Project Report

on

Voting System Using Blockchain(dApp)

Submitted to

Sant Gadge Baba Amravati University

In partial Fulfillment of the Requirement

For the Degree of

Bachelor of Engineering in

Computer Science and Engineering

Submitted by:

Mr. Pramey Deshmukh
Mr. Chinmay Gulhane
Mr. Mohd. Meeran Iqbal
Mr. Mohd Daniyal
Mr. Anurag Vinchurkar

Under the Guidance of

Dr. R. A. Zamare

Department of Computer Science and Engineering

Shri Sant Gajanan Maharaj College of Engineering,

Shegaon – 444 203 (M.S.)

2023-23

SHRI SANT GAJANAN MAHARAJ COLLEGE OF ENGINEERING,

SHEGAON – 444 203 (M.S.)

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

CERTIFICATE

This is to certify that **Mr. Pramey Deshmukh, Mr. Chinmay Gulhane, Mr. Mohd Daniyal, Mr. Mohd Meeran and Mr. Anurag Vinchurkar** students of final year B.E. in the year 2020-21 of Computer Science and Engineering Department of this institute has completed the project work entitled "**Voting System Using Blockchain(dApp)**" based on syllabus and has submitted a satisfactory account of his work in this report which is recommended for the partial fulfillment of degree of Bachelor of Engineering in Computer Science and Engineering.

Dr. R. A. Zamare	**Dr. S. B. Patil**	**Dr. S. B. Somani**
Project Guide	Head of Department	Principal

SHRI SANT GAJANAN MAHARAJ COLLEGE OF ENGINEERING,

SHEGAON – 444 203 (M.S.)

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

CERTIFICATE

This is to certify that the project work entitled "**Voting System Using Blockchain(dApp)**" submitted by that **Mr. Pramey Deshmukh**, **Mr. Chinmay Gulhane**, **Mr. Mohd Daniyal**, **Mr. Mohd Meeran** and **Mr. Anurag Vinchurkar** students of final year B.E. in the year 2020-21 of Computer Science and Engineering Department of this institute, is a satisfactory account of his work based on syllabus which is recommended for the partial fulfillment of degree of Bachelor of Engineering in Computer Science and Engineering.

Internal Examiner **External Examiner**

Date: **Date:**

Abstract

In any democratic country, Voting is a fundamental right of any citizen that enables them to choose the leaders of tomorrow. As a digital platform, they eliminate the need to cast your votes using paper or having to gather in person. They also protect the integrity of your vote by preventing voters from being able to vote multiple times.

Electronic voting or e-voting has fundamental benefits over paper based systems such as increased efficiency and reduced errors. The electronic voting system tends to maximize user participation, by allowing them to vote from anywhere and from any device that has an internet connection. The blockchain is an emerging, decentralized, and distributed technology with strong cryptographic foundations that promises to improve different aspects of many industries. Expanding e-voting into blockchain technology could be the solution to alleviate the present concerns in e-voting. Here we propose a blockchain-based voting system that will limit the voting fraud and make the voting process simple, secure and efficient.

Acknowledgement

The real spirit of achieving a goal is through the way of excellence and lustrous discipline. We would have never succeeded in completing my task without the cooperation, encouragement and help provided to me by various personalities.

We would like to take this opportunity to express my heartfelt thanks to my guide ***Dr. R. A. Zamare****, for her esteemed guidance and encouragement, especially through difficult times. Her suggestions broaden our vision and guide us to succeed in this work. We are also very grateful for her guidance and comments while studying part of our project and learnt many things under her leadership.*

We extend our thanks to ***Dr. S.B. Patil*** *Head of Computer Science & Engineering Department, Shri Sant Gajanan Maharaj College of Engineering, Shegaon for their valuable support that made us consistent performers.*

We also extend my thanks to ***Dr. S. B. Somani, Principal*** *Shri Sant Gajanan Maharaj College of Engineering, Shegaon for their valuable support.*

Also, we would like to thanks to all teaching and non-teaching staff of the department for their encouragement, cooperation, and help. Our greatest thanks are to all who wished me success especially my parents, my friends whose support and care makes me stay on earth.

Pramey Deshmukh
Chinmay Gulhane
Mohd. Meeran Iqbal
Mohd. Daniyal Mohd. Tahsin
Anurag Vinchurkar
Final Year B. E. Sem-VIII, CSE
Session 2022-23

Contents

Contents

List of Figures

List of Snapshots

1. Introduction

1.1 Problem Statement

The current traditional voting system has several limitations such as lack of transparency, security, and accountability. The system is vulnerable to fraud, manipulation, and hacking, which can compromise the accuracy and integrity of the results. Additionally, the traditional voting system involves a lot of manual processes, which can be time-consuming, expensive, and prone to errors.

Moreover, the current voting system is not accessible to all voters, especially those who are physically disabled, living in remote areas, or unable to travel to the voting centres. This leads to low voter turnout, which can affect the legitimacy of the election results.

Therefore, there is a need for a secure, transparent, and accessible voting system that can address the limitations of the traditional voting system. Blockchain technology offers a potential solution to this problem by providing a decentralized and distributed platform that can ensure the integrity and immutability of data. The proposed e-voting system based on blockchain technology aims to address these limitations and provide a more secure, transparent, and accessible voting process.

1.2 Introduction: -

Voting whether conducted through the traditional ballot or via electronic means forms the basis on which democracy depends. With the rise in technological impact on the youth of the country and the various anomalies faced by the current electoral process, using technology to modify the existing process is a necessity of the hour. However, for any new technique to take the place of current voting system, the said system needs to satisfy certain minimum criteria. Electronic Voting has taken centre place in research with the intention of minimizing the cost associated in setting up the voting process, while ensuring the electoral integrity is maintained by fulfilling privacy, security, and compliance requirements.

The current method, whether electronic or not has proved to be unsatisfactory with respect to transparency. It can be very difficult for the voters to be assured that the vote he/she has casted during the election reflects in the election result. Electronic voting using Direct Recording Electronic do not generate receipt on successful casting of votes. No record of election except vote count is made public by the government, which means that the voters are not assured of any external interference in case of government conducting the process of vote recounting. Replacing the traditional method with electronic method using Blockchain technique has the ability

to prevent potential frauds that may take place during election.

Blockchain technology is a distributed network of interconnected nodes. A copy of distributed ledger is assigned to each node, each of which contains a complete history of all the transactions that have been processed by the network. Each transaction processed generated a hash. The hash created depends not only on the current transaction but also on the hash of the previous transaction. Thus any small change on the data will impact the hash of the transaction. If a transaction is approved by a majority of nodes it is written to the block. This allows the users to remain autonomous while using the system. A basic analysis of Blockchain suggests that it provides the potential of making the voting process more secure and reliable.

1.3 Background

The first things that come to mind about the blockchain are cryptocurrencies and smart contracts because of the well-known initiatives in Bitcoin and Ethereum. Bitcoin was the first crypto-currency solution that used a blockchain data structure. Ethereum introduced smart contracts that leverage the power of blockchain immutability and distributed consensus while offering a crypto-currency solution comparable to Bitcoin. The concept of smart contracts was introduced much earlier by Nick Szabo in the 1990s and is described as “a set of promises, specified in digital form, including protocols within which the parties perform on these promises”. In Ethereum, a smart contract is a piece of code deployed to the network so that everyone has access to it. The result of executing this code is verified by a consensus mechanism and by every member of the network.

Today, we call a blockchain a set of technologies combining the blockchain data structure itself, distributed consensus algorithm, public key cryptography, and smart contracts. Below we describe these technologies in more detail.

Blockchain creates a series of blocks replicated on a peer-to-peer network. Any block in blockchain has a cryptographic hash and timestamp added to the previous block. A block contains the Merkle tree block header and several transactions. It is a secure networking method that combines computer science and mathematics to hide data and information from others that is called cryptography. It allows the data to be transmitted securely across the insecure network, in encrypted and decrypted forms.

As was already mentioned, the blockchain itself is the name for the data structure. All the written data are divided into blocks, and each block contains a hash of all the data from the previous block as part of its data. The aim of using such a data structure is to achieve provable immutability. If a piece of data is changed, the block’s hash containing this piece needs to be recalculated, and the hashes of all subsequent blocks also need to be recalculated. It means only the hash of the latest

block has to be used to guarantee that all the data remains unchanged. In blockchain solutions, data stored in blocks are formed from all the validated transactions during their creation, which means no one can insert, delete, or alter transactions in an already validated block without it being noticed. The initial zero-block, called the "genesis block," usually contains some network settings, for example, the initial set of validators (those who issue blocks).

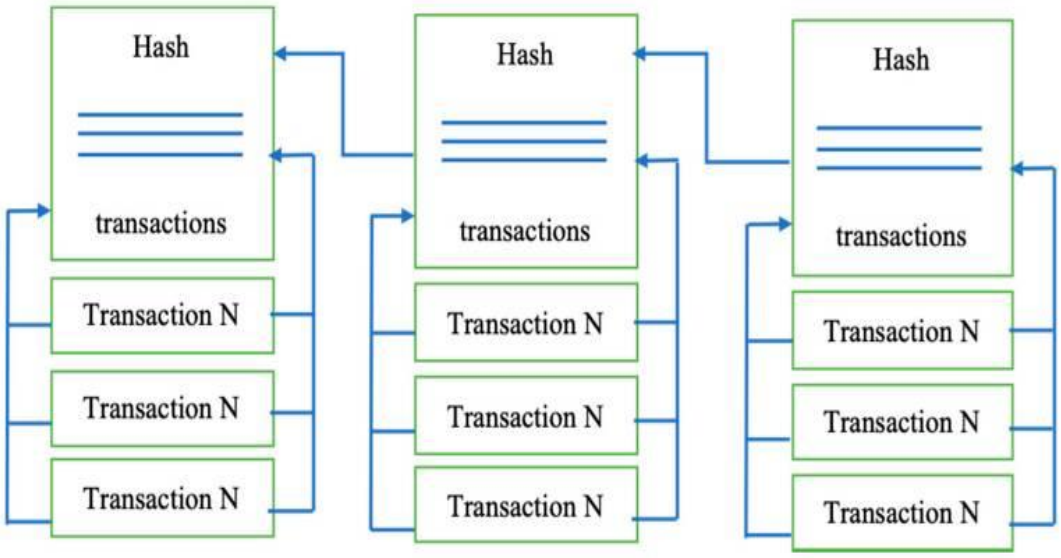


Figure 1.1 The Blockchain Structure

Blockchain solutions are developed to be used in a distributed environment. It is assumed that nodes contain identical data and form a peer-to-peer network without a central authority. A consensus algorithm is used to reach an agreement on blockchain data that is fault-tolerant in the presence of malicious actors. Such consensus is called Byzantine fault tolerance, named after the Byzantine Generals' Problem. Blockchain solutions use different Byzantine fault tolerance (BFT) consensus algorithms: Those that are intended to be used in fully decentralized self-organizing networks, such as cryptocurrency platforms, use algorithms such as proof-of-work or proof-of-stake, where validators are chosen by an algorithm so that it is economically profitable for them to act honestly. When the network does not need to be self-organized, validators can be chosen at the network setup stage. The point is that all validators execute all incoming transactions and agree on achieving results so that more than two-thirds of honest validators need to decide on the outcome.

Public key cryptography is used mainly for two purposes: Firstly, all validators own their keypairs used to sign consensus messages, and, secondly, all incoming transactions (requests to modify blockchain data) have to be signed to determine the requester. Anonymity in a blockchain context relates to the fact that anyone wanting

to use cryptocurrencies just needs to generate a random keypair and use it to control a wallet linked to a public key. The blockchain solution guarantees that only the keypair owner can manage the funds in the wallet, and this property is verifiable. As for online voting, ballots need to be accepted anonymously but only from eligible voters, so a blockchain by itself definitely cannot solve the issue of voter privacy.

Smart contracts breathed new life into blockchain solutions. They stimulated the application of blockchain technology in efforts to improve numerous spheres. A smart contract itself is nothing more than a piece of logic written in code.

Still, it can act as an unconditionally trusted third party in conjunction with the immutability provided by a blockchain data structure and distributed consensus. Once written, it cannot be altered, and all the network participants verify all steps. The great thing about smart contracts is that anybody who can set up a blockchain node can verify its outcome.

As is the case with any other technology, blockchain technology has its drawbacks. Unlike other distributed solutions, a blockchain is hard to scale: An increasing number of nodes does not improve network performance because, by definition, every node needs to execute all transactions, and this process is not shared among the nodes. Moreover, increasing the number of validators impacts performance because it implies a more intensive exchange of messages during consensus. For the same reason, blockchain solutions are vulnerable to various denial-of-service attacks. If a blockchain allows anyone to publish smart contracts in a network, then the operation of the entire network can be disabled by simply putting an infinite loop in a smart contract. A network can also be attacked by merely sending a considerable number of transactions: At some point, the system will refuse to receive anything else. In cryptocurrency solutions, all transactions have an execution cost: the more resources a transaction utilizes, the more expensive it will be, and there is a cost threshold, with transactions exceeding the threshold being discarded. In private blockchain networks, this problem is solved depending on how the network is implemented via the exact mechanism of transaction cost, access control, or something more suited to the specific context.

1.4 Existing System

In traditional voting systems, citizens must physically go to a designated polling place and cast their vote. The voting process is typically paper based, where voters mark their choices on a ballot paper and drop it into a ballot box. The counting of votes is also carried out manually, which can be time-consuming and prone to errors. This system can also be susceptible to fraud, as there is no easy way to verify the accuracy of the results.

Over the years, electronic voting (e-voting) systems have been developed and implemented. These systems aim to provide a more efficient and accurate way of voting. However, many e-voting systems have faced criticism due to concerns about the security, privacy, and transparency of the process.

Some existing e-voting systems use centralized servers to store and process votes. This can be problematic, as a single point of failure can compromise the entire system. Other systems use cryptography to secure the voting process, but these systems can be complex and difficult to implement.

Overall, the existing voting systems have limitations in terms of security, transparency, and accuracy, which can lead to a lack of trust in the voting process.

Snapshot 1 Traditional Voting system

2. Related work

Electronic voting (e-voting) has been a topic of interest for several decades. With the advancement of technology, there has been a growing interest in developing secure and reliable e-voting systems. However, traditional e-voting systems have been criticized for their lack of security, transparency, and auditability.
Blockchain technology has emerged as a potential solution to address the shortcomings of traditional e-voting systems. Blockchain technology utilizes a decentralized and distributed platform that provides a secure and tamper-proof environment for data storage and processing. Several researchers have proposed e-voting systems based on blockchain technology.

[1] In 2022, a group of researchers provided a comprehensive survey of blockchain-based e-voting systems, analysing their strengths and weaknesses. The authors identify the main challenges faced by these systems, such as scalability, security, and privacy, and provide recommendations for addressing them. In this work, an e-voting system, which has the characteristic of coercion-resistance, is proposed. They utilize receiver-deniable encryption in the registration phase to realize coercion-resistance. And we adopt blockchain technology to ensure that the process and results of our electronic voting system are fair and transparent. We also designed a time-release encryption algorithm in the tallying phase to make the smart contract decrypt ballots and tally after the appointed time. It can guarantee the fairness of our e-voting system further and avoid election fraud. Our scheme is proved coercion-resistant by simulating the election operations. And we also give detailed safety analysis of other security requirements. Finally, we discuss that the proposed scheme has better efficiency in a small-scale voting.

[2] In 2021, a group of researchers proposed a blockchain-based e-voting system that ensures transparency and voter anonymity. The authors utilize a hybrid blockchain architecture that combines public and private blockchains to ensure the accuracy and transparency of the voting process. It can guarantee the fairness of our e-voting system further and avoid election fraud. Our scheme is proved coercion-resistant by simulating the election operations. And we also give detailed safety analysis of other security requirements. Several research gaps in e-voting have presented that need to be taken into account for future studies. Scalability attacks, less transparency, use of untrusted systems and coercion resistance may have additional disadvantages and should be resolved. Since the blockchain-based e-voting systems are still required further testing, we are not fully aware of all the risks that are associated with the security and scalability of such systems. Implementing blockchain voting practices can bring unknown security risks and vulnerabilities. Blockchain systems require a more complex design in software and management skills. Finally, we discuss that the proposed scheme has a better efficiency in a small-scale voting.

[3] In 2020, a group of researchers proposed an e-voting system that utilizes smart contracts to automate the voting process and ensure the integrity of the results. The authors utilize the Ethereum blockchain platform to develop the system and provide a detailed analysis of its security and performance. In this paper we analyzed and discussed about the traditional voting system and the advantages of implementation blockchain based E-voting system that uses various blockchain based tools and using case study of manual voting process. The implementation uses blockchain as a centralized voting system. This system will use blockchain as a network as well as database to store voter's information or credentials which is going to use for their authentication. System will be using candidate's or voter's details for the voting process. After that we saw the comparison between traditional voting system used and the blockchain based e voting system.

[4] In 2020, a group of researchers proposed an e-voting system that utilizes blockchain technology and verifiable voting to ensure the accuracy and transparency of the voting process. This has provided an insufficient basis for government decision-makers and key election stakeholder to be able to make an informed decision on the merits of blockchain e-voting for national elections. To address this gap, we demonstrated how the architecture trade-off analysis method could be used to enable election stakeholders to understand the potential risks, challenges, and prospects of blockchain e-voting through a participatory architecture assessment and documentation process. The authors provide a detailed analysis of the system's security and performance and test it on a simulated network.

[5] In 2019, a group of researchers proposed an e-voting system that utilizes multi-party computation (MPC) and blockchain technology to ensure the security and privacy of the voting process. The authors provide a detailed analysis of the system's security and performance and test it on a simulated network. Blockchain is a special research topic that deserves a thorough evaluation because of its fast-growing popularity among researchers, businesses, and clients who are trying to solve numerous security problems using blockchain. Recently, the research community has been highlighting blockchain's failure to meet all needs and have started proposing decision schemes that differentiate whether blockchain is suitable for a selected application. These decision schemes are still not consistent among themselves. In this work, we have evaluated blockchain's suitability from a quantitative perspective. To the best of our knowledge, this work is the first to do so. Based on the results obtained in this work, we recommend researchers new to blockchain and entrepreneurs considering blockchain applications, to invest their efforts in ownership, supply chain management and telecommunication and transportation applications as they are the prominent areas where blockchain will most likely mature in the future and are the least risky

[6] In 2020, a group of researchers proposed an e-voting system that utilizes homomorphic encryption and blockchain technology to ensure the privacy and security of the voting process. Traditional voting emphasizes the authority of the state. BEV emphasizes voter transparency. The BEV process is transparent, decentralized, and bottom-up. BEV might not perform well in a society whose culture and values exhibit low compatibility with these values. Also, blockchains require much energy to perform authentication and validation, and they're slow. So, using them for national e-voting might not be practical yet. Finally, BEV will shift power away from central actors such as electoral authorities and government agencies. Thus, the technology is likely to face resistance from political leaders who benefit from the status quo. The authors provide a detailed analysis of the system's security and performance and test it on a simulated network.

[7] In 2020, a group of researchers proposed a auditable blockchain voting system. Most of the existing today voting systems suffer from inadequate transparency and lack of audit capabilities. Despite being the most important democratic process, voting is outside the control of common voters. They are not able to inspect and verify if the voting process was conducted correctly or whether their votes were really included in a vote pool. The common voters must rely on election officials' honesty, which is often not enough to build trust in a democratic system. Blockchain technology is a potential solution to these issues. The technology can be integrated into e-voting which in turn may provide the voters with audit capabilities and ability to supervise their votes. Blockchain-based e-voting system would reduce risk of election frauds and manipulations.

[8] In 2020, a group of researchers proposed a blockchain based voting system. In that, we got introduced to a blockchain-based electronic voting system that utilizes smart contracts to enable secure and cost-efficient election while guaranteeing voters privacy. We have shown that the blockchain technology offers a new possibility to overcome the limitations and adoption barriers of electronic voting systems which ensures the election security and integrity and lays the ground for transparency. Using an Ethereum private blockchain, it is possible to send hundreds of transactions per second onto the blockchain, utilizing every aspect of the smart contract to ease the load on the blockchain. For countries of greater size, some additional measures would be needed to support greater throughput of transactions per second.

In summary, the literature survey shows that blockchain technology has emerged as a potential solution to address the shortcomings of traditional e-voting systems. Several researchers have proposed e-voting systems based on blockchain technology that are secure, transparent, and auditable. The proposed systems have been evaluated and found to be secure and efficient. However, further research is needed to develop and improve e-voting systems based on blockchain technology.

3. Architecture of Blockchain

3.1 Components

These are the main architectural components of Blockchain:

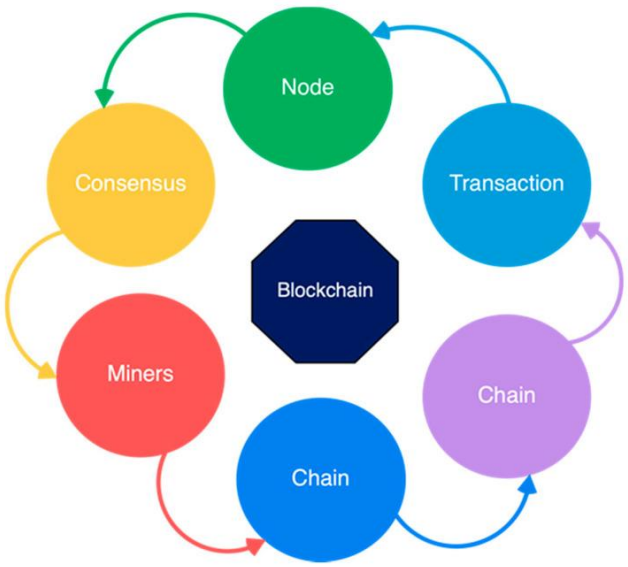


Figure 3.1 Core Components of Blockchain Architecture

- Node: Users or computers in blockchain layout (every device has a different copy of a complete ledger from the blockchain)
- Transaction: It is the blockchain system's smallest building block (records and details), which blockchain uses.
- Block: A block is a collection of data structures used to process transactions over the network distributed to all nodes.
- Chain: A series of blocks in a particular order.
- Miners: Correspondent nodes to validate the transaction and add that block into the blockchain system.
- Consensus: A collection of commands and organizations to carry out blockchain processes.

Blockchain architecture has many benefits for all sectors that incorporate blockchain. Here are a variety of embedded characteristics :

- Cryptography: Blockchain transactions are authenticated and accurate because of computations and cryptographic evidence between the parties involved;
- Immutability: Any blockchain documents cannot be changed or deleted;
- Provenance: It refers to the fact that every transaction can be tracked in the blockchain ledger;
- Decentralization: The entire distributed database may be accessible by all members of the blockchain network. A consensus algorithm allows control of the system, as shown in the core process;
- Anonymity: A blockchain network participant has generated an address rather than a user identification. It maintains anonymity, especially in a blockchain public system;
- Transparency: It means being unable to manipulate the blockchain network. It does not happen as it takes immense computational resources to erase the blockchain network.

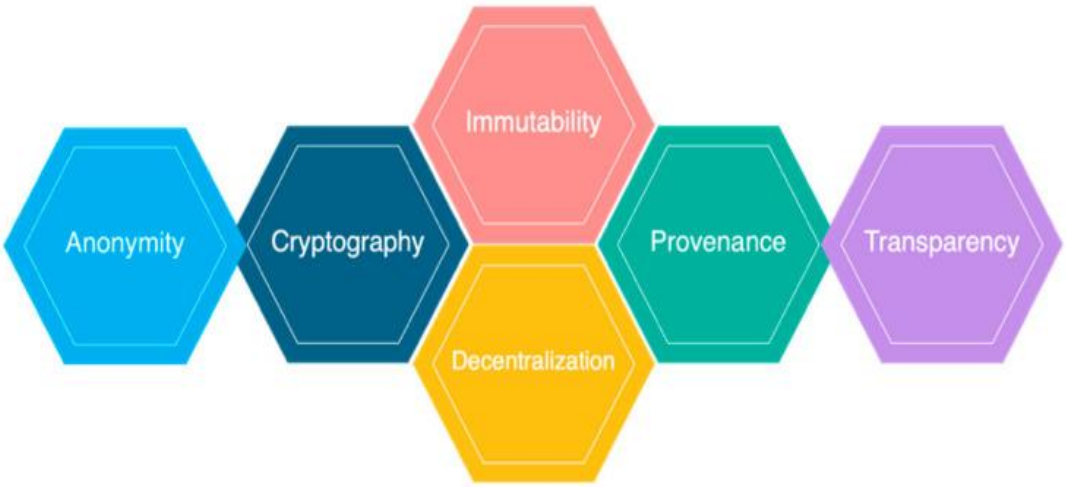


Figure 3.2 Characteristics of Blockchain Architecture

3.2 Blockchain Network

The blockchain network will be the foundation of the proposed system. The network will consist of multiple nodes that will store the voting data and ensure its integrity and immutability. The blockchain network will be decentralized and distributed, which means that there will be no central authority controlling the voting process.

The blockchain network will ensure that the voting data is secure and tamper-proof, and that the results are accurate and trustworthy.
Here are some important aspects and characteristics of a blockchain network:

- Decentralization: Blockchain networks are decentralized, meaning there is no central authority or single point of control. Instead, the network consists of multiple nodes, each participating in the validation and maintenance of the blockchain. This decentralized structure enhances security, transparency, and resistance to censorship or tampering.

- Distributed Ledger: The blockchain is a distributed ledger that records a chronological and immutable history of all transactions and data within the network. Each participating node maintains a copy of the entire blockchain, ensuring that all nodes have access to the same information. This distributed nature eliminates the need for a central database and enables transparency and consensus among participants.

- Consensus Mechanisms: Blockchain networks rely on consensus mechanisms to agree on the state of the blockchain and validate transactions. Different consensus algorithms, such as Proof of Work (PoW), Proof of Stake (PoS), or Delegated Proof of Stake (DPoS), are used to determine which nodes can add new blocks to the chain and reach a consensus on the validity of transactions. Consensus mechanisms ensure that all nodes in the network agree on the state of the blockchain, maintain its integrity, and prevent double-spending or fraudulent activities.

- Peer-to-Peer Communication: Nodes in a blockchain network communicate with each other in a peer-to-peer fashion, allowing them to exchange information and propagate transactions and blocks across the network. Peer-to-peer communication eliminates the need for intermediaries or centralized servers, increasing efficiency and reducing costs.

- Security and Immutability: Blockchain networks provide strong security and immutability of data. Once a transaction is added to a block and confirmed by the network, it becomes nearly impossible to alter or tamper with. The use of cryptographic algorithms, such as hashing and digital signatures, ensures the integrity and authenticity of transactions and blocks.

- Network Governance: Blockchain networks may have different governance models that determine how decisions are made regarding protocol upgrades, network rules, and consensus changes. Governance can be decentralized, with decisions made through consensus among network participants, or it can involve specific entities or organizations responsible for maintaining and evolving the network.

- Interoperability: Blockchain networks can be designed to interact and interoperate with other blockchain networks or external systems. Interoperability enables the exchange of assets, data, or information between different blockchains or with traditional systems, fostering collaboration and expanding the potential use cases of blockchain technology.

- Scalability: Scalability is an important consideration for blockchain networks as they aim to handle a growing number of transactions and users. Different scaling solutions, such as layer 2 protocols, sharding, or off-chain channels, are being explored to improve the scalability and throughput of blockchain networks while maintaining decentralization and security.

Blockchain networks are the foundation of blockchain technology, enabling secure and transparent transactions without the need for intermediaries. They provide a robust infrastructure for various applications, including cryptocurrencies, supply chain management, voting systems, decentralized finance (DeFi), and much more. As the technology continues to evolve, blockchain networks are being refined and optimized to meet the demands of real-world use cases and drive the adoption of decentralized solutions.

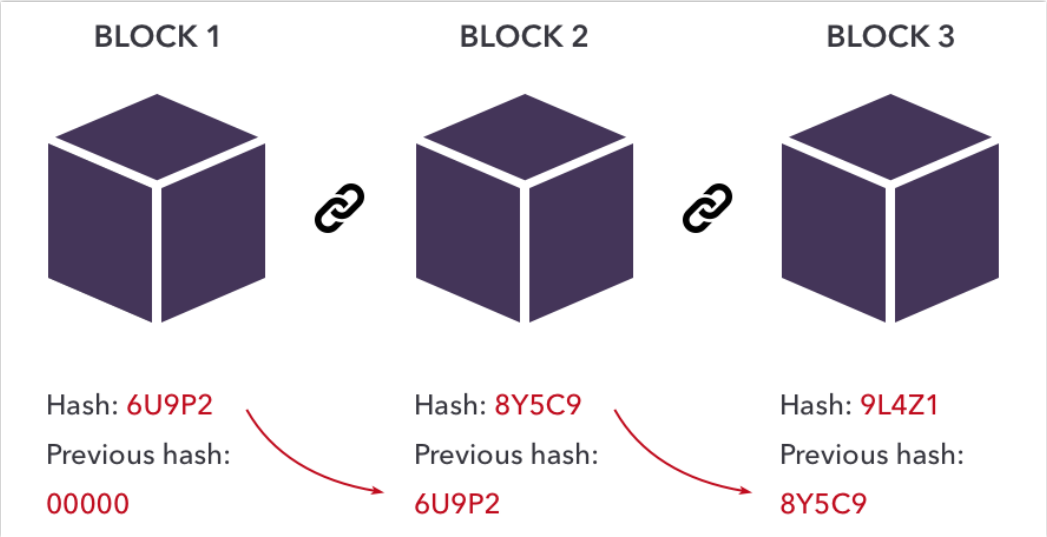


Figure 3.3 Block Structure

3.3 Smart Contracts

A smart contract is a self-executing computer program that is built on top of a blockchain network. Smart contracts are designed to automatically execute the terms of an agreement when certain conditions are met. They are used to automate the execution of contracts, agreements, and other types of transactions.

The key feature of a smart contract is that it is self-executing. Once the terms of the contract are met, the contract is automatically executed without the need for any intermediaries. Smart contracts are also immutable, which means that they cannot be altered once they are deployed on the blockchain.

Smart contracts are used in a variety of applications, including finance, real estate, supply chain management and more. They are particularly useful in situations where trust is an issue, as they provide a transparent and tamper-proof way of executing transactions.

One of the main advantages of using smart contracts is that they can help reduce transaction costs and increase efficiency. Because smart contracts are self-executing, they eliminate the need for intermediaries such as lawyers, brokers and other third parties. This can save time, money, and resources.

It is a piece of code that is stored and executed on a decentralized network, such as Ethereum. Smart contracts enable parties to interact and transact with each other directly without the need for intermediaries.

Here are some key characteristics and aspects of smart contracts:

- Digital Agreements: Smart contracts are digital representations of traditional legal agreements. They define the terms, conditions, and rules of a particular agreement or transaction. The terms are written in code, making them verifiable, transparent, and tamper-proof.

- Self-executing and Autonomous: Once deployed on a blockchain, smart contracts are self-executing, meaning they automatically perform the actions defined within the code when specific conditions are met. They operate without human intervention and follow a predetermined logic, eliminating the need for intermediaries or third parties.

- Decentralization and Trustlessness: Smart contracts operate on a decentralized network, such as a blockchain, which means they are not controlled by any central authority. The execution and validation of smart contracts rely on consensus mechanisms and cryptographic algorithms, ensuring trust and transparency among all participants.

- Immutable and Transparent: Smart contracts, once deployed on a blockchain, become part of a permanent and unalterable record. The code and its execution history are transparent and visible to all participants on the network. This immutability and transparency enhance security, as the terms of the contract cannot be modified or tampered with.

- Programmable and Flexible: Smart contracts can incorporate complex logic and calculations, allowing for programmable agreements with conditional statements, loops, and functions. This flexibility enables the implementation of various business rules and processes within the contract, automating tasks and streamlining operations.

- Triggered by Transactions: Smart contracts are typically executed in response to specific transactions or events on the blockchain. For example, a payment received or a specific condition met can trigger the execution of code within the smart contract, leading to the transfer of assets or the fulfillment of contractual obligations.

- Tokenization and DeFi: Smart contracts have played a significant role in the emergence of decentralized finance (DeFi) and tokenization. They enable the creation and management of digital tokens, such as cryptocurrencies or non-fungible tokens (NFTs), which can represent various assets or rights.

- Smart Contract Languages: Smart contracts are written in specific programming languages designed for blockchain platforms. For Ethereum, the most commonly used language is Solidity, although other languages like Vyper are also available. These languages provide syntax and features tailored to writing secure and efficient smart contracts.

Smart contracts have the potential to revolutionize traditional business processes by automating and digitizing agreements, reducing costs, improving efficiency, and eliminating intermediaries. They have applications in various industries, including finance, supply chain management, voting systems, decentralized applications (DApps), and more. However, it's important to note that while smart contracts can automate processes and enforce agreements, they cannot interpret real-world events or conditions directly. They rely on external data sources or oracles to interact with the outside world.

3.4 MetaMask

MetaMask is a popular cryptocurrency wallet and browser extension that enables users to interact with Ethereum-based decentralized applications (DApps) and manage their digital assets securely. It acts as a bridge between users and the Ethereum blockchain, providing a user-friendly interface for accessing and interacting with blockchain-based applications.

Here are some key features and aspects of MetaMask:

- Wallet Functionality: MetaMask serves as a digital wallet that allows users to store, manage, and transfer Ethereum and other ERC-20 tokens. Users can create multiple accounts within MetaMask and securely store their private keys, which provide access to their funds.

- Browser Extension: MetaMask is primarily available as a browser extension for popular web browsers like Google Chrome, Firefox, and Brave. Once installed, the MetaMask extension adds a small icon to the browser's toolbar, providing quick access to the wallet functionality.

- Ethereum Network Access: MetaMask connects users to the Ethereum blockchain, enabling them to send and receive Ether (ETH) and interact with Ethereum-based smart contracts and DApps. It supports both the Ethereum mainnet and various test networks, such as Ropsten, Rinkeby, and Kovan, allowing users to test and experiment with DApps in a development environment.

- Seamless DApp Integration: MetaMask simplifies the process of interacting with DApps. When a user visits a website that has integrated MetaMask, the extension automatically detects the DApp and displays a popup window. This window allows users to authorize transactions, sign messages, and interact with smart contracts directly from their MetaMask wallet.

- Enhanced Security: MetaMask provides a secure environment for managing digital assets. It stores private keys locally on the user's device and encrypts them with a user-defined password. MetaMask also supports hardware wallets like Ledger and Trezor, which offer additional layers of security by keeping private keys offline.

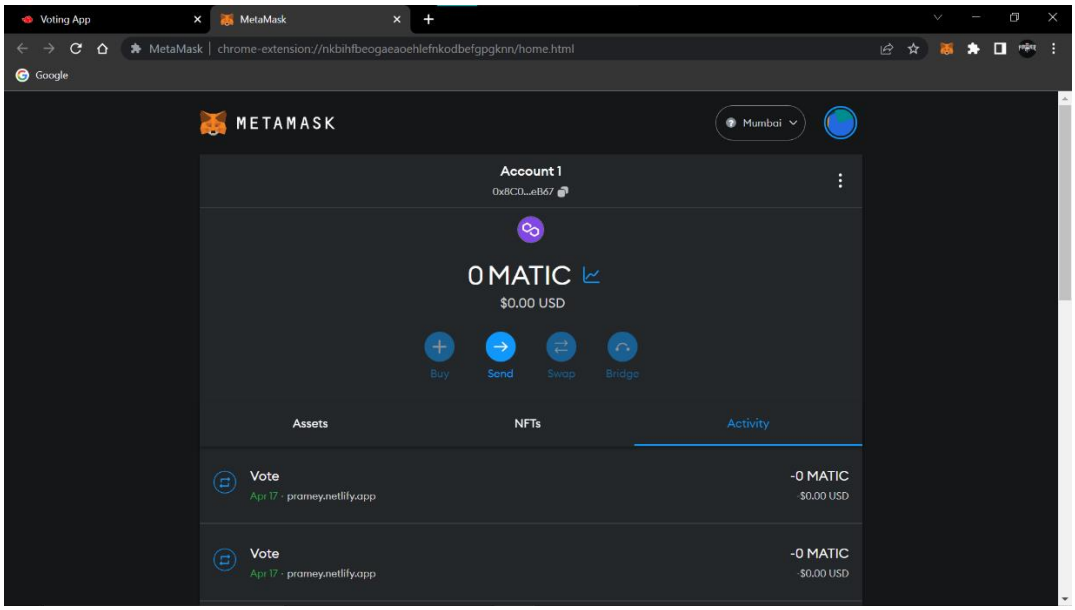
- Custom Network Configuration: MetaMask allows users to configure custom Ethereum networks, enabling them to connect to private or alternative networks beyond the Ethereum mainnet and testnets. This feature is useful for developers and organizations that operate on their own blockchain networks.

- Token Swapping and DeFi Integration: MetaMask integrates with decentralized finance (DeFi) protocols and platforms, allowing users to easily swap tokens, participate in liquidity pools, lend and borrow assets, and access other financial services directly from their wallet interface.

- Mobile App: In addition to the browser extension, MetaMask offers a mobile app for iOS and Android devices. The mobile app provides similar wallet functionality and allows users to access their accounts and interact with DApps on the go.

- Open-Source and Community-driven: MetaMask is an open-source project, which means that its source code is publicly available and can be reviewed, audited, and contributed to by the developer community. This transparency fosters trust and allows developers to verify the security and functionality of the wallet. Furthermore, MetaMask has an active community that provides support, documentation, and resources, making it easier for users and developers to get started and resolve any issues they may encounter.

MetaMask has gained popularity among Ethereum users, developers, and enthusiasts due to its user-friendly interface, secure wallet functionality, and seamless integration with Ethereum-based DApps. It has become a fundamental tool for anyone engaging with the Ethereum ecosystem, providing a convenient and secure way to manage digital assets and interact with blockchain-based applications.



Snapshot 2 MetaMask Account Activity

3.5 Ganache

Ganache (formerly known as TestRPC) is a local blockchain development tool that provides developers with a simulated Ethereum environment for testing and development purposes. It allows developers to create private, local blockchain networks that behave similarly to the Ethereum mainnet or testnets, but with faster block confirmations and no need for real Ether.

Here are some key features and characteristics of Ganache:

- Local Blockchain: Ganache creates a local Ethereum blockchain on your development machine. This blockchain operates locally, meaning it runs on your computer rather than being connected to the actual Ethereum network. This provides developers with a sandboxed environment to test and debug their decentralized applications (DApps) without incurring any costs or affecting the live network.

- Fast Block Confirmations: Unlike the Ethereum mainnet or public testnets, which have varying block confirmation times, Ganache provides near-instantaneous block confirmations. This allows developers to quickly observe the effects of their transactions, test different scenarios, and iterate on their code more rapidly.

- Pre-funded Accounts: Ganache automatically generates a set of pre-funded accounts for development purposes. These accounts come pre-loaded with test Ether (fake Ether), which can be used to simulate transactions and interactions with smart contracts on the local blockchain. Each account has a private key associated with it, allowing developers to sign and authorize transactions.

- Smart Contract Deployment: Ganache provides an interface for deploying and interacting with smart contracts on the local blockchain. Developers can compile their Solidity smart contracts using tools like Remix IDE or Truffle, and then deploy and test them on Ganache. This allows for quick iteration and debugging of smart contract logic and functionality.

- Network Customization: Ganache offers customization options for the local blockchain network. Developers can configure parameters such as the gas limit, block time, and network ID to mimic specific network conditions or test different scenarios. This flexibility enables developers to simulate a wide range of network conditions and edge cases during development and testing.

- Transaction Inspection and Debugging: Ganache provides a user-friendly interface where developers can inspect and analyze individual transactions, including their inputs, outputs, gas costs, and status. This makes it easier to debug and trace issues in smart contracts and transaction execution.

- Integration with Development Tools: Ganache is compatible with popular Ethereum development frameworks and tools such as Truffle, Remix IDE, and web3.js. Developers can seamlessly integrate Ganache into their development workflow, enabling them to write, compile, deploy, and test their smart contracts using familiar tools and libraries.

- Network Forking: Ganache offers network forking capabilities, allowing developers to create a fork of the Ethereum mainnet or any other public network. This feature enables developers to test and debug their applications against a snapshot of a specific Ethereum network's state, providing a realistic testing environment.

- Testing and Automation: Ganache is often used in combination with testing frameworks like Truffle and Hardhat to automate testing processes for smart contracts. Developers can write comprehensive test suites and run them against the local blockchain network, ensuring the correctness and reliability of their contracts.

- User Interface: Ganache provides a user-friendly graphical user interface (GUI) that displays essential information about the local blockchain network. The GUI shows details such as the available accounts, their balances, transaction history, and block information. It also allows developers to configure network settings and manage accounts.

- Block Explorer: Ganache includes a built-in block explorer that allows developers to inspect and explore the details of individual blocks and transactions. The block explorer provides information such as the block number, transaction hashes, gas usage, and more. This feature is helpful for understanding the behavior and flow of transactions within the local blockchain network.

Ganache is a valuable tool for Ethereum developers, as it allows them to rapidly iterate, test, and debug their DApps and smart contracts in a controlled and efficient environment. By providing a local blockchain with pre-funded accounts, fast block confirmations, and comprehensive development features, Ganache significantly streamlines the development process and helps ensure the robustness and reliability of Ethereum-based applications.

3.6 Remix IDE

Remix IDE is a web-based development environment that is used for writing, testing, and deploying smart contracts on the Ethereum blockchain. It is an integrated development environment specifically designed for developing and testing smart contracts for Ethereum-based decentralized applications (DApps). It provides a comprehensive set of tools and features that aid developers in writing, debugging, and deploying smart contracts on the Ethereum blockchain. It is a powerful tool that provides a user-friendly interface for developers to create and test smart contracts in Solidity, the programming language used for Ethereum-based applications.

Remix IDE provides several features that make smart contract development easier, including syntax highlighting, code completion, and debugging tools. It also allows developers to deploy their contracts to the Ethereum blockchain and interact with them using a built-in web3 provider.

One of the main advantages of Remix IDE is that it is an open-source tool that is constantly being updated and improved by the Ethereum community. This means that developers can benefit from the latest features and bug fixes, ensuring that their smart contracts are secure and reliable.

Here are some key features and components of Remix IDE:

- Code Editor: Remix IDE offers a code editor with syntax highlighting and auto-completion for writing smart contracts using Solidity, the most widely used programming language for Ethereum. It supports both Solidity versions 0.4.x and 0.5.x.

- Solidity Compiler: Remix includes a built-in Solidity compiler that allows developers to compile their smart contracts directly within the IDE. The compiler provides error messages, warnings, and detailed code analysis to help developers identify and resolve issues.

- Debugger: Remix provides a powerful debugging tool that allows developers to step through their smart contract code and inspect variables at each step. This helps in identifying and fixing logical errors or unexpected behavior in the contract.

- Deploy and Interact: Remix enables developers to deploy their smart contracts onto various Ethereum networks, such as the mainnet or testnets like Ropsten or Rinkeby. It also provides an interface to interact with deployed contracts, allowing developers to test contract functionality and execute transactions.

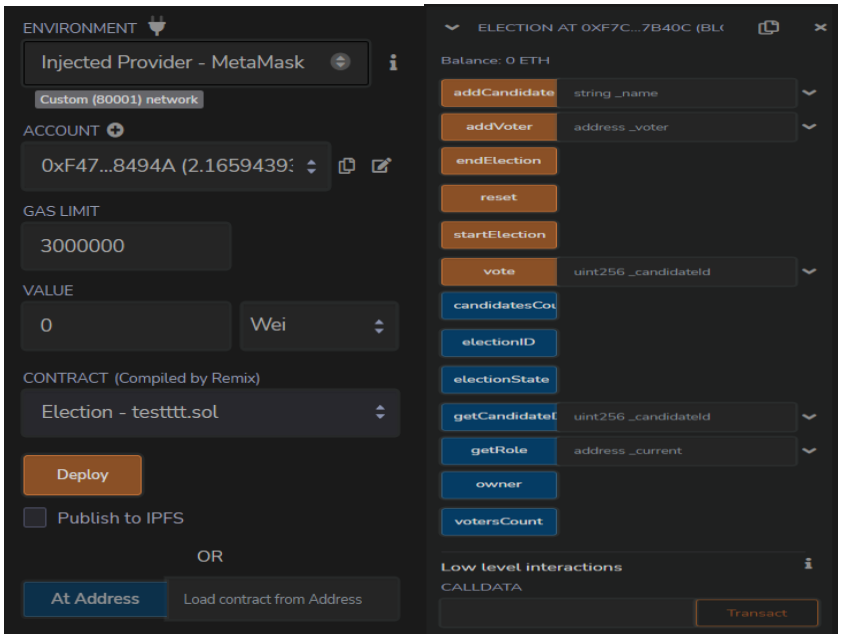
- Gas Estimation: Gas is the unit used to measure computational effort in Ethereum. Remix includes a gas estimation feature that helps developers estimate the gas cost of executing their smart contracts. This is crucial for optimizing contract performance and managing transaction costs.

- Plugin System: Remix IDE supports a plugin system that allows developers to extend its functionality. Developers can create and integrate their own plugins to add custom features or integrate with external tools and services.

- Integration with Remix Libraries: Remix provides a collection of pre-built libraries and contracts that developers can import and use in their projects. These libraries cover various functionalities such as token standards (ERC20, ERC721), multisig wallets, oracles, and more.

- Collaboration and Sharing: Remix IDE allows developers to collaborate on projects by sharing their code and contracts with others. It supports real-time collaboration, enabling multiple developers to work simultaneously on the same project.

Remix IDE is a widely used and highly regarded development environment in the Ethereum ecosystem. It provides an accessible and user-friendly interface, making it suitable for both beginner and experienced developers to build, test, and deploy smart contracts for Ethereum-based applications.



Snapshot 3 Remix IDE

3.7 Polygon Test Net Mumbai

Polygon (formerly Matic Network) is a Layer 2 scaling solution for Ethereum that aims to improve transaction speed and reduce fees. The Polygon ecosystem includes several components, including the Polygon mainnet, which is the live network used for production applications, and several testnets used for development and testing.
Testnets are essential for developers to test their applications and smart contracts before deploying them to the mainnet. Polygon provides several testnets, including the Mumbai Testnet, which is the most popular testnet used for developing and testing Polygon-based applications.

Developers can deploy their smart contracts and applications to the Mumbai Testnet using the same tools and processes used for the Ethereum mainnet. The testnet can be accessed through various developer tools, including Remix, Truffle, and Hardhat.
In summary, the Polygon Testnet provides a reliable and efficient environment for developers to test and deploy their applications before deploying them to the mainnet. The Mumbai Testnet is a fully functional Ethereum testnet that replicates the mainnet environment, making it easy for developers to test their applications under real-world conditions.

Here are some key details about Polygon Testnet Mumbai:

- Purpose: Testnets are alternate networks that mimic the mainnet (production network) but are meant for testing and experimentation. Polygon Testnet Mumbai allows developers to deploy and test their applications and smart contracts before deploying them on the live Polygon mainnet or other Ethereum networks.

- Compatibility: The Mumbai testnet is fully compatible with the Ethereum Virtual Machine (EVM) and supports the Solidity programming language, making it easy for developers familiar with Ethereum to transition to Polygon. This compatibility ensures that DApps and smart contracts developed on the Ethereum network can also be tested and deployed on the Polygon network.

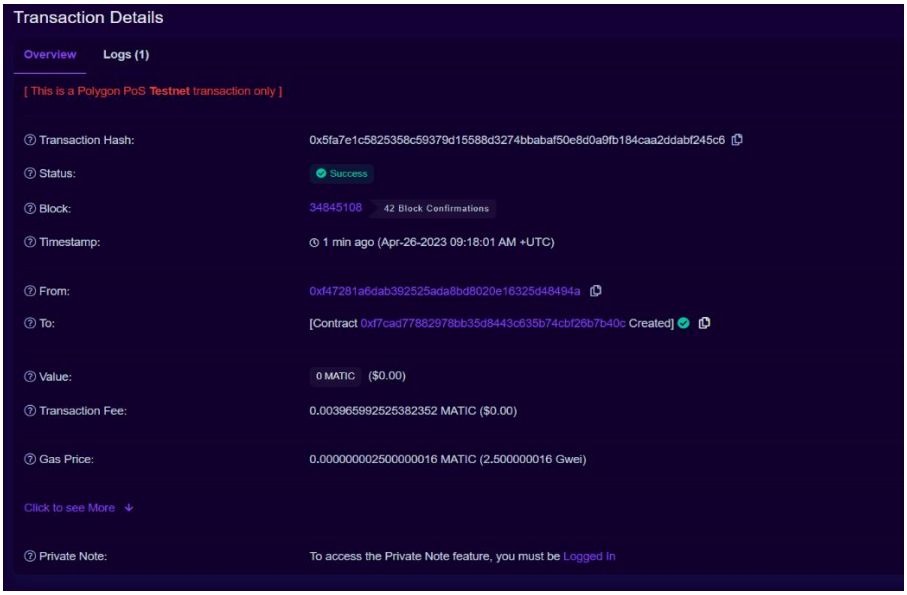
- Features: Mumbai testnet provides developers with access to various features and functionalities offered by the Polygon network, such as low transaction fees, fast block confirmations, and scalability. Developers can experiment with the layer 2 scaling solutions provided by Polygon, such as Plasma and Optimistic Rollups, to improve the performance and efficiency of their applications.

- Faucets: To facilitate testing, Mumbai testnet provides faucet services where developers can obtain test tokens (MATIC) for free. These tokens are used to cover gas fees and simulate transactions on the network. Faucets are typically web-based services that distribute a specific amount of test tokens to individual developer accounts.

- Developer Tools: Polygon Testnet Mumbai is compatible with popular Ethereum development tools and frameworks. Developers can use tools like Remix IDE, Truffle, Hardhat, or web3.js to write, compile, deploy, and interact with smart contracts on the Mumbai testnet.

- Community Support: Polygon has an active developer community that offers support, documentation, and resources for developers working with the Mumbai testnet. This includes developer forums, documentation, tutorials, and sample projects that can help developers get started and resolve any issues they may encounter.

By utilizing the Mumbai testnet, developers can thoroughly test their DApps and smart contracts on the Polygon network, ensuring their stability, security, and functionality before deploying them to the production environment. This helps in identifying and resolving any potential issues or vulnerabilities and provides a smoother user experience when the application is eventually deployed on the live network.



Snapshot 4 Transaction Details on the Test Net

3.8 Netlify

Netlify is a cloud-based hosting and serverless backend platform that provides a comprehensive solution for building, deploying, and managing modern web applications. The platform allows developers to focus on building their applications instead of worrying about infrastructure and server management.

❖ ***Features***

Netlify provides a range of features that make it a popular choice for web developers:

- Continuous Deployment: Netlify supports continuous deployment, which means that every time you push code to your Git repository, Netlify automatically builds and deploys your application. This makes it easy to deploy changes quickly and efficiently, without the need for manual deployment processes.

- Serverless Function: Netlify provides a serverless backend platform that enables developers to build and deploy serverless functions. These functions can be used to add dynamic functionality to your application, such as handling form submissions, sending emails, and processing payments.

- CDN: Netlify provides a global content delivery network (CDN) that delivers your application content to users from the server that is closest to them. This ensures faster load times and a better user experience.

- Analytics and Monitoring: Netlify provides analytics and monitoring tools that enable developers to track the performance of their applications, including page load times, error rates, and traffic.

- Forms: Netlify provides a form handling service that enables developers to collect form submissions from their applications. The service includes spam protection, form validation, and email notifications.

- Identity: Netlify provides an authentication and identity service that enables developers to add user authentication and authorization to their applications. The service includes user management, password recovery, and social login.

- Pricing: Netlify offers a free plan that includes basic features such as continuous deployment, serverless functions, and a global CDN. The paid plans start at $19 per month and include additional features such as analytics and monitoring, form handling, and identity services.

In short, Netlify is a powerful platform that enables developers to build and deploy modern web applications quickly and efficiently. Its serverless backend platform, CDN, analytics and monitoring tools, and form handling and identity services make it a popular choice for web developers.

Multimedia databases have drastically increased in size over the past ten years, particularly those kept up by the big web search engines like Google, Bing, and Ask. These search engines' hypertext search techniques are strong enough to produce results that are semantically relevant in response to text queries, but it is difficult to develop semantically meaningful search techniques for multimedia data, such as photos, video, and audio files.

Because of this lack of effectiveness, the majority of current research has focused on content-based picture retrieval in particular. In a nutshell, the topic of content-based image retrieval researches ways to use meaningful content extraction and comparison algorithms for images to index, browse, and query huge image databases.

The choice to update the images on the web page is made based on the degree of significance of the changes that have occurred in the images, and these content extraction methods are also employed for web refreshing approaches involving photos.

Hence, the primary topic of research in the field of content-based image retrieval is the design and development of algorithms and methodologies that can effectively retrieve image content. Because of this, many techniques for comparing photos to one another rely on the extraction of colour or texture descriptors and the organising of that data.

Because it can be translated into a three-dimensional coordinate system that closely resembles human perception, colour information is more widely used. Yet, colour is frequently inappropriate because there may be grayscale images with corresponding colour counterparts. While there are techniques for describing texture and shape, they cannot be used on complex images since they contain numerous minute elements.

4. Problems and Solutions of developing Online Voting System

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

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

Below is a brief overview of the solutions for satisfying these properties in online voting systems.

4.1 Eligibility

The solution to the issue of eligibility is rather apparent. To take part in online voting, voters need to identify themselves using a recognized identification system. The identifiers of all legitimate voters need to be added to the list of participants. But there are threats: Firstly, all modifications made to the participation list need to be checked so that no illegitimate voters can be added, and secondly, the identification system should be both trusted and secure so that a voter's account cannot be stolen or used by an intruder. Building such an identification system is a complex task in itself. However, because this sort of system is necessary for a wide range of other contexts, especially related to digital government services, researchers believe it is best to use an existing identification system, and the question of creating one is beyond the scope of work.

4.2 Non-reusability

At first, glance, implementing non-reusability may seem straightforward—when a voter casts their vote, all that needs to be done is to place a mark in the participation list and not allow them to vote a second time. But privacy needs to be taken into consideration; thus, providing both non-reusability and voter anonymity is tricky. Moreover, it may be necessary to allow the voter to re-vote, making the task even more complex. A brief overview of non-reusability techniques will be provided below in conjunction with the outline on implementing privacy.

4.3 Privacy

Privacy in the context of online voting means that no one except the voter knows how a participant has voted. Achieving this property mainly relies on one (or more) of the following techniques: blind signatures, homomorphic encryption, and mix-networks. Blind signature is a method of signing data when the signer does not know what they are signing. It is achieved by using a blinding function so that blinding and signing functions are commutative – Blind(Sign(message)) = Sign(Blind(message)). The requester blinds (applies blinding function to) their message and sends it for signing. After obtaining a signature for a blinded message, they use their knowledge of blinding parameters to derive a signature for an unblinded message. Blind signatures mathematically prevent anyone except the requester from linking a blinded message and a corresponding signature pair with an unblinded one.

4.4 Fairness

Fairness in terms of no one obtaining intermediate results is achieved straightforwardly: Voters encrypt their choices before sending, and those choices are decrypted at the end of the voting process. The critical thing to remember here is that if someone owns a decryption key with access to encrypted decisions, they can obtain intermediate results. This problem is solved by distributing the key among several keyholders. A system where all the key holders are required for decryption is unreliable—if one of the key holders does not participate, decryption cannot be performed. Therefore, threshold schemes are used whereby a specific number of key holders are required to perform decryption. There are two main approaches for distributing the key: secret sharing, where a trusted dealer divides the generated key into parts and distributes them among key holders (e.g., Shamir's Secret Sharing protocol); and distributed key generation, where no trusted dealer is needed, and all parties contribute to the calculation of the key (for example, Pedersen's Distributed Key Generation protocol).

4.5 Soundness and Completeness

On the face of it, the completeness and soundness properties seem relatively straightforward, but realizing them can be problematic depending on the protocol. If ballots are decrypted one by one, it is easy to distinguish between valid and invalid ones, but things become more complicated when it comes to homomorphic encryption. As a single ballot is never decrypted, the decryption result will not show if more than one option was chosen or if the poll was formed so that it was treated as ten choices (or a million) at once. Thus, we need to prove that the encrypted data

meets the properties of a valid ballot without compromising any information that can help determine how the vote was cast. This task is solved by zero-knowledge proof.

By definition, this is a cryptographic method of proving a statement about the value without disclosing the value itself. More specifically, range proofs demonstrate that a specific value belongs to a particular set in such cases.

The properties described above are the bare minimum for any voting solution. But all the technologies mentioned above are useless if there is no trust in the system itself. A voting system needs to be fully verifiable to earn this trust, i.e., everyone involved can ensure that the system complies with the stated properties. Ensuring verifiability can be split into two tasks: personal, when the voter can verify that their ballot is correctly recorded and tallied; and universal, when everyone can prove that the system as a whole works precisely. This entails the inputs and outputs of the voting protocol stages being published and proof of correct execution. For example, mix-networks rely on proof of correct shuffling (a type of zero-knowledge proof), while proof of correct decryption is also used in mix-networks and threshold decryption. The more processes that are open to public scrutiny, the more verifiable the system is. However, online voting makes extensive use of cryptography, and the more complex the cryptography, the more obscure it is for most system users. It may take a considerable amount of time to study the protocol and even more to identify any vulnerabilities or backdoors, and even if the entire system is carefully researched, there is no guarantee that the same code is used in real-time.

To address these issues, robust security measures must be implemented, such as encryption, authentication mechanisms, and regular system audits. Additionally, strict voter identification processes, including two-factor authentication and verification of voter eligibility, can help maintain the integrity of the system. Transparent and tamper-evident data storage and transmission protocols should also be employed to ensure the privacy and accuracy of votes. Continuous monitoring and quick response to any irregularities or breaches are vital to maintaining trust in the online voting system.

5. Security requirements

5.1 Anonymity

Throughout the polling process, the voting turnout must be secured from external interpretation. Any correlation between registered votes and voter identities inside the electoral structure shall be unknown.

5.2 Auditability & Accuracy

Accuracy, also called correctness, demands that the declared results correspond precisely to the election results. It means that nobody can change the voting of other citizens, that the final tally includes all legitimate votes, and that there is no definitive tally of invalid ballots.

5.3 Democracy/Singularity

A “democratic” system is defined if only eligible voters can vote, and only a single vote can be cast for each registered voter. Another function is that no one else should be able to duplicate the vote.

5.4 Vote Privacy

After the vote is cast, no one should be in a position to attach the identity of a voter with its vote. Computer secrecy is a fragile type of confidentiality, which means that the voting relationship remains hidden for an extended period as long as the current rate continues to change with computer power and new techniques.

5.5 Robustness and Integrity

This condition means that a reasonably large group of electors or representatives cannot disrupt the election. It ensures that registered voters will abstain without problems or encourage others to cast their legitimate votes for themselves. The corruption of citizens and officials is prohibited from denying an election result by arguing that some other member has not performed their portion correctly.

5.6 Lack of Evidence

While anonymous privacy ensures electoral fraud safeguards, no method can be assured that votes are placed under bribery or election rigging in any way. This question has its root from the start.

5.7 Transparency

It means that before the count is released, no one can find out the details. It avoids acts such as manipulating late voters' decisions by issuing a prediction or offering a significant yet unfair benefit to certain persons or groups as to be the first to know.

5.8 Availability and Mobility

During the voting period, voting systems should always be available. Voting systems should not limit the place of the vote.

5.9 Verifiable Participation/Authenticity

The criterion also referred to as desirability makes it possible to assess whether or not a single voter engaged in the election. This condition must be fulfilled where voting by voters becomes compulsory under the constitution (as is the case in some countries such as Australia, Germany, Greece) or in a social context, where abstention is deemed to be a disrespectful gesture (such as the small and medium-sized elections for a delegated corporate board).

5.10 Accessibility and Reassurance

To ensure that everyone who wants to vote has the opportunity to avail the correct polling station and that polling station must be open and accessible for the voter. Only qualified voters should be allowed to vote, and all ballots must be accurately tallied to guarantee that elections are genuine.

5.11 Recoverability and Identification

Voting systems can track and restore voting information to prevent errors, delays, and attacks.

5.12 Voters Verifiability

Verifiability means that processes exist for election auditing to ensure that it is done correctly. Three separate segments are possible for this purpose: (a) uniform verification or public verification that implies that anybody such as voters, governments, and external auditors can test the election after the declaration of the tally; (b) transparent verifiability against a poll, which is a weaker prerequisite for each voter to verify whether their vote has been taken into account properly.

Figure 5.1 Security Requirements

6. Future scope

The future scope for an e-voting system based on blockchain technology is promising, as it offers enhanced security, transparency, and auditability. By leveraging the decentralized and tamper-resistant nature of blockchain, each vote can be securely recorded and verified, minimizing the risk of fraud and manipulation. This can significantly improve the integrity of the voting process, increase trust among voters, and enhance the overall credibility of elections. Additionally, blockchain-based e-voting systems can provide transparency and auditability, allowing anyone to verify the authenticity of votes and ensuring a fair and accountable electoral process.

Furthermore, blockchain-based e-voting systems can offer improved accessibility, efficiency, and cost-effectiveness. By enabling remote voting through digital platforms and mobile applications, individuals with mobility constraints, those residing in remote areas, or overseas citizens can conveniently participate in the voting process. The automation of result tabulation and elimination of manual vote counting can lead to faster and more efficient elections, reducing administrative burdens and costs. Additionally, the decentralized nature of blockchain-based systems makes them resilient to DDoS attacks, ensuring accessibility and functionality during elections. Overall, the future scope for e-voting systems based on blockchain technology holds immense potential to transform the electoral process and strengthen democratic practices.

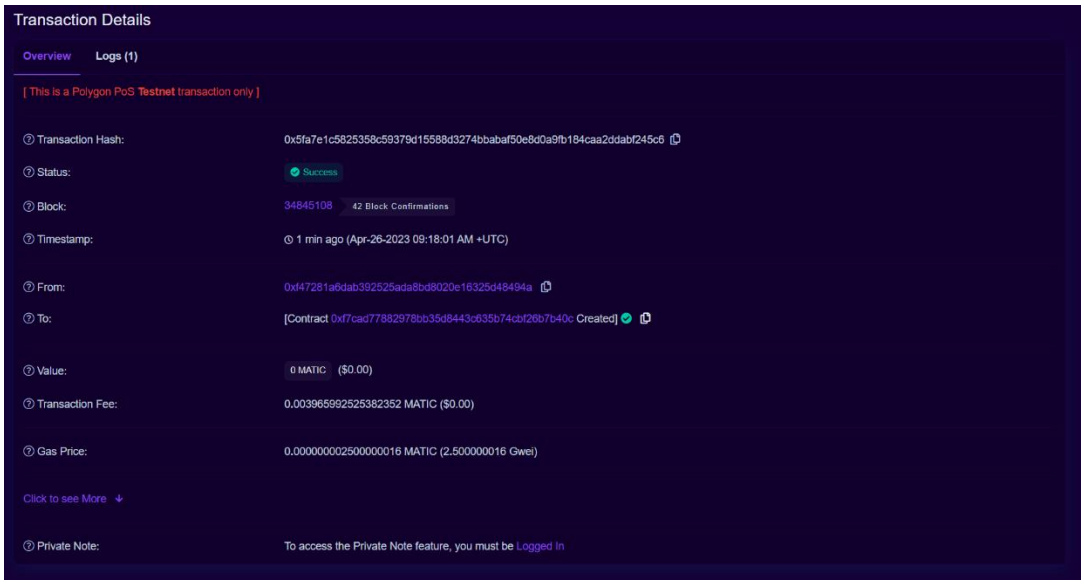
7. Conclusion

In conclusion, the proposed e-voting system based on blockchain technology has the potential to revolutionize the traditional voting process. The system provides numerous benefits, including increased security, transparency, and accuracy. Utilizing blockchain technology, the proposed e-voting system provides a tamper-proof and immutable record of all transactions, ensuring that the results of the election are accurate and trustworthy.

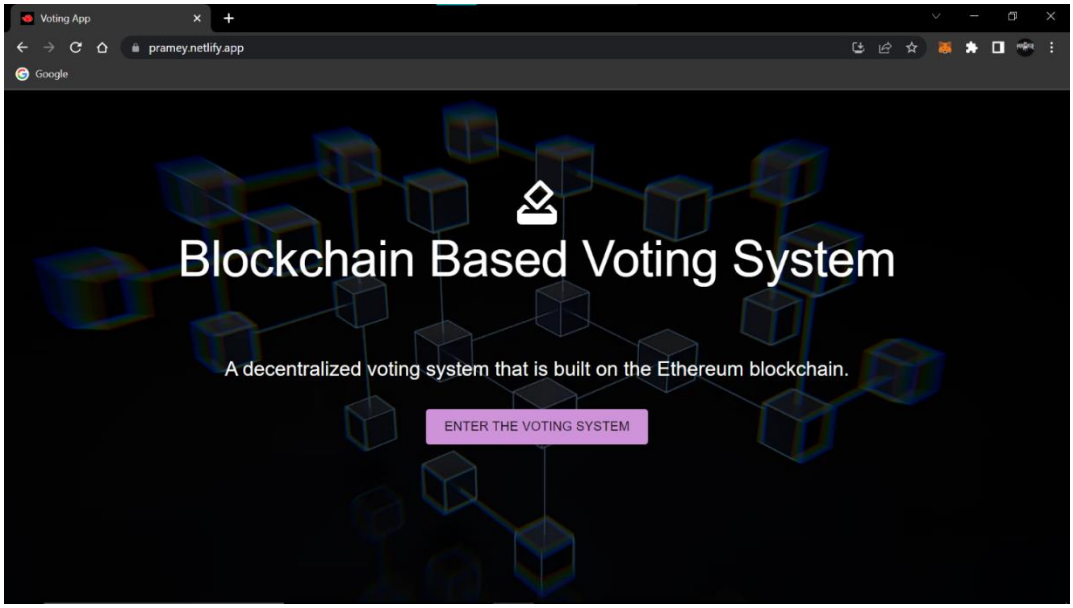
The use of smart contracts in the proposed system also automates the voting process, reducing the chances of human error and manipulation. The system's transparency and auditability features enable voters to verify their votes and ensure that their votes are counted. The proposed system's decentralized and distributed nature makes it resistant to attacks and manipulation, enhancing its security.

The evaluation of the proposed system will provide insights into its effectiveness and feasibility. The evaluation results will help identify areas for improvement and future development, ensuring that the proposed e-voting system continues to meet the evolving needs of voters and election officials.

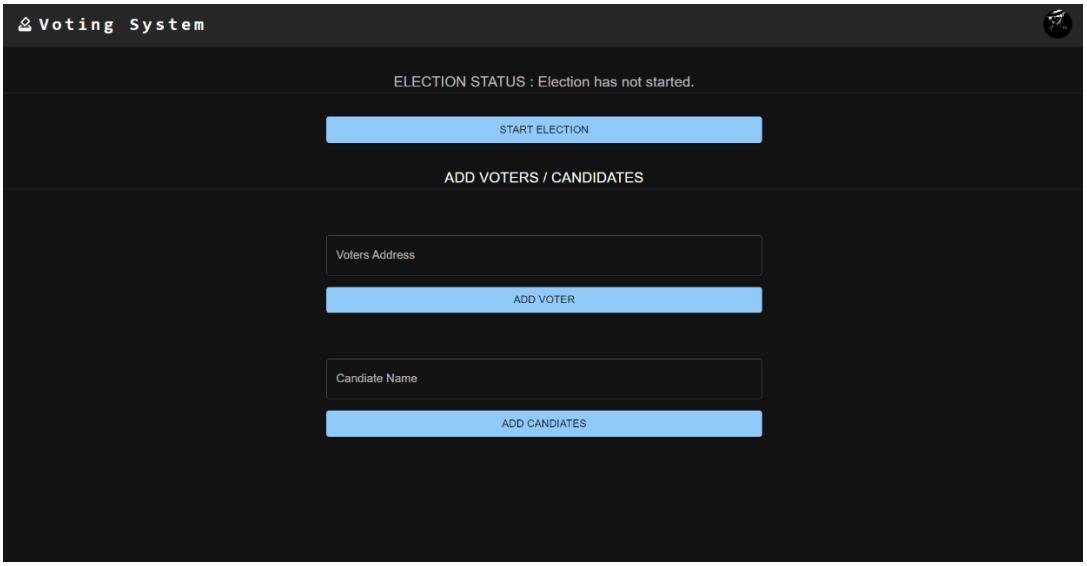
8. User Manual



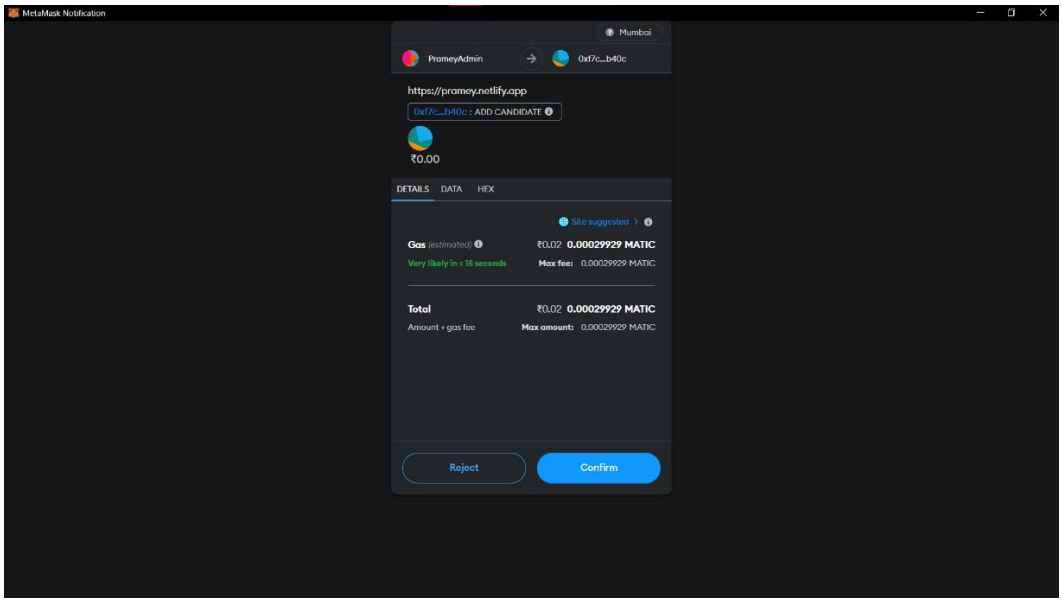
Snapshot 5 Deployed Contract on Polygon Test Network



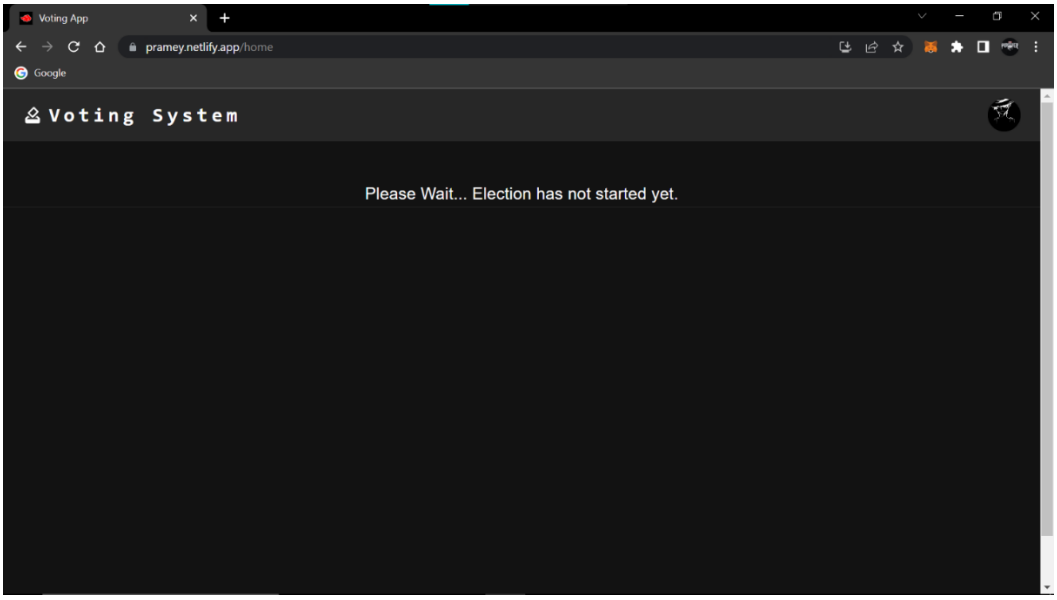
Snapshot 6 Home Page of Blockchain Voting System



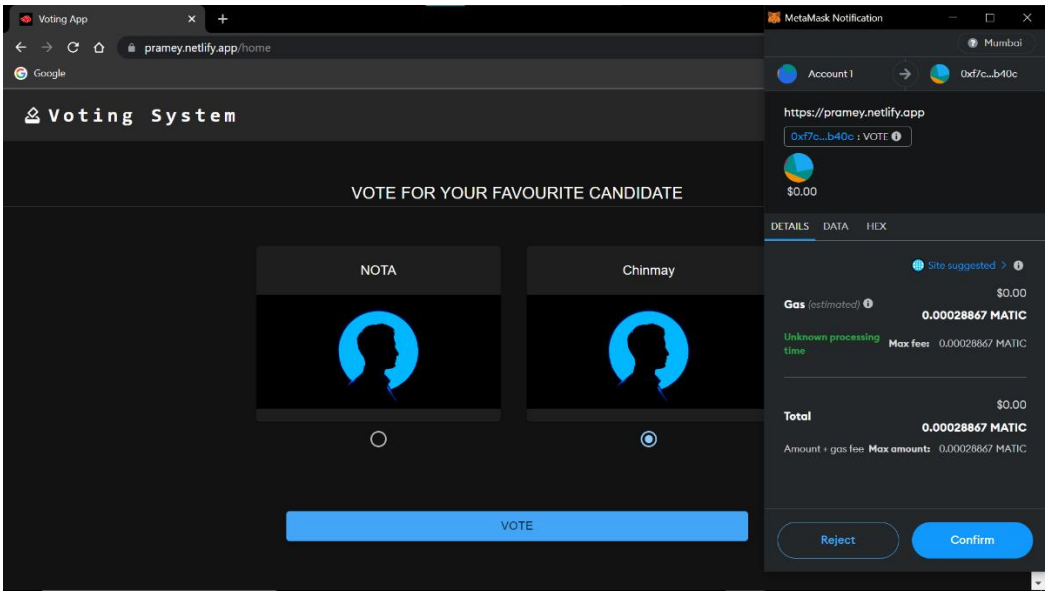
Snapshot 7 Admin User Interface



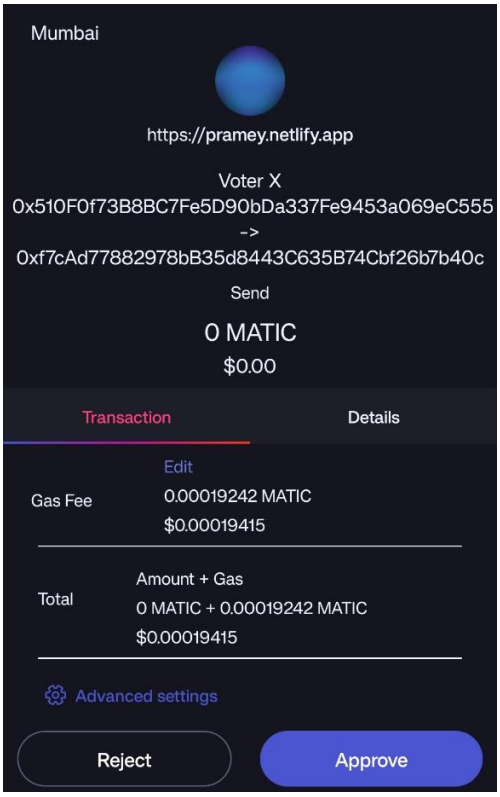
Snapshot 8 Transaction Conformation through MetaMask



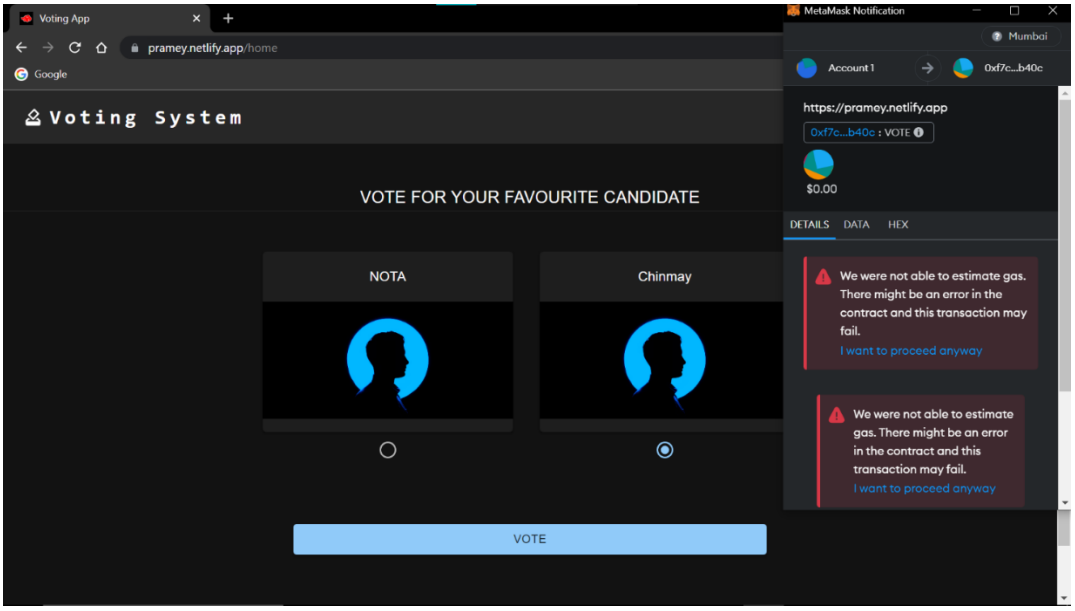
Snapshot 9 User Interface before start of an Election process



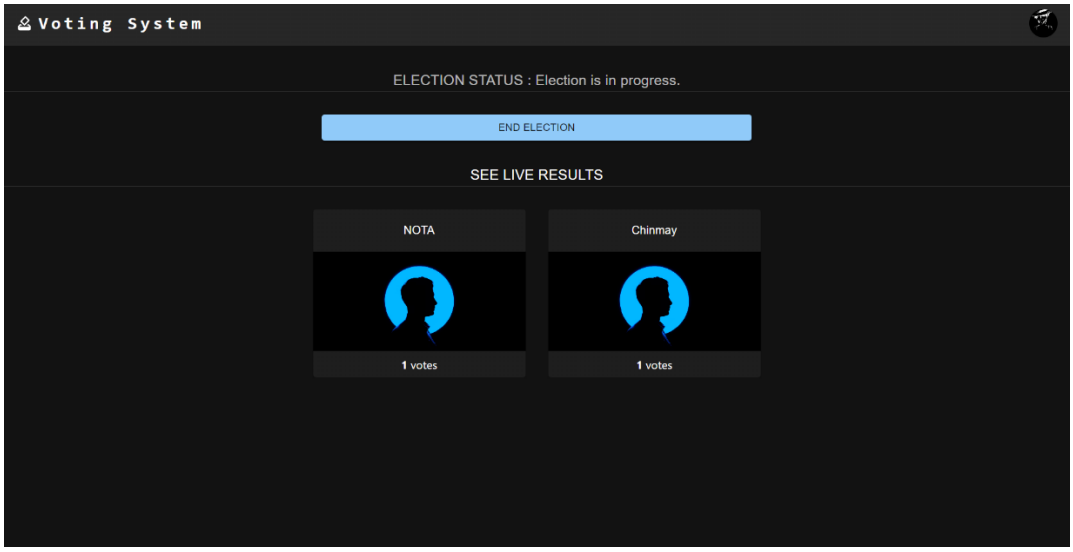
Snapshot 10 User Interface for Voting Process and Transaction Conformation



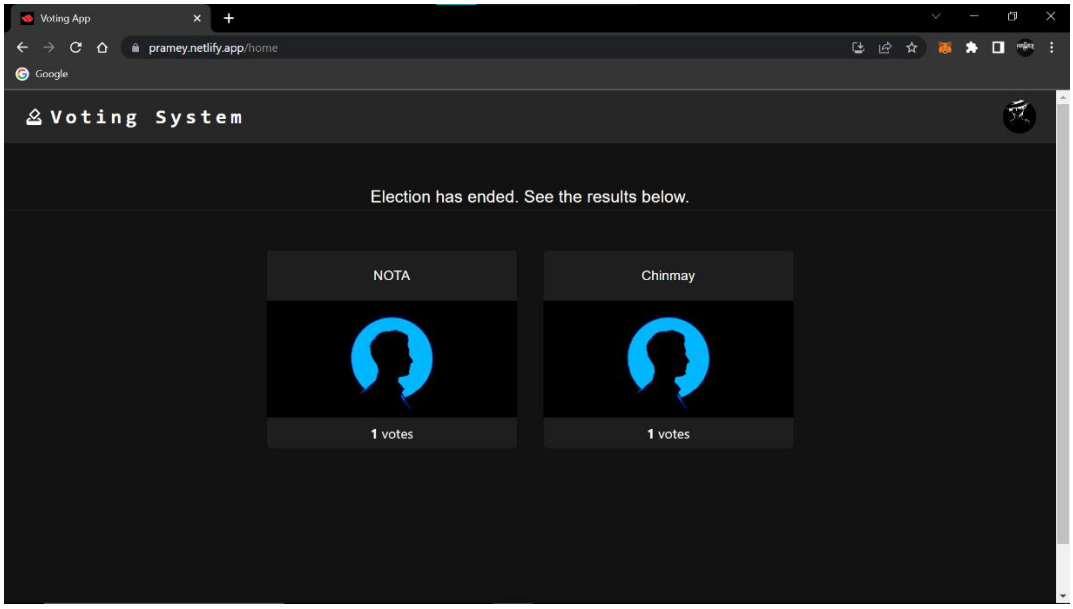
Snapshot 11 Transacation Conformation for Mobile Phone User



Snapshot 12 Transaction Failure in case of Double Voting



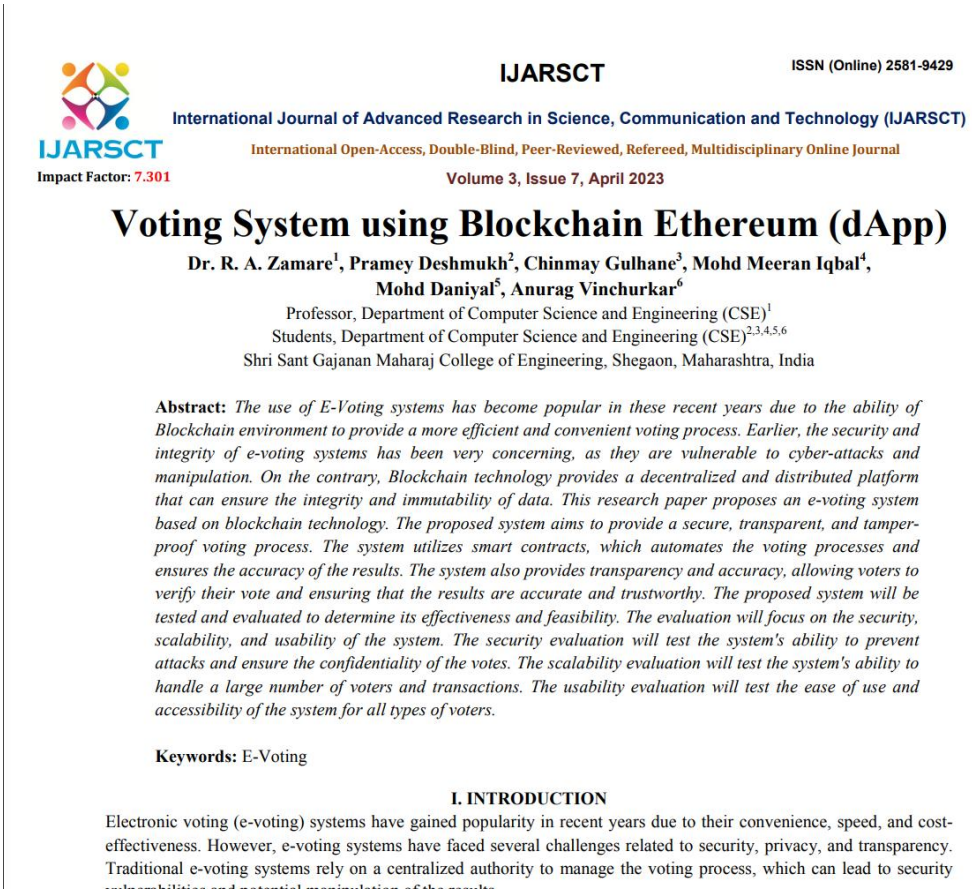
Snapshot 13 Admin User Interface during ongoing Election



Snapshot 14 Result Page for Voter

9. Publication details

Published Paper



IJARSCT
ISSN (Online) 2581-9429
International Journal of Advanced Research in Science, Communication and Technology (IJARSCT)
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
Impact Factor: 7.301
Volume 3, Issue 7, April 2023

Voting System using Blockchain Ethereum (dApp)

Dr. R. A. Zamare[1], Pramey Deshmukh[2], Chinmay Gulhane[3], Mohd Meeran Iqbal[4], Mohd Daniyal[5], Anurag Vinchurkar[6]
Professor, Department of Computer Science and Engineering (CSE)[1]
Students, Department of Computer Science and Engineering (CSE)[2,3,4,5,6]
Shri Sant Gajanan Maharaj College of Engineering, Shegaon, Maharashtra, India

Abstract: *The use of E-Voting systems has become popular in these recent years due to the ability of Blockchain environment to provide a more efficient and convenient voting process. Earlier, the security and integrity of e-voting systems has been very concerning, as they are vulnerable to cyber-attacks and manipulation. On the contrary, Blockchain technology provides a decentralized and distributed platform that can ensure the integrity and immutability of data. This research paper proposes an e-voting system based on blockchain technology. The proposed system aims to provide a secure, transparent, and tamper-proof voting process. The system utilizes smart contracts, which automates the voting processes and ensures the accuracy of the results. The system also provides transparency and accuracy, allowing voters to verify their vote and ensuring that the results are accurate and trustworthy. The proposed system will be tested and evaluated to determine its effectiveness and feasibility. The evaluation will focus on the security, scalability, and usability of the system. The security evaluation will test the system's ability to prevent attacks and ensure the confidentiality of the votes. The scalability evaluation will test the system's ability to handle a large number of voters and transactions. The usability evaluation will test the ease of use and accessibility of the system for all types of voters.*

Keywords: E-Voting

I. INTRODUCTION

Electronic voting (e-voting) systems have gained popularity in recent years due to their convenience, speed, and cost-effectiveness. However, e-voting systems have faced several challenges related to security, privacy, and transparency. Traditional e-voting systems rely on a centralized authority to manage the voting process, which can lead to security

Published Paper

DOI :- 10.48175/IJARSCT-9486

Certificates of the authors: -


INTERNATIONAL JOURNAL OF ADVANCED RESEARCH IN SCIENCE, COMMUNICATION AND TECHNOLOGY
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
IJARSCT
CERTIFICATE OF PUBLICATION
INTERNATIONAL STANDARD SERIAL NUMBER ISSN NO: 2581-9429
THIS IS TO CERTIFY THAT
Chinmay Gulhane
Shri Sant Gajanan Maharaj College of Engineering, Shegaon, Maharashtra, India
HAS PUBLISHED A RESEARCH PAPER ENTITLED
Voting System using Blockchain Ethereum (dApp)
IN IJARSCT, VOLUME 3, ISSUE 7, APRIL 2023
Certificate No: 042023-A1947
www.ijarsct.co.in
Crossref
DOI: 10.48175/IJARSCT-9486
www.doi.org
www.crossref.org
7.301
www.sjifactor.com
Editor-in-Chief


INTERNATIONAL JOURNAL OF ADVANCED RESEARCH IN SCIENCE, COMMUNICATION AND TECHNOLOGY
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
IJARSCT
CERTIFICATE OF PUBLICATION
INTERNATIONAL STANDARD SERIAL NUMBER ISSN NO: 2581-9429
THIS IS TO CERTIFY THAT
Mohd Meeran Iqbal
Shri Sant Gajanan Maharaj College of Engineering, Shegaon, Maharashtra, India
HAS PUBLISHED A RESEARCH PAPER ENTITLED
Voting System using Blockchain Ethereum (dApp)
IN IJARSCT, VOLUME 3, ISSUE 7, APRIL 2023
Certificate No: 042023-A1948
www.ijarsct.co.in
Crossref
DOI: 10.48175/IJARSCT-9486
www.doi.org
www.crossref.org
7.301
www.sjifactor.com
Editor-in-Chief


INTERNATIONAL JOURNAL OF ADVANCED RESEARCH IN SCIENCE, COMMUNICATION AND TECHNOLOGY
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
IJARSCT
CERTIFICATE OF PUBLICATION
INTERNATIONAL STANDARD SERIAL NUMBER ISSN NO: 2581-9429
THIS IS TO CERTIFY THAT
Mohd Daniyal
Shri Sant Gajanan Maharaj College of Engineering, Shegaon, Maharashtra, India
HAS PUBLISHED A RESEARCH PAPER ENTITLED
Voting System using Blockchain Ethereum (dApp)
IN IJARSCT, VOLUME 3, ISSUE 7, APRIL 2023
Certificate No: 042023-A1949
www.ijarsct.co.in
Crossref
DOI: 10.48175/IJARSCT-9486
www.doi.org
www.crossref.org
7.301
www.sjifactor.com
Editor-in-Chief


INTERNATIONAL JOURNAL OF ADVANCED RESEARCH IN SCIENCE, COMMUNICATION AND TECHNOLOGY
International Open-Access, Double-Blind, Peer-Reviewed, Refereed, Multidisciplinary Online Journal
IJARSCT
CERTIFICATE OF PUBLICATION
INTERNATIONAL STANDARD SERIAL NUMBER ISSN NO: 2581-9429
THIS IS TO CERTIFY THAT
Anurag Vinchurkar
Shri Sant Gajanan Maharaj College of Engineering, Shegaon, Maharashtra, India
HAS PUBLISHED A RESEARCH PAPER ENTITLED
Voting System using Blockchain Ethereum (dApp)
IN IJARSCT, VOLUME 3, ISSUE 7, APRIL 2023
Certificate No: 042023-A1950
www.ijarsct.co.in
Crossref
DOI: 10.48175/IJARSCT-9486
www.doi.org
www.crossref.org
7.301
www.sjifactor.com
Editor-in-Chief

REFERENCES

[1] Benabdallah, A. Audras, L. Coudert, N. El Madhoun and M. Badra, "Analysis of Blockchain Solutions for E-Voting: A Systematic Literature Review," in IEEE Access, vol. 10, pp. 70746-70759, 2022, doi: 10.1109/ACCESS.2022.3187688.

[2] S. Al-Maaitah, M. Qatawneh and A. Quzmar, "E-Voting System Based on Blockchain Technology: A Survey," *2021 International Conference on Information Technology (ICIT)*, Amman, Jordan, 2021, pp. 200-205, doi: 10.1109/ICIT52682.2021.9491734.

[3] M. Al-madani, A. T. Gaikwad, V. Mahale and Z. A. T. Ahmed, "Decentralized E-voting system based on Smart Contract by using Blockchain Technology," 2020 International Conference on Smart Innovations in Design, Environment, Management, Planning and Computing (ICSIDEMPC), Aurangabad, India, 2020, pp. 176-180, doi: 10.1109/ICSIDEMPC49020.2020.9299581.

[4] S. T. Alvi, M. N. Uddin and L. Islam, "Digital Voting: A Blockchain-based E-Voting System using Biohash and Smart Contract," 2020 Third International Conference on Smart Systems and Inventive Technology (ICSSIT), Tirunelveli, India, 2020, pp. 228-233, doi: 10.1109/ICSSIT48917.2020.9214250.

[5] K. Patidar and S. Jain, "Decentralized E-Voting Portal Using Blockchain," 2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT), Kanpur, India, 2019, pp. 1-4, doi: 10.1109/ICCCNT45670.2019.8944820.

[6] S. K. Vivek, R. S. Yashank, Y. Prashanth, N. Yashas and M. Namratha, "E-Voting Systems using Blockchain: An Exploratory Literature Survey," 2020 Second International Conference on Inventive Research in Computing Applications (ICIRCA), Coimbatore, India, 2020, pp. 890-895, doi: 10.1109/ICIRCA48905.2020.9183185.

[7] Benabdallah, A. Audras, L. Coudert, N. El Madhoun and M. Badra, "Analysis of Blockchain Solutions for E-Voting: A Systematic Literature Review," in IEEE Access, vol. 10, pp. 70746-70759, 2022, doi: 10.1109/ACCESS.2022.3187688.

[8] D. Golnarian, K. Saedi and B. Bahrak, "A decentralized and trustless e-voting system based on blockchain technology," 2022 27th International Computer Conference, Computer Society of Iran (CSICC), Tehran, Iran, Islamic Republic of, 2022, pp. 1-7, doi: 10.1109/CSICC55295.2022.9780507. `

[9] R. Taş and Ö. Ö. Tanrıöver, "A Systematic Review of Challenges and Opportunities of Blockchain for E-Voting," *Symmetry*, vol. 12, no. 8, p. 1328, Aug. 2020, doi: 10.3390/sym12081328.

[10] Ruhi Taş, Ömer Özgür Tanrıöver, "A Manipulation Prevention Model for Blockchain-Based E-Voting Systems", *Security and Communication Networks*, vol. 2021, Article ID 6673691, 16 pages, 2021. https://doi.org/10.1155/2021/6673691

[11] Cosmin-Iulian, I., Iftene, A., & Gifu, D. (2021). A Large-Scale E-voting System Based on Blockchain. In E. Insfran, F. González, S. Abrahão, M. Fernández, C. Barry, H. Linger, M. Lang, & C. Schneider (Eds.), *Information Systems Development: Crossing Boundaries between Development and Operations (DevOps) in Information Systems (ISD2021 Proceedings)*. Valencia, Spain: Universitat Politècnica de València.

[12] R. C. Agidi, "Artificial intelligence in nigeria financial sector," International Journal of Electronics and Information Engineering, vol. 11, no. 1, pp. 40–47, 2019.

[13] A. Ghosh, S. Gupta, A. Dua, and N. Kumar, "Security of Cryptocurrencies in blockchain technology: State-of-art, challenges and future prospects," Journal of Network and Computer Applications, vol. 163, Article ID 102635, 2020.

[14] M. S. Rahman, I. Khalil, A. Alabdulatif, and X. Yi, "Privacy preserving service selection using fully homomorphic encryption scheme on untrusted cloud service platform," Knowledge-Based Systems, vol. 180, pp. 104–115, 2019.