Report Code:

University of Chittagong

Department of Computer Science and Engineering

8th Semester B.Sc. Engineering Examination 2021

Course No.: CSE 800

Title: Transparent and Reliable Electronic Voting System using Blockchain: Bangladesh Perspective

Report Code:

University of Chittagong

Department of Computer Science and Engineering

8th Semester B.Sc. Engineering Examination 2021

Course No.: CSE 800

Student Name: Md. Al Amin
Student ID: 17701087
Session: 2016-2017
Hall: Shaheed Abdur Rab
Signature of Student:

Submission Date: August 01, 2023

ABSTRACT

For years we have been using paper ballots and recently some countries started using electronic voting machines, but both systems have their flaws. Running a paper ballot election is costly, and votes counted on paper ballots are prone to errors. To overcome issued faced by Electronic voting machines have come into play, but Electronic voting machines are also easy to manipulate, and prone to hack. To overcome these issues this research brings one of the most secure methods of E-voting using blockchain technology. Being decentralized, immutable, consensus blockchain can provide trust and transparent, anonymous voting. In this thesis we are implementing a electronic voting system using permissioned/private blokchain.

Keywords: E-voting, Blockchain, de-centralized voting, Consensus Algorithm.

Contents

List of Figures

Chapter 1

Introduction

In this chapter, the research's context is described. The research's problem definition and motivation are addressed below. This chapter includes research objectives and research contributions. Finally, this chapter provides the outline of how the rest of the thesis is organized.

1.1 Overview

In this digital era most of the countries still use Paper based voting known as ballot paper, before paper based voting people in democratic countries used to vote by voice or raising hands. Paper based voting is the traditional way of voting. In paper-based voting fraudulent activities like sealing the ballot paper before the election begins, or swapping the ballot box with a tempered ballot box while transporting the ballot boxes to the central election counting booths. Also in paper based voting, counting the votes takes days and there is no guarantee that a voter's vote is being cast accurately as polling staff counts the votes using hands. So paper based voting has some major issues like trust, and transparency.

To overcome human effort, error, or cost, Electronic voting machines are introduced. EVMs are nothing but the electronic version of paper based voting. Instead of paper ballots people vote using their biometric identity on a touch screen of EVM.

Electronic voting was first adopted by Estonian Governement in their national election. [8], After that Switzerland adopted electronic voting, then Norway adopted electronic voting for its council elections. The thing is electronic voting machines were invented to replace the paper ballot voting, so they also have to

provide total anonymity like the paper ballot system. But there have been many temperings over the years in electronic voting machines, there are so many security concerns and trust issues in electronic voting machines. A third party can intercept the voting count of EVM, or chip manufacturers can embed malicious code to EVM.

In 2018 Bangladesh first used Electronic voting machines in some general elections on a limited scale, but some machines stopped working, some couldn't identify the voters using biometric identity or some couldn't count votes properly for technical issues. [9] Also with EVM a voter cannot verify if his/her vote is casted to the chosen candidate. There is no transparency in electronic voting machines. Electronic voting machines use central servers which pose a threat such as a single source of failure means if the central server fails or gets hacked by someone, the vote count can be altered. So we need some e-voting system in which people can trust and has the full transparency in it and should be secure enough that hacking that system is almost impossible

Therefore we propose a completely decentralized electronic voting system using blockchain technology. An inherent feature of a decentralized blockchain, or chain of blocks, is security. Simply put, a new block containing voter information is created each time a vote is cast. They are chained together because each block includes the data from the block that was formed before it. The chain gets longer as more people vote. As the recorded data from block to block would no longer match, the chain would be invalid if someone try to hack an already-created block. They would also need to update all the blocks that followed.triggering fraud.

Its strength comes from the fact that the blockchain is copied and distributed to hundreds of computers known as public ledgers, unlike a centralized ledger where there is only one system counting votes, thus making it decentralized. The votes are counted by all the computers, not by a single person, who also confirms the accuracy of each submission. Additionally, a hacker cannot simply break into one computer or ledger. He would have to simultaneously hack into every computer connected to the network. Also blockchain uses cryptographic hashing, by which a digital signature is created with your vote or ID/Face ID/FingerPrint which is verified by only you, no one else can verify it.

1.2 Motivation

The main Motivation behind this research is to provide an effective, secured and transparent voting mechanism to be implemented in Bangladesh on which people can trust. As we can see already, paper based voting has so many flaws. Electronic voting machines also have some serious security flaws, as EVM can be hacked or compromised in the factory. Electronic voting machines also use a central server therefore if anyone can get access to the central server they can easily manipulate the data in the database. So to overcome these issues like availability, security, transparency and central database issues in this thesis I present a blockchain based e-voting system, which is immutable, consensus, decentralized and a cryptographic hash protected and publicly owned ledger database technology which can be easily applied to e-voting while preserving trust and transparency, reliability, availability etc.

1.3 Problem Statement

In this digital era of the internet many countries are still using paper based ballot voting or Electronic voting machines which do not provide full anonymity and transparency and trust to the voters. Also in these voting systems coercing, manipulating the results happen a lot in developing countries like Bangladesh. The problem that needs to be solved is how to bring transparency, trust, anonymity, verifiability and provide accurate results to the nation wide elections where no third-party cannot manipulate the election.

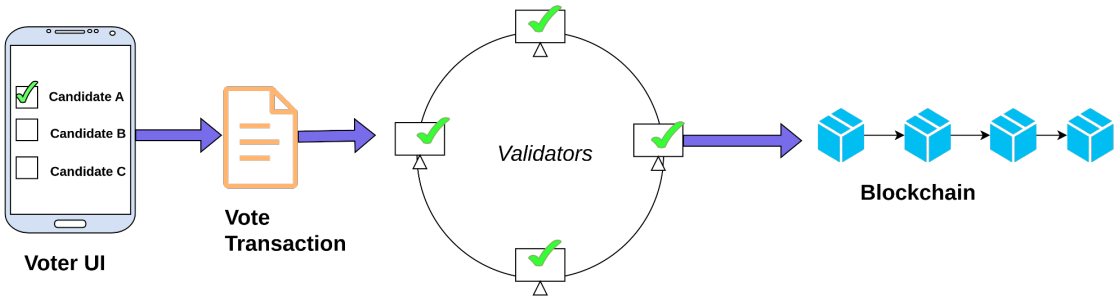

Figure 1.1: Problem Statement

Problem Description

1. Voter verifies his identity by the government Authentication server
2. Then Voter give his vote to the desired candidate
3. Voter verification is done via the Validator Nodes
4. If the vote is valid a block is mined by one of the validator nodes and adds the newly minded block to the permanent blockchain.
5. And a transaction hash is given to the voter where he can verify his vote whether or not his vote is casted accurately.

1.4 Research Objects and Goals

The main objective of this research is to provide a completely secure and anonymous e-voting and overcome the issues faced by paper based voting and fraudulent activities happening in electronic voting machines. The main objectives of the research paper can be further expanded as follows :

- Anonymity: users identity is completely hidden
- Verifiability: block is verified by all the public ledgers available in the blockchain
- Integrity: to provide integrity in the voting process.
- Transparency: voters can see if their vote is counted accurately.

- Instant results: consensus mechanism updates all the blocks in the system hence it can provides instant voting results
- Availability: people can vote from there smart phones wherever they are.
- Affordability : as public ledgers will contain the whole chain there is no need for costly EVMs and paper ballots where you need space and human resources to maintain the vote.

1.5 Key Contributions

To provide a decentralized secured e-voting this research focuses on the following points:

- To give anonymity to the voters
- To provide complete transparency in the voting process
- To provide immutability to the votes so that after the vote is counted no unauthorized third party cannot chance the vote
- To provide instant results of the voting
- To save financial costs and human resources

1.6 Thesis Organization

An outline of the content of the following chapter sin this thesis is presented below:

Chapter 2 - Background Concepts. This chapter provides the theoretical information necessary for understanding the procedures discussed in the methodology chapter.

Chapter 3 - Literature Review. This chapter provides a summary of blockchain based electronic voting related works that has been done by researchers

Chapter 4 - Methodology. In this chapter we thoroughly discuss the Methodology of our proposed system. This chapter shows the internal mechanism of how our voting system will work using decentralized, transparent and reliable blockchain.

Chapter 5 - Results. In this chapter we show the actual system snapshots while a demo election is started using our system.

Chapter 6 - Conclusions and Future Work. In this chapter we draw a conclusion about our proposed system and enlist necessary future works to improve the system.

Chapter 2

Background Concepts

As our proposed system will be based on blockchain technology. In this chapter we will discuss some important topics and underlying technology to understand blockchain in general and all the terms and keywords to understand our methodology.

It's very important to realise that without a thorough understanding of its history, essential elements, and architecture, as well as the discussions around it, blockchain is a difficult idea for most people to grasp. When people initially start their blockchain adventure, they often become confused by the various slightly varied definitions of blockchain that generate some quite restrictive beliefs. Blockchain is a concept created out of algorithms, technology, and unique ideas for the exchange of economic value; it is not a physical object that can be felt or seen, which is why there is misconception about it.

In this chapter, we'll examine the underlying ideas behind blockchain by first providing a succinct overview of its history. This background knowledge will make it easier for you to comprehend why there isn't a single, standardised definition of blockchain. After talking about the history of the blockchain, we'll take a quick look at some of its essential parts. We'll then examine its architecture, followed by any assisting notions and technologies.

We start by examining the decentralised network as the first of the essential elements. Next, we discuss cryptography. Since cryptography is essential to the operation of blockchain, you may consider it the secret ingredient. Blockchain would have no purpose without cryptography. We then talk about how to implement ledgers. In blockchain, the ledger stands in for the store or database. It keeps track

of both the history going back to the inception of the ledger and the state that was produced as a result of the most recent transaction that was committed.

The consensus, the core of blockchain, is the technique used to reach "agreement" among the nodes. Without depending on the conventional middlemen found in most transactional systems, consensus offers a safe way to execute transactions. You will better grasp the following after reading this chapter:

This chapter will help you get a good grasp on the following ideas:

- The architecture and fundamental elements of blockchain design
- How ledger databases work in blokchain
- The uses of cryptography (such as public/private keys, digital signature, hash functions) in blockchain
- Various consensus algorithms used in blockchain (PoW, PoS and PoA)

2.1 Blockchain

Blockchain is the crucial technology that matters for this study and the focus for further developments related to its application in the voting system. Hence, it is required to understand its concept well.

2.1.1 Concepts

In general definition, blockchain is like a giant distributed (Figure 2.1) ledger of peer-to-peer network of nodes. In blokchain everybody nodes what's happening in there shared ledger, and every nodes can participate on the contribution of it's security. So, if any transaction happens in the blockchain every nodes in that chain has to verify that transaction to be occured. It's like a democratic environment.

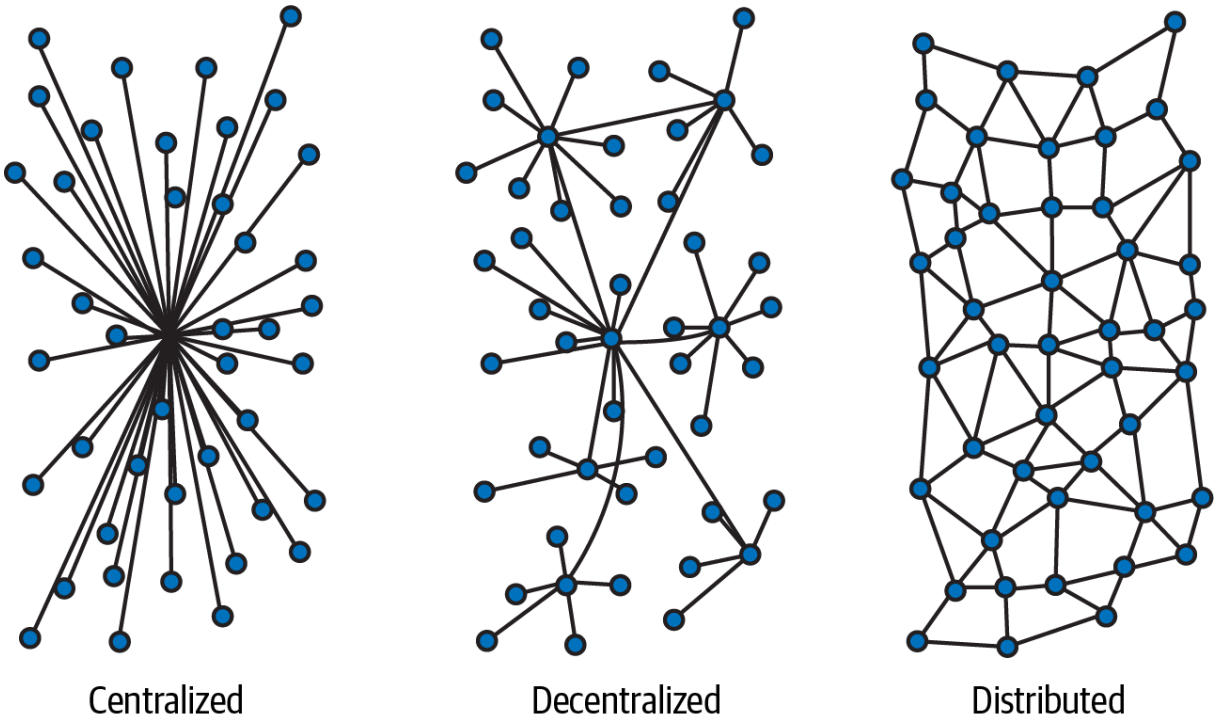

Figure 2.1: Types of Computer Networks [1]

But according to various research, we can define blokchain in various way to understand it further:

According to the white paper "BlockChain Technology: Beyond Bitcoin" written by Crosby, M., Nachiappan, Pattanayak, P., Verma, S. & Kalyanaraman, V. (2016), A distributed database of records, or public ledger, of all performed transactions or online activities that have been shared among participants in the network. Also, blockchain technology includes every transaction that ever made in the blockchain network" [10]

In other work developed by Osgood, R. (2016) [11], the author explains blockchain as "ever-growing ledger of records of transactions. Where the technology is managed by a network of computer nodes, all these nodes connected to a distributed network to validate the transactions. Whenever a transaction is validated by a node, the node is it is worthy of being added to the blockchain. As a result, verified transactions are grouped together and added to the blockchain as blocks.

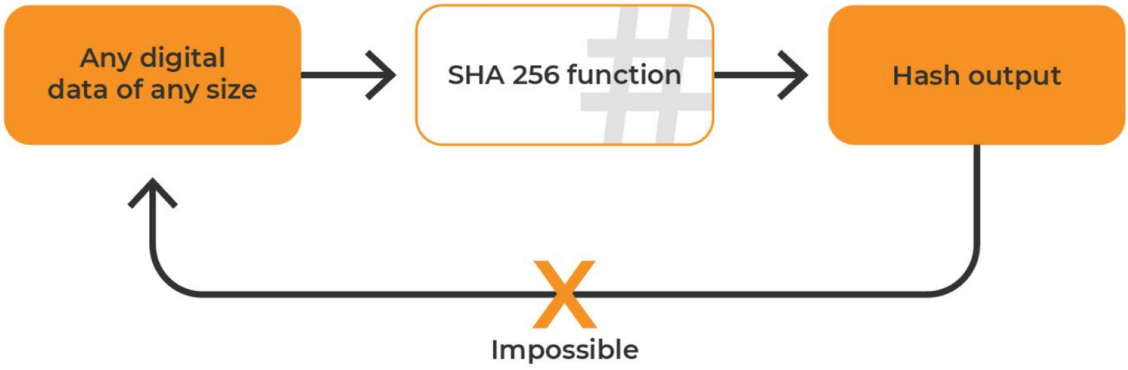

Figure 2.2: SHA 256 hash function block diagram [2]

2.2 Hash Functions

A hash function is an integral part of blockchain technology. Basically hash functions ensures security of a blockchain. It is a one-way function, meaning it cannot be reversed to get the original input from the output hash. The SHA- 256 hash function is used in blockchain. A cryptographic hash function is considered safe if it is able to protect against collisions, indicating that it is unlikely (if not impossible) to find two inputs that generate the same hash output. Two key security criteria for hash functions are hiding and puzzle-friendliness. These criteria are harder to break than preimage resistance, making hash functions like SHA256 suitable for use in blockchain design [12]. The actual benefit of the hash function in our concern SHA 256 is there is no way to predict/identify the input (i.e:files, text, transactions) from the hashed output of that input.

Therefore to become highly secured a hash functions needs to have the following characteristics:

- including an absence of weaknesses in the hash function
- Enormous number of arbitrary characters as possible output which is very hard to predict
- One way function whose input can’t be found from the output
- Small changes in the input creates a completely arbitrary hash

These requirements are met by SHA 256 hash function, so we will be using this hash function in our blockchain to make the chain completely secure and very hard to break.

2.3 Digital signature (ECDSA)

Digital signature is a public key cryptography which is another cryptographic technique utilized in blockchain technology. It's a Elliptic Curve Digital Signature Algorithm which is one of the most secure public key algorithms available out there. Due to its numerous beneficial characteristics, this sort of cryptography is very commonly used on the Internet. In the blockchain, using a digital signature to achieve non-repudiation is an efficient strategy. Blockchain technology is an appropriate platform for digital signatures since it needs to be a decentralized ledger and highly secured.

Digital signature is used in blockchain to maintain the non-repudiation. In our case it's needed to ensure secured voting transactions.
With digital signature you can:

- Encrypt your message in a way only the intended receiver can decrypt the message.
- Generates a digital signature of your message so that it verifies that you sent the message.
- Confirms that the message you have sent was not modified while transferring.

In the digital signature method, Everybody has a private and a public encryption key, which are different from each other and they are used to encrypt and decrypt messages. Your private key is a secret number you create at random. It is used to create digital signatures and decrypt the messages you sent. Your public key is produced from your private key and is intended to be shared publicly, as the name implies. It creates digital signatures and encrypts messages sent to you. Your public key is often used to determine your blockchain address, which is where transactions are transmitted to.

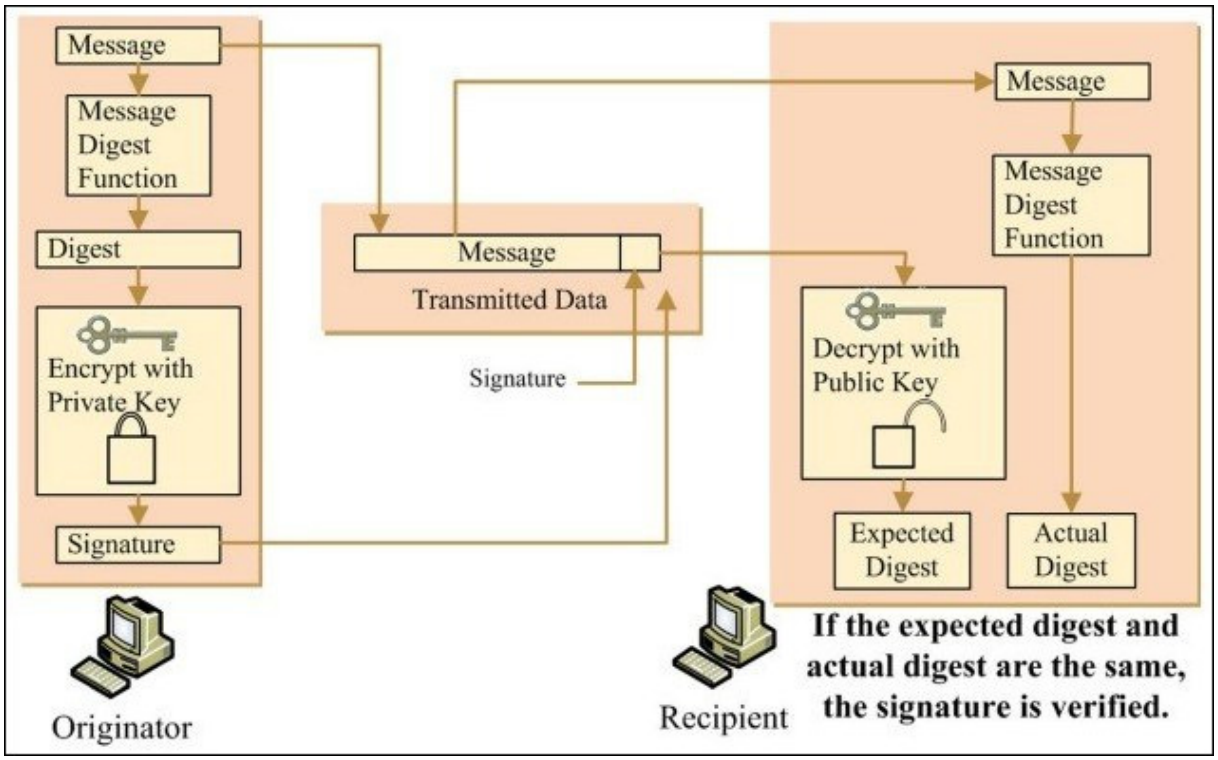

Figure 2.3: Digital Signature Verification in RSA [3]

2.4 Merkle Tree

Merkle tree, also known as hash tree is a special binary tree data structure that is used in blockchain. Merkle tree is used to preserve the data integrity of a block in the blockchain network [13]. Merkle tree is formed using recursively hashing all the pairs of child nodes of transactions. The root of the Merkle tree is called the Merkle Root. One interesting aspect of this tree is how it keeps track of the data integrity of a block. It's done by a hashing technique in which every hash of a node is the hashes of the child nodes of that node. So if one transaction is altered by a malicious user, the hash of that transaction will be changed, and like this all the way up to the hash of the root will also change thus making the node as invalid. Then the change will be automatically rejected by the blockchain peer-to-peer network instantly.

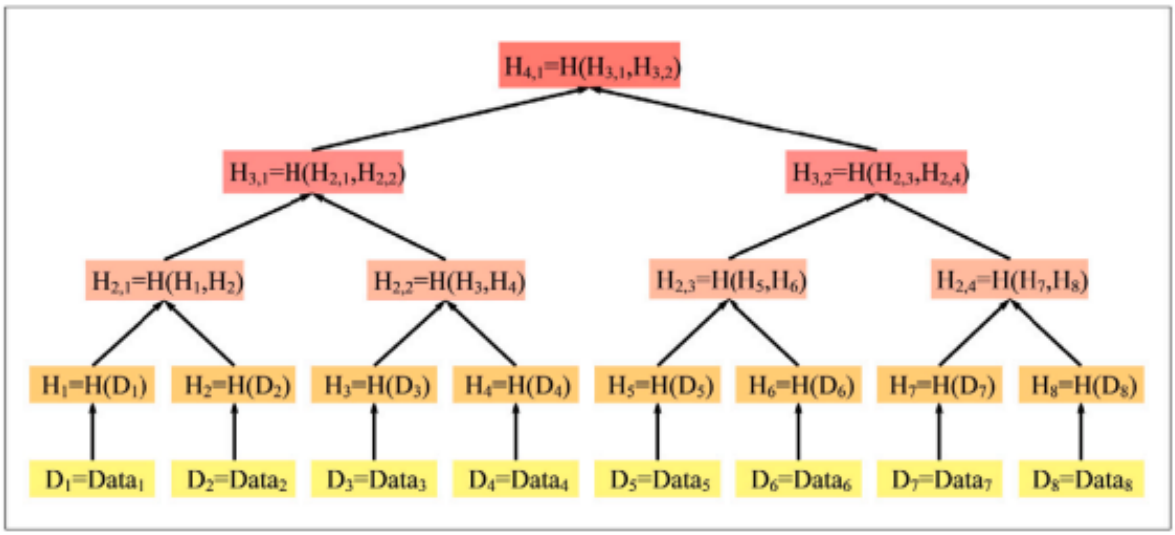

Figure 2.4: Structure of a Merkle Tree [4]

2.5 Block

Blockchain is nothing but a list numerous blocks whose are linked together in a immutable passion. A block usually contains Transactions info, Timestamp, Sender-Receiver Public keys, Nonce, Markle Root (Figure 2.5).

In order to create the immutable linked sequence known as the blockchain, each block in the chain has a cryptographic hash reference that connects to the preceding block. When a block is created, network nodes known as miners compete to validate the transactions within it. This validation process involves solving a complex mathematical puzzle such as PoW/PoS/PoA. The first miner to solve the hash value for the correct nonce has the authority to add that block and gets rewarded. Once a block is added and confirmed the miner gets rewarded in native currency of that blockc the records within it cannot be deleted or modified, providing transparency and permanence to the ledger [10]. This decentralized verification and approval process is critical to blockchain's security and integrity. Once a block is added, the records within it cannot be deleted or modified, providing transparency and permanence to the ledger. The interlinked blocks create a tamper-proof history of all activity on the blockchain since its creation [13].

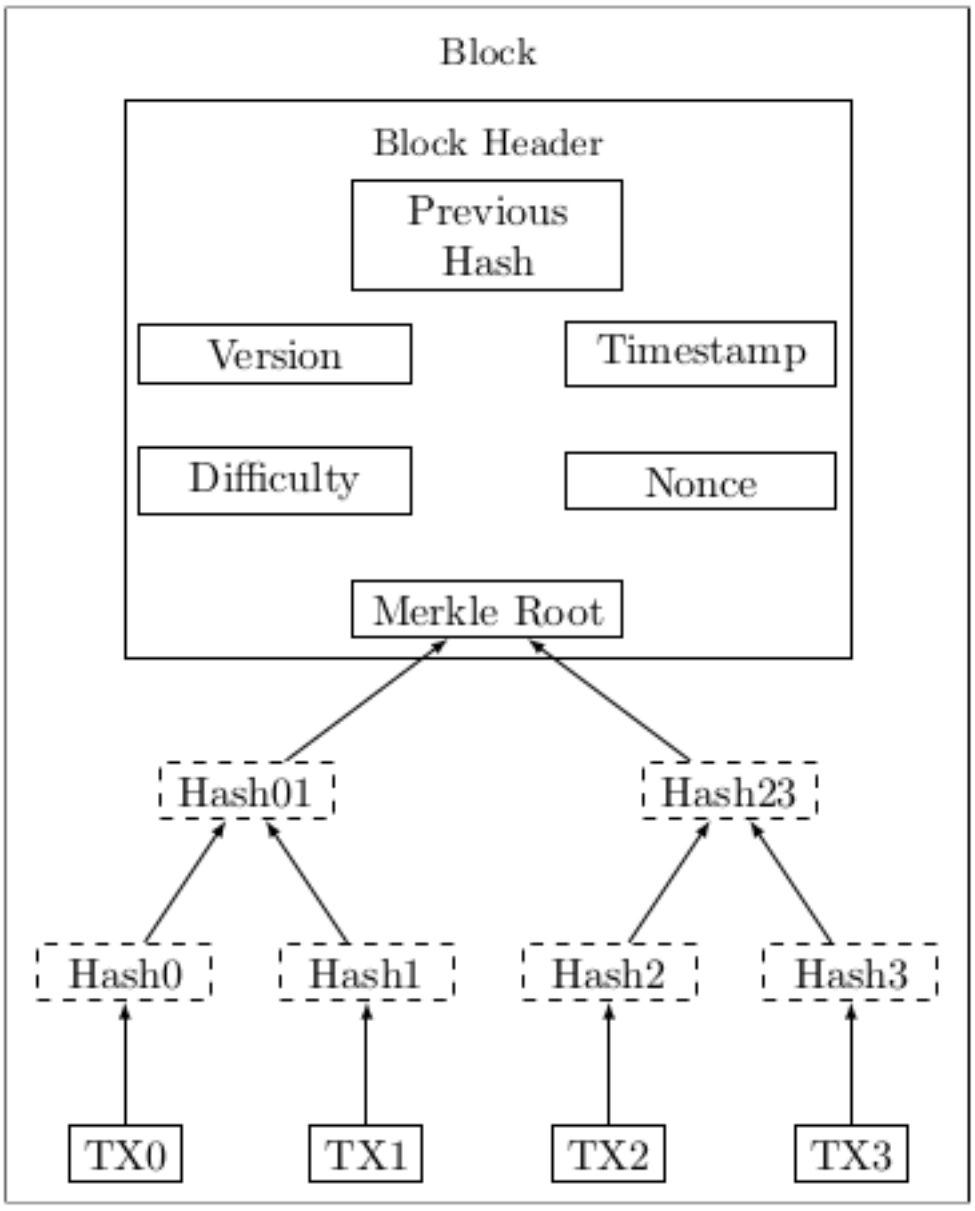

Figure 2.5: Structure of a Block in Bitcoin Network [5]

2.6 Transaction Process in Blockchain

In blockchain, each user has a pair of Private - Public keys. A user can be addressed by his Public key, On the other hand the private key can be used in digital signature when a user performs transactions.

When User A wants to send cryptocurrency to User B, User A initiates a transaction request using their private key to digitally sign the transaction. This verifies that User A authorized the transfer of funds from their address. The transaction data, including User B's public key address, is broadcast to the peer-to-peer network. Miners validate the transaction, check User A's signature against their public key, and add the transaction to the next block.

The network nodes then verify the transaction using User A's public key. If valid, the transaction is permanently recorded on the blockchain, transferring value from User A's address to User B's address.

User B can then use his private key to create a digital signature and unlock the funds from sender's address which completes the transaction initiated by User A. This system prevents double-spending and secures transfers on the blockchain.

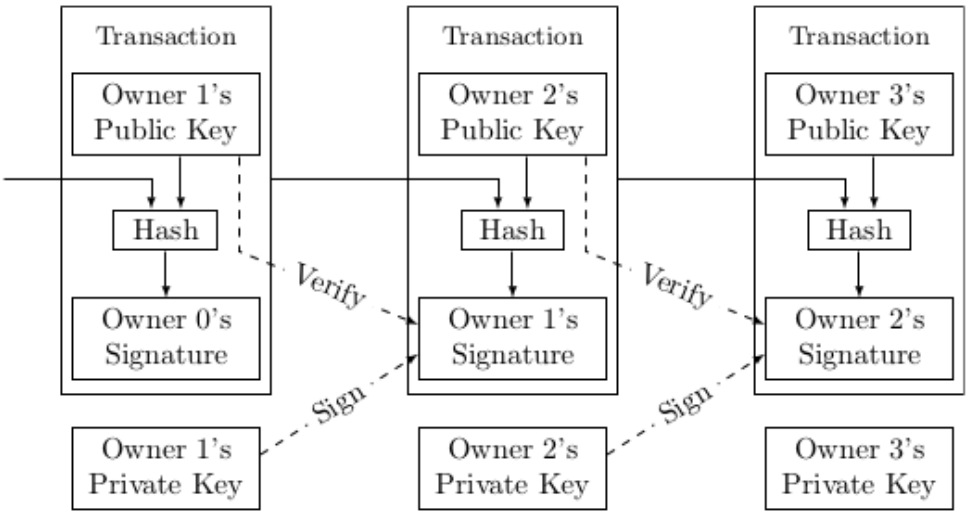

Figure 2.6: Transaction Scenerio between two parties [5]

2.7 Consensus Algorithms

In distributed systems and blockchain technology, knowing consensus algorithms are essential because they make sure that despite potential failures or bad actors, every node in the network agrees on a consistent state. Consensus algorithms are a crucial component of blockchain technology because as blockchain is fully distributed, where to agree on something depends on the voting result of every node in the blockchain. Also because of the consensus mechanism every node in the blockchain has the same copy of the blockchain.
There are mainly three types of consensus algorithms.

1. Proof-of-Work (PoA)
2. Proof-of-Stake (PoS)
3. Proof-of-Authority (PoA)

2.7.1 Proof-of-Work (PoW)

Over a decade before Satoshi Nakamoto's white paper, Proof of Work, a key component of Bitcoin, was developed. The idea was first put out by Moni Naor and Cynthia Dwork in 1993, was formalized by Markus Jakobsson and Ari Juels in 1999, and was later applied to digital currency by Hal Finney in 2004. He suggested a "reusable proof of work" system based on the SHA-256 cryptographic hashing algorithm.

This algorithm basically suggests that to be rewarded you have to show your proof of work that you have worked on the process of transaction verification. The miners are the ones that make efforts to add a new block in the blockchain using the Proof of Work mechanism. It mimics a race in which the winner produces the block (and receives the related rewards) and serves as the method for choosing the creator of the block.

Blockchain networks employ the Proof of Work (PoW) consensus algorithm to verify and safeguard the transactions. Computationally hard mathematical problems must be solved by the participants of the network, referred to as miners to add a new block to the network. The network accepts the answer once the first miner finds the hash fulfilling the hash condition, and other nodes may readily check if it is accurate(agreeing on consensus). Although this procedure uses a lot of energy, it guarantees that a lot of computational effort has been done to verify transactions and build new blocks. [14] This rigorous mining process secures the network because to alter the consensus algorithm an attacker needs the control of 51% computational power of the whole blockchain network which is nearly impossible and will cost too much.

Finding a nonce value (the main purpose of all the miners is to find it) that, when added with the rest of the data in the block makes a hash output with a specific amount of leading zeroes is the solution to the PoW puzzle. As a result, mining becomes practically a lottery where miners continually change the nonce and compute the hash until one of them is lucky enough to find a workable hash solution that fulfills the difficulty criterion. In order to find a solution on average every 10 minutes, the difficulty is constantly modified [15].

PoW makes it possible for public blockchain networks to operate decentralized without the need for access restriction or identity management. It offers a means

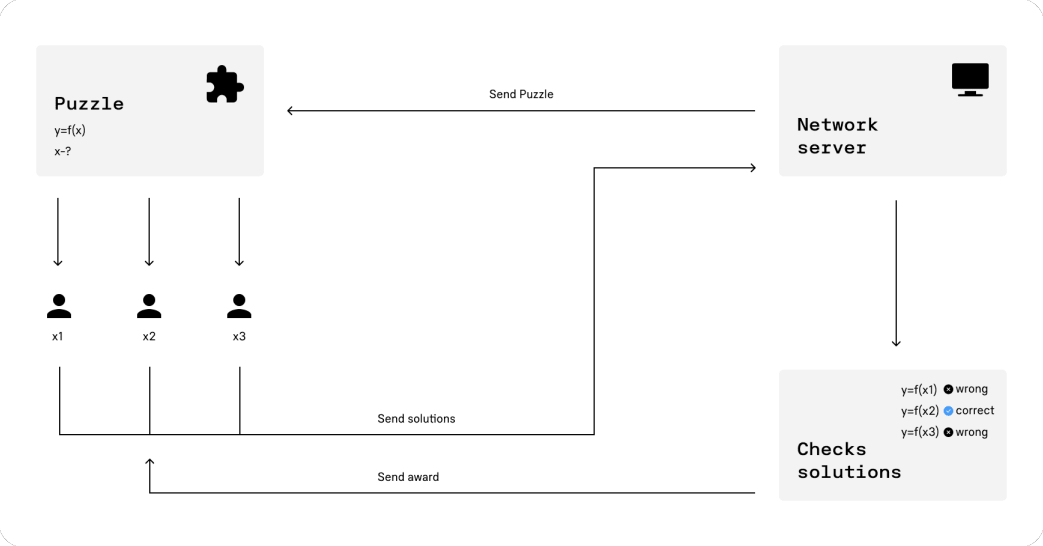

Figure 2.7: An overview of how PoW Works

to achieve widespread consensus in a permissionless environment by making the block generation process resource-intensive using computational problem solving. But research has been done and proposed alternatives Consensus Algorithms which don't consume as much energy as PoW.

2.7.2 Proof-of-Stake (PoS)

Another consensus algorithm used in modern blockchain called proof of stake (PoS) which is more energy-efficient than proof of work algorithm. Instead of miners competing on the basis of processing power, PoS systems choose validators based on the amount of the network's native coin(stake) they own. [16]

The basic idea is that validators lock up some of their cryptocurrency holdings as stake. They are then randomly selected to validate blocks and propose updates to the blockchain. The larger the stake a validator holds, the more likely they are to be chosen. Validators don't earn any mining reward blocks like PoW but they earn transaction fees only. If the validators try to do any mischievous activities they can lose part of their stake. [17]

Proof of Stake functions very similarly to investing in a business. You have the right to obtain investor dividends if you contribute part of your funds (stake) to a business. In Proof of Stake, you agree not to spend any of your stake in return for

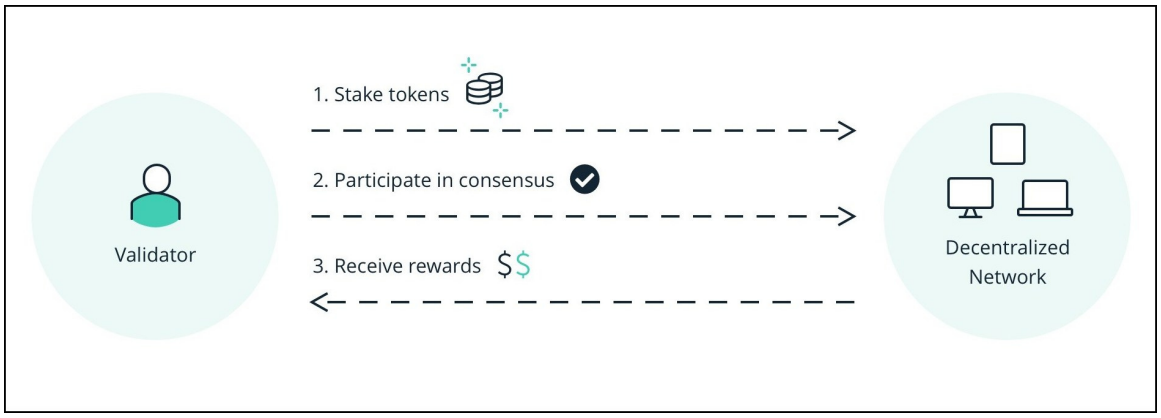

Figure 2.8: An overview of how PoS Works [6]

the opportunity to become a block maker and get the corresponding incentives (i.e. transaction fees).

However, some challenges for PoS include the ”nothing at stake” problem where validators can stake on multiple forks with no repercussions. Additionally, PoS is susceptible to various attacks if the stake thresholds are set too low.
Key advantages of Proof-of-Stake are

- Energy Efficiency: PoS doesn't require solving computationally hard puzzles like its counterpart PoW algorithm, saving nearly 99
- Security: Attacks or any malicious activity results in losing their whole stake of the validators therefore they don't try to do any such kind of work meanwhile securing the network.
- Low barrier to entry: doesn't require special mining rig/hardware to participate in the network as a validator, you need only stake (another of saying you have to be rich to begin with) to participate in the network.

Major blockchains like Ethereum have successfully transitioned to PoS from PoW based consensus called the 'Merge' with the goal of improving sustainability and energy efficiency [18]. However, PoW remains the dominant model for now.

2.7.3 Proof-of-Authority (PoA)

The Proof-of-Authority (PoA) consensus algorithm does not rely on mining/stake to validate blocks; instead, it uses authorized participant nodes, or "validators," to do the verification. Blocks are proposed and validated by validators in a round-robin passion. [19]
PoA works effectively for private blockchains where every member is a well-known entity. It does not require energy-intensive mining and prioritizes identification above computing power. Reduced decentralization and resilience in comparison to public networks is the main trade-off of PoA based consensus algorithm.
Here simple key points of how Proof of Authority consensus algorithm works:

1. Trusted Authorities: A group of pre-picked and reliable authorities are selected to serve as validators in a PoA blockchain network. These validators are often well-known organizations or people that have a high degree of trust and reputation within the network or community.

2. Block Creation: Validators build new blocks to the blockchain by adding transactions in turn. Only the authorized authorities are permitted to generate new blocks in PoA, unlike PoW or PoS, where anybody may participate.

3. Validation: A validator authenticates the creation of a block by signing it with a cryptographic key (digital signature). This signature serves as evidence that the block was made and verified by an authorized party.

4. Consensus: When the majority of the network's validators accept that a block is correct, consensus has been reached. In comparison to PoW, the process of reaching agreement is comparatively quick and energy-efficient because the validators are reliable, well-known entities.

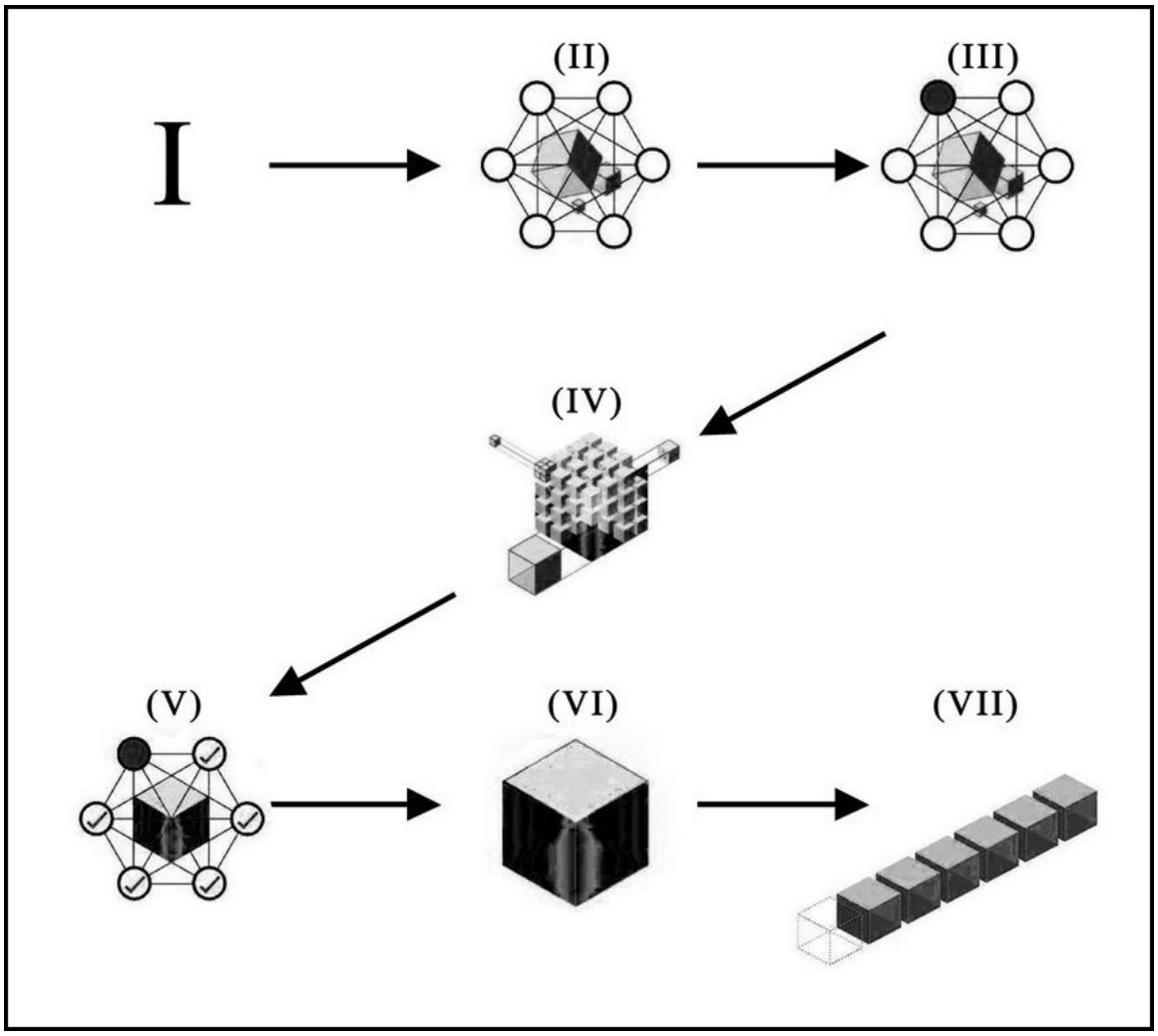

Figure 2.9: Adding a block to the blockchain using PoA consensus [7]

In the above Figure 2.9, steps are shown how Proof-of-Authority consensus algorithm works when adding a new block to the blockchain.

1. A transaction is happened in the network.
2. An authorized random node is selected as primary to further assess the transaction and start working on the validation procedure.
3. After successful validation of the transaction a block is generated by the primary node

4. Then the node is disseminated to the PoA network where other nodes will also verify the newly generated block.
5. If everything is okay, the block should be accepted by the other validator nodes in the PoA network.
6. Confirmed block is ready to be added to the blockchain.
7. The block is added to the permanent private/permissioned blockchain.

Chapter 3

Literature Review

Ayed studied the existing E-voting systems like I-voting, iVote used in some countries and figured out the flaws in these system and proposed a decentralised voting system using public blockchain which shouldn't be used as public blokchain can run into security issues like DDoS. [20]

Liu, Yi and Wang, Qi proposed blind signature protocol is used alongside blockchain to preserve voters's choices during the election and blockchain implemented as public to for transparency of the election. They used 3-tuple participants to implement the blockchain (Voters, Organizers, Inspectators). Though the work in the paper met lots of blockchain properties, it can be further optimized to support large scale election. [21]

Hjálmarsson used Ethereum blockchain network and smart contracts to make the blockchain more efficient and self executing process. The work is more robust and can support large scale nationwide elections as smart contracts are more efficient blocks in blockchain and smart contracts can execute themselves. [22]

McCorry, Patrick and Shahandashti, implemented the smart contracts on Open Vote Network that runs on Ethereum. This paper precisely implemented the voting system giving exactly what will be the cost to cast a single vote over the Ethereum network. Any election can be arranged by their readily available voting system. [23]

Çabuk, Umut Can and Adiguzel studied feasibility and suitability of blockchain if blockchain can be used in elections, as blockchain provides properties such as immutability (not be able to alter information), transparency of all the blocks (votes), nonrepudiation. Therefore blockchain technology in e-governance such as general elections is very important to consider. [24]

Monrat, A. A., Schelén, O., & Andersson, K. (2019) studied the blockchain and provides a comprehensive overview of blockchain technology, including its history, concepts, structure, types and applications across domains like finance, IoT, healthcare, and supply chain. It analyzes technical challenges of blockchain such as scalability, privacy, consensus mechanisms, and legal compliance issues. The paper also examines current opportunities and future directions for blockchain research including improving scalability, ensuring privacy and security, developing new consensus protocols, and enabling blockchain interoperability and standardization. Potential trends identified are integrating blockchain with artificial intelligence, big data analytics, and edge computing to create innovative solutions and applications. Overall, this valuable reference analyzes the current state and future potential of blockchain technology and applications. [25]

De Angelis, Stefano, et al applied CAP theorem to understand how effective proof-of-authority is suitable in Permissioned Blockchain. he authors analyze the trade-offs between consistency, availability, and partition tolerance, demonstrating how PBFT favors consistency over availability while PoA prioritizes availability. This work provides a useful framework for evaluating the strengths and weaknesses of consensus protocols for permissioned blockchains with regards to the CAP theorem. [26]

Chapter 4

Methodology

In this research we are proposing an Electronic Voting System that will leverage the blockchain technology using a peer-to-peer Proof-of-Authority (PoA) network and a blockchain-based Electronic Voting System that uses it to guarantee the security, transparency, and integrity of the voting process. By utilizing the immutability, integrity and decentralization features provided by blockchain, our technology seeks to revolutionize the election process by offering a secure and reliable platform for voting and vote counting.

Our system has 6 phases to successfully cast a vote:

1. Voter Authentication and Authorization
2. Displaying the voter his/her constituency voter User Interface
3. Voter votes using his public key address.
4. Verifying the votes by our Peer-to-Peer Proof-of-Authority Nodes.
5. Adding/rejecting vote to be included in the immutable blockchain ledger.
6. Displaying the voting transactions in the voter User Interface.

4.1 Voter Authentication

Below processes are needed to authenticate a user as a verified voter.

4.1.1 User Information Collection

In this phase we will get input from the voter such as National identification number (NID), Date of birth (DoB) and Permanent Address through our voter User Interface.

4.1.2 Connecting with Government Database through API

We will build a secure connection using Https/TLS protocol with the government database with appropriate API keys or Tokens.

4.1.3 Verification of Voter data

Voter provided data through our Voter User Interface will be checked against the government voter records. Based on that, the government verification service will either return true/false upon verification. This way we complete the Authentication process.

4.2 Displaying the voter User Interface

Upon successful authentication the system would provide a customized voter User Interface (UI) with the voter candidates data related to their individual constituency after the voter's successful authentication. The UI will give the voter information on the candidates, including their backgrounds, political affiliations, and major positions. A safe and simple electronic ballot that the voter may use to select their chosen candidate will also be included in the voter UI. To support a pleasant voting experience for the public, the interface will provide simplicity and accessibility. To preserve the voters' privacy during the process, the UI will also uphold the secrecy of their selections and adhere to all data protection laws.

4.3 Voter gives vote using his public key address

The voter will be given a special public key after the authentication, a cryptographic key used for secure identification and communication inside the voting system, after successful verification. The voter's identification will be connected to this public key, which will be safely preserved in the system.

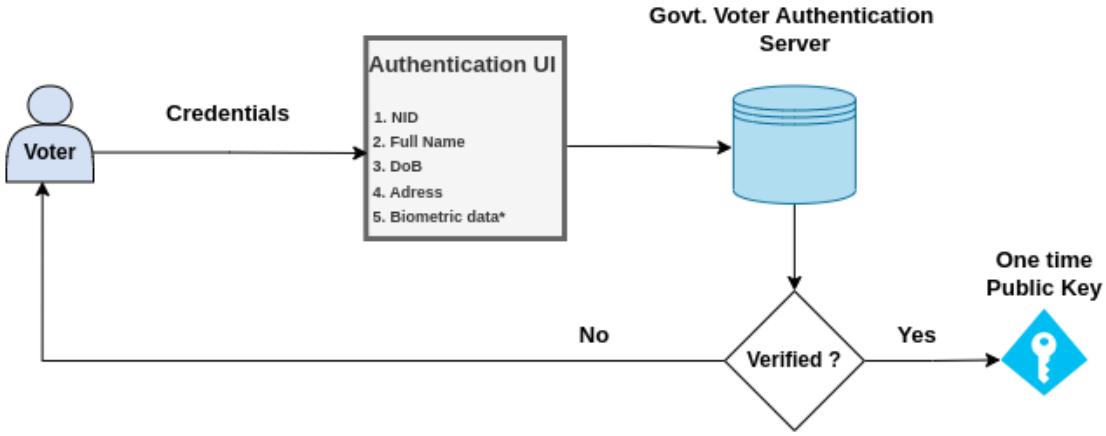

Figure 4.1: Workflow of Voter Verification

This public key will be used by the voter to encrypt their ballot when they cast their ballot, protecting the privacy of their selections. The blockchain network will then receive and process the encrypted ballot.

The integrity of the voting process is maintained by the public key encryption, which makes sure that only authorized parties, such election authorities, may decrypt and count the votes. Voting using a public key offers an extra degree of security since it stops votes from being tampered with or altered while being sent and stored.

In order to ensure that each voter may only cast one vote, avoid duplicate voting, and protect the election process integrity, the system cross-references the public key with the voter's identification. Also the auditing procedure is made easier by using a public key, enabling impartial observers to check the accuracy of the election results and spot any potential errors.

4.4 The Voting Process

4.4.1 Selecting the Candidate

The voting process starts by selecting the desired candidate to vote in the voter's constituency area. After the candidate selection is done, the voter submits a vote for his desired candidate. Then this voting transaction containing the encrypted ballot

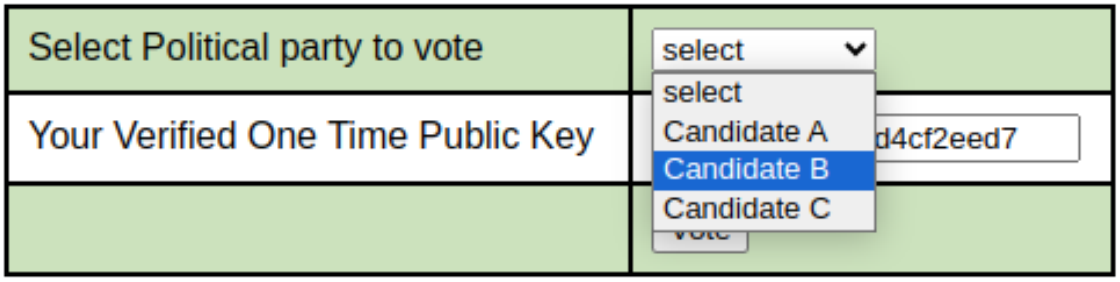

Figure 4.2: Selecting the Desired Candidate in the Voter UI

and voter's unique public key and is sent to the blockchain server in the backend hosted in a different ports on a secured network.

4.4.2 Verification of Voting in the Peer-to-Peer Network

When a transaction comes to the validator Nodes known as PoA (Proof-of-Authority) network the following verification techniques are applied to count the voting transaction as a valid vote.

1. The voting transaction is propagated to the validator nodes, then a validator is selected based on their reputation and authority also known as primary validator within the network.

2. Then the primary validator verifies the legitimacy of the transactions such as encrypted ballot, and associated public key, and checks if the public key is used before to vote.

3. The Primary validator may connect to the government validation service to complete the verification process.

4. If the transaction is valid, the Primary validator node focuses on creating a new block containing that specific vote information including voter information and generates a hash off of these information.

5. Then the Primary validator node creates a block and disseminates that block to the other nodes.

6. Then a consensus algorithm PoA (Proof-of-Authority) is invoked to confirm the validity of the block.

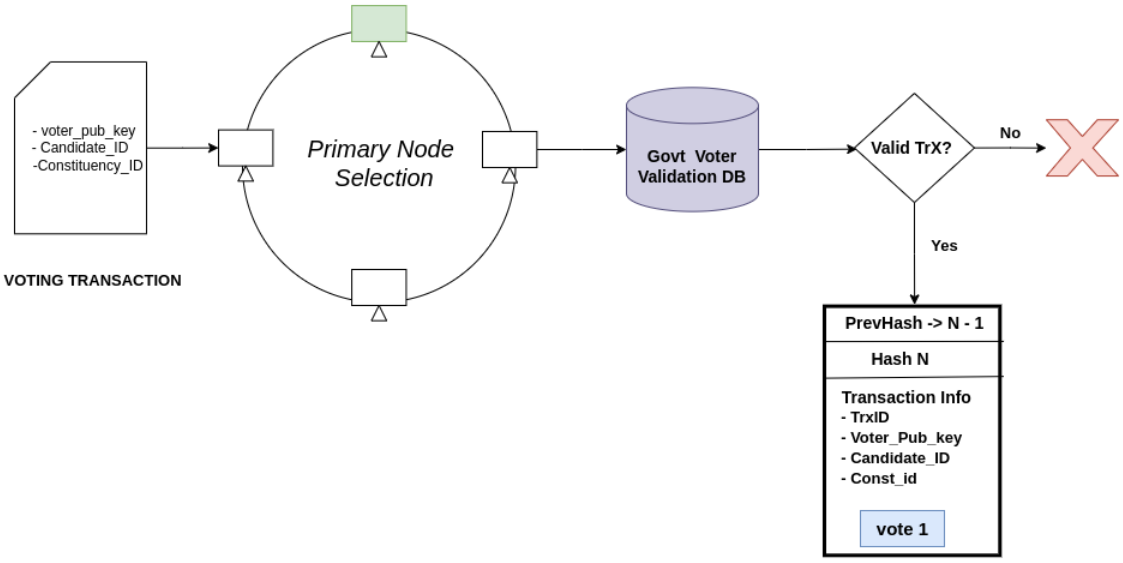

Figure 4.3: Generating a new block upon validating the voting transaction

4.4.3 Adding the newly created to the blockchain (PoA consensus algorithm)

After a valid block is generated by the Primary node in PoA network. Then this newly created block is broadcasted among other Authority Nodes. Then those Nodes accept the block as valid/invalid using a consensus mechanism known as Proof-Of-Authority. There are different consensus algorithm exists such as Proof-of-Work (used by bitcoin), Proof-of-Stake (used by Ethereum blockchain network) but we are using Proof-of-Authority or PoA as a consensus algorithm as it is the most suitable in our electronic voting system because we are using a private blockchain where highly secured nodes will act as a election commissioner representatives.

Now to add the newly created block containing a valid voting transaction. We need to go through the Peer-to-Peer PoA network. If every node in the PoA network accepts the block and marks it as a valid block then we will add this block to the permanent immutable blockchain ledger.

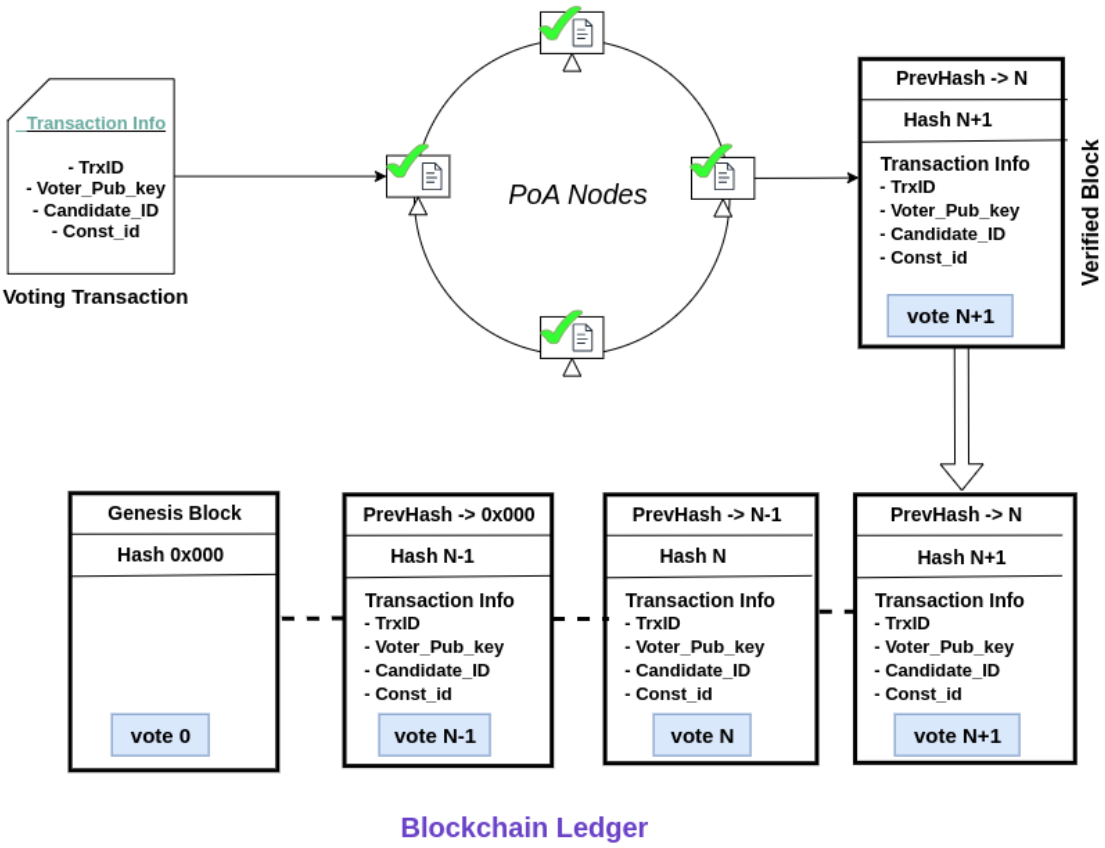

Figure 4.4: Adding New Voting Transaction Block using PoA consensus algorithm

4.4.4 Counting the Election Results

To count the results of the election we use an iterative method where we go through a JSON (JavaScript Object Notation) file which is given by our system. Though right now we show the instant result of the election there is room for modification to show the result after the election is finished. The Flowchart of counting result is shown in the next page.

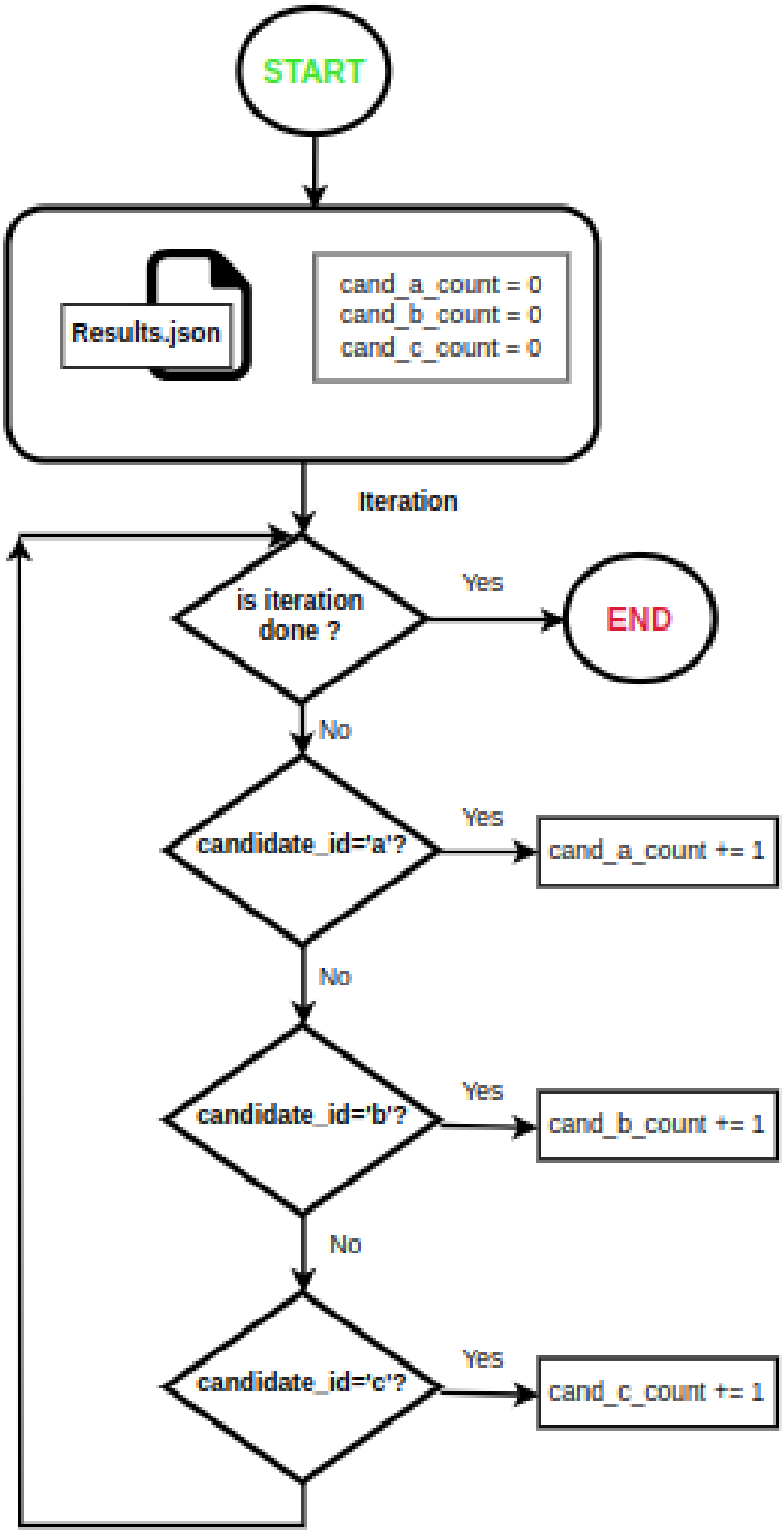

Figure 4.5: Flowchart of Counting the Voting Results

Chapter 5

Results

There is two types of results in our system

1. Results of Voting Transaction
2. Results of Overall Election

5.1 Result of Voting Transactions

In this result section, the voting transaction table serves as an immutable record of all votes cast in the e-voting system. Each row represents a single vote transaction. The Voter ID field contains the public key of the voter. TxID is a unique transaction ID generated when the vote is cast. Block Index indicates which block in the blockchain contains this vote transaction. Candidate Name stores the name of the candidate the voter selected. Voted Time contains a timestamp of when the vote was cast. This table allows for easy lookup and verification of each vote while maintaining voter privacy through the use of a Voter ID rather than name or other identifiable info. The blockchain ensures the table cannot be tampered with, supporting trust in the election results. Voting Transactions are shown in Figure 5.1

5.2 Election Result

A voter can see the Election Result instantly. Becuase in our system everything is automated and maintained by blockchain. Therefore we can see the updated Election Result in anytime of the Election Day. Election result is shown in Figure 5.2

Voter ID	TxID	Block Index	Candidate Name	Voted Time
ef45bdff8447...	d87fb4f9ae08...	7	Candidate A	2023-07-18 13:17
483523a9aaca...	0a0557f5112b...	6	Candidate C	2023-07-18 13:17
bd0fd255ecc7...	1a84360f8002...	5	Candidate B	2023-07-18 13:16
ce7d5f6a75fa...	84ec9f67bfb1...	4	Candidate A	2023-07-18 13:10
915c35b1f6d1...	d2bf821730b5...	3	Candidate B	2023-07-18 13:10
71686a8bee6d...	c8ab050e2e12...	2	Candidate A	2023-07-18 13:07
eb2ce0710985...	60becfa05fee...	1	Candidate A	2023-07-18 12:44

Figure 5.1: Voting transactions happening in Blockchain ledger

Election Result

Candidate Name	Total Votes
Candidate A	4
Candidate B	2
Candidate C	1

Figure 5.2: Election Result shown in our system

Chapter 6

Conclusions and Future Work

In this research, we have proposed a system for electronic voting using private blockchain and Proof-of-Authority as consensus algorithm. We have shown how blockchain can be transparent, reliable and effective to run election while providing complete security over voters information. In this system we have developed a permissioned/private blockchain which can handle hundreds of voting transactions per second.

In future work, We can improve our system by improving the following points:

- Make security stronger so that no outsiders can interfere with the blockchain in any way.
- Improve Scalability so that more users can use the system simultaneously.
- Maybe use robust open source private blockchain network like HyperLedger Fabric.
- Take nationwide surveys from citizens
- Feasibility study to run this system in a nationwide election.

References

[1] Mark Anthony Morris. Hands-On Smart Contract Development with Hyperledger Fabric V2 — oreilly.com. https://www.oreilly.com/library/view/hands-on-smart-contract/9781492086116/ch01.html. [Accessed 31-07-2023].

[2] SHA 256 from scratch with pen and paper — armantheparman.com. https://armantheparman.com/sha256/. [Accessed 31-07-2023].

[3] Weidong Fang, Wei Chen, Wuxiong Zhang, Jun Pei, Weiwei Gao, and Guohui Wang. Digital signature scheme for information non-repudiation in blockchain: a state of the art review. *EURASIP Journal on Wireless Communications and Networking*, 2020(1):1–15, 2020.

[4] Hegui Zhu, Yujia Guo, and Libo Zhang. An improved convolution merkle tree-based blockchain electronic medical record secure storage scheme. *Journal of Information Security and Applications*, 61:102952, 2021.

[5] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system. *Decentralized business review*, 2008.

[6] What is Proof-of-Stake (PoS)? — ledger.com. https://www.ledger.com/academy/blockchain/what-is-proof-of-stake. [Accessed 31-07-2023].

[7] Ugonna Chikezie, Tutku Karacolak, and Josue Campos Do Prado. Examining the applicability of blockchain to the smart grid using proof-of-authority consensus. In *2021 IEEE 9th International Conference on Smart Energy Grid Engineering (SEGE)*, pages 19–25. IEEE, 2021.

[8] Wikipedia. Electronic voting in Estonia — Wikipedia, the free encyclopedia. http://en.wikipedia.org/w/index.php?title=Electronic%20voting%

20in%20Estonia&oldid=1108900432, 2022. [Online; accessed 09-November-2022].

[9] family=Correspondent given i=S., given=Staff. EVM proves prone to abuse. 12 2018.

[10] Michael Crosby, Pradan Pattanayak, Sanjeev Verma, Vignesh Kalyanaraman, et al. Blockchain technology: Beyond bitcoin. *Applied Innovation*, 2(6-10):71, 2016.

[11] Ryan Osgood. The future of democracy: Blockchain voting. *COMP116: Information security*, pages 1–21, 2016.

[12] Maoning Wang, Meijiao Duan, and Jianming Zhu. Research on the security criteria of hash functions in the blockchain. In *Proceedings of the 2nd ACM Workshop on Blockchains, Cryptocurrencies, and Contracts*, pages 47–55, 2018.

[13] Zibin Zheng, Shaoan Xie, Hongning Dai, Xiangping Chen, and Huaimin Wang. An overview of blockchain technology: Architecture, consensus, and future trends. In *2017 IEEE international congress on big data (BigData congress)*, pages 557–564. Ieee, 2017.

[14] Gavin Wood et al. Ethereum: A secure decentralised generalised transaction ledger. *Ethereum project yellow paper*, 151(2014):1–32, 2014.

[15] Alex De Vries. Bitcoin's growing energy problem. *Joule*, 2(5):801–805, 2018.

[16] Fahad Saleh. Blockchain without waste: Proof-of-stake. *The Review of financial studies*, 34(3):1156–1190, 2021.

[17] Wenbo Wang, Dinh Thai Hoang, Peizhao Hu, Zehui Xiong, Dusit Niyato, Ping Wang, Yonggang Wen, and Dong In Kim. A survey on consensus mechanisms and mining strategy management in blockchain networks. *Ieee Access*, 7:22328–22370, 2019.

[18] The Merge — ethereum.org — ethereum.org. https://ethereum.org/en/roadmap/merge/. [Accessed 31-07-2023].

[19] Ali Dorri, Salil S Kanhere, Raja Jurdak, and Praveen Gauravaram. Blockchain for iot security and privacy: The case study of a smart home. In *2017 IEEE international conference on pervasive computing and communications workshops (PerCom workshops)*, pages 618–623. IEEE, 2017.

[20] Ahmed Ben Ayed. A conceptual secure blockchain-based electronic voting system. *International Journal of Network Security & Its Applications*, 9(3):01–09, 2017.

[21] Yi Liu and Qi Wang. An e-voting protocol based on blockchain. *Cryptology ePrint Archive*, 2017.

[22] Fririk Hjálmarsson, Gunnlaugur K Hreiarsson, Mohammad Hamdaqa, and Gísli Hjálmtỳsson. Blockchain-based e-voting system. In *2018 IEEE 11th international conference on cloud computing (CLOUD)*, pages 983–986. IEEE, 2018.

[23] Patrick McCorry, Siamak F Shahandashti, and Feng Hao. A smart contract for boardroom voting with maximum voter privacy. In *International conference on financial cryptography and data security*, pages 357–375. Springer, 2017.

[24] Umut Can Çabuk, Eylul Adiguzel, and Enis Karaarslan. A survey on feasibility and suitability of blockchain techniques for the e-voting systems. *arXiv preprint arXiv:2002.07175*, 2020.

[25] Ahmed Afif Monrat, Olov Schelén, and Karl Andersson. A survey of blockchain from the perspectives of applications, challenges, and opportunities. *IEEE Access*, 7:117134–117151, 2019.

[26] Stefano De Angelis, Leonardo Aniello, Roberto Baldoni, Federico Lombardi, Andrea Margheri, Vladimiro Sassone, et al. Pbft vs proof-of-authority: Applying the cap theorem to permissioned blockchain. In *CEUR workshop proceedings*, volume 2058. CEUR-WS, 2018.