humans are not really good at reading a bunch of ones and zeros. So, we came up with solidity for us to be able to read and write code much more effectively. Essentially this compiling process is just a way to translate human code to machine code as it mentioned earlier. This translation process does leave us open to vulnerabilities. In between solidity and byte-code there is a middle theoretical language called opcode which is literally a language that shows operational code or rather instructions. The instructions that the EVM must take to perform smart contracts. One really interesting thing about blockchain that use the EVM is that it is really easy to move any project or application from one chain to another.They both use EVM means if we have an application on a polygon it is very easy to move it over phantom or avalanche. We can move our project around where we like it to be. The EVM processes transactions sequentially one by one. That means it doesn't do many things all at a time and if a process does not work for whatever reason. For example, if we are trying to send someone one if but we actually only have three quarters of an if in our account then the transaction is skipped each time the EVM runs a transaction. We say that the state of the Evm is updated since the Evm is really just a collection of data of information each transaction that the Evm processes simply changes that data state. If one thing changes in the EVM, if just one number changes then we say that the state of the EVM has changed. Each transaction changes the state of the blockchain and if we wanted we could make a copy of the blockchain and roll it back to any state in the past that we wanted to. In short, what this means is that each time the EVM changes or processes a translation there is always a complete record of what the EVM consisted of before the transaction and after the transaction and this list of transactions is what we call the blockchain.

Chapter 4

Blockchain Based Secured Voting System Architecture

4.1 Proposed Architecture

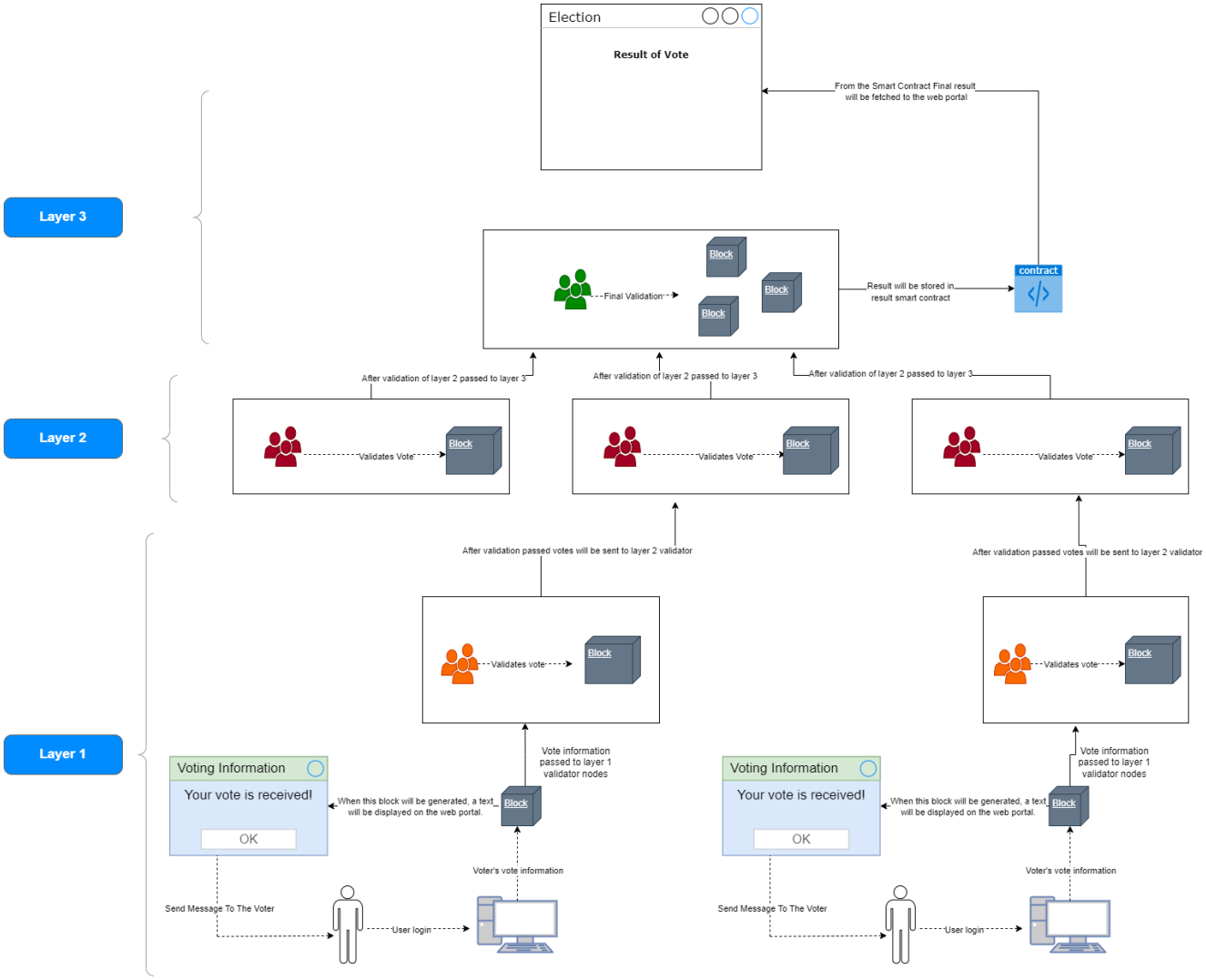


Figure 4.1: Workflow of Proposed Architecture

Once a voter has logged in with their credentials, a voting page will appear on the screen, displaying a list containing the candidates. Voters will choose their one desired candidate from the list and confirm their vote. After submitting a voter's vote, a message will be sent to the phone number of the voter that "Your vote is received!".

After placing the vote by the voter, a block will be created. Which then will be sent to validator nodes of layer 1. Validator nodes are selected randomly by using the consensus mechanism which is written as codes in the smart contract. Ethereum uses Proof-Of-Stake (POS) as consensus mechanism to select validator nodes. In our system, validator nodes will receive a single block for a single voter. Validator node will validate the vote under the predefined conditions. After successful validation, the vote block will be sent to the validator nodes of layer 2.

Then we have a second layer, where there will be certain number of validator nodes who receives the vote blocks from the first layer and validates them using a predefined set of conditions. Validators for this layer are also selected randomly by using Proof-Of-Stake (POS) consensus mechanism. After successful validation, the vote blocks will be sent to the third layer which is the top most layer of our architecture.

Lastly, the third layer is responsible for further validation of the votes based on certain conditions. After the successfull validation process of layer 2, the validation phase of top most layer will be performed by this layer's validator nodes. This layer conducts a final validation of the votes and calls the smart contract where the voting results will be saved and analyzed. The results will then be published on the website for maintaining the transparency.

4.2 Advantages of Using Blockchain Technology

Using blockchain technology for an electronic voting system has several benefits over the existing ballot paper-based voting system. In this section, we will take a look at a few of those essential characteristics:

Eliminate The Use of Paper Ballots: In the past, elections relied on paper ballots, where voters' votes were cast through the ballot and were physically counted, which presented logistical challenges because of the large number of ballots that needed to be stored and managed.

Less Human Error due to the Involvement of Technology: The number of people needed to cast a vote in an electronic election is much lower than in a traditional election with paper ballots. As a result, the chances of getting human errors are reduced.

Voting Systems That Cannot be Tampered With: Ballots cannot be tampered with owing to blockchain's immutability and the decentralized structure of electronic voting using a blockchain-based ballot counting system [19]. A vote that has already been cast cannot be undone.

Transparency and Integrity: Distributed ledger technologies like blockchain can increase the reliability of data storage by making it easier to verify transactions than with a central repository like a database [5]. If electronic votes are recorded in a distributed ledger like the blockchain, then voting systems based on those ledgers can be trusted to accurately reflect the will of the voters.

The Speed of Execution has Been Improved: Time spent on registering voters, casting ballots, and tallying results has been streamlined by the use of electronic management.

Cost-Effectiveness of Expenditure: Paper ballot costs (such as printing and marking), human labor costs (for management, counting, security, etc.), and logistical expenses (such as transporting and storing the ballots) are minimized because of this approach.

Allows Access From Remotely: Like before, there is no need to go to the polling station physically to cast a vote. Instead, they can cast votes from anywhere they are. Initiating a blockchain transaction with his/her credentials is how a voter can put his vote on record.

Privacy of Voters: Voters' identities and the candidates for whom they cast ballots should remain concealed in any voting system. Voter privacy is protected by blockchain technology's anonymous account address [13]. To protect user anonymity, blockchain employs a pseudo-identity system in which every node can generate a large number of public keys to serve as the pseudo-identity.

Distributed Denial of Service (DDoS) Attacks: Due to the decentralized nature of the data recorded in blockchains, every miner has a complete copy of the blockchain stored on their computer. Even if a malicious actor disables a node with a distributed denial of service attack (DDoS), the rest of the system will continue to function normally. The blockchain is always consistent since the node synchronizes it everytime it comes back online.

Auditability of Vote: Blockchain's public distributed ledger stores all relevant data and leaves a detailed record of blocks that can be used to verify the authenticity of votes cast [14] [11].

Validation of Vote: Every time a voter casts a ballot in the blockchain, he or she must use their private key to confirm the ballot and complete the transaction. A transaction is verified by a miner prior they initiate the mining process. Only a certain amount of verified transactions are included for each block mining.

4.3 Proposed Model

In this section, We focus on providing detailed description of the architecture of the model. Bangladesh Election Commission, compressed and publicly referred to as EC is the principal authority and layer of top level among our three layer architecture.

The election commission supervises the other two layers of blockchain networks which are respectively Division layer(mid layer) and District layer(ground layer).

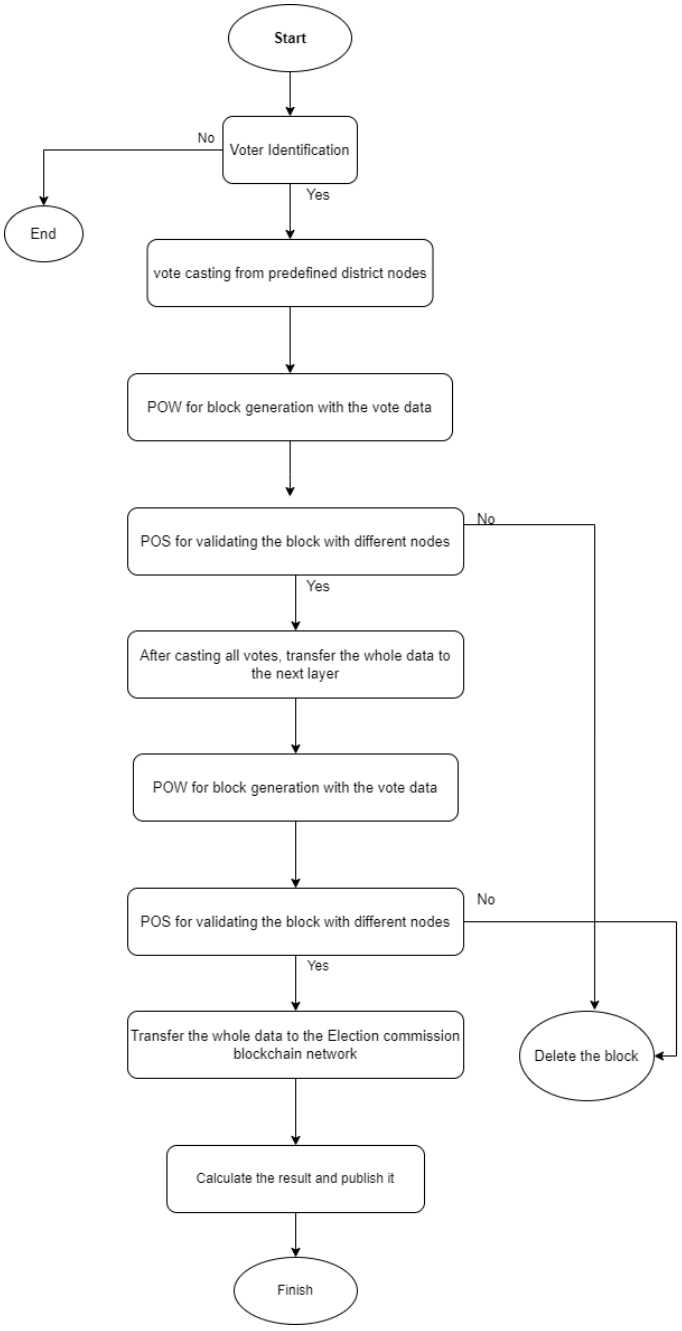


Figure 4.2: End-To-End Secure Multi Layer Electoral Process Architecture

The validator nodes in each layer determines the timestamp for block creation on the blockchain network, which indicates how long each layer will be active. In initial layer, there will be sixty-four blockchain networks, each of which will represent one of the electoral commission's sixty-four districts. Additionally, in middle layer, there will be eight blockchain networks, each of which will reflect one of the electoral commission's eight divisions. The division layer, which operates the ground layer, is represented at the top level of the ground layer, and the election commission, which is the final blockchain network, is represented at the top level of the division layer.

4.3.1 Activity Diagram

Here is the activity diagram of our proposed system:

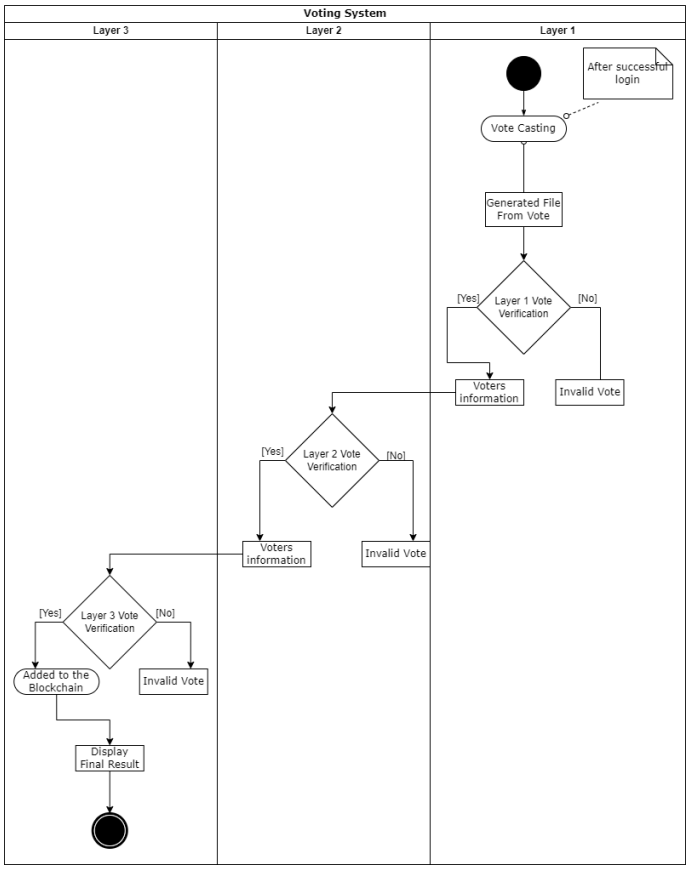


Figure 4.3: Activity Diagram of Our Proposed System

4.3.2 Layer 1 validator working plan

As we have previously mentioned, there are three layers to perform vote validation and at the ground level we will have district layers which are part of the eight division layers. When the Election commission start the voting process, layer one will initiate firstly. Layer one will consists of sixty-four sets of validator nodes. Each set of validator node will handle the validation process for each of the district of Bangladesh. Specific set of validator nodes will validate those voter's vote which is under their area and all of this will be predefined in the smart contract.
After the successful login of the voter, voter can cast his / her vote for their desired candidate and this vote data will be converted into a block which will be received by the specific set of validator nodes. Validator nodes will validate the vote based on this conditions that are written as codes in the smart contract:

- Is the voter alive or not?
- Voting area is right or not?
- Age >= 18 years ?

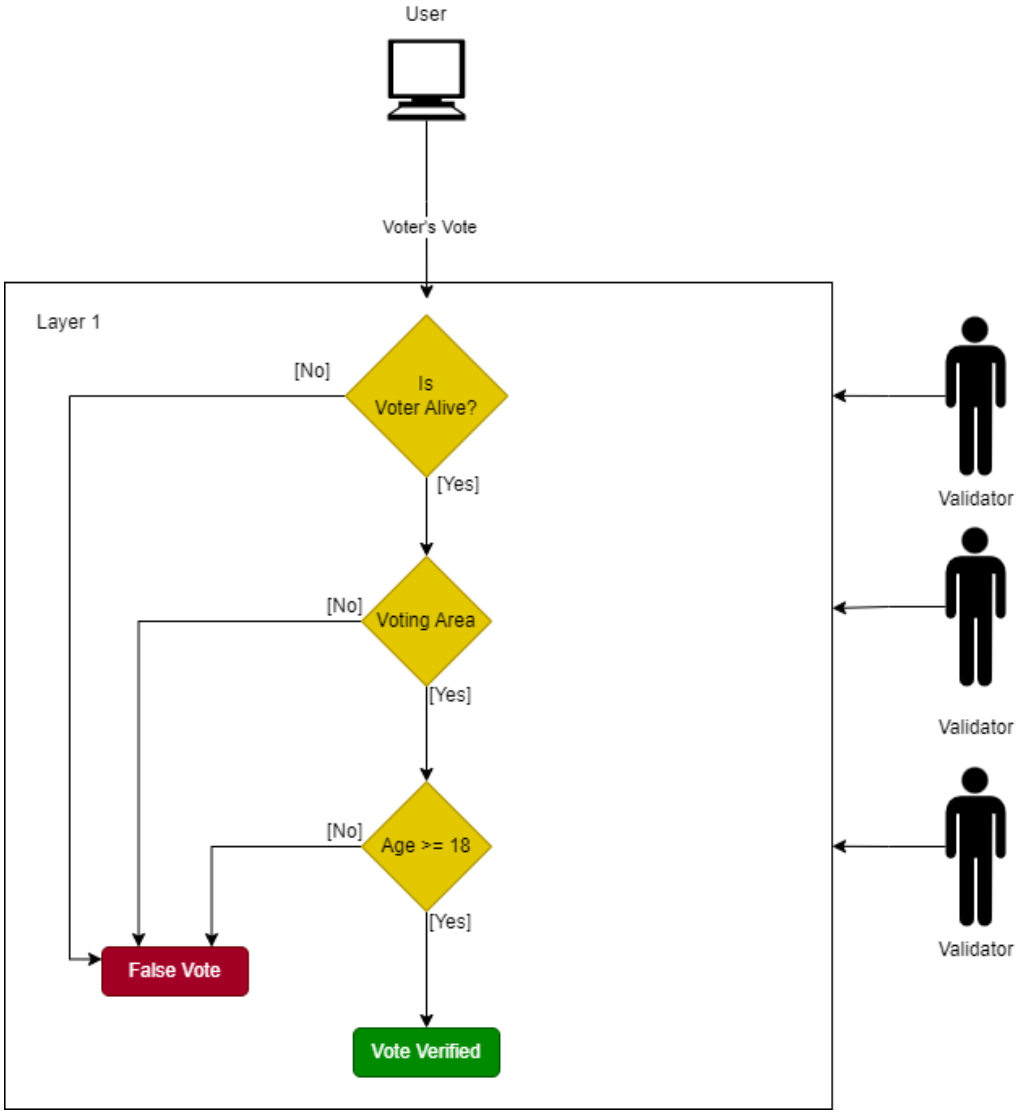


Figure 4.4: Layer 1 validator Working Plan

When this conditions will be fulfilled, only then the vote block will be sent to the Layer 2.

4.3.3 Layer 2 validator working plan

When the time limit of layer 1 will be over, layer 2 will be activated and the validation process will begin against each of the votes. In this phase, there will be in total eight sets of validator nodes which will handle the validation process for the eight divisions of Bangladesh. Each set of validator nodes will begin checking the vote blocks received from their respective sets of validator nodes from layer 1.
Validators will firstly recheck the validation process of layer 1, since there should not be any false vote which should not be passed. When a vote satisfies this condition, the validator nodes will check whether the voting area of the voter and the voting area of the chosen candidate is similar or not. If this condition is not satisfied, the vote block will not be sent to the next layer, otherwise the vote block will be sent to the next layer.

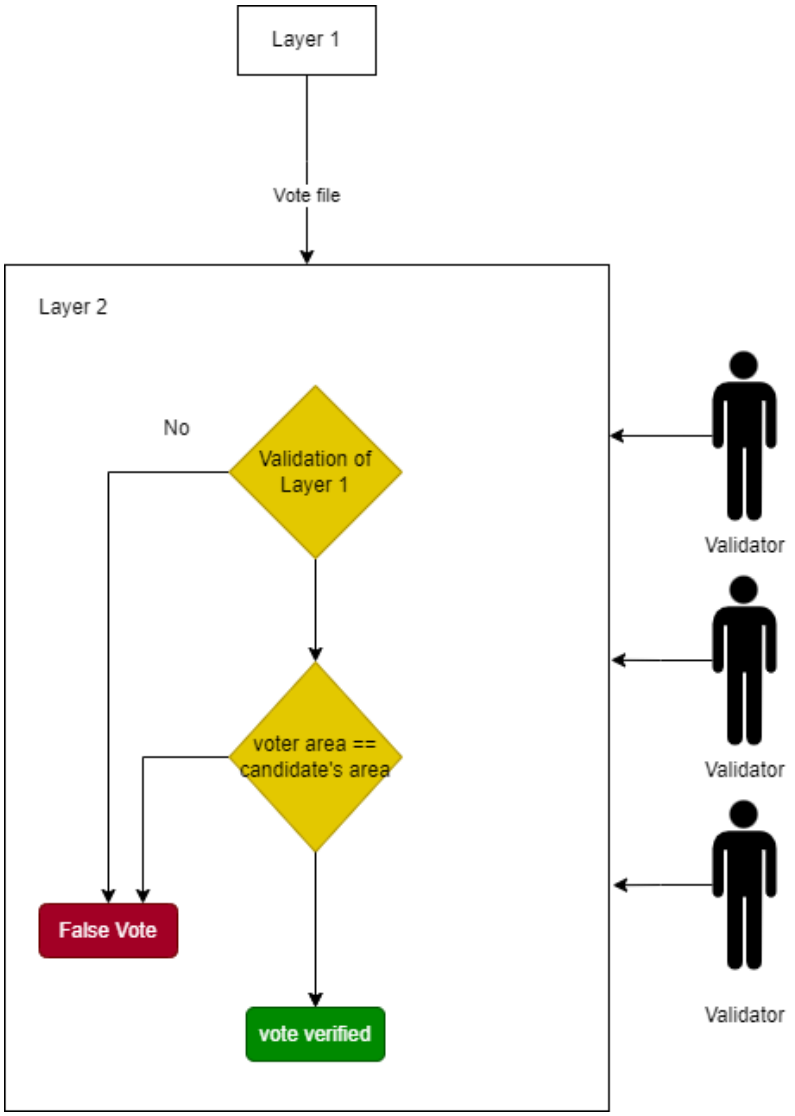


Figure 4.5: Layer 2 validator Working plan

4.4 Implementation

For implementing the model we propesd, we have build a smart contract where all the codes are written based on the terms and condition of e-voting. We have used Visual Studio Code (VS Code) as IDE to write our codes.

4.4.1 Solidity

To write our smart contract, we have used Solidity programming language which is highly used programming language by the blockchain developers. It is a contract-oriented language where the word contract can be compared with classes that we use in other programming languages and the syntax of it are much like JS (JavaScript) and C.

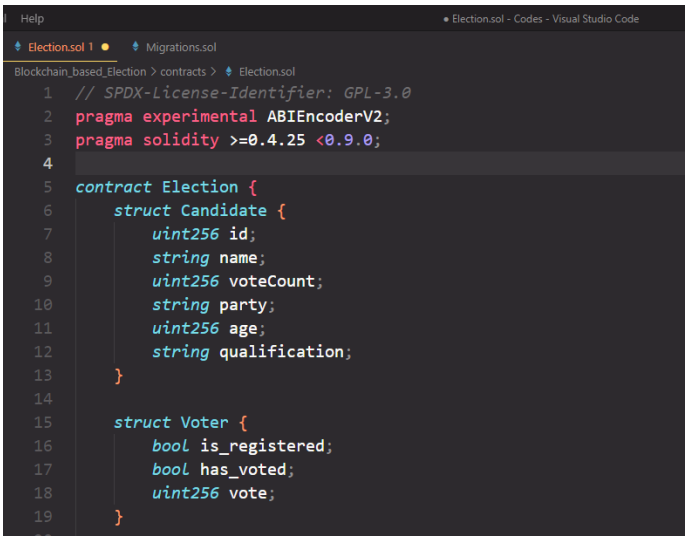


Figure 4.6: Solidity Programming Language

4.4.2 Ganache

To operate our smart contract in decentralized manner, we have used "Ganache" which is basically a private ethereum blockchain environment that supported us to emulate the ethereum blockchain in our local machine and that assisted us to interact with the smart contract which we have build. To mine locally, it uses an user friendly GUI(Graphical User Interface) for making the testing easy.
It assits to set up a local ethereum blockchain for testing smart contracts and it provides more facilities as compared to Remix IDE.

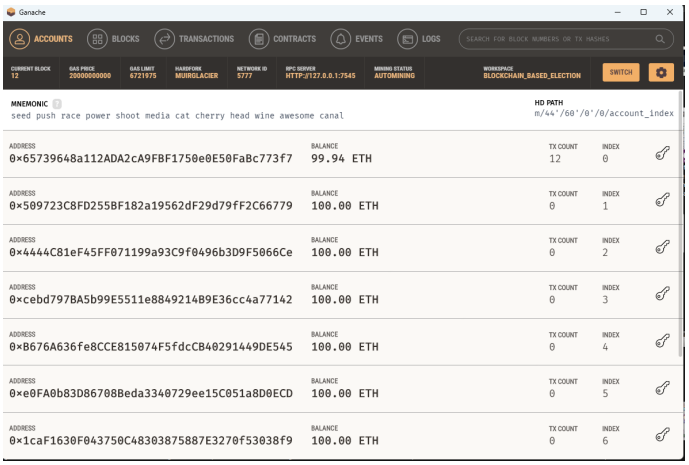


Figure 4.7: Ganache Window

4.4.3 Remix

It is an online-based development and testing environment for smart contracts. In this IDE, smart contracts can be debugged, deplyoed as well as tested [7].

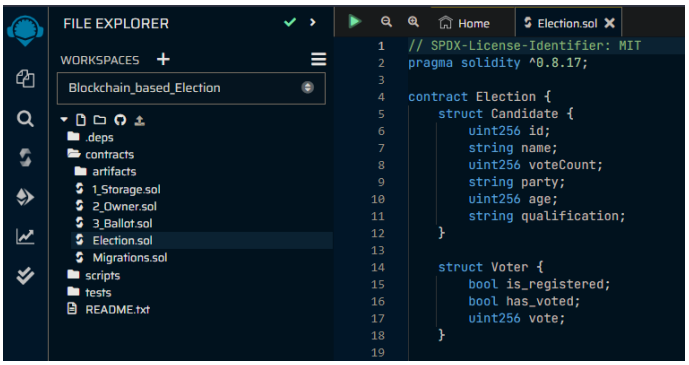


Figure 4.8: Remix Window

4.4.4 Metamask

Metamask is an online extension that is used in Google Chrome and Mozilla Firefox browsers. It is basically a cryptocurrency-wallet which helps to interact with the DApps(Decentralized Applications). It allow users to use their ethereum wallet via phone application as well as browser extension. This wallet participate as a verifier at each transaction make in blockchain. During every transaction a window pops-up to the participants to confirm the operation or deny it.

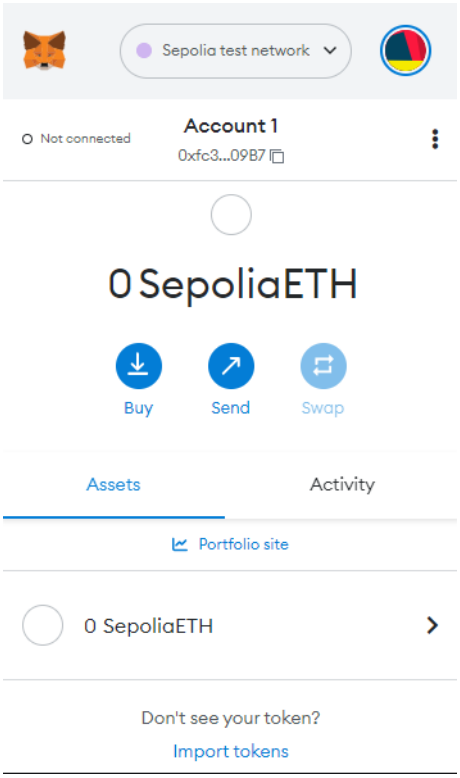


Figure 4.9: Metamask Window

4.4.5 Truffle

Truffle is a popular testing framwork as well as a development environment that uses EVM (Ethereum Virtual Machine) for blockchains. The goal of it is to make developer's life easier by assisting them in each phase of development such as providing initial application template to a local blockchain for testing the built DApp. Also, it is used to deploy the smart contracts.

4.4.6 ReactJS

Reactjs is a JavaScript library for building user interfaces, and it allows developers to build reusable UI components as well as manage the state of the application. It is used to create web applications that update in real-time without a page refresh.

4.4.7 TypeScript

TypeScript is a typed superset of JavaScript that compiles to plain JavaScript. It adds optional types, classes, interfaces, and other features to JavaScript, making it more maintainable and scalable.

4.4.8 Frontend building

For building the front-end, we have used ReactJs "& TypeScript.

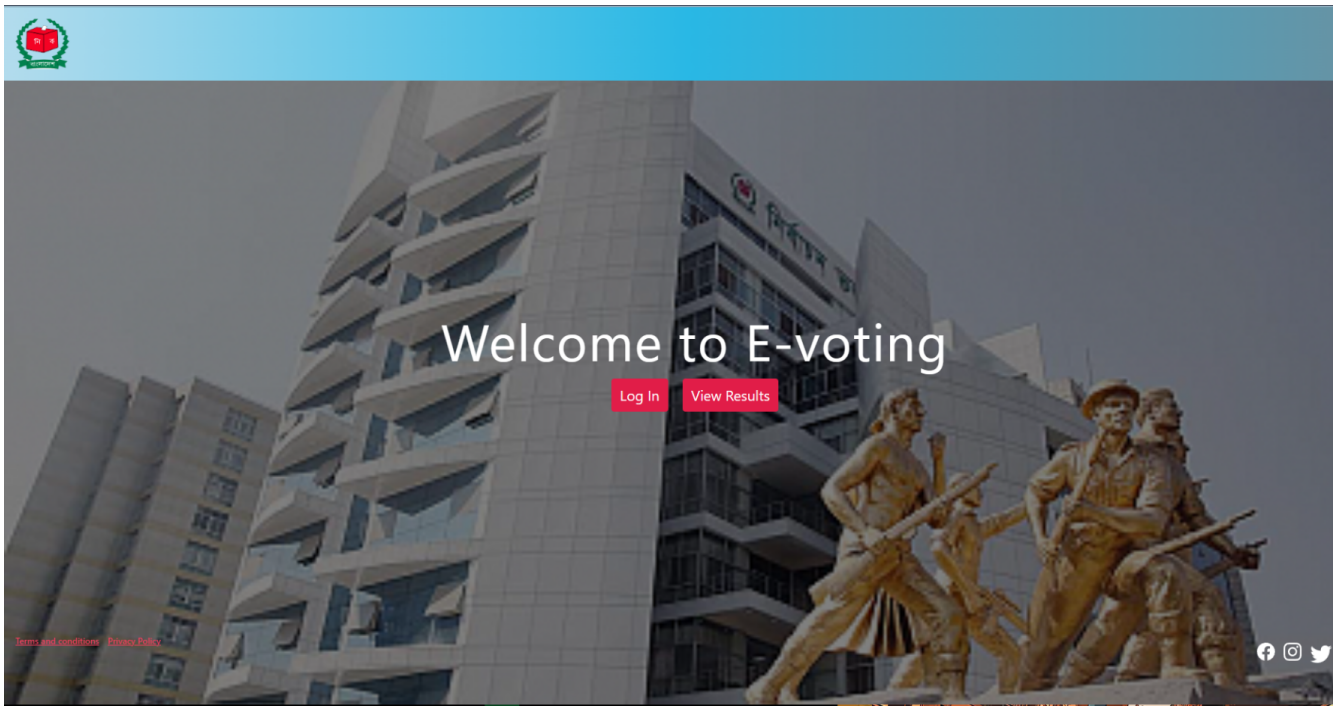


Figure 4.10: Web UI of E-voting

Using Reactjs and TypeScript together can provide several benefits for building a website. Some of these benefits include:

- **Improved productivity:** TypeScript's type checking and other features make it easier to catch errors early in the development process, which can save time and reduce the likelihood of bugs in the final product.

- **Better scalability:** React's component-based architecture and TypeScript's support for large projects make it easier to scale a website as it grows.

- **Improved maintainability:** TypeScript's type checking and other features make it easier to refactor and maintain a website's code-base over time.

- **Improved performance:** React's virtual DOM improves the performance of a website by minimizing the number of DOM updates and re-renders.

- **Better development experience:** TypeScript's type checking and other features can make development a more pleasant experience by reducing the number of runtime errors.

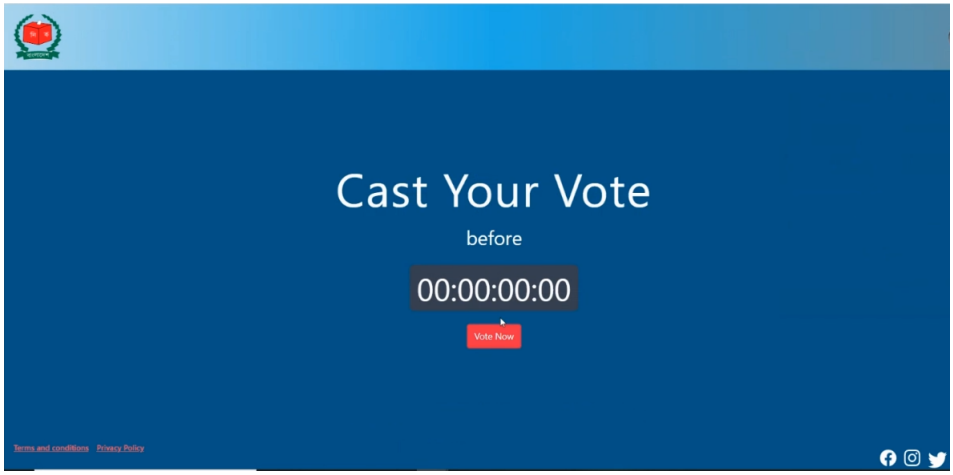


Figure 4.11: Web UI of Vote casting Page

4.5 Backend building

For building the backend of our proposed architecture, we have build a smart contract by using solidity programming language.

4.5.1 Pseudo Code of Smart Contact

Here are the Pseudo codes of the smart contract that we have build to implement our proposed model:

```
1  // SPDX-License-Identifier: GPL-3.0
2  pragma solidity >=0.4.25 <0.9.0;
3  library Types {
4          struct Voter {
5                  uint256 aadharNumber; // voter unique ID
6                  string name;
7                  uint8 age;
8                  uint8 stateCode;
9                  uint8 constituencyCode;
10                 bool isAlive;
11                 uint256 votedTo; // NID number of the candidate }
12         struct Candidate {
13 // Note: If we can limit the length to a certain number of bytes,
14 // we can use one of bytes1 to bytes32 because they are much cheaper
15                 string name;
16                 string partyShortcut;
17                 string partyFlag;
18                 uint256 nominationNumber; // unique ID of candidate
19                 uint8 stateCode;
20                 uint8 constituencyCode; }
```

Figure 4.12: Smart Contract Pseudo Code of - I

```
21         struct Results {
22                 string name;
23                 string partyShortcut;
24                 string partyFlag;
25                 uint256 voteCount; // number of accumulated votes
26                 uint256 nominationNumber; // unique ID of candidate
27                 uint8 stateCode;
28                 uint8 constituencyCode; } }
```

Figure 4.13: Smart Contract Pseudo Code of - II

```
1  // SPDX-License-Identifier: GPL-3.0
2  pragma solidity >=0.4.25 <0.9.0;
3  import "./Types.sol";
4  contract Ballot {
5          Types.Candidate[] public candidates;
6          mapping(uint256 => Types.Voter) voter;
7          mapping(uint256 => Types.Candidate) candidate;
8          mapping(uint256 => uint256) internal votesCount;
9          address electionChief;
10         uint256 private votingStartTime;
11         uint256 private votingEndTime;
12 /**
13 * @dev Creating a new ballot to choose one of 'candidateNames'
14 * @param startTime_ When the voting process will start
15 * @param endTime_ When the voting process will end */
16 constructor(uint256 startTime_, uint256 endTime_) {
17         initializeCandidateDatabase_();
18         initializeVoterDatabase_();
19         votingStartTime = startTime_;
20         votingEndTime = endTime_;
21         electionChief = msg.sender; }
22 /**
23 * @dev Get candidate list.
24 * @param voterNidNumber NID number of the current voter to send the relevent candidates list
25 * @return candidatesList_ All the politicians who participate in the election
   */
```

Figure 4.14: Smart Contract Pseudo Code of - III

```
26 function getCandidateList(uint256 voterNidNumber)
27   public
     view
     returns (Types.Candidate[] memory) {
28         Types.Voter storage voter_ = voter[voterNidNumber];
29         uint256 _politicianOfMyConstituencyLength = 0;
30 for (uint256 i = 0; i < candidates.length; i++) {
31         if (
32                 voter_.stateCode == candidates[i].stateCode &&
                  voter_.constituencyCode == candidates[i].constituencyCode
           )
33 _politicianOfMyConstituencyLength++;  }
34 Types.Candidate[] memory cc = new Types.Candidate[](
35 _politicianOfMyConstituencyLength  );
36 uint256 _indx = 0;
37 for (uint256 i = 0; i < candidates.length; i++) {
38     if (
           voter_.stateCode == candidates[i].stateCode &&
           voter_.constituencyCode == candidates[i].constituencyCode
       )
39 {
           cc[_indx] = candidates[i];
           _indx++;  } }
40 return cc; }
```

Figure 4.15: Smart Contract Pseudo Code of - IV

```
41  /**
42  * @dev Get candidate list.
43  * @param voterNidNumber NID number of the current voter to send the relevent candidates list
44  * @return voterEligible_ Whether the voter with provided aadhar is eligible or not */
45  function isVoterEligible(uint256 voterNidNumber)
46   public
        view
        returns (bool voterEligible_)
      {
47  Types.Voter storage voter_ = voter[voterNidNumber];
48  if (voter_.age >= 18 && voter_.isAlive) voterEligible_ = true;  }
49  /**
50  * @dev Know whether the voter casted their vote or not. If casted get candidate object.
51  * @param voterNidNumber NID number of the current voter
52  * @return userVoted_ Boolean value which gives whether current voter casted vote or not
53  * @return candidate_ Candidate details to whom voter casted his/her vote */
54  function didCurrentVoterVoted(uint256 voterNidNumber)
55  public
        view
        returns (bool userVoted_, Types.Candidate memory candidate_) {
56  userVoted_ = (voter[voterNidNumber].votedTo != 0);
57  if (userVoted_)
            candidate_ = candidate[voter[voterNidNumber].votedTo];  }
```

Figure 4.16: Smart Contract Pseudo Code of - V

```
58  /**
59  * @dev Give your vote to the candidate.
60  * @param nominationNumber Nid Number of the candidate
61  * @param voterNidNumber Nid Number of the voter to avoid re-entry
62  * @param currentTime_ To check if the election has started or not */
63  function vote(
        uint256 nominationNumber,
        uint256 voterNidNumber,
        uint256 currentTime_ )
64  public
        votingLinesAreOpen(currentTime_)
        isEligibleVote(voterNidNumber, nominationNumber) {
65  // updating the current voter values
        voter[voterNidNumber].votedTo = nominationNumber;
66  // updates the votes the politician
        uint256 voteCount_ = votesCount[nominationNumber];
        votesCount[nominationNumber] = voteCount_ + 1; }
67  function getVotingEndTime() public view returns (uint256 endTime_) {
68  endTime_ = votingEndTime; }
69  function updateVotingStartTime(uint256 startTime_, uint256 currentTime_)
70   public
        isElectionChief {
71  require(votingStartTime > currentTime_);
        votingStartTime = startTime_; }
```

Figure 4.17: Smart Contract Pseudo Code of - VI

```
72  function extendVotingTime(uint256 endTime_, uint256 currentTime_)
73  public
        isElectionChief {
74  require(votingStartTime < currentTime_);
        require(votingEndTime > currentTime_);
        votingEndTime = endTime_; }
75  function getResults(uint256 currentTime_)
76  public
        view
        returns (Types.Results[] memory) {
77  require(votingEndTime < currentTime_);
78  Types.Results[] memory resultsList_ = new Types.Results[](
            Candidates.length );
79  for (uint256 i = 0; i < candidates.length; i++) {
80   resultsList_[i] = Types.Results({
81  name: candidates[i].name,
82  partyShortcut: candidates[i].partyShortcut,
83  partyFlag: candidates[i].partyFlag,
84  nominationNumber: candidates[i].nominationNumber,
85  stateCode: candidates[i].stateCode,
86  constituencyCode: candidates[i].constituencyCode,
87  voteCount: votesCount[candidates[i].nominationNumber] }); }
88  return resultsList_; }
```

Figure 4.18: Smart Contract Pseudo Code of - VII

```
89  modifier votingLinesAreOpen(uint256 currentTime_) {
90  require(currentTime_ >= votingStartTime);
100 require(currentTime_ <= votingEndTime); _; }
101 modifier isEligibleVote(uint256 voterNid_, uint256 nominationNumber_) {
102 Types.Voter memory voter_ = voter[voterNid_];
103 Types.Candidate memory politician_ = candidate[nominationNumber_];
104  require(voter_.age >= 18);
105 require(voter_.isAlive);
106 require(voter_.votedTo == 0);
107 require(
        (politician_.stateCode == voter_.stateCode &&
          politician_.constituencyCode == voter_.constituencyCode) ); _ }
108  modifier isElectionChief() {
109 require(msg.sender == electionChief);  _; }
110 /**
111 * Dummy data for Candidates
112 * In the future, we can accept the same from construction,
113 * which will be called at the time of deployment */
```

Figure 4.19: Smart Contract Pseudo Code of - VIII

Chapter 5

Result Analysis

5.1 Final vote verification and publication of voting result

Figure 5.1: Web UI of Party selection

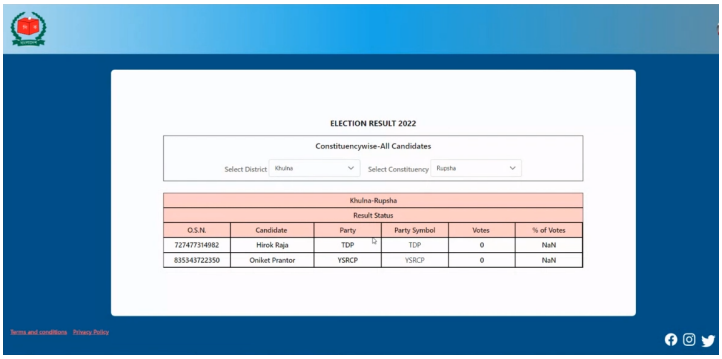


Figure 5.2: Result Window

5.2 Cost Analysis

In our system, we are using a public blockchain. Economically, public blockchains offer a wide range of advantages, considering they are fully decentralized and easily accessible to everyone. Those may be slower than other blockchain networks, but

they are highly secure for higher nodes and decentralization, reducing the risks of data breaches. The cost of blockchain development can be divided into consulting, designing, development, quality assurance, and maintenance cost, where 10 percent could be allocated for consulting, 15 for design, 25 for quality assurance, and the rest 50 percent for development. A simple blockchain-based system usually costs approximately $20,000 to $60,000 and can reach up to $200,000 or more.

The value and utility of cryptocurrencies are rapidly increasing. As we are currently using Ethereum networks that are free. Thus, we just need a digital wallet and cryptocurrencies to make the transaction, and we are using Ether as cryptocurrency. There is no need for governments to purchase existing cryptocurrency; instead, they can create their own. The resulting cost savings will be substantial. In our system, a transaction will happen at a minimal gas fee or gas cost, and the storage requirement is also minimal.

5.3 Difficulties that are being faced for Blockchain-based electronic voting system

Difficulties that are being faced for Blockchain-based electronic voting system:

Verification of voters: A difficult task is verifying the voter. Either a list of eligible voters must be input into the system ahead of time, or the voter must have some sort of unique reference id that can be used to authenticate their identity.

Shared Key Management: Distributing secret passcodes to all eligible voters is another difficult task. The organizer may be able to fix this problem by using a secure channel to send out the passcode, such as the organization's official email domain or a personal RSA.

Adoption: Voters and elected officials may oppose blockchain-based electronic voting systems because they may be skeptical of the technology or unwilling to alter long-standing voting procedures.

Interoperability: Integrating your new system with the government's already established voting procedures and infrastructure can be a challenge.

Regulation and legal compliance: It can be difficult to ensure that the system follows all applicable laws and regulations, especially given the large variety of these that exist around the world.

High Power Consumption: Extensive computing for block mining is the foundation of the blockchain's success. By adjusting the difficulty of each block to the level of risk associated with its use, performance may be maximized.

Phishing Attack: An adversary can conduct a phishing attack against an e-voting system by transmitting a fake smart contract address along with the application binary interface (ABI) [26].

Chapter 6

Conclusion and Future Work

All political regimes use elections as a symbol of democracy since they are an integral part of the democratic political process. Manipulation for own benefit is a common scenario in an election. With our proposed system, we try to ensure that every voter in Bangladesh can have faith in a decentralized, distributed, and transparent voting technology. This system seeks to address the problems with both paper-based voting and Electronic Virtual Machines. As there requires a lot more paper which is made up of cellulose, to be specific trees for traditional paper-based voting, our system ensures to lessen the usage of paper, which indirectly conserves trees. We are hoping for a better future for voting.

The goal of this research is to analyze the various techniques of implementation of blockchain technology and find out an efficient way to implement blockchain in e-voting so that it can resolve the current limitations and shortcomings of e-voting to ensure transparency, anonymity, scalability along with privacy and encourage to use blockchain-based e-voting in wider level. By our proposed scheme, to ensure an additional level of security, the Ethereum blockchain platform is prioritized over the hyper-ledger fabric, and to ensure privacy, Keccak- 256 encryption method is used.

Moreover, we can use randomized question sessions for voter identification, where voters will be required to answer random questions based on their identity. However, blockchain is still in its early stages, and it is such a vast topic that a lot more studies are required to incorporate e-voting using blockchain to eliminate all the existing limitations and replace the existing analog voting system with a digital decentralized blockchain implemented e-voting system.

Our system is designed in software-based architecture. In the future, further improvements can be made in two ways: a better voter and candidate authentication process and, secondly, integrating hardware with our software-based system.

As for now, our research is mainly focused on the vote-casting process. In the future, the voter and the candidate authentication process will be our next scope of work, where the voter and candidate will be verified before the time period of the vote-casting process. Thus it will reduce the workload of the vote-casting process.

To conclude, we can use KYC (Know Your Customer), such as biometric finger-

prints, as well as OCR (Optical Character Recognition), for voter identification. In OCR, identification can be made by making the voter hold their NID card in front of a webcam so that it can be scanned as a document of proof.

Bibliography

[1] S. Verba and N. H. Nie, *Participation in America: Political democracy and social equality*. University of Chicago Press, 1987.

[2] B. Engelen, "Why compulsory voting can enhance democracy," *Acta politica*, vol. 42, no. 1, pp. 23–39, 2007.

[3] S. Nakamoto, "Bitcoin whitepaper," *URL: https://bitcoin. org/bitcoin. pdf-(: 17.07. 2019)*, 2008.

[4] H. Jonker and W. Pieters, "Anonymity in voting revisited," in *Towards Trustworthy Elections*, Springer, 2010, p. 2.

[5] G. Zyskind, O. Nathan, *et al.*, "Decentralizing privacy: Using blockchain to protect personal data," in *2015 IEEE Security and Privacy Workshops*, IEEE, 2015, pp. 180–184.

[6] A. Barnes, C. Brake, and T. Perry, "Digital voting with the use of blockchain technology," *Team Plymouth Pioneers-Plymouth University*, 2016.

[7] I. Bashir, *Mastering Blockchain*. Packt Publishing, 2017, p. 57, ISBN: 9781787125445. [Online]. Available: https://books.google.com.bd/books?id=dMJbMQAACAAJ.

[8] J. Fortin-Rittberger, P. Harfst, and S. C. Dingler, "The costs of electoral fraud: Establishing the link between electoral integrity, winning an election, and satisfaction with democracy," *Journal of Elections, Public Opinion and Parties*, vol. 27, no. 3, pp. 350–368, 2017.

[9] N. Prusty, *Building Blockchain Projects*. Packt Publishing, 2017, pp. 26–28, ISBN: 9781787122147. [Online]. Available: https://books.google.com.bd/books?id=oq1EvgAACAAJ.

[10] K. M. Khan, J. Arshad, and M. M. Khan, "Secure digital voting system based on blockchain technology," *International Journal of Electronic Government Research (IJEGR)*, vol. 14, no. 1, pp. 53–62, 2018.

[11] M. Pawlak, J. Guziur, and A. Poniszewska-Marańda, "Voting process with blockchain technology: Auditable blockchain voting system," in *International Conference on Intelligent Networking and Collaborative Systems*, Springer, 2018, pp. 233–244.

[12] E. Yavuz, A. Koc, U. C. Çabuk, and G. Dalkiliç, "Towards secure e-voting using ethereum blockchain," *2018 6th International Symposium on Digital Forensic and Security (ISDFS)*, pp. 1–7, 2018.

[13] W. Zhang, Y. Yuan, Y. Hu, S. Huang, S. Cao, A. Chopra, and S. Huang, "A privacy-preserving voting protocol on blockchain," in *2018 IEEE 11th International Conference on Cloud Computing (CLOUD)*, IEEE, 2018, pp. 401–408.

[14] S. Wang, X. Tang, Y. Zhang, and J. Chen, "Auditable protocols for fair payment and physical asset delivery based on smart contracts," *IEEE Access*, vol. 7, pp. 109 439–109 453, 2019.

[15] J. Chai, "Blockchain based voting system with ethereum blockchain," Ph.D. dissertation, The Ohio State University, 2020.

[16] A. Indapwar, M. Chandak, and A. Jain, "E-voting system using blockchain technology," *Int. J. of Advanced Trends in Computer Science and Engineering*, vol. 9, no. 3, 2020.

[17] D. Pawar, "Implementation of secure voting system using blockchain," *International Journal of Engineering Research and*, vol. V9, Jul. 2020. DOI: 10.17577/IJERTV9IS060974.

[18] P. Shejwal, A. Gaikwad, M. Jadhav, N. Nanaware, N. Shikalgar, *et al.*, "E-voting using block chain technology," *International Journal of Scientific Development and Research (IJSDR)*, vol. 4, no. 5, pp. 583–588, 2020.

[19] S. Zhang, L. Wang, and H. Xiong, "Chaintegrity: Blockchain-enabled large-scale e-voting system with robustness and universal verifiability," *International Journal of Information Security*, vol. 19, no. 3, pp. 1–19, 2020.

[20] Y. Abuidris, R. Kumar, T. Yang, and J. Onginjo, "Secure large-scale e-voting system based on blockchain contract using a hybrid consensus model combined with sharding," *Etri Journal*, vol. 43, no. 2, pp. 357–370, 2021.

[21] J. Huang, D. He, M. S. Obaidat, P. Vijayakumar, M. Luo, and K.-K. R. Choo, "The application of the blockchain technology in voting systems: A review," vol. 54, no. 3, 2021, ISSN: 0360-0300. [Online]. Available: https://doi.org/10.1145/3439725.

[22] P. Mccorry, M. Mehrnezhad, E. Toreini, S. F. Shahandashti, and F. Hao, "On secure e-voting over blockchain," *Digital Threats: Research and Practice (DTRAP)*, vol. 2, no. 4, pp. 1–13, 2021.

[23] M. Pawlak and A. Poniszewska-Marańda, "Implementation of auditable blockchain voting system with hyperledger fabric," in *International Conference on Computational Science*, Springer, 2021, pp. 642–655.

[24] N. Sundarajulu, M. J. Ilanthendral, *et al.*, "Online voting system using blockchain mechanism," *NVEO-NATURAL VOLATILES & ESSENTIAL OILS Journal/ NVEO*, pp. 5710–5714, 2021.

[25] M. Woda and Z. Huzaini, "A proposal to use elliptical curves to secure the block in e-voting system based on blockchain mechanism," in *International Conference on Dependability and Complex Systems*, Springer, 2021, pp. 466–476.

[26] J. Goyal, M. Ahmed, and D. Gopalani, "A privacy preserving e-voting system with two-phase verification based on ethereum blockchain," 2022.

[27] M. Dengo and F. P. Milani, "Blockchain voting : A systematic literature review."

[28] *Difference between sha-256 and keccak-256*, https://www.geeksforgeeks.org/difference-between-sha-256-and-keccak-256/, Accessed: 2023-01-16.

[29] D. geroni. (). "Private-blockchain-vs-consortium-blockchain," [Online]. Available: https://101blockchains.com/private-blockchain-vs-consortium-blockchain/. (accessed: 03.11.2020).

[30] *One-person, one-vote rule*, https://www.law.cornell.edu/wex/one-person_one-vote_rule, Accessed: 2023-01-16.

[31] *The pros and cons of evms*, https://www.thedailystar.net/opinion/cybernautic-ruminations/news/the-pros-and-cons-evms-1637551, Accessed: 2023-01-16.