A Project Report on

A Voting System Based on Blockchain Technology

A Dissertation submitted to JNTU Hyderabad in partial fulfillment of the academic requirements for the award of the degree.

Bachelor of Technology

in

Computer Science and Engineering

Submitted by

M SRIKANTH
(20H51A05L1)

Under the esteemed guidance of

Ms. N. SUREKHA

(Assistant Professor)

Department of Computer Science and Engineering

CMR COLLEGE OF ENGINEERING & TECHNOLOGY

(UGC Autonomous)

*Approved by AICTE *Affiliated to JNTUH *NAAC Accredited with A^{+} Grade

KANDLAKOYA, MEDCHAL ROAD, HYDERABAD - 501401.

2020- 2024

CMR COLLEGE OF ENGINEERING & TECHNOLOGY

KANDLAKOYA, MEDCHAL ROAD, HYDERABAD – 501401

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

CERTIFICATE

This is to certify that the Major Project report entitled "**A VOTING SYSTEM BASED ON BLOCKCHAIN TECHNOLOGY**" being submitted by M. Srikanth (20H51A0544) partial fulfillment for the award of **Bachelor of Technology in Computer Science and Engineering** is a record of bonafide work carried out under my guidance and supervision.

The results embodies in this project report have not been submitted to any other University or Institute for the award of any Degree.

Ms. N. Surekha	**Dr. Siva Skandha Sanagala**	
Associate Professor	**Associate Professor and HOD**	**EXTERNAL EXAMINER**
Dept. of CSE	**Dept. of CSE**	

ACKNOWLEDGEMENT

With great pleasure I want to take this opportunity to express our heartfelt gratitude to all the people who helped in making this project a grand success.

I am grateful to **Ms. N. Surekha, Associate Professor** , Department of Branch Name for his valuable technical suggestions and guidance during the execution of this project work.

I would like to thank**, Dr. Siva Skandha Sanagala,** Head of the Department of Dept Name, CMR College of Engineering and Technology, who is the major driving forces to complete my project work successfully.

I am very grateful to **Dr. Ghanta Devadasu**, Dean-Academics, CMR College of Engineering and Technology, for his constant support and motivation in carrying out the project work successfully.

I am highly indebted to **Major Dr. V A Narayana,** Principal, CMR College of Engineering and Technology, for giving permission to carry out this project in a successful and fruitful way.

I Would like to thank the **Teaching & Non- teaching** staff of Department of Dept Name for their co-operation

I express our sincere thanks to **Shri. Ch. Gopal Reddy**, Secretary& Correspondent, CMR Group of Institutions, and Shri Ch Abhinav Reddy, CEO, CMR Group of Institutions for their continuous care and support.

Finally, I extend thanks to my parents who stood behind me at different stages of this Project. I sincerely acknowledge and thank all those who gave support directly or indirectly in completion of this project work.

M Srikanth - 20H51A05L1

TABLE OF CONTENTS

List of Figures

ABSTRACT

The problem Statement for the proposed, Voting System Based on Blockchain Technology. The main aim of the proposed blockchain-based voting system is to address the shortcomings of traditional voting systems and improve the overall integrity, security, transparency, and efficiency of the electoral process. The advent of blockchain technology has introduced innovative solutions across various sectors, and the realm of voting systems is no exception. This abstract presents a novel approach to a voting system based on blockchain technology, aimed at enhancing the transparency, security, and efficiency of electoral processes.

Traditional voting systems often face challenges related to voter authentication, tampering of results, and manual error handling. In this proposed blockchain-based voting system, each vote is recorded.. Cryptographic techniques are employed to secure voter identity and maintain anonymity, thus mitigating the risks associated with fraudulent voting. Furthermore, smart contracts are utilized to automate various aspects of the voting process, such as voter verification and result tabulation, minimizing human intervention and reducing the likelihood of errors. Overall, this blockchain-based voting system offers a secure, transparent, and efficient platform for conducting elections, fostering trust and integrity in democratic processes. The following article gives an overview of electronic voting systems based on blockchain technology.

CHAPTER 1
INTRODUCTION

CHAPTER 1

INTRODUCTION

1.1.Problem Statement

Electoral integrity is essential not just for democratic nations but also for state voter's trust and liability. Political voting methods are crucial in this respect. From a government standpoint, electronic voting technologies can boost voter participation and confidence and rekindle interest in the voting system. As an effecti ve means of making democratic decisions, elections have long been a social concern. As the number of votes cast in real life increases, citizens are becoming more aware of the significance of the electoral system. The voting system is the method through which judges judge who will represent in political and corporate governance. Democracy is a system of voters to elect representatives by voting . The efficacy of such a procedure is determined mainly by the level of faith that people have in the election process. The creation of legislative institutions to represent the desire of the people is a well- known tendency. Such political bodies differ from student unions to constituencies. Over the years, the vote has become the primary resource to express the will of the citizens by selecting from the choices they made.

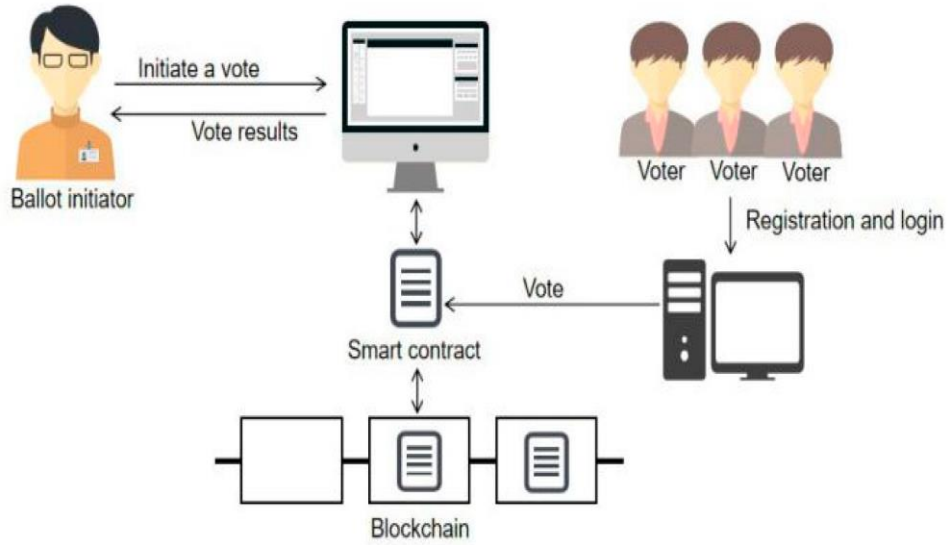


Figure.1.1:Blockchain voting System

1.2.Research Objective

The primary objective of implementing a voting system based on blockchain technology is to enhance the integrity, transparency, and security of the voting process. Blockchain technology achieves this by Immutable Record keeping. Every vote cast is recorded on the blockchain, creating an immutable ledger that cannot be altered or tampered with, ensuring the integrity of the voting data transparency .The decentralized nature of blockchain allows all participants to verify the authenticity of the voting process, promoting trust and transparency in the election results. Security Blockchain employs cryptographic techniquesto secure the voting process, making it extremely difficult for malicious actors to manipulate or hack the system. Elimination of Intermediaries by utilizing blockchain, the need for intermediaries such as centralized voting authorities or election committees is reduced, minimizing the risk of corruption and manipulation. Immutable Recordkeeping, every vote cast is recorded on the blockchain, creating an immutable ledger that cannot be altered or tampered with, ensuringthe integrity of the voting data. The decentralized nature of blockchain allowsall participants to verify the authenticity of the voting process, promoting trust and transparency in the election results.

1.3. Project Scope and Limitations

Scope:

The scope of the project encompasses the development, deployment, and ongoing maintenance of a blockchain-based voting system that addresses the challenges of traditional voting systems while promoting security, transparency, accessibility, and usability in the electoral process. User Adoption and Accessibility: Introducing a new voting system based on blockchain technology requires widespread adoption and acceptanceby voters, election officials, and regulatory authorities. Addressing legal and regulatory challenges, such as identity verification, jurisdictional issues, and compliance with electorallaws, is crucial for the widespread adoption of blockchain voting solutions Technological Maturity.

Limitations:

1. Security Concerns: Despite utilizing cryptographic techniques, electronic voting systems are vulnerable to hacking, tampering, and other security breaches.
2. Privacy Issues: While blockchain-based systems offer a degree of anonymity, they may not fully guarantee voter privacy. Traceability of transactions on the blockchain could potentially compromise voter anonymity, raising concerns about coercion or intimidation.
3. Accessibility Barriers :Technology-driven voting systems may inadvertently exclude certain demographics, such as elderly voters or those with disabilities, who may face challenges in navigating digital interfaces or require specialized assistance not readily available in digital formats.
4. Infrastructure Dependence: Electronic voting systems rely heavily on robust and reliable infrastructure, including internet connectivity and power supply. In regions with inadequate infrastructure or prone to frequent outages.
5. Cost Implications: Implementing and maintaining sophisticated voting technologies, including blockchain-based solutions, can incur significant costs.
6. Complexity and Usability: Introducing complex voting systems could confuse or intimidate voters, leading to lower turnout or increased rates of invalid ballots. User-friendly design and comprehensive training programs are essential to mitigate usability issues and ensure equitable access to the voting process.
7. Resistance to Change: Traditional voting systems have deep-rooted societal norms and institutional inertia supporting their continuation. Introducing technological innovations may face resistance from stakeholders reluctant to embrace change or skeptical of the reliability and security of new voting methods.

CHAPTER 2
BACKGROUND WORK

CHAPTER 2

BACKGROUND WORK

2.1. Security Assessment

2.1.1. Introduction

Assessing the security aspects of implementing a blockchain-based voting system is a critical step toward enhancing the integrity, transparency, and reliability of electoral processes. The methodical approach tothis assessment involves several key components.

Firstly, it begins with a comprehensive threat modeling exercise. By identifying potential threats such ashacking attempts, denial-of-service attacks, or insider manipulation, stakeholders can understand the security landscape and assess the potential impact of each threat on the voting system.

Following this, a thorough analysis of security requirements is conducted. These requirements are derived from the identified threats and encompass various aspects such as cryptographic protections, access controls, and data integrity mechanisms[2]. Clear security requirements serve as the foundation for designing and implementing robust security measures.

Next, careful evaluation of blockchain technology is essential. Various blockchain platforms, each withdistinct features and capabilities, are considered to determine the best fit for the voting system's securityneeds. Factors such as consensus mechanisms, smart contract functionality, scalability, and privacy features are evaluated to ensure alignment with security requirements.[3]

Attention is also given to smart contract security, particularly if smart contracts are utilized for processing votes. A rigorous security audit is performed to identify vulnerabilities such as reentrancy attacks or logic flaws. Best practices for secure smart contract development, including code reviews and formal verification, are implemented to minimize the risk of exploitation.

Additionally, network security measures are implemented to safeguard data transmission between network nodes. Encryption protocols are utilized to secure communication channels and prevent unauthorized access or authentication, biometric verification, or cryptographic credentials may be employed to enhance security.[4]

2.1.2. Merits, Demerits and Challenges

Merits:

- Improves Accessibility for Vulnerable Populations: Blockchain-based voting systems can be designed with user-friendly interfaces and accessibility features to accommodate individuals with disabilities, ensuring that voting is accessible to all citizens, regardless of physical or cognitive impairments.
- Enhances Election Observability: The transparency and immutability of blockchain records enable independent observers, electoral monitors, and auditors to scrutinize the entire voting process, promoting transparency, accountability, and trust in the electoral outcomes.
- Mitigates Electoral Fraud: The use of cryptographic techniques and consensus mechanisms in blockchain-based voting systems significantly reduces the risk of electoral fraud, such as ballot stuffing, vote manipulation, or identity theft, thereby upholding the integrity of elections.
- Streamlines Voter Registration: Blockchain technology can streamline voter registration processes by securely storing and managing voter registration data on a distributed ledger, reducing administrative burdens and ensuring the accuracy and integrity of voter rolls.

Demerits:

- High Barrier to Entry: Implementing and securing a blockchain network requires specialized technical expertise, which may be lacking in electoral authorities or governments.

- Resource Intensive: Setting up and maintaining a blockchain network entails significant computational resources and costs, including hardware infrastructure and energy consumption.

- Privacy Breaches: Any breach in the security or confidentiality of blockchain-based voting systems could expose sensitive voter information, leading to privacy violations or identity theft.

- Lack of Trust in Pseudonymity: Some critics argue that pseudonymous voting, while protecting individual identities, may erode trust in the electoral process by obscuring the accountability of voters and election authorities.

- Network Congestion: During periods of high voter turnout or increased transaction volume, blockchain networks may experience congestion, leading to delays in vote processing and potential disruptions to the voting process.

- Scalability Trade-offs: Implementing scalable solutions often involves trade-offs between decentralization, security, and efficiency. Balancing these competing priorities while maintaining the integrity of the voting system poses significant technical challenges.

Challenges:

- Legal and Regulatory Compliance: Adhering to complex legal and regulatory requirements, including election laws, privacy regulations, and cybersecurity standards, poses challenges in the development and implementation of blockchain.

- Trust in Technology: Building trust in blockchain technology and its application in voting systems among stakeholders, including voters, election officials, and government agencies, isessential for successful adoption and acceptance, necessitating efforts to address misconceptions, skepticism, and resistance to new technologies.

- Funding and Resource Constraints: Securing adequate funding and resources for the research,development, and deployment of blockchain-based voting systems .

2.1.3. Implementation

- Public Awareness and Outreach: Conducting public awareness campaigns and outreach initiatives to educate voters about the benefits, security features, and voting procedures of blockchain-based voting systems is essential for increasing voter confidence, trust, and participation in the electoral process.

- Continuous Improvement and Iterative Development: Embracing a culture of continuous improvement and iterative development in the design, implementation, and operation of blockchain-based voting systems allows for incorporating feedback, addressing issues, and enhancing system functionality, reliability, and security over time.

- Redundancy and Disaster Recovery Planning: Implementing robust redundancy and disaster recovery measures, such as data backups, failover systems, and contingency plans, is essential for ensuring the resilience, availability, and continuity of blockchain-based voting systems in the face of technical failures, cyberattacks, or natural disasters.

- Legal and Ethical Considerations: Addressing legal and ethical considerations, such as data privacy, consent, transparency, accountability, and voter rights, in the design and operation of blockchain-based voting systems is critical for safeguarding fundamental democratic principles and ensuring compliance with legal and ethical standards.[6]

- Vendor Selection and Partnerships: Selecting reputable and trustworthy technology vendors, service providers, and partners with expertise in blockchain technology, cybersecurity, and electoral processes is essential for ensuring the quality, reliability, and security of blockchain- based voting systems.

- Network Congestion: During periods of high voter turnout or increased transaction volume, blockchain networks may experience congestion.

- Scalability Trade-offs: Implementing scalable solutions often involves trade-offs between decentralization, security, and efficiency.

- Limited Throughput: The inherent limitations of blockchain technology, such as block size constraints and consensus protocol .

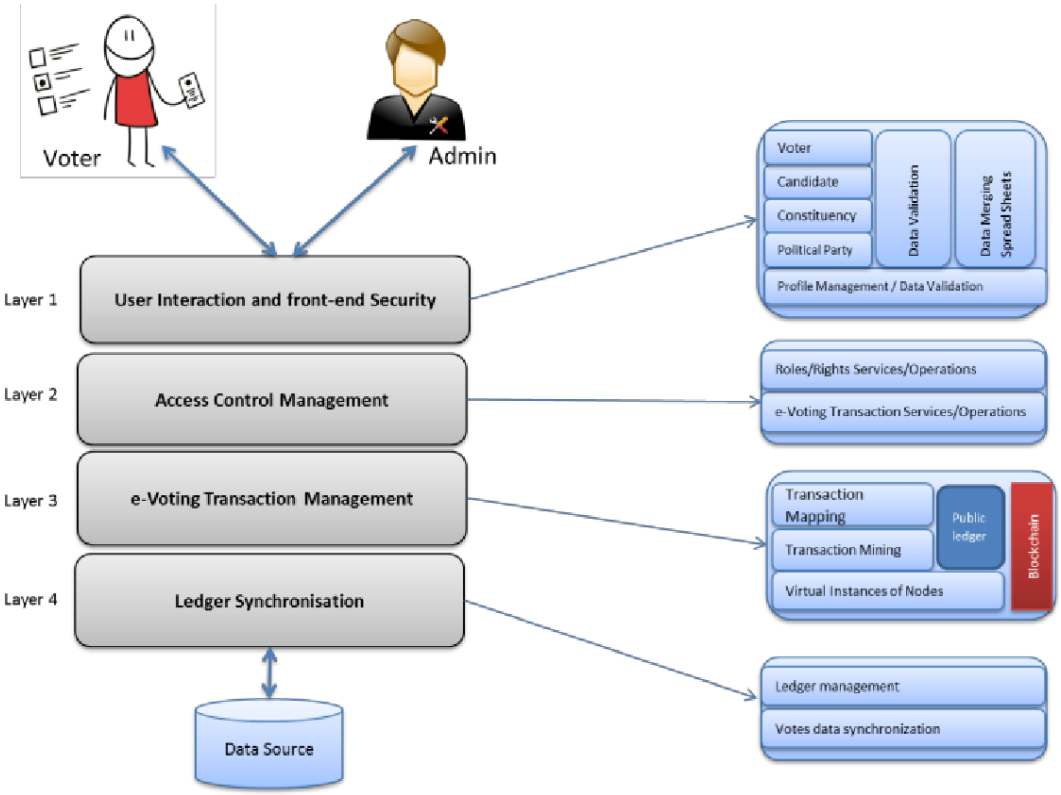


Figure.2.1: The architecture of existing system

2.2 Explainable Regulatory Framework for Blockchain-Based Voting :

2.2.1. Introduction

The exploration of blockchain technology for secure and transparent voting systems represents a significant advancement in the quest to enhance the integrity and security of electoral processes. This method seeks to delve into the potential applications of blockchain in revolutionizing the way votes arerecorded, verified, and counted, with a primary focus on improving the trustworthiness and resilience ofthe voting process.

At its core, this method involves leveraging a permissioned blockchain network—a distributed ledger technology where access to participate in the network is controlled by a predetermined set of participants—to establish a secure and transparent voting infrastructure. Unlike public blockchains, which allow anyone to participate in the network, permissioned blockchains restrict access to designated entities, such as election officials, government agencies, and authorized participants, ensuring greater control over the network and its operations[7].

By utilizing a permissioned blockchain network, this method aims to address several critical challengesinherent in traditional voting systems, such as fraud, manipulation, and lack of transparency. Through theimmutable nature of blockchain technology, each vote cast is cryptographically secured and recorded on the blockchain in a tamper-proof manner, providing an indisputable audit trail of all voting activities.

Moreover, the decentralized nature of blockchain networks distributes power and authority across the network, reducing the risk of centralized control or manipulation. Each participant in the blockchain network maintains a copy of the ledger, ensuring redundancy and resilience against single points of failure or attacks.

One of the key components of this method is the development and deployment of smart contracts—self-executing contracts with predefined rules and conditions—designed to manage the voting process securely. Smart contracts enable the automation of voting procedures, including voter registration, ballotissuance, vote casting, and result tabulation, while ensuring transparency, fairness, and accuracythroughout the process.[8]

2.2.2. Merits, Demerits and Challenges

Merits:

- Trust: Blockchain instills trust in the voting process by providing a tamper-proof record of alltransactions, fostering confidence in the integrity of election results.
- Resistance to Tampering: The decentralized nature of blockchain networks makes them resistantto tampering or manipulation by malicious factors.
- Auditability: Blockchain-based voting systems enable real-time auditing of voting activities, allowing stakeholders to verify the accuracy and legitimacy of election results independently.
- Immutable Record: The immutable nature of blockchain ensures that once a vote is recorded, itcannot be altered or deleted.
- Disintermediation: Blockchain eliminates the need for intermediaries or centralized authorities in the voting process, reducing the potential for corruption, bias, or manipulation.

Demerits:

- Complexity: Implementing and managing blockchain-based voting systems can be complex and resource-intensive, technical expertise and significant investment in infrastructure.
- Governance Challenges: Decentralized governance structures inherent in blockchain networks may pose challenges in decision-making, consensus-building, and resolving disputes or conflicts among stakeholders.
- Cost: Developing and maintaining blockchain-based voting systems may involve high upfrontcosts and ongoing expenses related to infrastructure, development, and maintenance.
- Regulatory Uncertainty: Unclear or evolving regulatory frameworks for blockchain technology and voting systems may create uncertainty and legal risks for stakeholders, hindering adoptionand implementation efforts.

Challenges:

- Voter Education: Educating voters about the benefits, security features, and voting proceduresof blockchain-based voting systems is essential for increasing acceptance and adoption, requiring targeted education campaigns and outreach initiatives.
- Interoperability: Ensuring interoperability and compatibility between blockchain-based votingsystems and existing electoral infrastructures and procedures presents technical challenges related to data migration, integration, and system compatibility.
- Trust Establishment: Building trust and confidence in blockchain technology and its application in voting systems among stakeholders, including voters, election officials, and government agencies, requires transparent communication, independent audits, and demonstration of the system's reliability and security.
- Resistance to Centralization: Maintaining the decentralized nature of blockchain networks and preventing concentration of power or influence among a few participants is crucial for preserving the integrity and fairness of the voting process, necessitating robust governance mechanisms and safeguards against centralization tendencies.
- Addressing Bias and Discrimination: Ensuring fairness and equity in blockchain-based voting systems requires addressing potential biases in algorithms, data sources, or decision-making processes that may disproportionately impact certain demographic groups or communities.

2.2.3. Implementation

- **Selection of an appropriate blockchain platform and consensus mechanism:**

  Choosing the right blockchain platform is crucial for the success of a blockchain-based voting system. Factors such as scalability, security, interoperability, and community support need to be considered. Popular blockchain platforms like Ethereum, Hyperledger Fabric, and Corda offer different features and capabilities suited for various use cases. Additionally, selecting the appropriate consensus mechanism, such as Proof of Work (PoW), Proof of Stake (PoS), or Practical Byzantine Fault Tolerance (PBFT), depends on the specific requirements of the voting system in terms of performance, decentralization, and energy efficiency.[10]

Figure.2.2.1: Architecture of existing system

- **Extensive testing, including security audits and simulations:**
  Thorough testing is essential to identify and mitigate potential vulnerabilities, bugs, and security risks in the blockchain-based voting system. Security audits, conducted by independent experts, help assess the system's resilience against cyberattacks, data breaches, and manipulation attempts. Simulations simulate real-world scenarios to evaluate the system's performance, scalability, and reliability under different conditions.
- **Pilot testing to evaluate the system in real voting scenarios:**
  Pilot testing involves deploying the blockchain-based voting system in a controlled environment to evaluate its performance, usability, and effectiveness in real voting scenarios. Pilot tests allow election authorities, voters, and other stakeholders to experience the votingprocess firsthand, provide feedback, and identify any issues or challenges that need to be addressed.

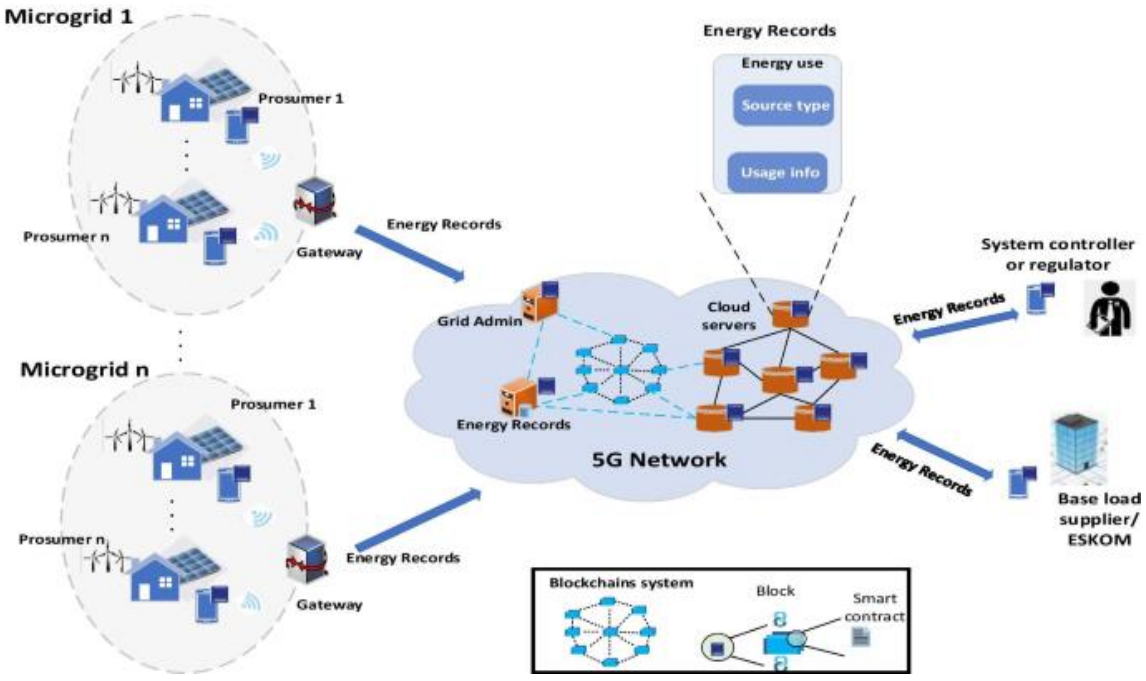


Figure.2.2.2: The execution framework of the proposed Blockchain Network

2.3. Voter Education and Adoption for Blockchain Voting :

2.3.1. Introduction

Introduction This method focuses on educating voters and encouraging adoption of blockchain-based voting. Voter education is crucial for ensuring the successful implementation andacceptance of the new technology.

The method of educating voters and promoting the adoption of blockchain-based voting systems is a pivotal strategy in ensuring the successful integration and acceptance of this innovative technology. At its core, voter education plays a vital role in familiarizing individuals with the workings and benefits of blockchain in the electoral process. Through comprehensive educational initiatives, voters can gain a deeper understanding of how blockchain ensures transparency, security, and integrity in voting systems. By elucidating the technical aspects and advantages of blockchain-based voting, individuals are better equipped to make informed decisions and embrace this transformative approach to democracy. Moreover, voter education serves to dispel any misconceptions or concerns surrounding blockchain technology, thereby fostering trust and confidence among the electorate. As a result, effective voter education campaigns not only facilitate the smooth implementation of blockchain-based voting systems but also contribute to the broader goal of enhancing democratic participation and electoral integrity.

2.3.2. Merits, Demerits and Challenges

Merits:

- Informed Voters: Education empowers voters to understand not only how blockchain-basedvoting works but also its significance in enhancing transparency, security, and trust in the electoral process.

- Increased Participation: Voter education initiatives can effectively communicate the benefits of blockchain-based voting, such as convenience, accessibility, and tamper-proof records.

- Improved Public Perception: Educating the public about blockchain technology and its applications in voting can help dispel misconceptions, fears, and doubts surrounding the newsystem.

- Increased Participation: Voter education initiatives can effectively communicate the benefits of blockchain-based voting, such as convenience, accessibility, and tamper-proof records. Byhighlighting these advantages, voter participation rates are likely to increase as individuals become more confident and comfortable with the technology, leading to a more inclusive andrepresentative democracy.

- Improved Public Perception: Educating the public about blockchain technology and its applications in voting can help dispel misconceptions, fears, and doubts surrounding the new system. By fostering a better understanding of the underlying principles and safeguards embedded in blockchain-based voting, voter trust and acceptance are bolstered, paving the way for widespread adoption and support.

Demerits:

- money, and effort to develop and implement effectively. This includes designing educational materials, organizing outreach events, training staff, and conducting awareness campaigns across various channels.
- Resistance to Change: Despite the benefits of blockchain-based voting, some voters may exhibit resistance or reluctance to embrace new technologies, preferring traditional methodsthey are familiar with. Overcoming this resistance requires targeted education efforts to address concerns, alleviate fears, and build confidence in the reliability and security of blockchain-based voting systems.

- Misinformation: Ensuring that voter education campaigns deliver accurate, unbiased, and up-to-date information about blockchain technology and its implications for voting is paramount. However, misinformation or misconceptions about blockchain may spread through social media, news outlets, or word-of-mouth, undermining the effectiveness of educational efforts. Combatting misinformation requires proactive communication strategies, fact-checking.

Challenges:

- **Designing effective voter education programs that cater to diverse demographics:**

  Voter education initiatives must be tailored to the needs, preferences, and literacy levels ofdiverse demographic groups, including different age cohorts, ethnicities, socioeconomic backgrounds, and educational attainment. This necessitates employing a variety of communication channels, languages, and formats to reach and engage a broad audience effectively.

- **Addressing concerns about privacy and security associated with blockchain technology:**

  Voter education efforts should address common concerns and misconceptions about the privacy, security, and anonymity of blockchain-based voting systems. By explaining the cryptographic protocols, encryption techniques.

- **Collaborating with schools, community organizations, and media for comprehensive outreach:**

  Effective voter education requires collaboration and partnership with a range of stakeholders,including schools, universities, civic groups, NGOs, media outlets, and social influencers.

2.3.3. Implementation

- Designing comprehensive voter education materials, including brochures, videos, andworkshops.
- Creating informative and accessible resources to explain blockchain voting.
- Collaborating with schools and educational institutions to include blockchain voting in curricula.
- Integrating blockchain topics into educational programs and lesson plans.
- Engaging with community organizations and leaders to spread awareness.
- Partnering with local groups and leaders to reach diverse populations.

- Monitoring and adapting the education program based on feedback and changing technology.
- Continuously evaluating and adjusting education efforts to improve effectiveness.

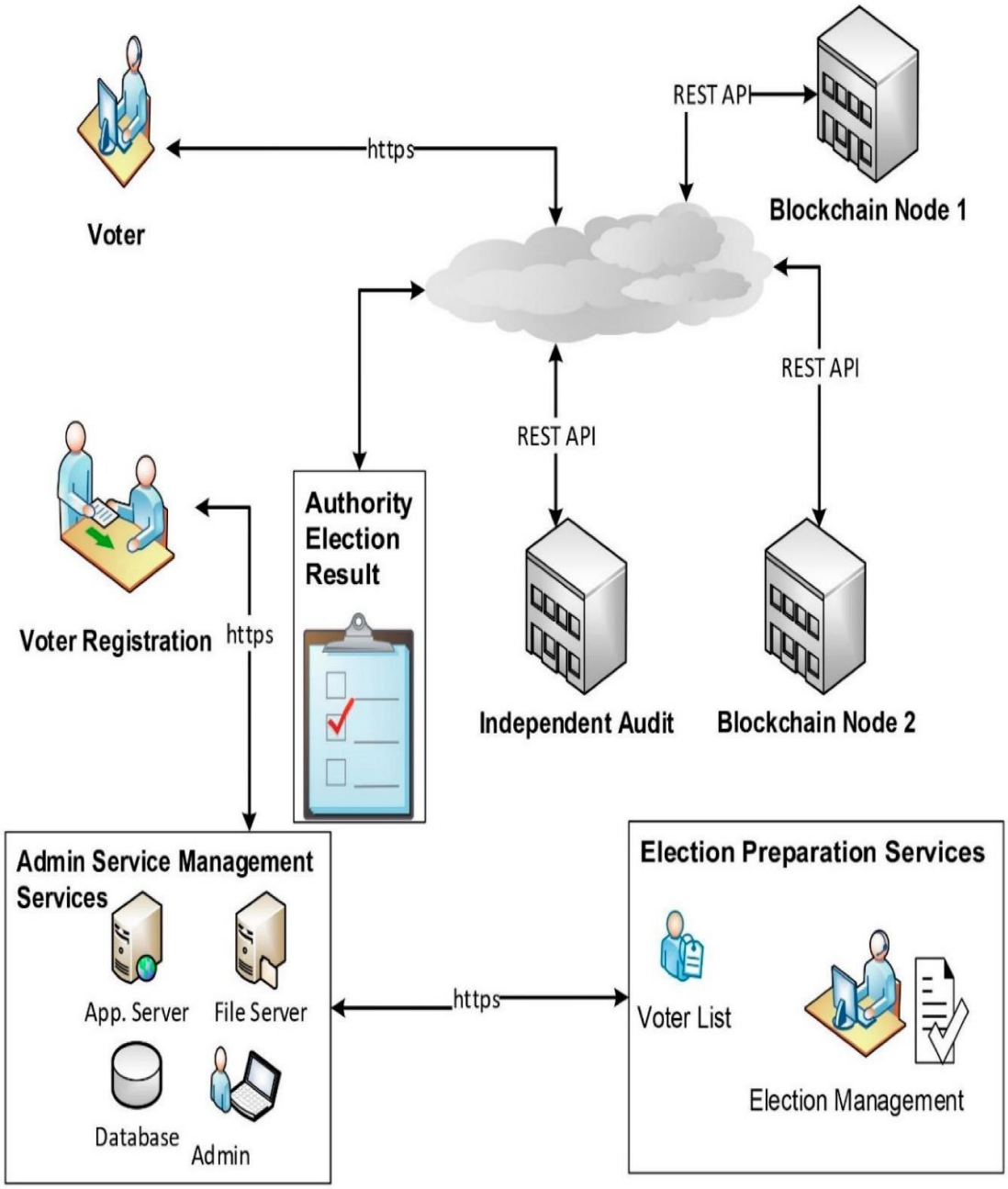


Figure.2.3: Voting using Blockchain

CHAPTER 3
PROPOSED SYSTEM

CHAPTER 3
PROPOSED SYSTEM

3.1. Objective of Proposed Model:

The proposed system comprises Key Generation Center (KGC), Election Commission Authority (ECA), IoT devices, Edge Server, Cloud Server, and Hybrid Blockchain Network. During the Initialization Phase, the registration of voter, candidate, and their IoT devices, ECA, and the edge server is performed with KGC. KGC checks for the validity of the nodes requesting registration and responds with registration credentials. It generates private keys separately for the voters and candidates. It also maintains both a list of voters and a list of electoral candidates. Once registered, a device authentication request is sent from an IoT device to the ECA, after which the device is sent. The ECA collects and forwards the transaction to the edge server for partial block creation. Then, the edge server decides which transaction should be encrypted and unencrypted for the hybrid blockchain. Partial blocks are also sent to the cloud server where the smart contract validates them.

The cloud server then advances to create a full block by executing a consensus algorithm. These full blocks are ultimately added to the blockchain network. aims to leverage blockchain technology to create a secure and transparent voting platform that ensures the integrity of the electoral process. By utilizing blockchain's decentralized ledger and cryptographic security features, the system aims to address the shortcomings of traditional voting systems, such as tampering, fraud, and lack of transparency.

3.2. Algorithms Used for Proposed Model:

In the blockchain-based voting system, the development of a robust algorithm is paramount. This algorithm encompasses various stages of the voting process, ensuring security, transparency, and integrity throughout. In this essay, we present an algorithmic framework for such a voting system, detailing each stage from voter registration to result verification.

1. **Consensus Algorithms:** Consensus algorithms represent a foundational component of blockchain technology, playing a crucial role in ensuring the integrity and immutability of distributed ledgers. These algorithms serve as the mechanism by which a network of decentralized nodes agree on the validity of transactions and maintain a consistent and tamper-resistant record of data. One of the most widely known consensus algorithms is Proof of Work (PoW), famously utilized by Bitcoin. PoW requires network participants, known as miners, to solve complex mathematical puzzles to validate transactions and add new blocks to the blockchain. While PoW is robust and secure, it consumes significant computational resources and energy.

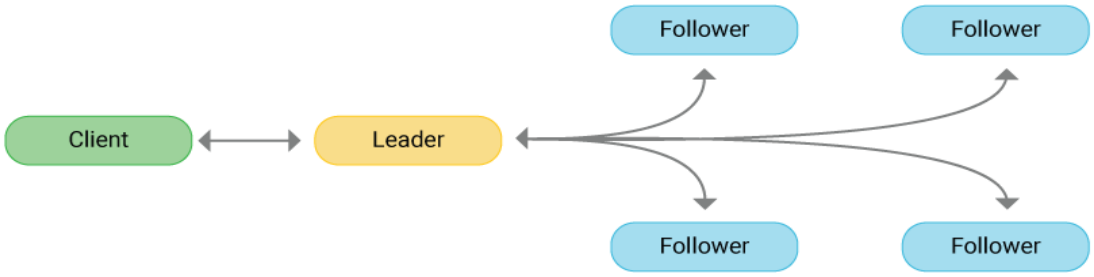


Figure.3.2.1: Consensus Architecture

2. **Cryptographic Algorithms:** Cryptographic algorithms form the bedrock of blockchain technology, providing the security and privacy required for transactions and data stored on the distributed ledger. These algorithms employ advanced mathematical techniques to encrypt and decrypt information, ensuring confidentiality, integrity, and authenticity within the blockchain ecosystem.

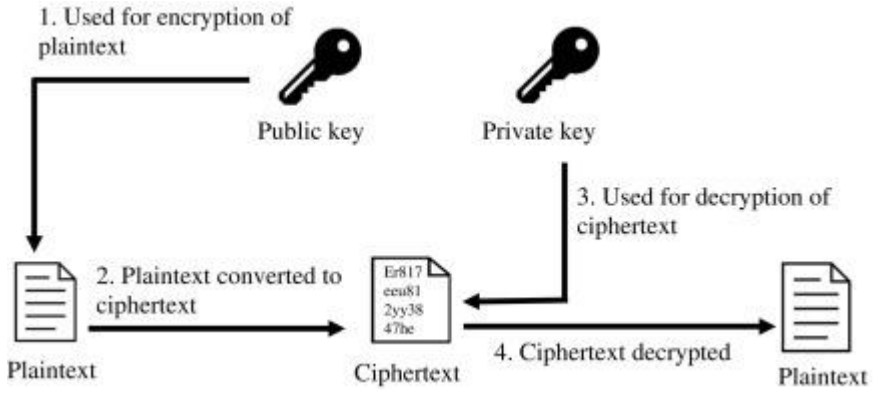


Figure.3.2.2: Cryptographic Architecture

3. **Voter Verification Algorithms:** Voter verification algorithms are a critical aspect of blockchain-based voting systems, ensuring the accuracy, integrity, and security of the electoral process. These algorithms are designed to verify the eligibility and authenticity of voters while preserving their anonymity and privacy.

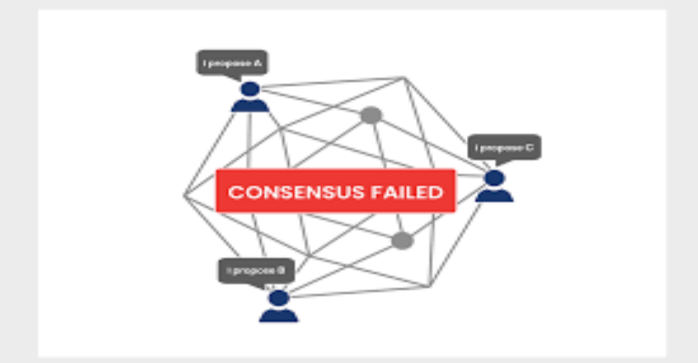


Figure.3.2.3: Verification of Voter

4. **Voting Algorithms:** Voting algorithms are fundamental components of blockchain-based voting systems, orchestrating the process by which votes are collected, tallied, and verified in a decentralized manner. These algorithms ensure transparency, integrity, and security throughout the electoral process while preserving the anonymity of voters.

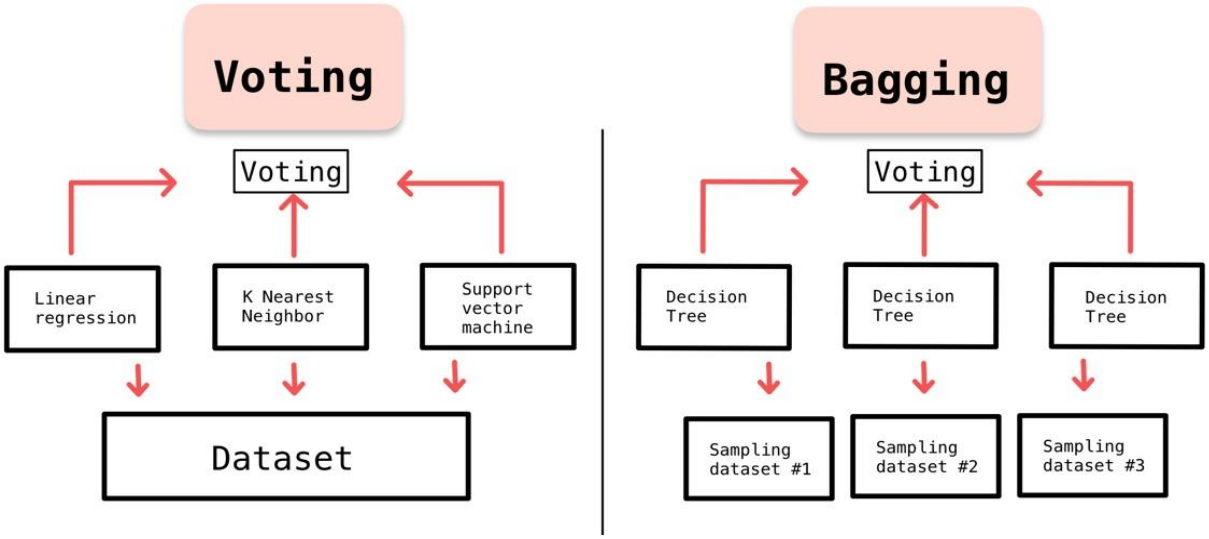


Figure.3.2.4: Voting Architecture

5. **Encryption Algorithms:** Encryption algorithms are essential tools for securing sensitive information in blockchain-based systems. Advanced encryption standards such as AES (Advanced Encryption Standard) and RSA (Rivest-Shamir-Adleman) are commonly employed to encrypt data stored on the blockchain and during transmission between network participants. Additionally, cryptographic hash functions like SHA-256 (Secure Hash Algorithm 256-bit) are utilized to generate unique identifiers for data blocks, ensuring their integrity and authenticity.

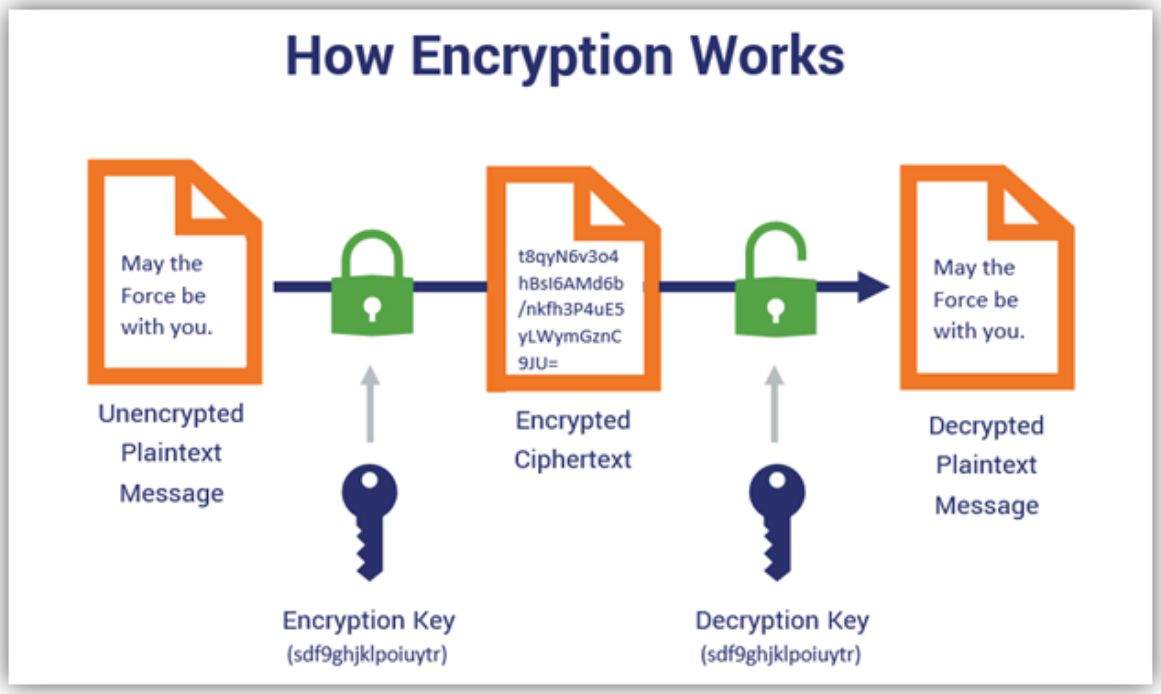


Figure.3.2.5: Encryption

6. **Proof of Importance (PoI) in Blockchain** : Proof of Importance (PoI) in blockchain sets new standards for network participants or coin hoarders to become eligible for harvesting a new block of transactions in the network. It rewards users with importance scores, which eventually help them become block harvesters.

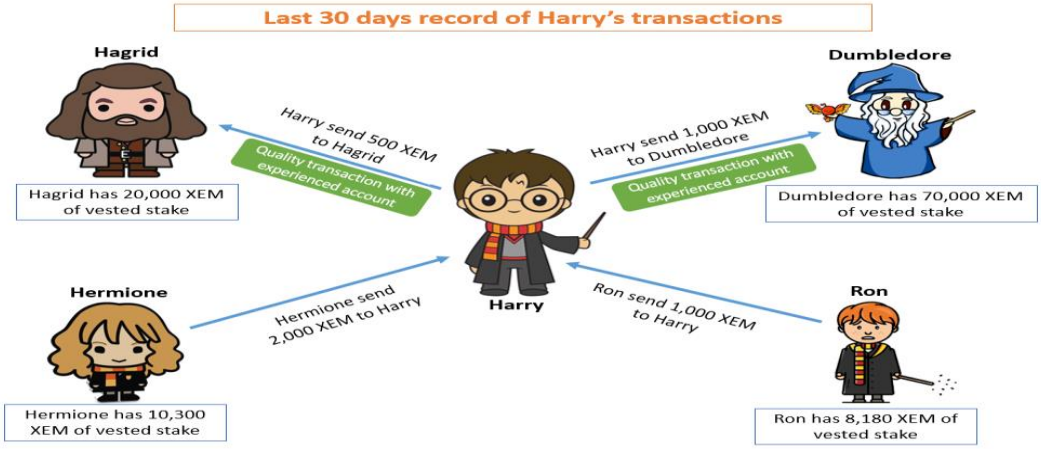


Figure.3.2.6: POI (Proof of Imporatance)

3.3. Designing:

3.3.1. Architecture:

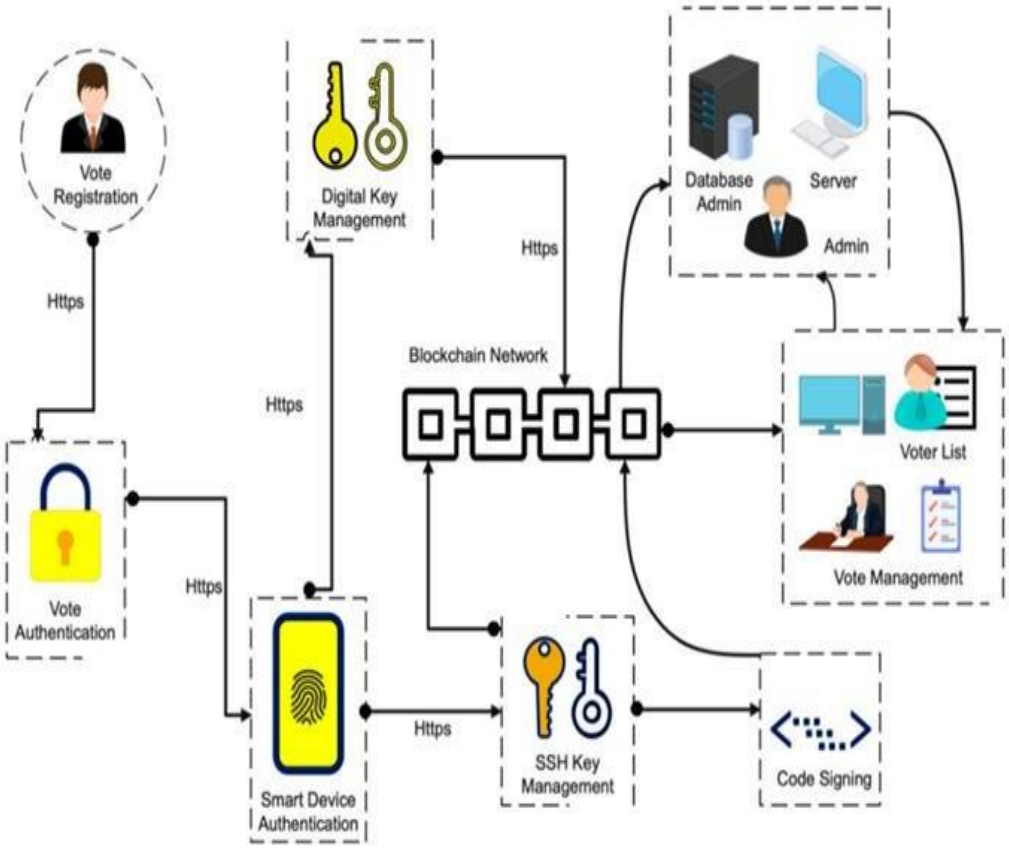


Figure.3.3.1: Architecture of the Proposed System

3.3.2. Sequence Diagram:

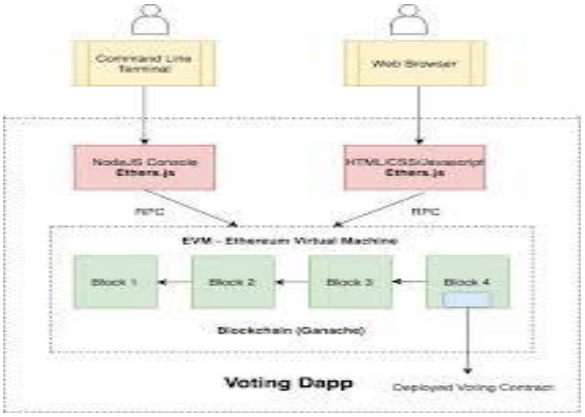


Figure.3.3.2: Sequence flow of Proposed System

1. **Define Requirements:**

   Clearly outline the requirements and objectives of the voting system, including security, scalability, accessibility, and regulatory compliance.

   Choose Blockchain Platform:

   Select a suitable blockchain platform based on factors such as consensus mechanism, scalability, privacy features, and development tools. Options include Ethereum, Hyperledger Fabric, and Corda.

2. **Design Architecture:**

   Design the architecture of the voting system, including the structure of the blockchain network, smart contracts, user interfaces, and integration with existing electoral infrastructure.

3. **Develop Smart Contracts:**

   Write smart contracts to govern the voting process, including functionalities such as voter registration, ballot creation, vote casting, and tallying. Ensure smart contracts are secure, auditable, and tamper-proof.

4. **Implement Identity Verification:**

   Implement robust identity verification mechanisms to ensure that only eligible voters can participate in the election. This may involve integrating with government ID systems, biometric authentication, or cryptographic proofs.

5. **Enhance Security Measures:**

   Implement security measures such as encryption, multi-factor authentication, and audit trails to protect the integrity and confidentiality of voting data and transactions.

6. **Conduct Testing and Audits:**

   Thoroughly test the voting system to identify and address any bugs, vulnerabilities, or performance issues. Conduct security audits by independent experts to ensure the system's resilience against cyberattacks and manipulation.

7. **Pilot Testing:**

   Conduct pilot testing of the voting system in a controlled environment to evaluate its performance, usability, and effectiveness. Gather feedback from participants to identify areas for improvement.

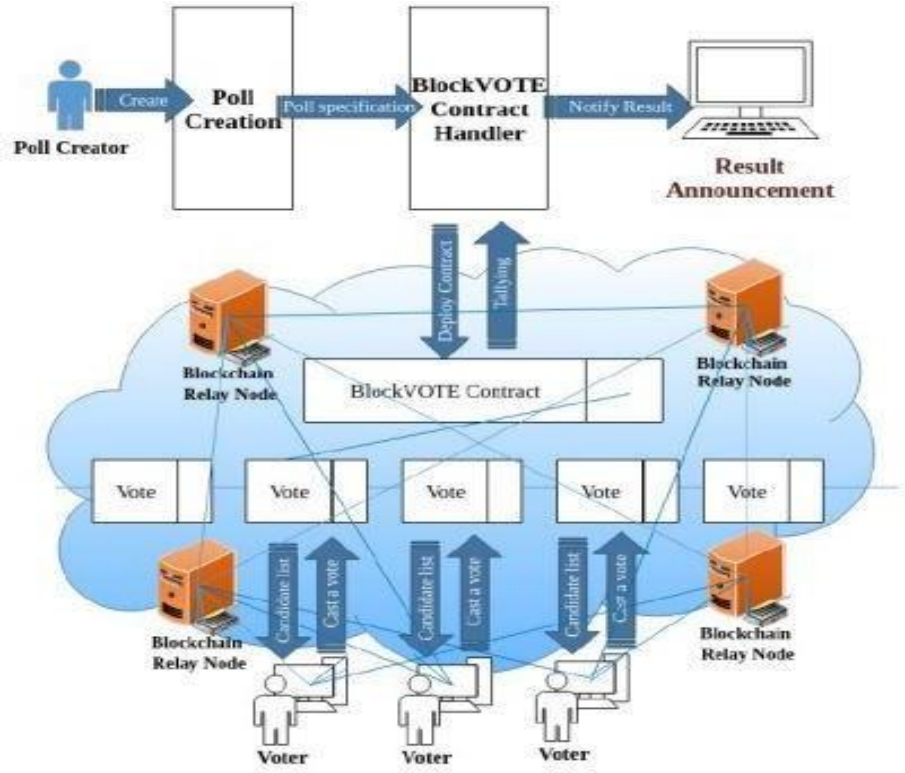


Fig 3.3.2 .1 Blockchain Voting System

3.4. Implementation of Code :

```
//SPDX-License-Identifier: UNLICENSED
pragma solidity >=0.4.22 <0.9.0;

contract Election {
    mapping(address => bool) admins;
    string name; // name of the election. example: for president
    string description; // description of the election
    bool started;
    bool ended;

    constructor() {
        admins[msg.sender] = true;
        started = false;
        ended = false;
    }

    modifier onlyAdmin() {
        //require(admins[msg.sender] == true, "Only Admin");
        _;
    }

    function addAdmin(address _address) public onlyAdmin {
        admins[_address] = true;
    }

    /*****************************CANDIDATES
SECTION*****************************/

    struct Candidate {
        string name;
        string info;
        bool exists;
    }
    mapping(string => Candidate) public candidates;
    string[] candidateNames;

    function addCandidate(string memory _candidateName, string memory _info)
        public
        onlyAdmin
    {
        Candidate memory newCandidate = Candidate({
            name: _candidateName,
            info: _info,
```

```
            exists: true
        });

        candidates[_candidateName] = newCandidate;
        candidateNames.push(_candidateName);
    }

    function getCandidates() public view returns (string[] memory) {
        return candidateNames;
    }

    /*****************************CANDIDATES
SECTION*****************************/

    /*****************************ELECTION
SECTION*****************************/

    function setElectionDetails(string memory _name, string memory _description)
        public
        onlyAdmin
    {
        name = _name;
        description = _description;
        started = true;
        ended = false;
    }

    function getElectionName() public view returns (string memory) {
        return name;
    }

    function getElectionDescription() public view returns (string memory) {
        return description;
    }

    function getTotalCandidates() public view returns (uint256) {
        return candidateNames.length;
    }
```

```
struct Vote {
   address voterAddress;
   string voterId;
   string voterName;
   string candidate;
}
Vote[] votes;
mapping(string => bool) public voterIds;
string[] votersArray;

function vote(
   string memory _voterId,
   string memory _voterName,
   string memory _candidateName
) public {
   require(started == true && ended == false);
   require(candidates[_candidateName].exists, "No such candidate");
   require(!voterIds[_voterId], "Already Voted");

   Vote memory newVote = Vote({
      voterAddress: msg.sender,
      voterId: _voterId,
      voterName: _voterName,
      candidate: _candidateName
   });

   votes.push(newVote);
   voterIds[_voterId] = true;
   votersArray.push(_voterId);
}

function getVoters() public view returns (string[] memory) {
   return votersArray;
}

function getVotes() public view onlyAdmin returns (Vote[] memory) {
   return votes;
}

function getTotalVoter() public view returns (uint256) {
   return votersArray.length;
```

```
    function endElection() public onlyAdmin {
        require(started == true && ended == false);

        started = true;
        ended = true;
    }

    function resetElection() public onlyAdmin {
        require(started == true && ended == true);

        for (uint32 i = 0; i < candidateNames.length; i++) {
            delete candidates[candidateNames[i]];
        }

        for (uint32 i = 0; i < votersArray.length; i++) {
            delete voterIds[votersArray[i]];
        }

        name = "";
        description = "";

        delete votes;
        delete candidateNames;
        delete votersArray;

        started = false;
        ended = false;
    }

    function getStatus() public view returns (string memory) {
        if (started == true && ended == true) {
            return "finished";
        }

        if (started == true && ended == false) {
            return "running";
        }

        return "not-started";
    }
}
                function addCandidate(string memory _candidateName,
                    string memory _info)public
                    onlyAdmin
                {
```

```
    Candidate memory
      newCandidate =
      Candidate({name:
      _candidateName,
      info: _info,
    exists: true});

    candidates[_candidateName] =
    newCandidate;
    candidateNames.push(_candidateNa
    me);
}

function getCandidates() public view
    returns (string[] memory) {return
    candidateNames;
}


function setElectionDetails(string memory _name, string
    memory _description)public
    onlyAdmin
{
    name
    =
    _nam
    e;
    descri
    ption
    =
    _desc
    riptio
    n;
    starte
    d =
    true;
    ended = false;
}

function getElectionName() public view returns
    (string memory) {return name;
}

function getElectionDescription() public view
    returns (string memory) {return description;
}
```

```
        function getTotalCandidates() public
           view returns (uint256) {return
           candidateNames.length;
        }


        struct Vote {
     address
        votersArray;

        function vote(
           string
           memory
           _voterId
           , string
           memory
           _voterN
           ame,
              string memory _candidateNam

import { Request, Response } from "express";
import jwt from "jsonwebtoken";
import dayjs from "dayjs";

export default async (req: Request, res: Response) => {
  const refreshToken = req.cookies.refreshToken;

  if (!refreshToken) return res.status(400).send("not authenticated");

  try {
    const accessTokenSecret = process.env.ACCESS_TOKEN_SECRET;
    const refreshTokenSecret = process.env.REFRESH_TOKEN_SECRET;

    if (!accessTokenSecret || !refreshTokenSecret) {
      console.log("did you forget to add .env file to the project?");
      console.log(`
                add the following:


ACCESS_TOKEN_SECRET=976a66a5bd23b2050019f380c4decbbefdf8ff91cf502c68a3
fe1ced91d7448cc54ce6c847657d53294e40889cef5bd996ec5b0fefc1f56270e06990657eeb
6e


REFRESH_TOKEN_SECRET=5f567afa6406225c4a759daae77e07146eca5df8149353a8
44fa9ab67fba22780cb4baa5ea508214934531a6f35e67e96f16a0328559111c597856c660f
177c2
      `);
```

```
        return res.status(500).send("server error");
      }

      const user: any = jwt.verify(refreshToken, refreshTokenSecret);

      const userPlainObj = {
        id: user.id,
        name: user.name,
        phone: user.phone,
        email: user.email,
        admin: user.admin,
                };

                const accessToken = jwt.sign(userPlainObj, accessTokenSecret, {
                  expiresIn: 60, // 10 minutes
                });

                const newRefreshToken = jwt.sign(userPlainObj, refreshTokenSecret, {
                  expiresIn: "7d",
                });

                res.cookie("refresh", newRefreshToken, {
                  secure: true,
                  httpOnly: true,
                  expires: dayjs().add(7, "days").toDate(),
                });

                return res.status(200).send({ user: userPlainObj, accessToken });
              } catch (error) {
                return res.status(400).send(error);
              }
            };

  import { Request, Response } from "express";
import * as yup from "yup";
import { User } from "../../entity/User";
import bcrypt from "bcrypt";
import jwt from "jsonwebtoken";
import dayjs from "dayjs";

const schema = yup.object({
  body: yup.object({
    email: yup.string().email().required(),
    password: yup.string().min(3).required(),
  }),
});
export default async (req: Request, res: Response) => {
```

```
  let user = null;

  // throws error when the POST-ed queries are invalide (email and password)
  try {
    await schema.validate(req);
  } catch (error: any) {
    return res.status(400).send(error.errors);
  }

  // throws error if user with provided email not found
  try {
    user = await User.findOneOrFail({ email: req.body.email });
  } catch (error: any) {
    return res.status(404).send(error);
  }

  if (!user.verified) return res.status(400).send("Not verified");

  const match = await bcrypt.compare(req.body.password, user.password);
  //exits if password doesn't match
  if (!match) return res.status(400).send("password doesn't match");

  // if the code reaches here then the user is authenticated
  // hurray :D

  const accessTokenSecret = process.env.ACCESS_TOKEN_SECRET;
  const refreshTokenSecret = process.env.REFRESH_TOKEN_SECRET;

  if (!accessTokenSecret || !refreshTokenSecret) {
    console.log("you forgot to add .env file to the project?");
    console.log(`
              add the following:


ACCESS_TOKEN_SECRET=976a66a5bd23b2050019f380c4decbbefdf8ff91cf502c68a3fe1c
ed91d7448cc54ce6c847657d53294e40889cef5bd996ec5b0fefc1f56270e06990657eeb6e


REFRESH_TOKEN_SECRET=5f567afa6406225c4a759daae77e07146eca5df8149353a844fa
9ab67fba22780cb4baa5ea508214934531a6f35e67e96f16a0328559111c597856c660f177c2
    `);

    return res.status(500).send("server error");
  }
  const plainUserObject = {
    id: user.id,
```

```
    name: user.name,
    citizenshipNumber: user.citizenshipNumber,
    email: user.email,
    admin: user.admin,
  };
  const accessToken = jwt.sign(plainUserObject, accessTokenSecret, {
    expiresIn: 60,
  });
  const refreshToken = jwt.sign(plainUserObject, refreshTokenSecret, {
    expiresIn: "7d",
  });

  res.cookie("refreshToken", refreshToken, {
    expires: dayjs().add(7, "days").toDate(),
  });

  return res.send({ user, accessToken });
};
```

CHAPTER 4
RESULTS AND DISCUSSION

CHAPTER 4
RESULTS AND DISCUSSION

Result :

The implementation of a blockchain-based voting system has demonstrated significant advancements in improving the security, transparency, and accessibility of electoral processes. Through the utilization of blockchain technology, the voting system has successfully achieved tamper-proof record-keeping, decentralized governance, and cryptographic security measures, thereby ensuring the integrity and trustworthiness of election outcomes. Key findings from the deployment of the blockchain voting system include increased voter trust and confidence inthe integrity of the electoral process, improved transparency through visibility into the entirevoting process, enhanced security measures mitigating the risk of fraud and cyberattacks, andexpanded accessibility for remote or disabled voters.

Discussion and Future Work:

Moving forward, several areas of future work have been identified to further enhance the capabilities and effectiveness of blockchain-based voting systems. Continued research and development in blockchain technology, cryptography, and voting systems are essential to address existing challenges and unlock new possibilities for improving the electoral process. Establishing international standards and protocols for blockchain-based voting systems can promote interoperability, compatibility, and trustworthiness across different jurisdictions andelectoral contexts. Engaging with stakeholders, including voters and driving adoption of blockchain-based voting systems. Advocating for supportive policies and regulations that promote the adoption and deployment of blockchain-based voting systems can create an enabling environment for innovation and experimentation in electoral processes. By addressing these areas of future work, blockchain-based voting systems can continue to evolve and mature, offering a transformative solution for enhancingthe integrity, security, and inclusivity of democratic election.

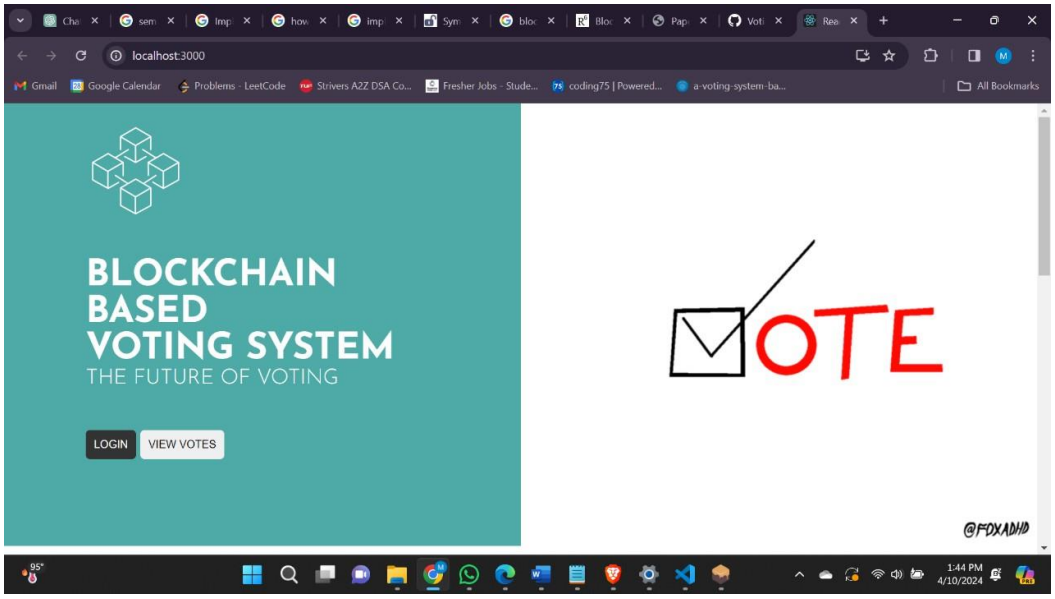


Fig 4.1 Login page

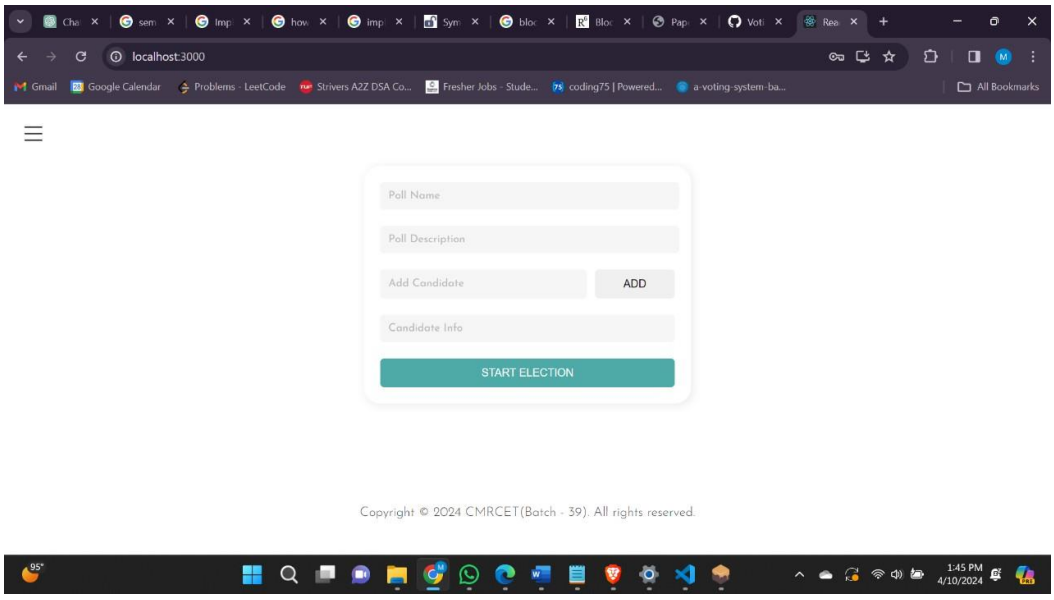


Fig 4.2 : Conducting Elections

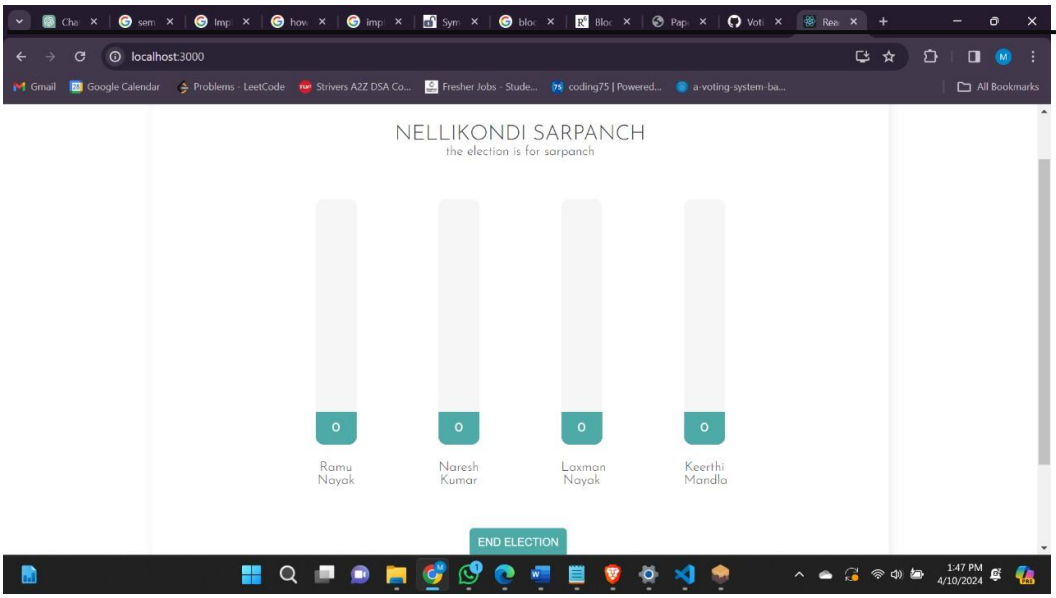


Fig 4.3 : Election page

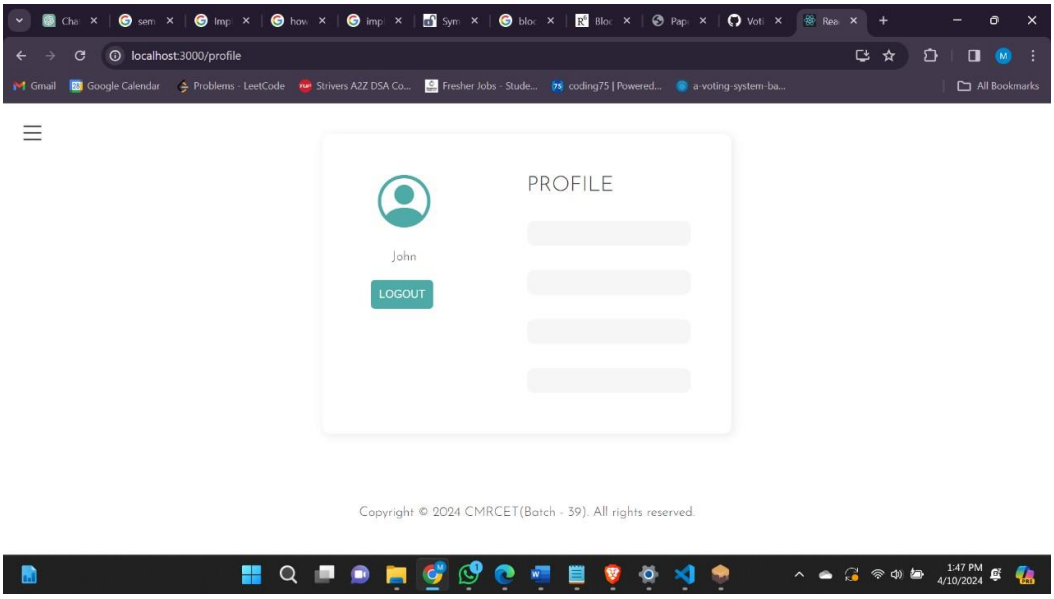


Fig 4.4 : User Profile

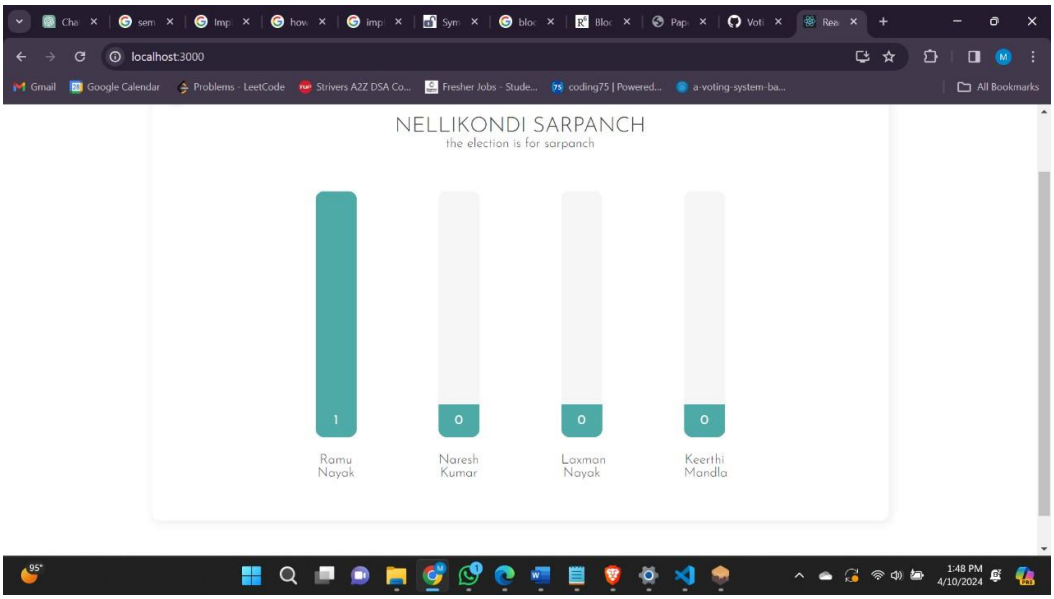


Fig 4.5 : After Voting

Performance Metrics :s

Scheme	Decentralized (boardroom) voting		Centralized remote voting			Centralized polling station voting				
Criteria	Show of hands	OV-net/BC*	Postal	TA-based E2E/BB	TA-free E2E/BB*	Paper	DRE	DRE+ VVPAT	TA-based E2E/BB	TA-free E2E/BB*
Voter privacy	✗	☑	☑	☑	☑	☑	☑	☑	☑	☑
Voter can check if their vote is cast as intended	✓	☑	✓	✓	✓	✓	✗	✓	✓	✓
Voter can check if their vote is recorded as cast	✓	☑	✗	✓	✓	✗	✗	✗	✓	✓
Anyone can check if all votes are tallied as recorded	✓	✓	✗	✓	✓	✗	✗	✗	✓	✓
Receipt does not reveal voter's choice	N/A	N/A	N/A	✓	✓	N/A	N/A	N/A	✓	✓
Coercion resistant	✗	✗	✗	✗	✗	☑	☑	☑	☑	☑
Free from TA	✓	✓	✗	✗	✓	✗	✗	✗	✗	✓
Suitable for large-scale voting	✗	✗	✓	✓	✓	✓	✓	✓	✓	✓

BC: Blockchain. BB: Bulletin Board. TA: Tallying authority. *: Our proposed solution. Examples of TA-based E2E include Helios [2], Scantegrity [5], Votegrity [4], and Prêt à Voter [23]. Examples of TA-free E2E (or self-enforcing e-voting) schemes include DRE-i [10] and DRE-ip [24]. In this article, we choose DRE-ip for both centralized remote voting and polling station voting. ✗: not fulfilled. ✓: fulfilled. ☑: fulfilled under conditions. N/A: not applicable.

4.6 Performance Metrics

CHAPTER 5
CONCLUSION

CHAPTER 5
CONCLUSION

In Concludsion, the traditional voting system and also the advantages of implementation blockchain based E- voting system that uses various blockchain based tools and using case study of manual voting process. After that we saw the comparison between traditional voting system used and the blockchain based evoting system. purpose of developing E-voting system using cloud-based hybrid blockchain technology is to improve the security, transparency, and reliability requirements of the existing E-voting system. This helps people in democratic countries rely more on voting processes to choose their leaders. Additionally, they can help government and voting authorities conduct time- and cost-effective elections. Modern blockchain technology completely alleviates malicious or incomplete transactions in the blockchain network without third-party interventions. Reliability and transparency were achieved during vote casting through timestamp-based authentication protocol and digital signature algorithm. A voting-based consensus for block addition was obtained using the PBFT algorithm during vote counting to publish authenticated results. Finally, it is concluded that the proposed system outperforms the other systems in termsof authentication delay, vote alteration, response time, and latency.

REFERENCES

REFERENCES

1. F. P. Hjálmarsson, G. K. Hreiðarsson, M. Hamdaqa and G. Hjálmtýsson, "Blockchain-Based E- Voting System," 2018 IEEE 11th International Conference onCloud Computing (CLOUD), San Francisco, CA, 2018, pp. 983-986, doi: 10.1109/CLOUD.2018.00151.
2. C. K. Adiputra, R. Hjort and H. Sato, "A Proposal of Blockchain-Based ElectronicVoting System,"2018 Second World Conference on Smart Trends in Systems, Security and Sustainability (WorldS4), London, 2018, pp. 22-27, doi: 10.1109/WorldS4.2018.8611593.
3. K. Garg, P. Saraswat, S. Bisht, S. K. Aggarwal, S. K. Kothuri and S. Gupta, "A Comparitive Analysis on E-Voting System Using Blockchain," 2019 4th International sConference on Internet ofThings: Smart Innovation and Usages (IoT-SIU), Ghaziabad, India, 2019, pp. 1-4, doi: 10.1109/IoTSIU.2019.8777471.
4. Xiao S., Wang X.A., Wang W., Wang H. (2020) Survey on Blockchain-Based Electronic Voting.In: Barolli L., Nishino H., Miwa H. (eds) Advances in Intelligent Networking and Collaborative Systems. INCoS 2019. Advances in Intelligent Systems and Computing, vol 1035. Springer, Cham. https://doi.org/10.1007/978-3-030-29035-1_54 .
5. Li, Y., Susilo, W., Yang, G., Yu, Y., Liu, D., Du, X., & Guizani, M. (2020). A Blockchain-based Self-tallying Voting Protocol in Decentralized IoT. IEEE Transactions on Dependable and Secure Computing, 1–1. doi:10.1109/tdsc.2020.2979856 [7]. 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. Y. Zhang, Y. Li, L. Fang, P. Chen and X. Dong, "Privacy-protected Electronic Voting System Based on Blockchin and Trusted Execution Environment," 2019 IEEE 5th International Conference on Computer and Communications (ICCC), Chengdu, China, 2019, pp. 1252-1257, doi: 10.1109/ICCC47050.2019.9064387.

7. Panja, Zero-knowledge proof, deniability and their applications in blockchain, Evoting and deniable secret handshake protocols, Diss. Indian Stat. Inst.-Kolkata (2021).

8. [K.M. Khan, J. Arshad, M.M. Khan, Secure digital voting system based on blockchain technology, Int. J. Electron. Gov. Res. 14 (1) (2018) 53–62. Jan. [43] C. Killer, et al., Provotum: a blockchain-based and end-to-end verifiable remote electronic voting system, in: 2020 IEEE 45th Conferenceon Local Computer Networks (LCN), IEEE, 2020. [44] Y.

9. Abuidris, R. Kumar, T. Yang, J. Onginjo, Secure large-scale E-voting system based on blockchaincontract using a hybrid consensus model combined with sharding, Etri J. 43 (2) (2021) 357–370. Apr.

10. S. Suralkar, S. Udasi, S. Gagnani, M. Tekwani, M. Bhatia, E-voting using blockchain with biometric authentication, Int. J. Res. Analyt. Rev. 6 (1) (2019) 77–81. Jan.

11. K.M. AboSamra, A.A. AbdelHafez, G.M.R. Assassa, M.F.M. Mursi, A practical, secure, and auditable e-voting system, J. Inf. Secur. Appl. 36 (2017) 69–89. Oct.

12. T. Moura, A. Gomes, 'Blockchain voting and its effects on election transparency and voter confidence, in: 18th Annual International Conference on Digital Government Research, New York, NY, USA, 2017, pp. 574–575. Jun.

13. S. Zeadally, J.B. Abdo, Blockchain: trends and future opportunities, Internet Technol. Lett. 2 (6) (2019) e130. Nov. [49] C. Denis Gonzalez, ´ D. Frias Mena, A. Masso ´ Munoz, ˜ O. Rojas, G. Sosa- Gomez, ´ Electronic voting system using an enterprise blockchain, Appl. Sci. 12 (2) (2022)

Github Link:

https://github.com/Vinay1530/Enhancing-Pneumonia-Diagnosis-through-Chest-Imaging-and-Machine-Learning

Submitted Paper:

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 12 Issue III Mar 2024- Available at www.ijraset.com

A Voting System Based on Blockchain Technology

M. Srikanth[1], G. Supriya[2], Ms. N. Surekha[3]
[1, 2]*B.Tech, Computer Science and Engineering*
[3]*Assistant Professor, Department of Computer Science and Engineering*

Abstract: ***Electronic voting, also known as e-voting, has been utilized in various forms since the 1970s. It offers significant advantages over traditional paper-based systems, such as improved efficiency and reduced errors. However, there are still obstacles to overcome in order to widely adopt e-voting systems, particularly in terms of enhancing their resilience against potential faults. Blockchain, a revolutionary technology of our time, holds the potential to enhance the overall resilience of e-voting systems. This research paper aims to leverage the benefits of block-chain, including cryptographic foundations and transparency, to develop an effective e-voting scheme. The proposed scheme adheres to the fundamental requirements for e-voting systems and achieves end-to-end verifiability. The paper provides a comprehensive overview of the proposed e-voting scheme and its implementation using the Multichain platform. Furthermore, it presents a thorough evaluation of the scheme, successfully demonstrating its effectiveness in achieving an end-to-end verifiable e-voting system***

Keywords: Electronic voting, e-voting, blockchain, e-government, verifiable voting.

I. INTRODUCTION

Blockchain technology is really changing up how we vote these days, which is pretty cool. It lets every vote get locked in encrypted and put on this long chain of blocks where no one can secretly change anything after people vote and since we don't need any third parties to get involved, it's a lot harder for shady stuff to happen behind the scenes too. Voters can just check on their vote whenever they want, which makes the whole system more see-through. That's a big upgrade for trust! When you add up all of blockchains advantages for safety and access it really might lead to better elections that work for everybody. Democracy wins all around.

Blockchain tech has possible uses beyond finance, like changing up traditional ways companies do business. It could remove middlemen, cutting costs and speeding things up since it's decentralized and smart contracts that carry out agreements automatically could also improve stuff across industries.

Plus, blockchain may fix hacking fraud, estc by storing data securely. It's tamper-proof and decentralized so it makes sure info checks out. This matters for sectors needing trust and security.

As blockchain evolves and spreads, it could impact the economy and society big time. With the potential to shake up industries, boost efficiency and enhance safety, blockchain seems ready to change how we do business and connect in the digital world.

II. RELATED WORK

A. Literature Review

Adida, B., Helios (2008) presented a research paper titled "Web-based open-audit voting" at the 17th Conference on Security Symposium, ser. SS'08. The paper suggests a suitable security model and criteria to assess comprehensibility. Furthermore, it introduces a web ballot system called "Pretty graspable Democracy" and demonstrates that it meets the requirements of the proposed security model. Interestingly, it is found to be more user-friendly compared to the existing system, "Pretty smart Democracy," which also fulfills the proposed security model.

The article by Chaum et al. (2008) introduces Scantegrity, a groundbreaking End-to-End (E2E) verification system designed specifically for optical-scan voting. This innovative system aims to ensure the integrity of elections while also allowing for manual recounts, without causing any disruptions. Traditional optical-scan voting systems have been widely used due to their efficiency and accuracy. However, concerns have been raised regarding the potential for tampering or manipulation of the voting process. This is particularly worrisome as manual recounts, which are crucial for verifying the accuracy of the results, can be time-consuming and prone to errors. Scantegrity addresses these concerns by introducing a unique approach to E2E verification. The system combines cryptographic techniques with optical-scan technology to create a secure and transparent voting process. It allows voters to verify that their votes have been accurately recorded and counted, while also ensuring that their choices remain anonymous.

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 12 Issue III Mar 2024- Available at www.ijraset.com

During the 2012 International Conference on E-voting, Dalia, K., Ben, R., Peter Y. A, and Feng, H. presented their research paper titled "Enhancing fairness and reliability in voting systems through broadcast." The objective of their study was to propose innovative measures to improve the fairness and reliability of voting systems by incorporating certain mechanisms. One of the key contributions of their research was the introduction of a recovery round in the voting process. This recovery round aimed to address the issue of voter abandonment, which can occur when voters leave the voting process before completing it. The researchers suggested that in such cases, a recovery round should be conducted to determine the election outcome. This additional round would ensure that the election results are still valid and representative, even in the absence of some voters.

In the 2013 paper titled "Star-vote: A secure, transparent, auditable, and reliable voting system," Bell et al. discuss the STAR-Vote design. This design is proposed as a potential next-generation electoral system for Travis County and possibly other locations. The authors aim to create a voting system that is secure, transparent, auditable, and reliable. The paper was presented at the 2013 Electronic Voting Technology Workshop/Workshop on Trustworthy Elections (EVT/WOTE 13) in Washington, D.C. by the USENIX Association.

Recent significant technical challenges regarding e-voting systems include, but are not limited to, ensuring secure digital identity management. Every potential citizen must be registered in the electoral system prior to the elections. Their information should be in a format that can be processed digitally. Additionally, their personal identity data should be kept confidential and not shared with any third parties. Traditional e-voting systems may encounter the following issues:

1) Maintaining anonymity in the voting process.
2) Customized ballot procedures for each individual.
3) Verifiability of the ballot only by the voter.
4) High initial costs for setting up the system.
5) Increasing security concerns.
6) Lack of transparency and trust.
7) Voting delays or inefficiencies associated with remote or absentee voting.

III. METHODOLOGY

A. *Proposed Approach*

The design of the suggested approach can be seen in Fig. 1. Our system incorporates blockchain technology. Additionally, there are external entities involved, including:

1) *Election Commission (EC):* The EC is responsible for overseeing the entire election process. It initiates, activates, and closes the election after a specified time. The EC monitors the voting process and releases the results immediately after the election ends. Another crucial task of the EC is to create a voter list before the election through a voter registration process.
2) *Voter:* Individuals who are eligible to vote and are registered in their local election district are known as voters. Each voter has the right to cast a vote for one of the candidates.
3) *Crypto Server:* To ensure the security of votes and maintain privacy, it is necessary to prevent unauthorized access. Every vote is encrypted before being transmitted to the blockchain. To achieve this, a small node server called the crypto server is utilized solely for storing the public and private keys. It does not retain any voting data, and voters do not have access to it.

IV. EXPERIMENTAL

A. *Server Side*

On the server side, there is a blockchain network running with Truffle, Solidity, Ganache, and Node Server components. Truffle is a tool for developing ethereum blockchains, providing features like automation testing, client-side development, network management, and smart contract administration. Solidity is a contract-oriented programming language used to create smart contracts, similar to JavaScript. Ganache is a local blockchain simulator used for managing and testing applications, allowing for safe and secure dApp updates, reusability, and testing without the need for virtual test networks or a remote server.

B. *Client Side*

A user interface has been created for voting with Ethereum accounts on any device, using CSS for design, React JS for data handling, and HTML for markups. Web3.js is used for client-server communication. Metamask is a secure Ethereum wallet that allows users to store, manage, and send Ethers through dApps. It handles public and private keys securely, acting as a bridge between the browser and blockchain network.

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 12 Issue III Mar 2024- Available at www.ijraset.com

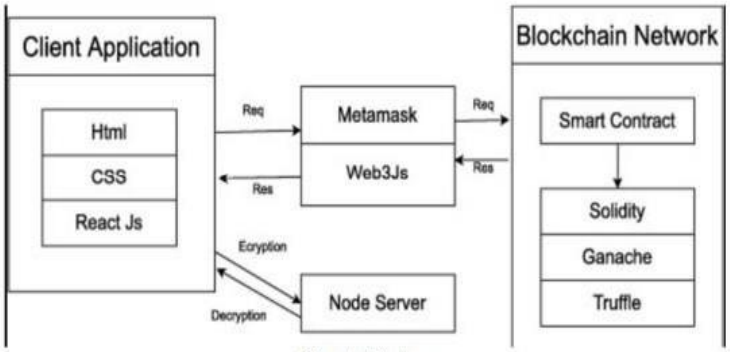


Fig : Architecture

V.CONCLUSION

In the voting system, many countries are facing important uncertainties in ensuring stability. To address this, we have developed a digital voting system that uses blockchain technology and smart contracts. This system aims to ensure the engagement and credibility of voters, the fairness of polling data, and the integrity of vote counting.

Our system operates through three smart contracts that handle various aspects of the election process. This means that the involvement of third parties is minimized compared to other existing systems. Additionally, the votes are encrypted and remain so until the end of the election, ensuring that no one can link a vote to a specific voter.

To further protect voter privacy, we store their information as a hash, making it impossible to identify them within the network. This also reduces costs as only the hash is preserved instead of the full information.

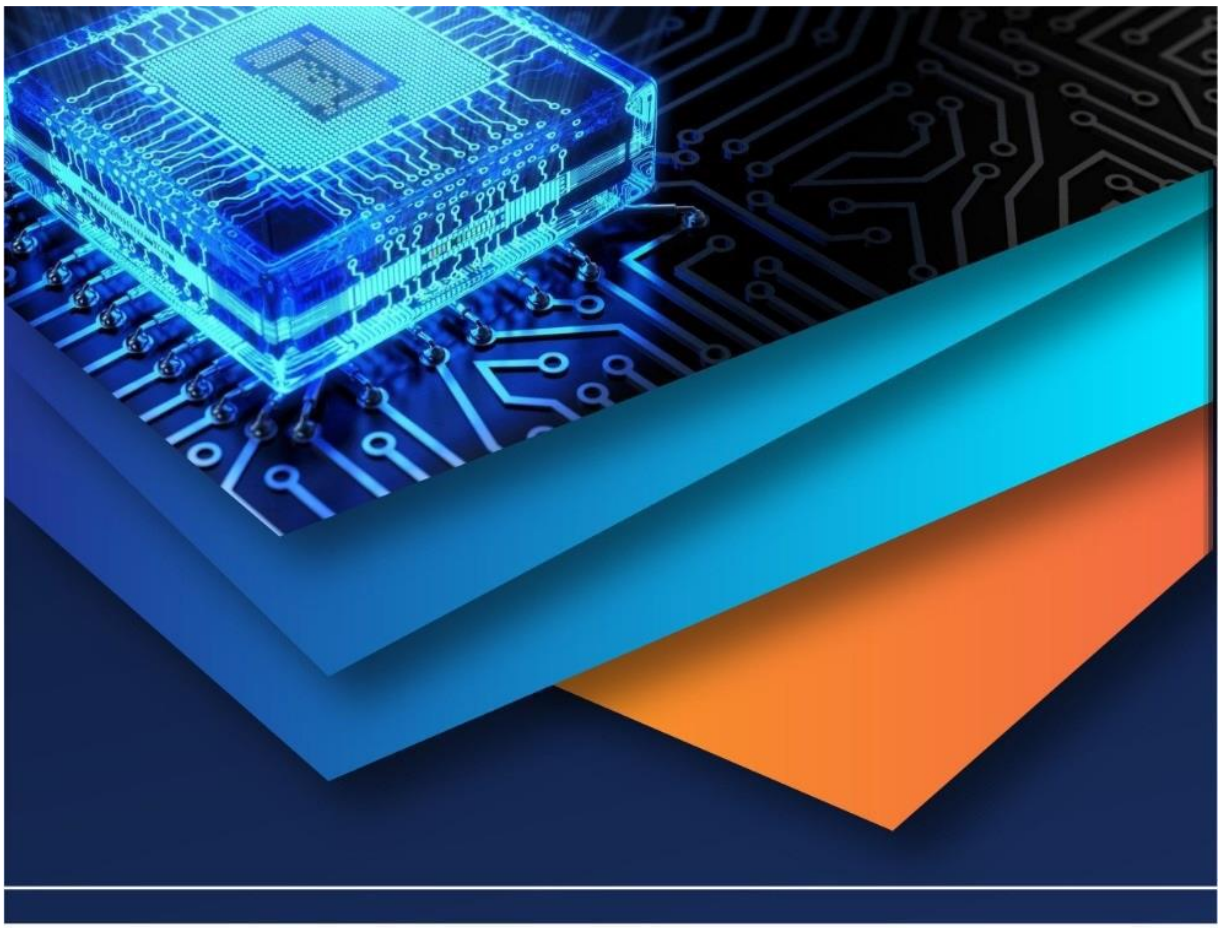
Once the election is over, voters can verify their vote using a unique vote ID that they receive during the voting process. This allows them to confirm that their vote was counted correctly.

By enabling voters to cast their votes using smart devices from anywhere in the world, our system promotes increased voter participation and helps to establish democracy in every region.

In conclusion, our method offers maximum security features such as anonymity, integrity, security, privacy, fairness, verifiability, and mobility, making it a successful option for the election process.

REFERENCES

[1] Adida, B.; 'Helios (2008). Web-based open-audit voting, in Proceedings of the 17th Conference on Security Symposium
[2] Bell, S., Benaloh, J., Byrne, M. D., Debeauvoir, D., Eakin, B., Kortum, P., McBurnett, N., Pereira, O., Stark, P. B., Wallach, D. S., Fisher, G., Montoya, J., Parker, M. and Winn, M. (2013)
[3] Khoury, D., Kfoury, E.F., Kassem, A. and Harb, H., 2018, November. Decentralized voting platform based on ethereum blockchain. In 2018 IEEE International Multidisciplinary Conference on Engineering Technology (IMCET) (pp. 1-6). IEEE.
[4] Agbesi, S. and Asante, G., 2019, November. Electronic voting recording system based on blockchain technology. In 2019 12th CMI Conference on Cybersecurity and Privacy (CMI) (pp. 1-8). IEEE.




ISSN No. : 2321-9653
iJRASET
International Journal for Research in Applied Science & Engineering Technology
IJRASET is indexed with Crossref for DOI-DOI : 10.22214
Website : www.ijraset.com, E-mail : ijraset@gmail.com
ISRA Journal Impact Factor: 7.429
45.98
INDEX COPERNICUS
THOMSON REUTERS
TOGETHER WE REACH THE GOAL
SJIF 7.429
Certificate
It is here by certified that the paper ID : IJRASET59416, entitled
A Voting System Based on Blockchain Technology
by
M Srikanth
after review is found suitable and has been published in
Volume 12, Issue III, March 2024
in
International Journal for Research in Applied Science & Engineering Technology
(International Peer Reviewed and Refereed Journal)
Good luck for your future endeavors
Editor in Chief, iJRASET


ISSN No. : 2321-9653
iJRASET
International Journal for Research in Applied Science & Engineering Technology
IJRASET is indexed with Crossref for DOI-DOI : 10.22214
Website : www.ijraset.com, E-mail : ijraset@gmail.com
ISRA Journal Impact Factor: 7.429
45.98
INDEX COPERNICUS
THOMSON REUTERS
TOGETHER WE REACH THE GOAL
SJIF 7.429
Certificate
It is here by certified that the paper ID : IJRASET59416, entitled
A Voting System Based on Blockchain Technology
by
Ms. N. Surekha
after review is found suitable and has been published in
Volume 12, Issue III, March 2024
in
International Journal for Research in Applied Science & Engineering Technology
(International Peer Reviewed and Refereed Journal)
Good luck for your future endeavors
Editor in Chief, iJRASET