VOTING SYSTEM USING BLOCKCHAIN

By

Nilesh Kumar Singh (2101641550051)

Anjali Singh (2101641550019)

Abhinav Singh (2101641550005)

Atul Gupta (210141550030)

Submitted to the Department of

Computer Science and Engineering

Pranveer Singh Institute of Technology,
Kanpur

(Dr. A.P.J. Abdul Kalam Technical University, Lucknow)

Dec, 2024

VOTING SYSTEM USING BLOCKCHAIN

Nilesh Kumar Singh (2101641550051)

Anjali Singh (2101641550019)

Abhinav Singh (2101641550005)

Atul Gupta (210141550030)

Submitted to the

Department of Computer Science and Engineering

Under the supervision of

Mr Malay Tripathi (Assistant Professor)

In Partial Fulfillment of the Requirements for the Degree of

BACHELOR OF TECHNOLOGY
(Internet Of Things)

Dr. APJ Abdul Kalam Technical University, Lucknow

TABLE OF CONTENT

DECLARATION

We hereby declare that the project entitled **"Online Voting System Using Blockchain"** submitted for the B. Tech. (IOT) degree is our original work and the project has not formed the basis for the award of any other degree, diploma, fellowship or any other similar titles. The best of our knowledge and belief, it contains no material previously published or written by any other person nor material which to a substantial extent has been accepted for the award of any other degree or diploma of the university or other institute of higher learning, except where due acknowledgment has been made in the text.

Signature:

Name: Nilesh Kumar Singh

Roll No: 2101641550051

Date:

Signature:

Name: Atul Gupta

Roll No: 2101641550030

Date:

Signature:

Name: Anjali Singh

Roll No: 2101641550019

Date:

Signature:

Name: Abhinav Singh

Roll No: 2101641550005

Date:

CERTIFICATE

This is to certify that the project titled **"Online Voting System Using Blockchain"** is the bonafide work carried out by,

Nilesh Kumar Singh (2101641550051)

Anjali Singh (2101641550019)

Abhinav Singh (2101641550005)

Atul Gupta (2101641550030)

In partial fulfillment of the requirements for the award of the degree of Bachelor of Technology student of B.Tech (CS_IOT) of Pranveer Singh Institute Of Technology, Kanpur affiliated to Dr. A.P.J. Abdul Kalam Technical University, Lucknow, Uttar Pradesh (India) during the academic year 2023-24, andthat the project has not formed the basis for the award previously of any other degree, diploma, fellowship or any other similar title.

Place:

Dr. Malay Tripathi
(Associate Professor)
Project Supervisor
Pranveer Singh Institute Of Technology, Kanpur

Date:

ACKNOWLEDGEMENT

We would like to express our gratitude towards our project mentor, **Dr Malay Tripathi, Associate Professor** , without whose guidance and support this work would not have been possible.

We would also like to thanks him for always motivating us to take up challenging and interesting projects that develop our knowledge in new domains

Lastly, we would like to thank our parents, family and friends for keeping us motivated in all our life's Endeavour's.

Signature:

Name: Nilesh Kumar Singh

Roll No: 2101641550051

Date:

Signature:

Name: Atul Gupta

Roll No: 2101641550030

Date:

Signature:

Name: Anjali Singh

Roll No: 2101641550019

Date:

Signature:

Name: Abhinav Singh

Roll No: 2101641550005

Date:

ABSTRACT

Phishing websites have proven to be a major security concern. Several cyberattacks risk the confidentiality, integrity, and availability of company and consumer data, and phishing is the beginning point for many of them. Many researchers have spent decades creating unique approaches to automatically detect phishing websites. While cutting-edge solutions can deliver better results, they need a lot of manual feature engineering and aren't good at identifying new phishing attacks. As a result, finding strategies that can automatically detect phishing websites and quickly manage zero-day phishing attempts is an open challenge in this field. The web page in the URL which hosts that contains a wealth of data that can be used to determine the web server's maliciousness. Machine Learning is an effective method for detecting phishing.It also eliminates the disadvantages of the previous method. We conducted a thorough review of the literature and suggested a new method for detecting phishing websites using features extraction and a machine learning algorithm. The goal of this research is to use the dataset collected to train ML models and deep neural nets to anticipate phishing websites.

CHAPTER-1

INTRODUCTION

1. INTRODUCTION

The Internet is the greatest thing invented by humanity. But there are some flaws on the internet. Consider a situation where you are depositing money or casting a vote, there is a single point of authority, and we are supposed to believe him/her with our data/money/vote. The limitation of the present system is a single point of control/failure. The Authority may or may not be telling the truth or corrupted. The solution to this is to employ a decentralised and distributed system where the consensus of the users/peers is used to evaluate the transactions/votes/data. We are creating a web portal for casting a vote online. But our work is not over, Securing the casted vote is a challenging one. Many fraudsters try to manipulate the data in their favour. In our case, It doesn't occur because we created it with the help of blockchain technology.

1.1 PRIOR WORK

In a democratic country like India (which is the largest democracy in the world), Voting plays a major role in the selection of government officials as well as showing our opinion how the governing body to be formed. Time to time, researches are conducted in order to tackle the difficulties in the centralized voting system to make it more anonymous, reliable and secure while preventing any kind of fraud. Even though the use of e-voting through the electronic medium, we have to face well-known problems of maintenance and fraud. Currently, various researches are conducting in order to make secure and reliable voting system while tackling issues of anonymity and security. Through Decentralized System, focus is drifting towards making Voting Process simple, secure and anonymity in the hand of the public. This paper presents a literature review on the papers and the techniques used to tackle voting challenges.

1.2 PROBLEM DEFINITION

Decentralized e-voting is preferably executed online rather than traditional voting. This introduces various, distinctive challenges concerning primarily transparency, privacy, correctness, and integrity. It is crucial to understand that solving these fundamental challenges is an open research question. Nonetheless, for this report, it is assumed that blockchain technology provides transparency and immutability due to its cryptographic properties and can offer insights into some of the challenges. Therefore, it is a feasible foundation for the intended system. However, blockchain alone might not provide the optimal solution for an electronic voting system. In order to narrow down the subject and define a primary set of questions correlated to the research, one

main challenge will consequently be introduced. The main challenge will additionally be systematically broken further down into subtasks, each constrained and defined in order to facilitate a quantitative research and generate a proof of concept which is stated as the following. How does one implement a minimum valuable decentralized voting system, utilizing blockchain technology and being capable of handling voting, showing votes and verifying correctness? This challenge consequently harvests several concerns. The central research will nonetheless define three requirements for the intended voting system. The requirements are constructed as subtasks of the central task, namely the challenge of building a decentralized voting system. The subtasks incorporate the following areas of research, all of which define the area of research with specific questions.

1.3 PROJECT OVERVIEW/SPECIFICATIONS

The objective of this venture is to construct a web application utilizing blockchain innovation where individuals can vote from anyplace in the event that he/she have a substantial Citizenship of individual nation where he/she needs to vote and ensure each and every vote to guarantee that each and each vote things. The endless lion's share of the continuous work examines security, precision, respectability, speed, security, and survey capacity be that as it may existing systems are frail for ambushes at a few degree.

Disadvantages of Existing System

1. Centralized architecture.
2. Attack prone.
3. Not trustable.
4. Non-transparent vote casting process.

The existing systems are likely to be attacked and are either easily hackable or very difficult to maintain. Data integrity and security are the major concerns and the proposed solution should be able to deal with all the limitations of the existing system

1.4 HARDWARE SPECIFICATIONS

1) Processor type : Intel core i3 and above

2) Processor speed : Minimum 2.00 GHz and above

3)RAM : 4-8 GB

4)HARD DISK : 400 GB or more

5)Monitor : 800x600 or higher resolution

6) Keyboard : 110 keys enhanced

1.5 RELATED WORK

The e-voting concept and the blockchain technology share a common fate, that is, both of them started to be used publicly and commercially, before the academic studies pave the way for better solutions and standardization. Due to lack of academic collaborations, their development has been conducted predominantly out of the academia, until recently. For example; a promising collaborative project mostly funded by the European Union, called “An innovative cyber voting system for Internet terminals and mobile phones” was ended prematurely, without concluding with a voting system as a product. Hence, in this section we preferred to focus more on public and commercial advances, without ignoring researches. A. E-Voting Applications Your paper must use a page size corresponding to A4 which is 210mm (8.27") wide and 297mm (11.69") long. The Since 1990s, e-voting, at least as an idea, is being placed in laws and regulations in many countries. But, only a few of these countries has ever used a real implementation during official elections or referenda. And even fewer of them are still using e-voting. Two main reasons we have noticed of quitting use of e-voting are broad suspicion of frauds and implementational/deployment costs. We have looked through some of the remarkable examples throughout the world. However, the e-voting attempts are surely not limited to these, especially the voting machines were used widely, and are still in use in some states. They are out of our scope and not comprehensively included in our survey. More information on them and their security flaws, can be found elsewhere. Trust, Autonomy and intermediaries are three big problems which we are facing in present time like we are obliged to trust banks for securing our money for our transactions. We depends upon these third parties to ensure our privacy and security in terms of our data

CHAPTER-2

BACKGROUND OF THE PROJECT

2. BACKGROUND OF PROJECT

2.1 BLOCKCHAIN

A blockchain is a distributed data structure that is replicated and shared among the members of a network. It was introduced with Bitcoin to solve the double-spending problem". Blockchains are essentially decentralized, distributed, public ledgers. The ledger is organized into blocks, where each block is a digital piece of information about transactions. Each block characteristically contains a cryptographic hash of the previous block to assure there is a standard order to the blocks. This links the blocks and builds symbolically a chain and gives the blockchain two essential properties; a modification of the earlier block will invalidate all the previous, and anyone can verify the whole chain given the first genesis block. Blocks are created based on the latest block of the most current chain and are processed by nodes in a Peer-to-Peer network. Every creation follows a consensus mechanism, which is essentially a protocol, in order to agree which transactions are legitimate and added to the blockchain. This is feasible with cryptography and necessary to assure correctness. The protocol assures that everyone has the same pieces of information about the transactions. Information on the blockchain is transparent and anyone can view the content of a blockchain. Transactions on the blockchain are not completely anonymous. However, information about the users is limited to their digital signature.

2.1.1 TRANSACTIONS

A transaction is a set of instructions for modifying the state of the blockchain. Transaction fees are a part of public blockchain networks in order to have the transactions processed by specialized nodes, or so-called miners, and confirmed by the network . Miners perform computational work for a financial reward. In order to fundamentally understand what a state of a blockchain is, it is necessary to shortly introduce Unspent Transaction Outputs (UTXOs for short) for the following reason. In Bitcoin, the transfer of value is actualized through transactions. Bitcoin's state is represented by its global collection of UTXOs, that is, Bitcoin does not maintain user account balances. A user's account balance is the sum total of each individual UTXO, for which that user holds the corresponding private key. In contrast, there are other blockchains that are able to manage account balances and more, for example Ethereum which is a transaction-based state machine, meaning that all transaction-based state machine concepts may be built on it.

2.1.2 DIGITAL WALLETS

Each user that wants to make a transaction is associated with an asymmetric key pair, a private key, and a public key. The public key is associated with a digital wallet which serves as an address to the user, with no connection to the user's identity. It is public, available to anyone. The private key, on the other hand, is kept secret to assure only the owner of that wallet can sign valid transactions. Transactions are considered valid when they are signed with the user's private key, providing a digital signature which makes it unfeasible to forge. Transactions are therefore unique and only the owner can generate the unique digital signature.

2.1.3 MINERS

As mentioned, transactions are only valid when they are signed by the sender. They are broadcasted to the network where they are collected and packed into blocks by miners, who then, partially given the public key attached to each transaction, validate the signatures and build the next block. Hence, blocks are built by miners on the network, solving asymmetric, non-deterministic puzzles by means of a consensus mechanism . This was originally addressed in the Bitcoin paper and solves the famous double-spending problem, which is basically the risk that a digital currency can be spent twice . Fundamentally, Bitcoin solved the double-spending problem and can as a consequence assure integrity, at least to a certain extent. Hypothetically, a group of miners could potentially control more than 50% of the network computing power and forge the blockchain. This group would then gain a monopoly over the blockchain and be able to prevent new transactions, only allowing certain users to transact or forge transactions. This hypothesis is called 51%-Attack.

2.2 ETHEREUM

Shortly after blockchain technology was introduced and implemented with Bitcoin, a new era of digital currency was born, giving rise to crypto economics, which Ethereum originates from. However, it is an adaptation of its core properties with the purpose to create a decentralized network with memory, for a whole variety of other applications. Ethereum is a general purpose blockchain that understands a general-purpose programming language. It is able to store data and is capable of enforcing the protocol's correct execution. Ethereum was released in 2015 and became a framework for applications that were in need of decentralization and a concept of shared memory. It allows developers to write smart contracts and put them on the blockchain.

The logo of Ethereum is:

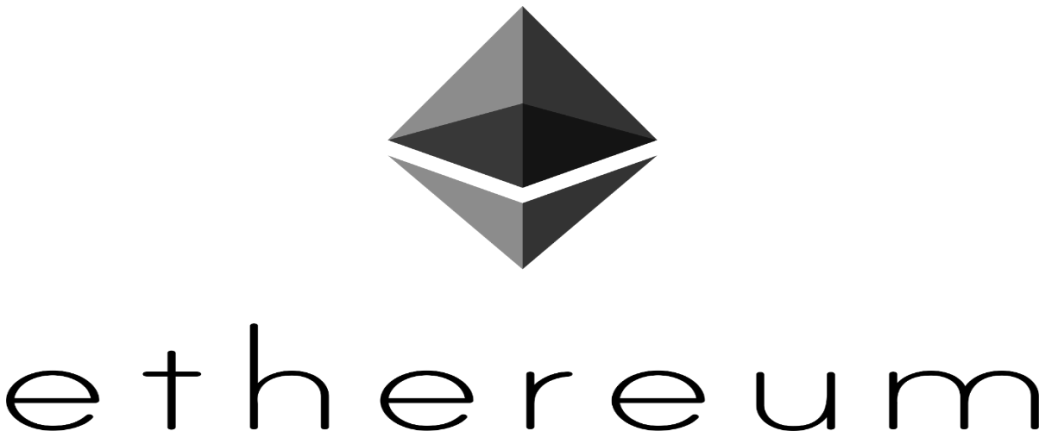


Figure 2.1: Logo of Ethereum

2.2.1 SMART CONTRACTS

The idea behind a smart contract was originally by Nick Szabo . The concept is analogous to the notion of a vending machine. It is a device which implements the conditions of an agreement. Essentially, a user inputs a given amount of currency which yields a specific output; contrary, a user does not input the given amount which yields no output . This is the core idea behind Ethereum. It is basically a software containing rules for negotiating the terms of the contract which govern the behavior of accounts within the Ethereum state. Since the smart contract of Ethereum is implemented on the blockchain, the contract is visible to all the users.

2.2.2 SOLIDITY

In order to build such contracts there is a specialized programming language named Solidity. It is a high-level, object-oriented language for implementing smart contracts that are represented similarly to classes in object-oriented languages. The contracts are a collection of code and data in state variables. These embody its functionality and state . The contracts are deployed at a specific address on the Ethereum blockchain. Contracts obtain specific rules who grant permissions to who and what to read and write on the contract. There are for example four types of visibilities for functions and state variables: external, public, internal or private. They have to be specified and serve a similar function to those in other object-oriented languages, namely public and private variables. It is

important to understand that everything inside a contract is visible to anyone observing the blockchain. A private variable only prevents others from accessing and modifying the information. However, it is still visible to anyone outside of the blockchain.

The logo of solidity is:

Figure 2.2 : the logo of solidity

2.2.3 ARCHITECTURE

Unlike Bitcoin, Ethereum has the property that every block contains something called the state root. It is a special kind of data structure called Merkle tree that stores the entire state of the system. It allows a node, given only the most recent block, to synchronize with the blockchain quickly, without processing any historical transactions. Like the basic Merkle tree, any piece of data inside the tree to be securely authenticated against a root hash . It also has the property that data can be added, removed or modified in the tree quickly, without making changes to the entire structure. The tree is used in Ethereum to store transactions, receipts, accounts and the storage of each account.

2.3 PARTICIPANTS

• **Voters**: It contain set of all eligible voters defined by V={v1, v2, v3.....vn}, where n is the total numbers of eligible voters.

• **Organizers**: It contain set of all Election Organizer (EO)=1, which is responsible for managing and verifying the voter identity during the election.

• **Inspectors:** It is responsible for inspect the organizer behavior and limit the power of the organizer.

CHAPTER- 3

LITERATURE SURVEY

3. LITERATURE SURVEY

3.1 OVERVIEW

We have proposed an electronic voting system based on the Blockchain technology. The system is decentralized and does not rely on trust. Any registered voter will have the ability to vote using any device connected to the Internet. The Blockchain will be publicly verifiable and distributed in a way that no one will be able to corrupt it. We as well illustrated the limitations with our system, which will be addressed in future research papers. The blockchain voting system is decentralized and completely open, yet it ensures that voters are protected. This implies that anybody may count the votes with blockchain electronic voting, but no one knows who voted to whom.

3.2 REVIEWS OF RELATED PAPER

1. Singh, A., & Chatterjee, K. (2018, September). Secevs: Secure electronic voting system using blockchain technology. In 2018 International Conference on Computing, Power and Communication Technologies (GUCON) (pp. 863-867). IEEE.

In todays digital environment, the voting system move from paper based to a digital system. A digital e-voting system have many properties such as transparency, decentralization, irreversibility, and non-repudiation. The growth in digital e-voting system arises many security and transparency issues. In this paper, we used the blockchain technology in digital e-voting system to solve the security issues and fulfill the system requirements. It offers new opportunities to deploy a secure e-voting system in any organization or country. The solution is far better as compared to other solution because, it is a decentralized system, contain the results in the form of bit-coins, having different locations. We will also analyze the security of our proposed voting system, which shows our protocol is more secure as compared to other solutions.

2. Bosri, R., Uzzal, A. R., Al Omar, A., Hasan, A. T., & Bhuiyan, M. Z. A. (2019, August). Towards a privacy-preserving voting system through blockchain technologies. In 2019 IEEE Intl Conf on Dependable, Autonomic and Secure Computing, Intl Conf on Pervasive Intelligence and Computing, Intl Conf on Cloud and Big Data Computing, Intl Conf on Cyber Science and Technology Congress (DASC/PiCom/CBDCom/CyberSciTech) (pp. 602-608). IEEE.

To this day, abstention rates continue to rise, largely due to the need to travel to vote. This is why remote e-voting will increase the turnout by allowing everyone to vote without the need to travel. It will also minimize the risks and obtain results in a faster way compared to a traditional vote with paper ballots. In fact, given the high stakes of an election, a remote e-voting solution must meet the highest standards of security, reliability, and transparency to gain the trust of citizens. In literature, several remote e-voting solutions based on blockchain technology have been proposed. Indeed, the blockchain technology is proposed today as a new technical infrastructure for several types of IT applications because it allows to remove the TTP and decentralize transactions while offering a transparent and fully protected data storage. In addition, it allows to implement in its environment the smart-contracts technology which is used to automate and execute agreements between users. In this paper, we are interested in reviewing the most revealing e-voting solutions based on blockchain technology.

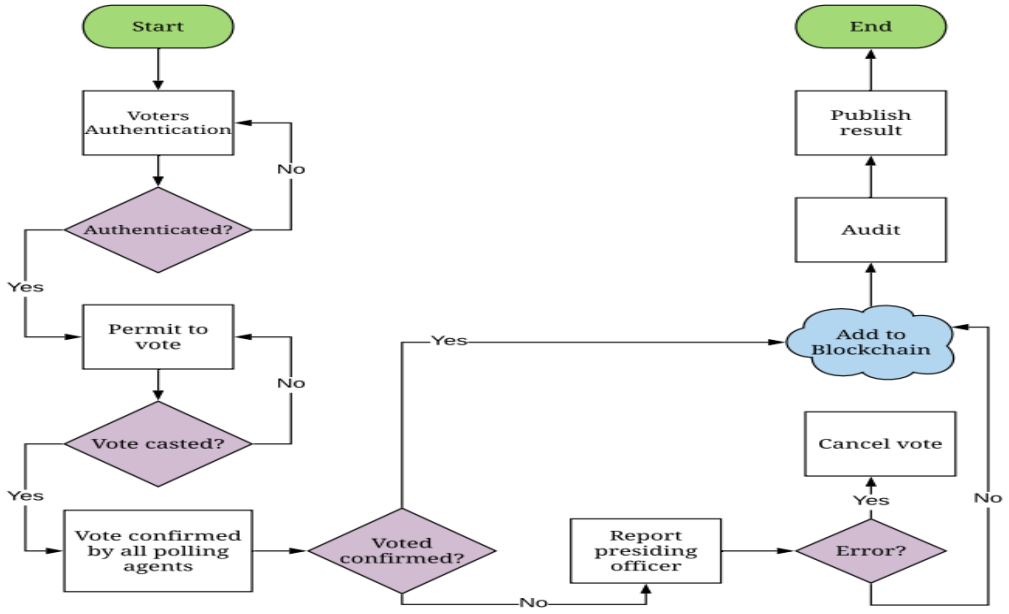


Figure 3.1: Overall voting process in flow diagram

3. Kshetri, N., & Voas, J. (2018). Blockchain-enabled e-voting. Ieee Software, 35(4), 95-99

The development of digital technology has changed the lives of many people in terms of the velocity and convenience of completing tasks. This technology has also been applied to the process of voting, yet electronic voting is seldom used. The existing electronic voting scheme operates by applying various encryption algorithms. This type of electronic voting can be problematic since the administrator is given full authority. The administrator cannot always be trusted, and the contents of the ballot could be forged or tampered by a single point of failure. To resolve these problems, researchers continue to apply blockchain technology to electronic voting.

4. Hjálmarsson, F. Þ., Hreiðarsson, G. K., Hamdaqa, M., & Hjálmtýsson, G. (2018, July). Blockchain based e-voting system. In 2018 IEEE 11th international conference on cloud computing (CLOUD) (pp. 983-986). IEEE

Building a secure electronic voting system that offers the fairness and privacy of current voting schemes, while providing the transparency and flexibility offered by electronic systems has been a challenge for a long time. In this work-in-progress paper, we evaluate an application of blockchain as a service to implement distributed electronic voting systems. The paper proposes a novel electronic voting system based on blockchain that addresses some of the limitations in existing systems and evaluates some of the popular blockchain frameworks for the purpose of constructing a blockchain-based e-voting system.

5. Benabdallah, A., Audras, A., Coudert, L., El Madhoun, N., & Badra, M. (2022). Analysis of blockchain solutions for e-voting: A systematic literature review. IEEE Access

To this day, abstention rates continue to rise, largely due to the need to travel to vote. This is why remote e-voting will increase the turnout by allowing everyone to vote without the need to travel. It will also minimize the risks and obtain results in a faster way compared to a traditional vote with paper ballots. In fact, given the high stakes of an election, a remote e-voting solution must meet the highest standards of security, reliability, and transparency to gain the trust of citizens. In literature, several remote e-voting solutions based on blockchain

technology have been proposed. Indeed, the blockchain technology is proposed today as a new technical infrastructure for several types of IT applications because it allows to remove the TTP and decentralize transactions while offering a transparent and fully protected data storage. In addition, it allows to implement in its environment the smart-contracts technology which is used to automate and execute agreements between users. In this paper, we are interested in reviewing the most revealing e-voting solutions based on blockchain technology.

3.3 FEASIBILITY STUDY

Applications involving e-voting and the Blockchain technology have big social impacts, too. These impacts can further be listed as the value obtained from the provided ease of use and the people's perception of trust to these so-called "high tech" systems. Generally, the e-Government services enabled wider, easier, and faster access to the government services for the people, including the ones living in remote settlements and the ones who are very busy and/or mobile. So that it can be seen as a powerful tool that reinforces the government-citizen relationships . While the eGovernment itself is not directly related to the democracy, the concept of e-voting extends the e-Government to provide means of democracy, called e-Democracy. The ease of use and the financial benefits of such e-services are no more under discussion , but the perception of trust, a newer concern brought by the services related to e-democracy, might be shadowing these benefits, when it comes to e-voting. Independent from the topic and theme, if the majority of the voters do not trust the proposed e-voting system, then this system should not be accepted as the only way of voting. This applies even if the concerns are totally void and unsound or just conspiracy. This also explains why Estonia still holds both traditional and online elections together. Several studies showed that the trust in such electronic voting systems are considerably low (or at least not high as the traditional systems) , and some institutions and researchers started to propose ways to improve that trust already. The trust in e-voting, if can be increased successfully, would even increase the overall trust to the general political system, especially in the developing countries . Use of blockchain technology, which is used in the popular cryptocurrency Bitcoin (and many others) may strengthen the perception of trust, since Bitcoin and other cryptocurrency transactions are widely known to supply trust to the transactions, even between untrusted parties, as long as users are aware of some security countermeasures.

CHAPTER -4

SYSTEM ANALYSIS AND DESIGN

4. SYSTEM ANALYSIS & DESIGN

4.1. REQUIREMENT SPECIFICATION

Our target is to build a model which allows a user to cast vote providing immutabilty, security, speed, transparency also provides a decentralized model i.e if one server goes down or something happens on a particular node, other nodes can function normally and do not have to wait for victim node's recovery.

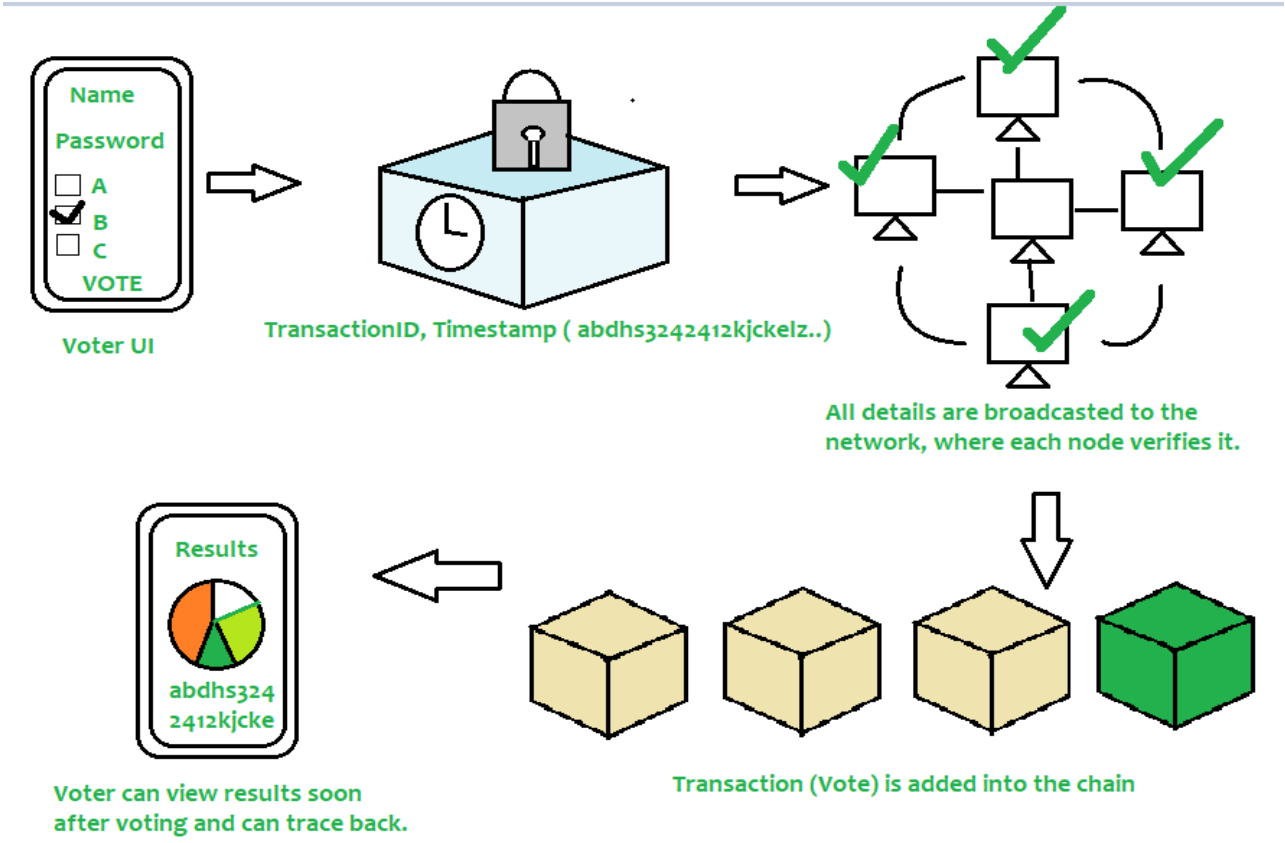


Figure 4.1: Model for decentralized voting system using blockchain

The purpose of the smart contracts is to act as a back-end for the system. They contain different variables, functions and providing rules for how the voting process works. Due to the limitations

of Ethereum, such as private variables that are not truly private and all transactions being public, solutions for keeping data inaccessible had to be made. Specialized tools were used to support the development of smart contracts: A web application was made to act as a GUI for the election process. This application was developed using React. The application simulates the original design. It generates voter IDs, stores them, retrieves a public key to encrypt the vote on the client side using a cryptographic library. The application then stores encrypted votes over transactions made to the smart contract. Due to constraints in Solidity, there is no easy way to fetch a whole map or array from the smart contract. This had to be done manually by getting each vote one by one from the contract and decrypt them in the process. There are several third-party dependencies used for the Web application to make the application more user-friendly. The prototype consists of five parts, each built to simulate how the election would take place in reality.The four parts of the Web application are presented with different GUIs.

4.2 OBJECTIVES:

The objective of an E-voting system using blockchain is to create a secure and transparent platform for conducting fair and democratic voting processes. This system utilises blockchain technology to ensure the accuracy and security of the voting process by providing an immutable and decentralised ledger of all transactions.

4.3 METHODOLOGY:

The working methodology of an E-voting system using blockchain can be summarised in the following steps: 3.2.1 Identity verification Voters are required to register and provide their identity information to be verified before being able to vote. The identity verification process is conducted by a trusted third-party organisation. Identity verification is an essential aspect of an online polling system using blockchain technology. The goal of identity verification is to ensure that the person casting the vote is authorised to do so and that the voting process is conducted fairly and securely. The process of identity verification involves several steps, including collecting personal information from the voter, verifying the identity of the voter, and ensuring that the voter is eligible to vote. Blockchain technology provides a secure and transparent platform for identity verification. The blockchain ledger can be used to store and verify identity information, which ensures the

accuracy and security of the voting 10 process. The blockchain ledger is decentralised, which means that there is no central authority or control, and the risk of fraud is significantly reduced. The identity verification process starts with the collection of personal information from the voter, such as name, address, and date of birth. This information is stored on the blockchain network, where it can be accessed and verified by the network participants. Once the personal information is collected, the identity of the voter is verified using various methods, such as facial recognition or biometric authentication. This ensures that the person casting the vote is the same person whose identity has been verified. Ultimately, the voter's eligibility to vote is checked, which includes their citizenship or age. that is additionally tested the usage of the facts saved at the blockchain community. It's far a critical aspect of an online polling machine, the use of blockchain generation. The use of the blockchain era affords a comfortable and obvious platform for verifying voter identification, ensuring the accuracy and safety of the vote casting procedure. The decentralised nature of the blockchain network considerably reduces the chance of fraud and guarantees that the voting system is performed fairly and securely.

4.3.1 Creation of a digital ballot:

A digital ballot is created, and candidates or propositions are listed. The creation of a digital ballot is an essential aspect of an online polling system using blockchain technology. The digital ballot is a list of candidates or propositions that voters can choose from when casting their vote. The goal of creating a digital ballot is to ensure that the voting process is fair and 11 transparent, and that all eligible voters have an equal opportunity to cast their vote. To create a digital ballot, the blockchain network first collects all the candidates or propositions that will be included in the ballot. This information is then verified to ensure that it meets the eligibility criteria for inclusion in the ballot. Once the information is verified, it is added to the blockchain network, and a digital ballot is created. The digital ballot is designed to be user-friendly and accessible to all eligible voters. It may include information about each candidate or proposition, such as their name, party affiliation, and a brief description of their platform. The digital ballot may also include instructions on how to cast a vote and how to verify that the vote has been successfully recorded on the blockchain network. The usage of the blockchain era within the creation of a virtual ballot affords numerous benefits. The decentralised nature of the blockchain community ensures that the vote casting procedure is transparent and comfy, as there may be no valuable authority controlling the system. Moreover, the

blockchain ledger offers an immutable file of all transactions, which guarantees that the integrity of the voting manner is maintained. The digital ballot is designed to be user-friendly, transparent, and secure, ensuring that all eligible voters have an equal opportunity to cast their vote. The use of blockchain technology provides a decentralised and immutable ledger, which ensures that the voting process is conducted fairly and transparently, without the risk of fraud or manipulation

4.3.2 Encryption of Votes:

Voters cast their votes anonymously, and the vote is encrypted using advanced cryptography. Encryption of votes is an vital element of an online polling gadget the use of the blockchain era. The purpose of encrypting votes is to make certain that the votes are nameless, comfortable, and can not be manipulated or tampered with. Encryption is performed through the usage of superior cryptographic algorithms, which make certain that the votes are securely saved at the blockchain network. Once a voter has solid their vote, the vote is encrypted using superior cryptographic algorithms. This ensures that the vote is anonymous and can not be traced back to the voter who solidified it. The encrypted vote is then delivered to the blockchain network, in which it can be validated and counted. Using blockchain generation in the encryption of votes affords numerous advantages. The decentralised nature of the blockchain network ensures that the vote casting method is obvious and comfortable, as there's no critical authority controlling the system. In addition, the usage of cryptography ensures that the votes are cosy and cannot be manipulated or tampered with. To ensure that the encryption of votes is secure, the cryptographic algorithms used are constantly updated and reviewed. This ensures that the voting process remains secure and that the risk of fraud or manipulation is minimised. The use of advanced cryptographic algorithms ensures that the votes are anonymous, secure, and cannot be manipulated or tampered with. The decentralised nature of the blockchain network ensures that the voting process is transparent and secure, providing voters with confidence in the integrity of the voting process. The use of cryptography is constantly reviewed and updated, ensuring that the voting process remains secure and that the risk of fraud or manipulation is minimised. 13

4.3.3 Distribution of the encrypted votes:

The encrypted votes are distributed across the blockchain network, which consists of multiple nodes, each of which has a copy of the ledger.The distribution of encrypted votes is a crucial aspect of an online polling system using blockchain technology. Once the votes have been validated and counted, the next step is to distribute the encrypted votes to authorised participants who have accessto the decryption key. This distribution process ensures that the authorised participants can decrypt the votes and tally them up. The distribution of encrypted votes is carried out through a process known as key management. The decryption key is generated by the blockchain network, and only authorised participants have access to it. These participants use the key to decrypt the encrypted votes, tally them up, and record the results on the blockchain ledger. The decentralised nature of the blockchain network ensures that the distribution process is transparent and secure, as there is no central authority controlling the process. The use of blockchain technology in the distribution of encrypted votes provides several benefits. The decentralised nature of the blockchain network ensures that the distribution process is transparent and secure, providing voters with confidence in the integrity of the voting process. Additionally, the use of key management ensures that only authorised participants have access to the decryption key, minimising the risk of fraud or manipulation. To ensure that the distribution of encrypted votes is secure, the key management process used is constantly updated and reviewed. This ensures that the voting process remains secure and that the risk of fraud or manipulation is minimised. The key management ensures that only authorised participants have access to the decryption key, minimising the risk of fraud or manipulation

4.3.4 Validation of votes:

The blockchain network validates the encrypted votes to ensure their authenticity and accuracy. Validation of votes is an essential aspect of an online polling system using blockchain technology. The goal of validating votes is to ensure that only authorised votes are counted, and the vote process is fair and transparent. Validation of votes is achieved by using consensus algorithms, which ensure that all nodes on the blockchain network agree on the validity of a vote. Once a vote has been cast, it is added to the blockchain network, where it is verified and validated by the nodes on the network. The consensus algorithm ensures that all nodes on the network agree on the validity of the vote

before it is recorded on the blockchain ledger. This process ensures that only authorised votes are counted, and the voting process is fair and transparent. The use of blockchain technology in the validation of votes provides several benefits. The decentralised nature of the blockchain network ensures that the voting process is transparent and secure, as there are no central authority controls. Additionally, the use of consensus algorithms ensures that the voting process is fair and that all authorised votes are counted. To ensure that the validation of votes is secure, the consensus algorithms used are constantly updated and reviewed. This ensures that the voting process remains secure and that the risk of fraud or manipulation is minimised. The use of consensus algorithms ensures that all authorised votes are counted, and the voting process is fair and transparent. The decentralised nature of the blockchain network ensures that the voting process is transparent and secure, providing voters with confidence in the integrity of the voting process. The use of consensus algorithms is constantly reviewed and updated, ensuring that the voting process remains secure and that the risk of fraud or manipulation is minimised.

4.3.5 Counting of votes:

Once the validation is complete, the votes are counted, and the results are posted on the blockchain network for public verification. Counting votes is a crucial step in the online polling system using blockchain technology. Once the votes have been cast and validated, the next step is to count them accurately. Counting votes on the blockchain network involves using cryptographic algorithms to decrypt the encrypted votes and tally. The counting process is carried out by authorised participants who have access to the decryption key. These participants decrypt the encrypted votes, tally them up, and record the results on the blockchain ledger. The decentralised nature of the blockchain network ensures that the counting process is transparent and secure, as there are no central authority controls. The use of blockchain technology in the counting of votes provides several benefits. The decentralised nature of the blockchain network ensures that the counting process is transparent and secure, providing voters with confidence in the integrity of the voting process. Additionally, the use of 16 cryptography ensures that the votes are secure and cannot be manipulated or tampered with. To ensure that the counting of votes is accurate, the cryptographic algorithms used are constantly updated and reviewed. This ensures that the voting process remains secure and that the risk of fraud or manipulation is minimised. Counting votes is a critical aspect of an online polling system using blockchain technology. The use of cryptographic algorithms ensures that the votes

are decrypted securely and accurately tallied up. The decentralised nature of the blockchain network ensures that the counting process is transparent and secure, providing voters with confidence in the integrity of the voting process. The use of cryptography is constantly reviewed and updated, ensuring that the voting process remains secure and that the risk of fraud or manipulation is minimised. The use of blockchain technology provides several advantages, including transparency, security, and immutability. Because the ledger is decentralised, there is no central authority, and the risk of fraud is significantly reduced. Additionally, since the blockchain is immutable, the integrity of the voting process is maintained, and the results can be verified at any time. In conclusion, a polling system using blockchain provides a secure, transparent, and trustworthy platform for conducting fair and democratic elections.

Algorithm 1 Electronic Voting System

1: procedure INPUT:(voter User Id, voter Password)

2: OUTPUT: Complete vote in the form of blockchain

3: BEGIN

4: The voter registered with the voting system.

5: Get the voter ID, choose the password and private key.

6: if (voter Id == registered voter Id) and (voter is eligible) then

7: Enter your password.

8: else

9: voter is not registered or he is not eligible.

10: if (Password is correct) then

11: Open the candidate choosing page and choose the candidate.

12: else

13: Enter the correct password.

14: Encryption of voting data- ENCRY P TpubkeyUEC (vote)

15: Signing the encrypted data - SIGNV prikey(EpubkeyUEC (vote))

16: Generation of the block BLOCK(block header+encrypted block data).

17: END

4.3.6 SMART CONTRACTS

The purpose of the smart contracts is to act as a back-end for the system. They contain different variables, functions and providing rules for how the voting process works. Due to the limitations of Ethereum, such as private variables that are not truly private and all transactions being public, solutions for keeping data inaccessible had to be made. Specialized tools were used to support the development of smart contracts.

4.3.10 CRYPTOGRAPHY

In order to avoid visible results while the election is running, votes were encypted using an open source library called ecrypto, which in turn is wrapped in an open source Javascript library eth-crypto, specifically built for Ethereum transactions It utilizes ECDSA encryption algorithm that is originally implemented by the Ethereum blockchain.

CHAPTER 5

PROPOSED METHODOLOGY

Designing an e-voting system using blockchain technology involves several key modules to ensure security, transparency, and user accessibility.

5.1 USER AUTHENTICATION MODULE:

MetaMask, a popular browser extension for managing Ethereum-based assets, will be integrated for user authentication. MetaMask's secure and decentralised nature ensures a trustworthy authentication process. Users will log in securely using their MetaMask credentials, adding an additional layer of protection against unauthorised access.

5.2 VOTER REGISTRATION MODULE:

Implement a user-friendly voter registration process. Validate and store voter information securely on the blockchain using smart contracts. Link MetaMask wallet addresses to individual voter profiles for seamless authentication during the voting process. Develop a verification mechanism to ensure the validity of voter registrations. Utilise blockchain's transparency to allow stakeholders to audit the voter registration process. Implement additional security measures to prevent fraudulent registrations.

5.3 BLOCKCHAIN INTEGRATION MODULE:

Choose a suitable blockchain platform, such as Ethereum, for recording and storing votes securely. Utilise smart contracts to define the rules and logic of the election, ensuring transparency and immutability. Develop smart contracts that handle the voting process, ensuring one vote per eligible voter. Include logic for vote counting, result determination, and other election-related processes. Implement robust error handling to address any unforeseen issues during the voting period

5.4 VOTING MODULE:

Enable users to cast their votes securely using MetaMask. Implement a userfriendly interface that guides voters through the voting process. Ensure that each voter can only cast one vote to maintain the integrity of the election. Design the voting process to maintain voter anonymity. Use cryptographic techniques to encrypt and protect voter data, preventing the identification of individual votes. Leverage blockchain's decentralised nature to enhance the privacy of the voting process.

5.5 VERIFICATION MODULE:

Provide a transparent verification process for voters to confirm that their votes have been recorded accurately. Enable users to access a public ledger containing encrypted vote details without

compromising individual voter identities. Implement mechanisms for voters to report any discrepancies or issues with their votes. Ensure that the blockchain is tamper-resistant, preventing any unauthorised alterations to the recorded votes. Implement regular audits to verify the integrity of the voting data stored on the blockchain. Utilise cryptographic hashing to secure the immutability of the vote records.

4.6 RESULT MODULE:

Design a module for counting and presenting election results in a clear and understandable format. Implement visualisation tools to display results graphically, aiding stakeholders in interpreting the outcome. Ensure that results are accessible to all stakeholders in a transparent manner. Implement measures to prevent tampering with election results. Leverage blockchain's consensus mechanisms to validate and confirm the accuracy of the results. Provide stakeholders with tools to independently verify the results for increased transparency.

4.7 SECURITY MODULE:

Implement robust access control measures to prevent unauthorised access to the e-voting system. Utilise role-based access controls to ensure that only authorised personnel can modify system configurations or access sensitive data. Utilise advanced encryption techniques to secure voter data and communication channels. Implement end-to-end encryption for all user interactions within the system. Regularly update encryption protocols to address emerging security threats. Conduct normal protection audits and vulnerability checks to perceive and cope with capability weaknesses within the gadget. establish a protocol for right away addressing and patching security vulnerabilities. Collaborate with security experts to stay knowledgeable about cutting-edge threats and mitigation techniques. Incorporating these detailed modules and considerations will contribute to the development of a robust, secure, and transparent e-voting system using blockchain technology

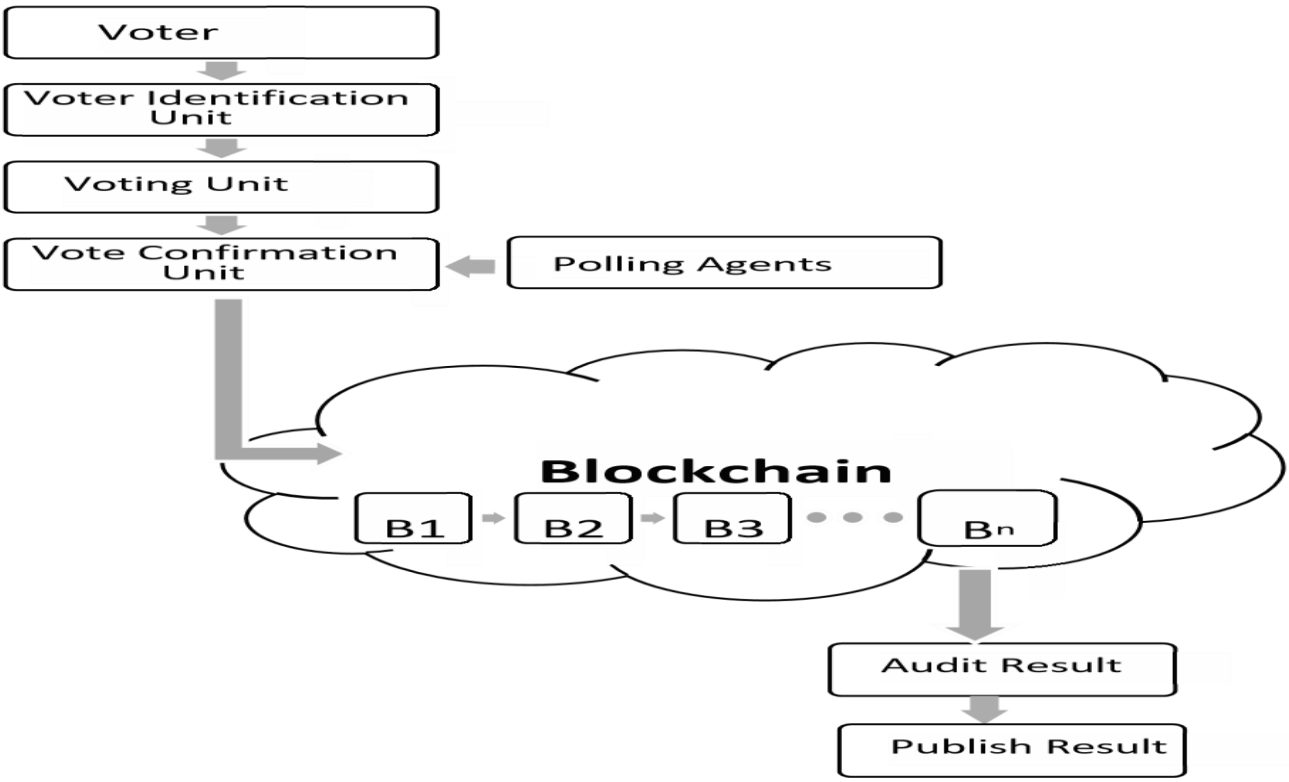
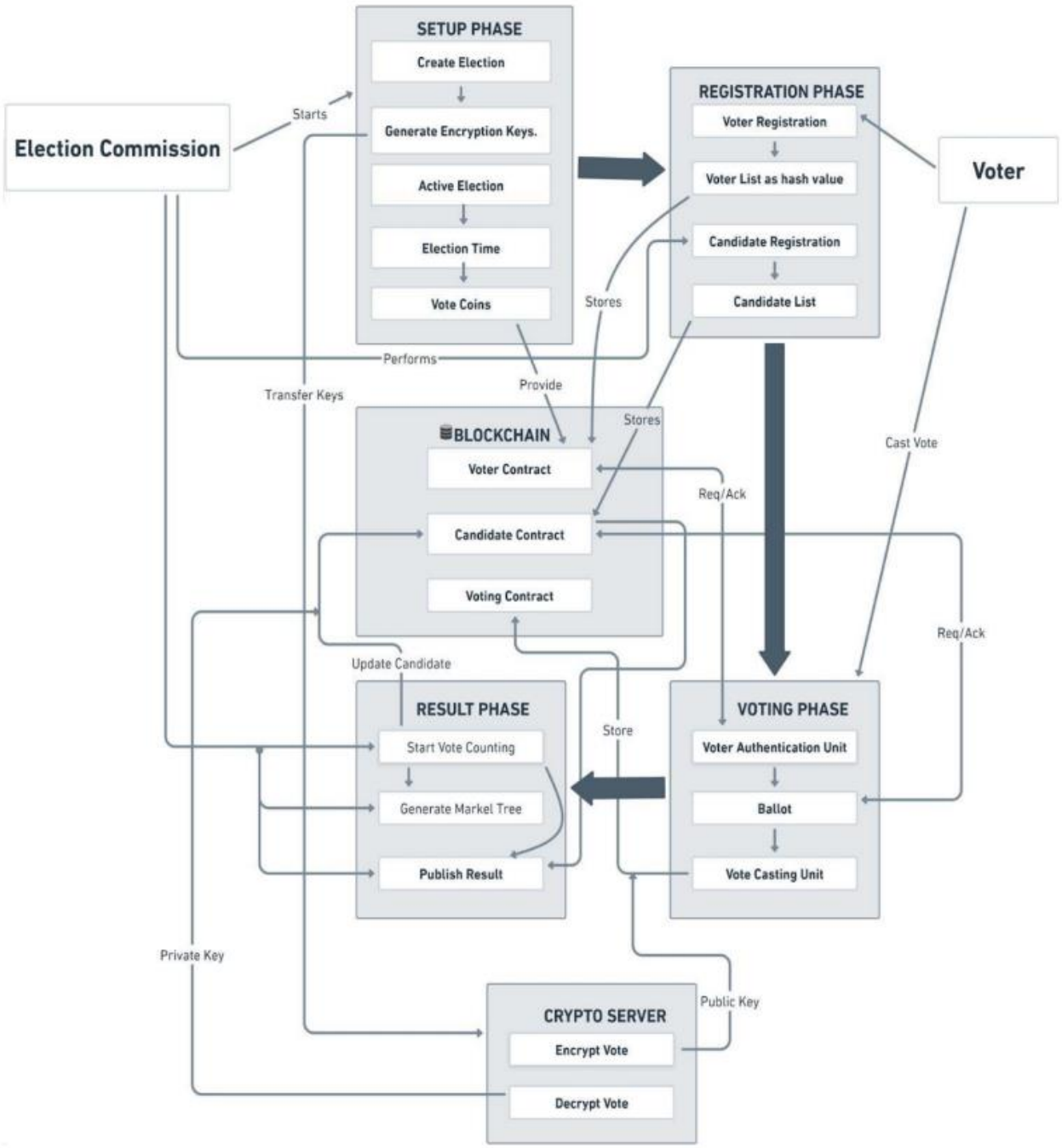


Figure 5.1: Flowchart of Online voting system using Blockchain

5.2 Figure : Architecture Of System



CHAPTER-6

CONCLUSIONS AND FUTURE SCOPES

6.1 CONCLUSIONS:

Conclusively, blockchain-based online polling platforms offer a potentially effective means of providing a promising solution for improving and enhancing voting process integrity. By leveraging the security, transparency, and decentralisation inherent in blockchain, many of the issues with traditional voting systems can be resolved by using online polling platforms. The voting process is protected against fraud, tampering, and hacking by the tamper-proof ledger of blockchain technology. The use of cryptographic techniques ensures voter anonymity while still allowing for transparent verification of voting results. Integrating with tools like Metamask provides a user-friendly interface for voter authentication, enhancing accessibility and usability. However, implementing online polling in blockchain technology also poses challenges, such as ensuring inclusivity, protecting voter privacy, and navigating regulatory frameworks. Addressing these challenges requires careful planning, robust technological infrastructure, and collaboration with stakeholders. Finally after the results are published you are able to view and even can download it as PDF files. Overall, blockchain-enabled online polling has the power to increase trust in democratic institutions, democratise politics, and increase voter turnout. Blockchain-based online polls can open the door to more inclusive, safe, and transparent elections in the digital era with continued innovation and improvement.

6.2 FUTURE SCOPES:

Increased Adoption: As blockchain technology matures and gains wider acceptance, online polling systems should become more widely used by governments, organisations, and communities around the world. This adoption will drive further innovation and refinement of blockchain-based voting platforms.

Enhanced Security Features: Future developments in blockchain technology will likely introduce even more robust security features to protect against emerging threats. This could include advancements in encryption techniques, multi-factor authentication methods, and consensus techniques to guarantee the voting process's integrity.

Scalability Solutions: Blockchain networks still struggle with scalability, especially when it comes to managing massive online polling events with millions of participants. Online polling platforms will be able to perform better when blockchain scalability solutions like sharding, sidechains, or layer 2 protocols become more advanced.

Smart Contract Integration: Voter registration, ballot counting, and result tabulation are just a few of the electoral procedures that smart contract self-executing contracts with the terms of the deal clearly written into code can automate. Future advancements in clever contract technology will enable more complex and sophisticated voting mechanisms to be implemented on blockchain-based platforms.

Mobile and IoT Integration: Due to the widespread use of mobile and Internet of Things (IoT) devices, future online polling platforms may leverage these technologies to enhance accessibility and convenience for voters. Mobile voting apps and IoT-enabled voting devices could enable voters to participate in polls from anywhere, at any time, using their smartphones or connected devices.

Global Impact: Blockchain-powered online polling has the potential to democratise the voting process on a global scale, enabling disenfranchised populations, such as refugees, expatriates, and those living in authoritarian regimes, to participate in elections and have their voices heard.

Research and Collaboration: Research, development, and cooperation between academia and industry should continue, and government stakeholders will drive innovation in blockchain-based online polling technology. Interdisciplinary efforts involving experts in computer science, cryptography, political science, and law will be essential for addressing the technical, social, and regulatory challenges associated with online voting.

CHAPTER-7

TESTING

7. TESTING

INTRODUCTION

Testing plays a crucial role in the product development lifecycle, serving as a phase where errors from previous stages are identified and addressed. Its primary purpose is to ensure quality assurance and establish the reliability of the software. Once the implementation is complete, a test plan is devised, and a predefined set of test data is employed to execute the tests. Each test serves a distinct purpose, collectively verifying the proper integration of system elements and the successful execution of allocated functions. Through testing, the product's conformance to its intended functionality is validated. This phase represents the final step in the organization's internal verification and validation activities.

7.1 TESTING PROCESS

In the world today, technology is used to create several machines and make life easier. The software could have multiple bugs and might not be working as it is intended to. Hence testing is required to control and make sure that the software is error-free. It identifies all the defects that the software and makes sure the software is meeting the required specifications. Testing is also very cost-effective. It prevents failure from occurring in the future. It will also be cheaper to fix the bugs when it is in an earlier stage. It also improves the quality of the products after it is tested. This project uses Mocha as the testing framework to unit test and integration test all of our test cases for the application. Following strategies are used.

(i) Unit Testing: This is the first and the most important level of testing. Its need begins from the moment a programmer develops a unit of code. Every unit is tested for various scenarios. Detecting and fixing bugs during early stages of the Software Lifecycle helps reduce costly fixes later on. It is much more economical to find and eliminate the bugs during early stages of application building process. Hence, Unit Testing is the most important of all the testing levels. As the software project progresses ahead it becomes more and more costly to find and fix the bugs. Steps for Unit Testing are:-

Step 1: Creation of a Test Plan

Step 2: Creation of Test Cases and the Test Data

Step 3: Creation of scripts to run the test cases wherever applicable

Step 4: Execution of the test cases, once the code is ready

Step 5: Fixing of the bugs if present and re testing of the code

Step 6: Repetition of the test cycle until the Unit is free from all types of bugs.

7.2 TESTING ANALYSIS

The first benefit that blockchain can bring about is transparency. We know that without transparency, people can become discouraged about the legitimacy of their votes and can lead to questions about tampering and falsified results. Transparency makes for a trustworthy democracy which then leads to more positive outcomes from the votes. This is why it is important that all records are accurate and kept safely. Blockchain and its decentralised ledger can bring about trust at every stage of the voting process.

By using blockchain, votes can be tallied and stored on an immutable public ledger. This means that they can be tracked and counted while being visible to everyone. In turn, by allowing voters to see live records of the number of votes coming in, everyone will be able to see the legitimacy of the voting, making for a transparent and trustworthy voting system.

One of the most important factors of voting is security. Currently, voting systems are very open to hacks. Without substantial security mechanisms in place, malicious actors can enter the system and alter the outcome. This is where blockchain comes in. The technology has the ability to introduce a seemingly unhackable system.

All votes could be verified as soon as voting is finished to ensure they are all counted correctly. Without blockchain, this would have to be done by a central body overseeing the process. This causes many questions to arise about the trust of these central bodies. But with blockchain and its decentralised ledger system, there is no need for a potentially fallible or corruptible central body.

People want privacy when voting and don’t always want others to know who or what they voted for.

Blockchain allows for anonymity when voting. As with transactions on the blockchain, voters can use their private keys to keep themselves anonymous. They can then vote in the system without the worry of others knowing how they voted. Having the ability to guarantee anonymity might then encourage more people to take part in and use the voting system.

Current voting systems often take time to collate and process answers. Often when voting stations are in different areas and offices are not all together, it can be difficult to gather all the information quickly and efficiently. This then leads to time and cost issues. But blockchain can transform all of this. Instead of having to wait for a large number of people to communicate manually, all organisers

will be able to see the outcome instantly on the blockchain. Results can be gathered and processed quickly and straight after the voting has finished.

7.3 OUTPUT

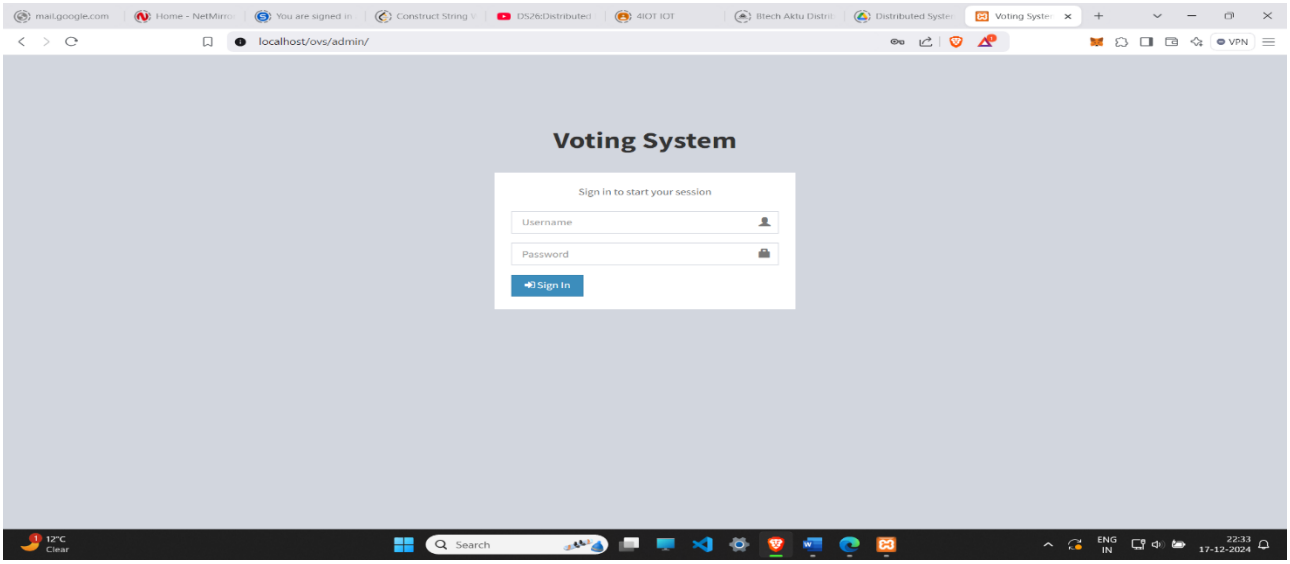


Figure 7.1: Main page

Figure 6.1 is the main page when web app is launched which can be accessed only by administrator.

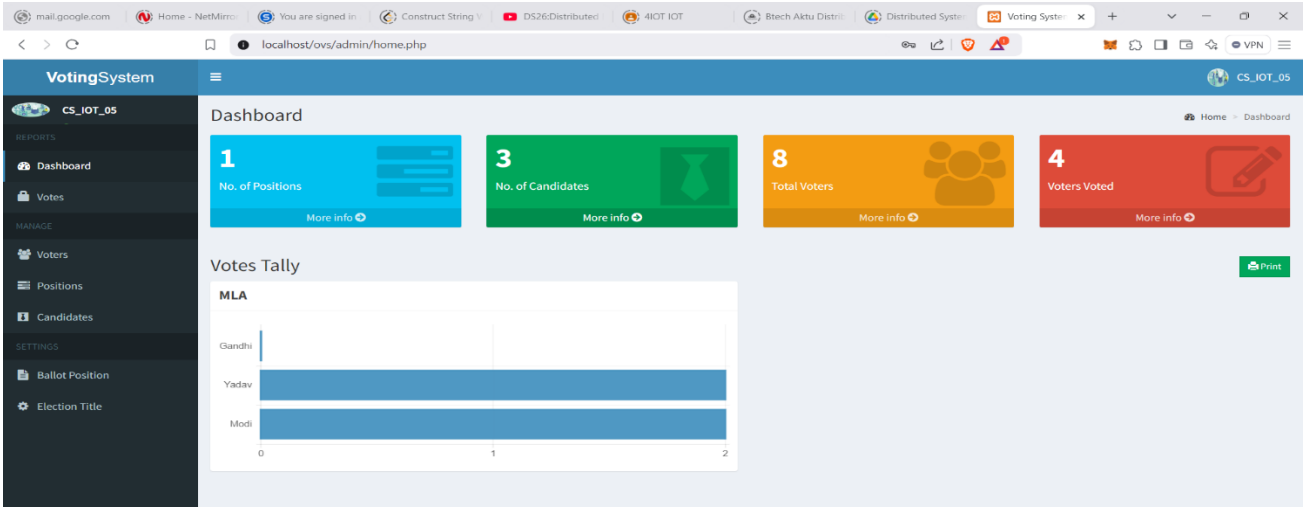


Figure 7.2: Main homepage

Figure 6.2 is also part of main page when scrolled which give blocks where administrator can register candidates and voters and also start/stop voting to get winner.

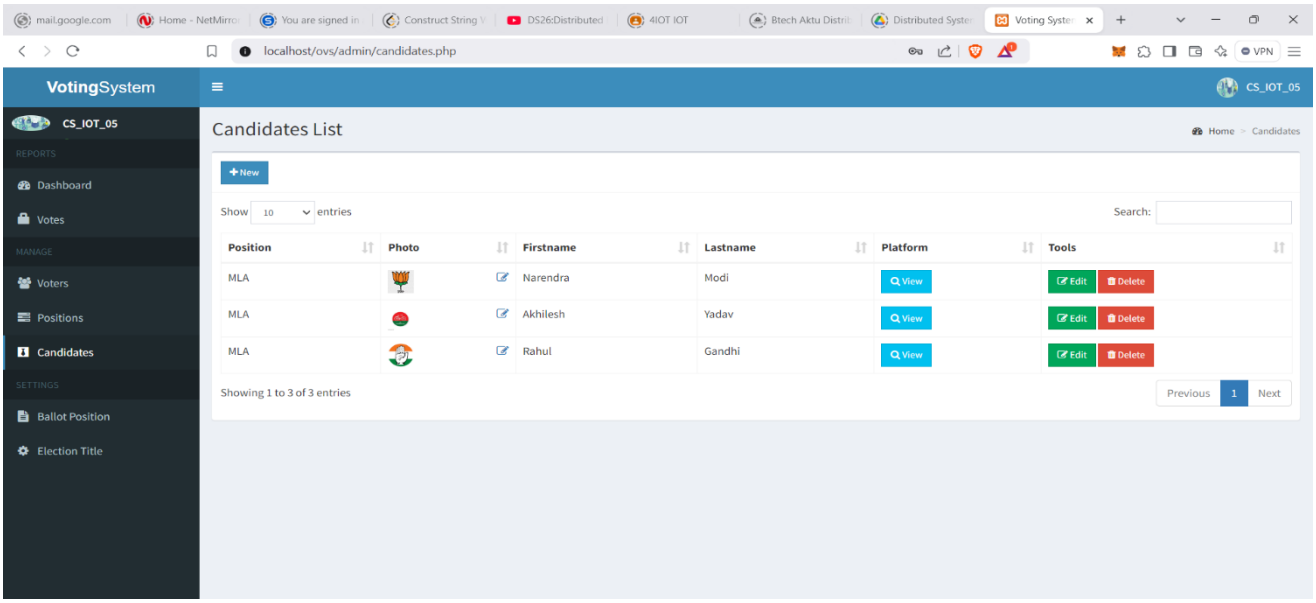


Figure 7.3: Candidate register page

Figure 6.3 shows pop-up when admin registers candidate by providing Name, Age and candidates account address. Pop-up occurs to confirm transaction by metamask wallet.

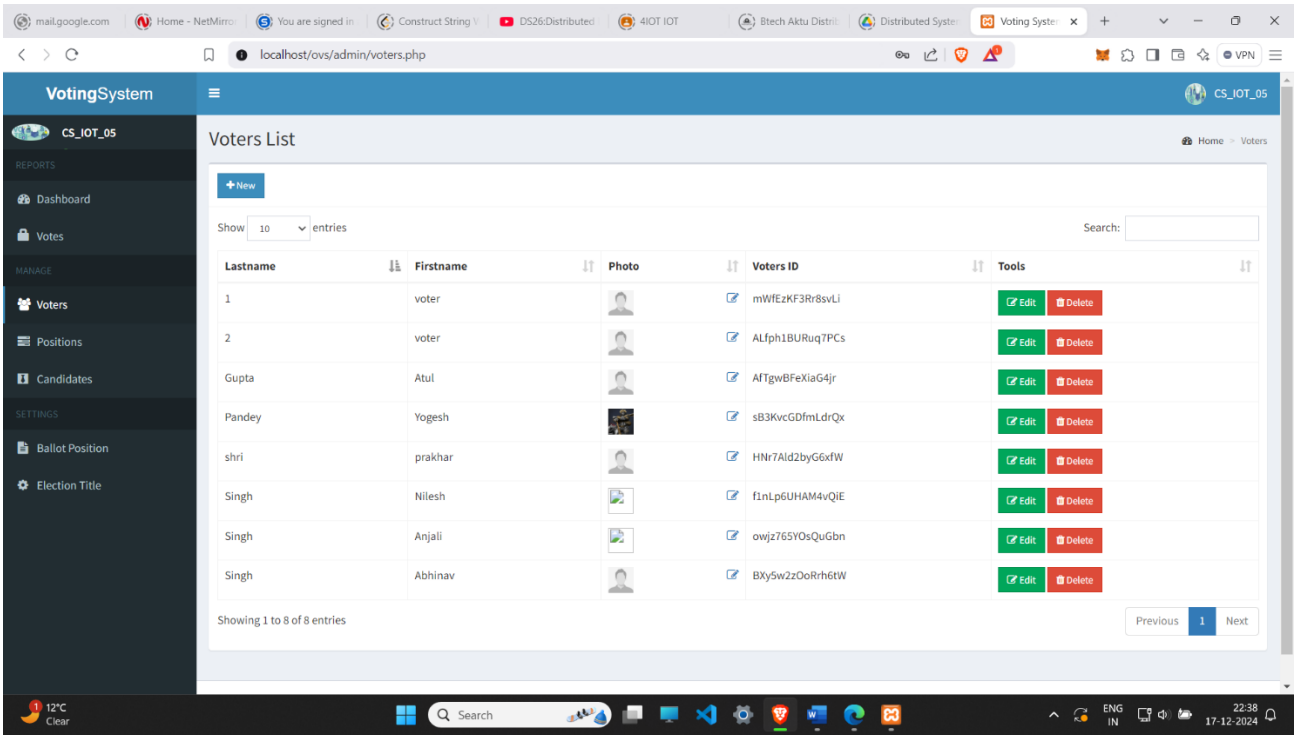


Figure 7.4: Voter Registration

Figure 6.4 shows voting panel(routed) when voting is not started it is accessible by voters.

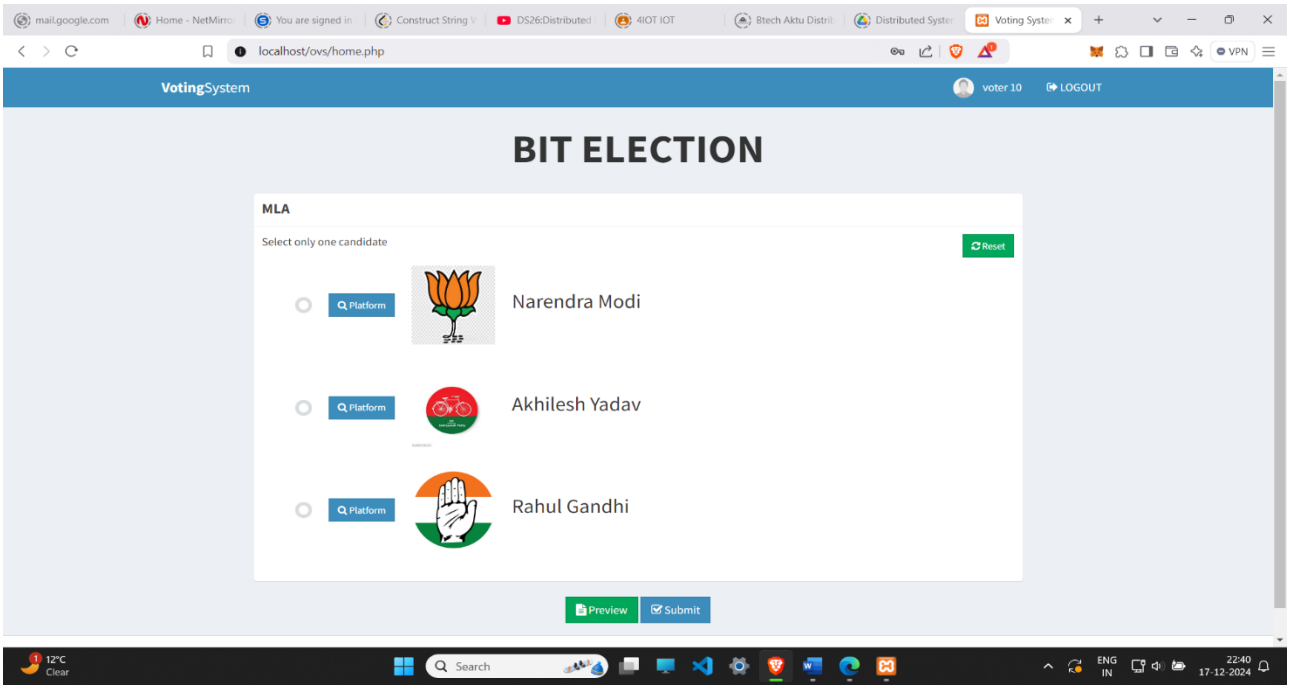


Figure 7.5: voting started

Figure 6.5 shows voting panel when voting started. It shows list of candidates who are registered for election.

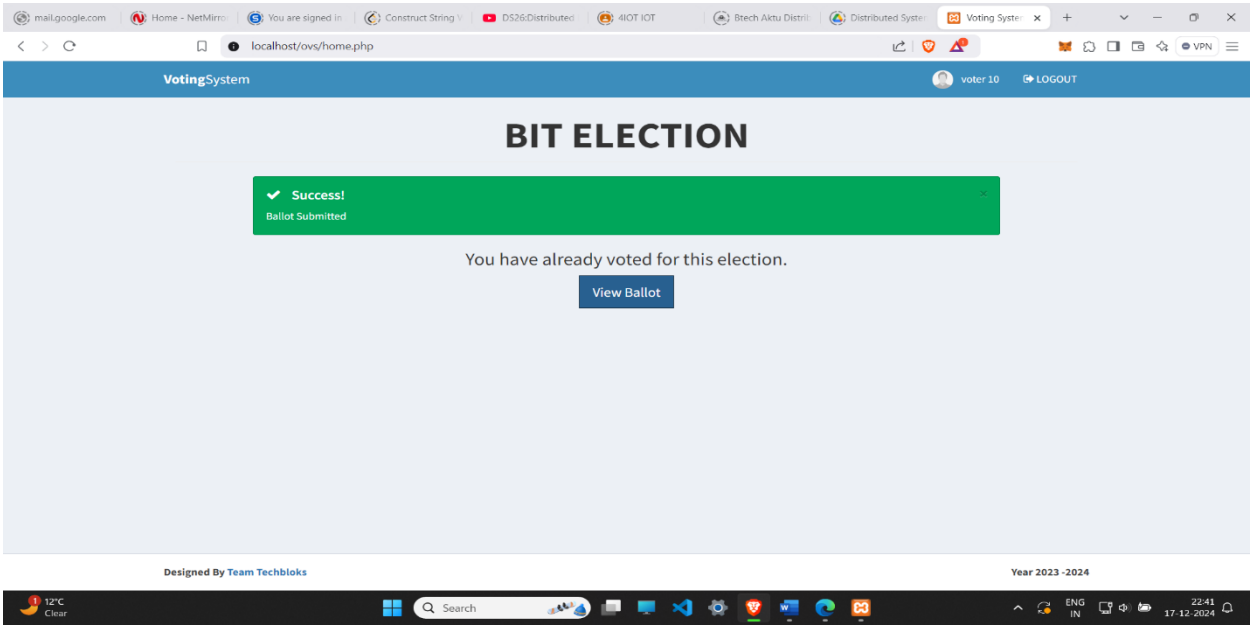


Figure 7.6: Pop-up when vote is done by voter

Figure 6.6 shows pop-up when voter tries to vote to any candidate, which is done by clicking on vote button in candidate's block and then confirming transaction.

CHAPTER-8
RESULTS AND DISCUSSION

8.1 DISCUSSIONS

Voter Authentication:

Voters would need to authenticate themselves using their Metamask wallets. Through a browser extension, Metamask offers users a safe method to interact with decentralised applications (DApps) and manage their Ethereum accounts. Metamask Integration: The online polling platform would integrate with the well-known Ethereum wallet browser addon Metamask. With Metamask, users may sign transactions and safely store their Ethereum accounts. Additionally, users can communicate with decentralised apps (DApps) straight from their browser by using Metamask.

Wallet Address Verification:

When a voter accesses the online poling platform, they would be prompted to connect their Metamask wallet. The platform would request access to the voter's Ethereum address to verify their identity. The wallet address serves as a unique identifier for the voter within the blockchain network.

Privacy Protection:

Throughout the authentication process, the online polling platform should prioritise the privacy of the voter. While the platform verifies the user's identity, it should not collect or store any personally identifiable information beyond the Ethereum address. This ensures that the voting process remains anonymous and confidential. Submitting Votes: Once authenticated, to prevent potential fraud or misuse, the authentication token issued to the voter's Metamask wallet should be single-use and valid only for the current voting session. Voters can submit their votes through the online polling platform. Each vote is encrypted and recorded on the blockchain as a transaction. The vote is transparent and verifiable, but the voter's name is kept anonymous.

Blockchain Consensus:

One blockchain network is used to record the votes. It might be a permissioned blockchain with designated validators or a public blockchain like Ethereum, depending on how the system is designed. The consensus mechanism ensures that all transactions (i.e., votes) are valid and agreed upon by the network.

Immutable Record:

Votes on the blockchain are unchangeable once they are registered, thus they cannot be manipulated or changed. Due to their transparency and impossibility of manipulation after the fact, the results guarantee the integrity of the voting process. Real-Time Results: As votes are recorded on the blockchain, real-time information on the vote results can be obtained from the polling platform. Users can track the progress of the poll and see how their votes contribute to the overall outcome. Verification: Anyone with blockchain access can audit the results after the polling period has ended. Since every vote is openly recorded, the results may be independently verified. This promotes

confidence in the fairness of the electoral process.

8.2 COST BENEFIT ANALYSIS:

Conducting a cost-benefit analysis for an electronic voting system that integrates blockchain technology with MetaMask involves assessing the benefits and drawback so implementing the solutions. Expenses cover the system's original creation, implementation, and upkeep, including software development, security precautions, blockchain infrastructure setup, and continuing support. It is also important to consider user and administrator raining. The main advantages are greater accessibility, security, and transparency. Election results can be trusted more because blockchain technology provides tamper-proof record-keeping. Voting becomes simple and convenient with the help of MetaMask integration, which makes blockchain engagement more approachable. Moreover, it lowers the possibility of fraud and manipulation, improving the democratic process's integrity. Additional advantages include expediting the voting process overall, possibly lowering administrative expenses, and speeding up the tallying of ballots. Furthermore, blockchain-based electronic voting can increase voter participation especially with tech-savvy populations. In conclusion, although blockchain e-voting systems may need a sizable initial expenditure, in the long run, the advantages in terms of efficiency, security, and transparency exceed the drawbacks, hence fortifying democratic processes.

REFERENCES

1. Singh, A., & Chatterjee, K. (2018, September). Secevs: Secure electronic voting system using blockchain technology. In *2018 International Conference on Computing, Power and Communication Technologies (GUCON)* (pp. 863-867). IEEE.

2. Bosri, R., Uzzal, A. R., Al Omar, A., Hasan, A. T., & Bhuiyan, M. Z. A. (2019, August). Towards a privacy-preserving voting system through blockchain technologies. In *2019 IEEE Intl Conf on Dependable, Autonomic and Secure Computing, Intl Conf on Pervasive Intelligence and Computing, Intl Conf on Cloud and Big Data Computing, Intl Conf on Cyber Science and Technology Congress (DASC/PiCom/CBDCom/CyberSciTech)* (pp. 602-608). IEEE.

3. Kshetri, N., & Voas, J. (2018). Blockchain-enabled e-voting. *Ieee Software*, *35*(4), 95-99.

4. Hjálmarsson, F. Þ., Hreiðarsson, G. K., Hamdaqa, M., & Hjálmtýsson, G. (2018, July). Blockchain-based e-voting system. In *2018 IEEE 11th international conference on cloud computing (CLOUD)* (pp. 983-986). IEEE.

5. Benabdallah, A., Audras, A., Coudert, L., El Madhoun, N., & Badra, M. (2022). Analysis of blockchain solutions for e-voting: A systematic literature review. *IEEE Access*.

6. Garg, K., Saraswat, P., Bisht, S., Aggarwal, S. K., Kothuri, S. K., & Gupta, S. (2019, April). A comparitive analysis on e-voting system using blockchain. In *2019 4th International Conference on Internet of Things: Smart Innovation and Usages (IoT-SIU)* (pp. 1-4). IEEE.

7. Ayed, A. B. (2017). A conceptual secure blockchain-based electronic voting system. *International Journal of Network Security & Its Applications*, *9*(3), 01-09.

8. Patidar, K., & Jain, S. (2019, July). Decentralized e-voting portal using blockchain. In *2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT)* (pp. 1-4). IEEE.

.