

BLOCKCHAIN VOTING SYSTEM DEVELOP SECURE AND TRANSPARENT VOTING SYSTEM

Submitted in partial fulfillment of the requirements for the award of
Bachelor of Engineering degree in Computer Science and Engineering

By

B. Sai Krishna Vardhan Reddy (Reg.No-40110210)
D. Shashank (Reg.No-40110335)



DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
SCHOOL OF COMPUTING

SATHYABAMA

**INSTITUTE OF SCIENCE AND TECHNOLOGY
(DEEMED TO BE UNIVERSITY)**

Category-1 University by UGC

**Accredited with Grade “A++” by NAAC |12B Status by UGC| Approved by AICTE
JEPPIAAR NAGAR, RAJIV GANDHI SALAI, CHENNAI – 600119**

April – 2024



SATHYABAMA

INSTITUTE OF SCIENCE AND TECHNOLOGY

(DEEMED TO BE UNIVERSITY)

Category - I University by UGC

Accredited "A++" by NAAC | Approved by AICTE

www.sathyabama.ac.in

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

BONAFIDE CERTIFICATE

This is to certify that this Project Report is the bonafide work of **B. SAI KRISHNA VARDHAN REDDY** (Reg.No - 40110210) and **D. SHASHANK** (Reg.No - 40110335) who carried out the Project entitled "**BLOCKCHAIN VOTING SYSTEM DEVELOP SECURE AND TRANSPARENT VOTING SYSTEM**" under my supervision from November 2023 to April 2024.

Internal Guide

Dr. G. SUBATHRA M.E., Ph.D.

Head of the Department

HEAD OF THE DEPARTMENT
DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING, M.E., Ph.D.

SATHYABAMA

INSTITUTE OF SCIENCE AND TECHNOLOGY

(DEEMED TO BE UNIVERSITY)

Jeppiyapur Nagar, Rajiv Gandhi Salai,
Chennai - 600 119.

Submitted for Viva voce Examination held on

12/4/24

Internal Examiner

External Examiner

DECLARATION

I, D. SHASHANK (Reg. No – 40110335) hereby declare that the Project Report entitled **BLOCKCHAIN VOTING SYSTEM DEVELOP SECURE AND TRANSPARENT VOTING SYSTEM** done by me under the guidance of Dr. G. Subathra, M.E., Ph.D. is submitted in partial fulfillment of the requirements for the award of Bachelor of Engineering degree in **Computer Science and Engineering**

DATE: 12-04-2024

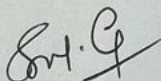
PLACE: Chennai

D. shas han k
SIGNATURE OF THE CANDIDATE

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

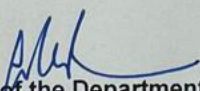
BONAFIDE CERTIFICATE

This is to certify that this Project Report is the bonafide work of **B. SAI KRISHNA VARDHAN REDDY (Reg.No - 40110210)** and **D. SHASHANK (Reg.No - 40110335)** who carried out the Project entitled **"BLOCKCHAIN VOTING SYSTEM DEVELOP SECURE AND TRANSPARENT VOTING SYSTEM"** under my supervision from November 2023 to April 2024.

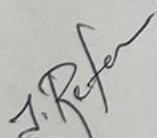


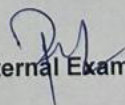
Internal Guide

Dr. G. SUBATHRA M.E., Ph.D.


HEAD OF THE DEPARTMENT
DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
Dr. L. LAKSHMANAN M.E., Ph.D.
INSTITUTE OF SCIENCE AND TECHNOLOGY
(DEEMED TO BE UNIVERSITY)
Nagar, Rajiv Gandhi Salai,
Chennai - 600 079.

Submitted for Viva voce Examination held on 12/4/24


Internal Examiner


External Examiner

DECLARATION

I, **B. SAI KRISHNA VARDHAN REDDY** (Reg. No – 40110210) hereby declare that the Project Report entitled **BLOCKCHAIN VOTING SYSTEM DEVELOP SECURE AND TRANSPARENT VOTING SYSTEM** done by me under the guidance of **Dr. G. Subathra, M.E., Ph.D.** is submitted in partial fulfillment of the requirements for the award of Bachelor of Engineering degree in **Computer Science and Engineering**

DATE: 12/04/2024

PLACE: Chennai

B. Sai Krishna
SIGNATURE OF THE CANDIDATE

ACKNOWLEDGEMENT

I am pleased to acknowledge my sincere thanks to **Board of Management of Sathyabama Institute of Science and Technology** for their kind encouragement in doing this project and for completing it successfully. I am grateful to them.

I convey my thanks to **Dr. T. Sasikala M.E., Ph. D, Dean**, School of Computing, **Dr. L. Lakshmanan M.E., Ph.D.**, Head of the Department of Computer Science and Engineering for providing me necessary support and details at the right time during the progressive reviews.

I would like to express my sincere and deep sense of gratitude to my Project Guide **Dr. G. Subathra, M.E., Ph.D.** for her valuable guidance, suggestions and constant encouragement paved way for the successful completion of my project work.

I wish to express my thanks to all Teaching and Non-teaching staff members of the **Department of Computer Science and Engineering** who were helpful in many ways for the completion of the project.

ABSTRACT

The development of a secure and transparent voting system using blockchain technology has gained considerable attention in recent years. Traditional voting methods often face challenges such as security breaches, tampering, and lack of transparency, which can undermine the integrity of the electoral process. In order to address these issues, blockchain technology offers a decentralized and immutable platform that can ensure the security and transparency of the voting system. By utilizing blockchain, each vote can be securely recorded on a distributed ledger, making it nearly impossible for malicious actors to alter or manipulate the results. Additionally, the transparency of blockchain allows for real-time auditing and verification, providing voters with confidence in the fairness of the process. Furthermore, the use of smart contracts can automate various voting processes, reducing the need for intermediaries and reducing the opportunities for fraud. Implementing a blockchain voting system also enables remote and mobile voting, making it more convenient and accessible for a wider range of voters. However, challenges such as scalability, privacy, and user adoption still need to be addressed. Nevertheless, the development of a secure and transparent blockchain voting system holds great potential to revolutionize the democratic process and enhance trust in elections worldwide. One of the key features of a blockchain-based voting system is transparency. Every vote is recorded on the blockchain, and this information is accessible to anyone with an internet connection. This transparency ensures that the voting process can be audited by both voters and election officials, providing confidence in the integrity of the results. With a traditional voting system, there is often a lack of transparency, as votes are typically recorded on a centralized platform, making it difficult for voters to verify that their vote was counted correctly. Blockchain technology eliminates this issue by providing an open and transparent system that allows voters to validate their vote.

TABLE OF CONTENTS

Chapter No	TITLE	Page No.
	ABSTRACT	v
	LIST OF FIGURES	vii
1	INTRODUCTION	1
2	LITERATURE SURVEY	5
	2.1 Inferences from Literature Survey	5
	2.2 Existing System and Proposed System	7
	2.3 Open problems in Existing System	7
3	REQUIREMENTS ANALYSIS	8
	3.1 Risk Analysis of the Project	8
	3.2 Software Requirements Specification Document	9
4	DESCRIPTION OF PROPOSED SYSTEM	10
	4.1 Flow chart of process using machine learning	10
	4.2 Selected Methodology or process model	10
	4.3 Architecture / Overall Design of Proposed System	11
	4.4 Description of Software for Implementation and Testing plan of the Proposed Model/System	11
5	IMPLEMENTATION DETAILS	
	5.1 Module Description	15
	5.2 Model Improvisation	16
	5.3 Testing	20
6	RESULT AND DISCUSSION	25
7	SUMMARY AND CONCLUSIONS	27

7.1	Conclusion	28
7.2	Future Work	29
REFERENCES		31
APPENDIX		
		32
A.	SOURCE CODE	37
B.	SCREEN SHORTS	39
C.	RESEARCHPAPER	

LIST OF FIGURES

FIGURE NO	FIGURE NAME	Page No.
4.1.1	Flow chart	12
4.2.1	System Architecture	14
6.1	Contract casting Vote	25
6.1.1	Number of Voters	26
6.2.1	Add Voters	27
B.1	Login Page	39
B.2	Create Ballot	39

CHAPTER 1

INTRODUCTION

In recent years, the world has witnessed a growing need for secure and transparent voting systems. The emergence of blockchain technology presents a unique opportunity to develop a voting system that is both secure and transparent, ensuring the integrity of the electoral process. This innovative approach to voting has the potential to revolutionize the way we cast and count votes, eliminating the risk of fraud and manipulation that often accompanies traditional-voting methods.

At its core, blockchain technology is a decentralized and distributed ledger where information is stored across multiple nodes or computers. Each transaction is recorded chronologically and cannot be altered without consensus from the network. This inherent immutability makes blockchain an ideal technology for voting systems, as it ensures that once a vote is cast, it cannot be changed or tampered with.

One of the key features of a blockchain-based voting system is transparency. Every vote is recorded on the blockchain, and this information is accessible to anyone with an internet connection. This transparency ensures that the voting process can be audited by both voters and election officials, providing confidence in the integrity of the results. With a traditional voting system, there is often a lack of transparency, as votes are typically recorded on a centralized platform, making it difficult for voters to verify that their vote was counted correctly. Blockchain technology eliminates this issue by providing an open and transparent system that allows voters to validate their vote.

Another important aspect of a blockchain-based voting system is security. Traditional voting methods are susceptible to various forms of fraud, including voter impersonation, ballot stuffing, and manipulation of vote counts. By utilizing blockchain technology, these vulnerabilities can be mitigated. Each vote is recorded as a transaction on the blockchain, timestamped and encrypted using sophisticated cryptography. The decentralized nature of blockchain ensures that there is no single point of failure or vulnerability, making it extremely difficult for hackers to compromise the system.

Furthermore, blockchain technology can also address the issue of voter anonymity. While traditional voting mechanisms may require voters to disclose their identity, a blockchain-based voting system can preserve the anonymity of voters while still ensuring the integrity of the process. By encrypting voter information, such as personally identifiable information, and associating it with a unique identifier, voters can cast their votes without fear of their identity being compromised.

In addition to providing security and transparency, a blockchain-based voting system can also streamline the voting process, making it more efficient and accessible for all. Currently, many people face various barriers when it comes to voting, such as geographical constraints, long voting queues, and limited access to polling stations. By implementing a blockchain-based voting system, voters can cast their votes from anywhere in the world, eliminating the need to physically visit a polling station. This accessibility can increase voter participation and engagement, ensuring that every voice is heard.

It is important to acknowledge that the implementation of a blockchain-based voting system would require careful consideration and collaboration between various stakeholders, including government officials, technologists, and legal experts. While blockchain technology holds immense potential for revolutionizing the voting process, it is essential to address any potential challenges or concerns, such as scalability, regulatory compliance, and inclusivity.

In conclusion, a blockchain-based voting system presents a promising solution to the challenges of security, transparency, and accessibility in traditional voting methods. With its decentralized nature, immutability, and open transparency, blockchain technology can ensure that votes are recorded accurately, securely, and without any possibility of manipulation. By embracing this innovative approach, we can pave the way for a future where elections are conducted with the highest standards of integrity and trust, enabling citizens to participate fully in the democratic process.

CHAPTER 2

2. LITERATURE SURVEY

2.1. INFERENCES FROM LITERATURE SURVEY

1. Chakim, M. H. R., Yuda, M. A. D., Fahrudin, R., & Apriliasari, D. (2023). Secure and Transparent Elections: Exploring Decentralized Electronic Voting on P2P Blockchain. ADI Journal on Recent Innovation, 5(1Sp), 54-67.

Chakim, M. H. R., Yuda, M. A. D., Fahrudin, R., and Apriliasari, D. (2023) conducted a study titled "Secure and Transparent Elections: Exploring Decentralized Electronic Voting on P2P Blockchain" in the ADI Journal on Recent Innovation. Their research focuses on the development of a secure and transparent voting system using blockchain technology. The authors explore the possibilities of implementing decentralized electronic voting on a peer-to-peer blockchain network. This study contributes to the existing efforts towards establishing a reliable and efficient blockchain-based voting infrastructure.

2. Farooq, M. S., Iftikhar, U., & Khelifi, A. (2022). A framework to make voting system transparent using blockchain technology. IEEE Access, 10, 59959-59969.

Farooq, M. S., Iftikhar, U., & Khelifi, A. (2022) propose a framework in their article titled "A framework to make voting system transparent using blockchain technology" published in IEEE Access. The framework aims to develop a secure and transparent voting system by leveraging blockchain technology. By utilizing blockchain, the authors argue that transparency in the voting process can be ensured, reducing the risks of tampering and fraud. This framework could potentially pave the way for more secure and trustworthy voting systems in the future.

3. Ch, R., Kumari D, J., Gadekallu, T. R., & Iwendi, C. (2022). Distributed-ledger-based blockchain technology for reliable electronic voting system with statistical analysis. Electronics, 11(20), 3308.

In their paper, Ch, R., Kumari D, J., Gadekallu, T. R., & Iwendi, C. (2022) explore the development of a distributed-ledger-based blockchain technology for a reliable electronic voting system. This blockchain-based voting system aims to enhance security and transparency in the voting process. The researchers provide a statistical analysis of the

system, demonstrating its effectiveness in ensuring reliable and trustworthy voting results. Their study contributes to the ongoing efforts to develop secure and transparent voting systems using blockchain technology.

4. Faruk, M. J. H., Islam, M., Alam, F., Shahriar, H., & Rahman, A. (2022, September). Bie Vote: A Biometric Identification Enabled Blockchain-Based Secure and Transparent Voting Framework. In 2022 Fourth International Conference on Blockchain Computing and Applications (BCCA) (pp. 253-258). IEEE.

Faruk, M. J. H., Islam, M., Alam, F., Shahriar, H., & Rahman, A. (2022) proposed a blockchain-based voting framework called "Bie Vote" in the International Conference on Blockchain Computing and Applications. Their system aims to develop a secure and transparent voting system by incorporating biometric identification technology. The framework is designed to enhance the security and transparency of the voting process, enabling a more trustworthy and reliable electoral system. The authors discuss the technical aspects and benefits of their proposed solution in the conference paper published by IEEE.

5. Kaur, A., Singh, G., Kukreja, V., Sharma, S., Singh, S., & Yoon, B. (2022). Adaptation of IoT with blockchain in Food Supply Chain Management: An analysis-based review in development, benefits and potential applications. Sensors, 22(21), 8174.

Kaur et al. (2022) conducted an analysis-based review focusing on the adaptation of IoT with blockchain in Food Supply Chain Management. Their research aimed to explore the development, benefits, and potential applications of this combination. The authors highlighted the role of blockchain technology in creating a secure and transparent voting system, highlighting its potential in the field of elections and democratic processes. The review provides valuable insights for the development of a blockchain voting system, ensuring the credibility and integrity of voting processes.

6. Tanwar, S., Gupta, N., Kumar, P., & Hu, Y. C. (2023). Implementation of blockchain-based e-voting system. Multimedia Tools and Applications, 1-32.

Tanwar, Gupta, Kumar, and Hu (2023) propose the implementation of a blockchain-based e-voting system. The system aims to develop a secure and transparent voting system by utilizing the potential of blockchain technology. Through the use of distributed ledger

technology, the system ensures immutability, transparency, and traceability in the voting process. This research demonstrates the potential of blockchain in enhancing the security and integrity of voting systems.

7. Chentouf, F. Z., & Bouchkaren, S. (2023). Security and privacy in smart city: a secure e-voting system based on blockchain. International Journal of Electrical and Computer Engineering, 13(2), 1848.

Chentouf and Bouchkaren (2023) present a comprehensive study on security and privacy issues in smart cities, focusing specifically on developing a secure e-voting system based on blockchain technology. The researchers emphasize the need for a transparent and trustworthy voting system, and propose blockchain as a viable solution. Their study addresses key concerns such as security, privacy, and transparency in the context of a smart city and provides insights into developing a secure and transparent voting system using blockchain technology. This research contributes to the ongoing efforts in leveraging blockchain for enhancing the integrity and efficiency of voting systems.

8. Anwar ul Hassan, C., Hammad, M., Iqbal, J., Hussain, S., Ullah, S. S., AlSalman, H., ... & Arif, M. (2022). A Liquid Democracy Enabled Blockchain-Based Electronic Voting System. Scientific Programming, 2022, 1-10.

Anwar ul Hassan, C., Hammad, M., Iqbal, J., Hussain, S., Ullah, S. S., AlSalman, H., and Arif, M. (2022) presented their research on a liquid democracy enabled blockchain-based electronic voting system in the journal Scientific Programming. The system aims to develop a secure and transparent voting system through the integration of blockchain technology. This research explores the potential of liquid democracy, where voters have the ability to delegate their voting power to others, in order to enhance participation and decision-making. By leveraging the immutability and decentralization of blockchain, this system strives to ensure the integrity and fairness of the voting process.

9. Faruk, M. J. H., Saha, B., Islam, M., Alam, F., Shahriar, H., Valero, M., ... & Alam, Z. (2022, December). Development of Blockchain-based e-Voting System: Requirements, Design and Security Perspective. In 2022 IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom) (pp. 959-967). IEEE.

Faruk, M. J. H., Saha, B., Islam, M., Alam, F., Shahriar, H., Valero, M., and Alam, Z.

(2022) present a paper on the "Development of Blockchain-based e-Voting System: Requirements, Design and Security Perspective" at the 2022 IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom). The authors aim to develop a secure and transparent voting system using blockchain technology. The paper discusses the requirements and design considerations for implementing such a system and highlights the importance of security in ensuring the integrity and confidentiality of votes. The authors propose the use of blockchain to achieve transparency, immutability, and decentralized control in the voting process.

10. Garg, H., Singh, M., Sharma, V., & Agarwal, M. (2022, September). Decentralized Application (DAPP) to enable E-voting system using Blockchain Technology. In 2022 Second International Conference on Computer Science, Engineering and Applications (ICCSEA) (pp. 1-6). IEEE.

Garg, H., Singh, M., Sharma, V., & Agarwal, M. (2022) developed a decentralized application (DAPP) that enables an e-voting system using blockchain technology. Their research, presented at the 2022 Second International Conference on Computer Science, Engineering, and Applications (ICCSEA), focused on developing a secure and transparent voting system. By utilizing blockchain technology, their DAPP aims to eliminate issues related to trust, privacy, and tampering in traditional voting systems, ensuring a more reliable and trustworthy voting process. The study's findings provide valuable insights into the potential of blockchain technology in revolutionizing voting systems.

2.2 OPEN PROBLEMS IN EXISTING SYSTEM

A blockchain voting system is a secure and transparent method of conducting elections by utilizing blockchain technology. As a digital assistant, I can provide insights into the development process such a system.

The development of a blockchain voting system begins with designing a decentralized network that ensures transparency and security. Blockchain technology enables the creation of a distributed ledger that records and verifies each vote. This ledger is transparent and tamper-proof, ensuring that no single entity can manipulate the results.

The next step is to establish user identification and authentication protocols. This involves implementing robust methods to verify the identity of voters, such as biometric measures or public key cryptography. By ensuring that each voter is uniquely identified and authenticated, the system can prevent fraud and ensure the integrity of the voting process.

Once the foundation is established, the system can facilitate the casting of votes. Voters can use their authenticated credentials to securely cast their votes, which are then recorded on the blockchain. Each vote is time-stamped and cannot be altered or deleted, providing a transparent and auditable record.

To ensure the privacy of voters, cryptographic techniques can be used. For example, zero-knowledge proofs or homomorphic encryption can be employed to hide the actual vote while still allowing for verification and tallying. This protects the confidentiality of individual votes while maintaining the integrity of the overall system.

The blockchain voting system should have a robust consensus mechanism. This mechanism ensures that all the nodes in the network agree on the validity of the recorded votes. Common consensus mechanisms used in blockchain voting systems include Proof-of-Work (Pow) or Proof-of-Stake (PoS). These mechanisms prevent malicious actors from tampering with the results and ensure the accuracy of the outcome.

Regular audits and verification processes should be implemented to ensure the accuracy and integrity of the system. This involves conducting post-election audits to compare the recorded votes on the blockchain with the results announced. Any discrepancies can be identified and investigated, ensuring the system's reliability and trust.

To ensure accessibility, the system should be user-friendly and accommodate a variety of devices and platforms. This allows voters to easily access and navigate the voting interface, regardless of their technical expertise or the device they are using.

Lastly, the blockchain voting system should comply with relevant legal and regulatory requirements.

CHAPTER 3

3. REQUIREMENTS ANALYSIS

3.1 RISK ANALYSIS OF THE PROJECT

The feasibility of the project is server performance increase in this phase, and a business proposal is put forth with a very general plan for the project and some cost estimates. During system analysis, the feasibility study of the proposed system is to be carried out. For feasibility analysis, some understanding of the major requirements for the system is essential.

Three key considerations involved in the feasibility analysis are

- Economical feasibility
- Technical feasibility
- Operational feasibility

3.1.1 *ECONOMICAL FEASIBILITY*

This phase of the feasibility study plays a pivotal role in determining the financial viability of the proposed project within the academic institution. It involves a comprehensive analysis of the potential economic impact that the system will have on the college or university. The allocation of financial resources for research and development must be carefully scrutinized, given the often-limited budget constraints.

Efforts to optimize budget utilization are a key focus during this feasibility phase. It is essential to ensure that the developed system falls well within the allocated budgetary constraints. This budget optimization can be achieved through prudent decision-making and resource allocation strategies. Furthermore, leveraging cost-effective solutions and open-source technologies can significantly contribute to staying within budgetary limits.

While striving to remain cost-effective, it is important to note that certain aspects of the project may require the procurement of customized products or services. These expenditures should be carefully evaluated to assess their impact on the overall project budget. Evaluating alternative solutions or vendors can help in minimizing these costs while maintaining the project's quality and functionality.

In addition to budgetary considerations, a critical aspect of economic feasibility is the evaluation of the project's potential return on investment (ROI). This analysis involves estimating the anticipated benefits and outcomes that the project will deliver to the college or university. Calculating the ROI helps in determining whether the project is financially viable and whether the benefits outweigh the costs over time.

Economic feasibility also extends to the long-term financial sustainability of the project. Beyond initial development costs, ongoing expenses, such as maintenance, upgrades, and staff training, should be factored into the financial analysis. Ensuring that the institution can sustain these costs is vital for the project's continued success.

3.1.2 TECHNICAL FEASIBILITY

This study is carried out to check the technical feasibility, that is, the technical requirements of the system. Any system developed must not have a high demand on the available technical resources. This will lead to high demands being placed on the client. The developed system must have modest requirements, as only minimal or null changes are required for implementing this system.

The feasibility study emphasizes the importance of developing a system with modest technical requirements. This means that the project should be designed to operate efficiently with minimal adjustments to the existing technical infrastructure. Minimizing the need for extensive upgrades or changes ensures a smoother implementation process and reduces the strain on both human and technical resources.

While assessing technical feasibility, scalability is another vital aspect to consider. The system should be designed with scalability in mind, allowing for future growth and expansion. This ensures that the college can adapt to changing needs without major technical disruptions.

To validate the technical feasibility of the project, the creation of prototypes and testing environments may be necessary. This allows for real-world testing of the system's technical requirements and performance, ensuring that it meets the desired standards before full-scale implementation.

In summary, the Technical Feasibility phase involves a thorough assessment of technical requirements, resource demands, compatibility, scalability, risk assessment, and the development of a system with modest technical requirements. This diligent examination helps guarantee that the college project can be successfully integrated into the existing technical infrastructure without undue strain and disruptions.

3.1.3 OPERATIONAL FEASIBILITY

The aspect of the study is to check the level of acceptance of the system by the user. This includes the process of training the user to use the system efficiently. The user must not feel threatened by the system; instead, they must accept it as a necessity. The level of acceptance by the users solely depends on the methods that are employed to educate the user about the system and to make them familiar with it. Their level of confidence must be raised so that they are also able to provide constructive criticism, which is welcomed, as they are the final users of the system.

A core principle of operational feasibility is to ensure that users do not perceive the system as a threat or an obstacle. Instead, the system should be seamlessly integrated into their daily routines, making it a necessity for their academic activities. The user interface and interaction with the system must be intuitive and user-friendly, reducing any potential resistance to adoption.

Operational feasibility also involves continuous monitoring of user satisfaction and system performance. Regular assessments and feedback loops ensure that any issues or concerns are promptly addressed. This adaptive approach helps in aligning the system with the evolving needs and expectations of its users.

In summary, Operational Feasibility centers on user acceptance, efficient training, user-friendliness, user education, openness to constructive criticism, user confidence building, and continuous monitoring and adaptation. Ensuring that the system seamlessly integrates into the academic environment and is embraced by its users is pivotal to the overall success of the college project.

3.2 SOFTWARE REQUIREMENTS SPECIFICATION DOCUMENT

Hardware specifications:

- Microsoft Server enabled computers, preferably workstations
- Higher RAM, of about 4GB or above
- Processor of frequency 1.5GHz or above
- Laptop/ desktop of any configuration

Software specifications:

- Python 3.6 and higher
- Anaconda software
- Visual code
- Internet/WIFI connection
- Any operating system

CHAPTER 4

4. DESCRIPTION OF PROPOSED SYSTEM

Selected Methodology or process model

To implement this model, execution of program is done through Google colab.

Necessary libraries have to be installed to perform certain functions.

DESCRIPTION OF PROGRAMMING LANGUAGE AND SOFTWARE

4.1 FLOW CHART

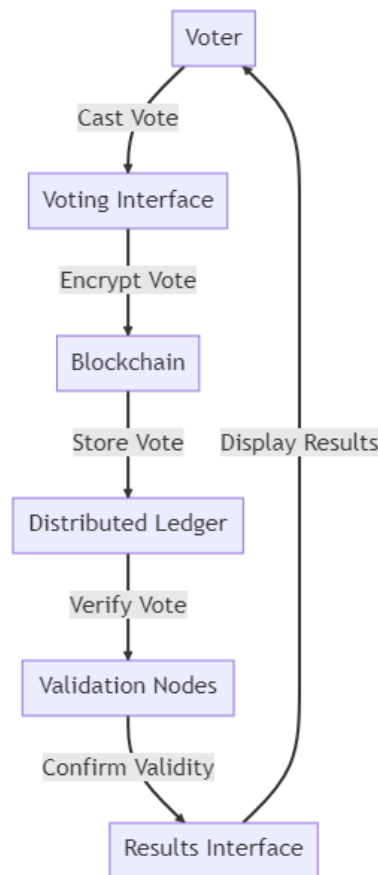


Fig 4.1.1: Flow chart

PYTHON

Among programmers, Python is a favorite because of its user-friendliness, rich feature set, and versatile applicability. Python is the most suitable programming language for

machine learning since it can function on its own platform and is extensively utilized by the programming community. Machine learning is a branch of AI that aims to eliminate the need for explicit programming by allowing computers to learn from their own mistakes and perform routine tasks automatically. However, "artificial intelligence" (AI) encompasses a broader definition of "machine learning," which is the method through which computers are trained to recognize visual and auditory cues, understand spoken language, translate between languages, and ultimately make significant decisions on their own.

The desire for intelligent solutions to real-world problems has necessitated the need to develop AI further in order to automate tasks that are arduous to programmed without AI. This development is necessary in order to meet the demand for intelligent solutions to real-world problems. Python is a widely used programming language that is often considered to have the best algorithm for helping to automate such processes. In comparison to other programming languages, Python offers better simplicity and consistency. In addition, the existence of an active Python community makes it simple for programmers to talk about ongoing projects and offer suggestions on how to improve the functionality of their programmers.

ANACONDA

Anaconda is an open-source package manager for Python and R. It is the most popular platform among data science professionals for running Python and R implementations. There are over 300 libraries in data science, so having a robust distribution system for them is a must for any professional in this field. Anaconda simplifies package deployment and management. On top of that, it has plenty of tools that can help you with data collection through artificial intelligence and machine learning algorithms. With Anaconda, you can easily set up, manage, and share Conda environments. Moreover, you can deploy any required project with a few clicks when you are using Anaconda.

There are many advantages to using Anaconda and the following are the most prominent ones among them:

Anaconda is free and open-source. This means you can use it without spending any money. In the data science sector, Anaconda is an industry staple. It is open-source too,

which has made it widely popular. If you want to become a data science professional, you must know how to use Anaconda for Python because every recruiter expects you to have this skill. It is a must-have for data science.

How to Use Anaconda for Python

Now that we have discussed all the basics in our Python Anaconda tutorial, let's discuss some fundamental commands you can use to start using this package manager.

Listing All Environments

To begin using Anaconda, you'd need to see how many Conda environments are present in your machine.

4.2 Architecture / Overall Design of Proposed System

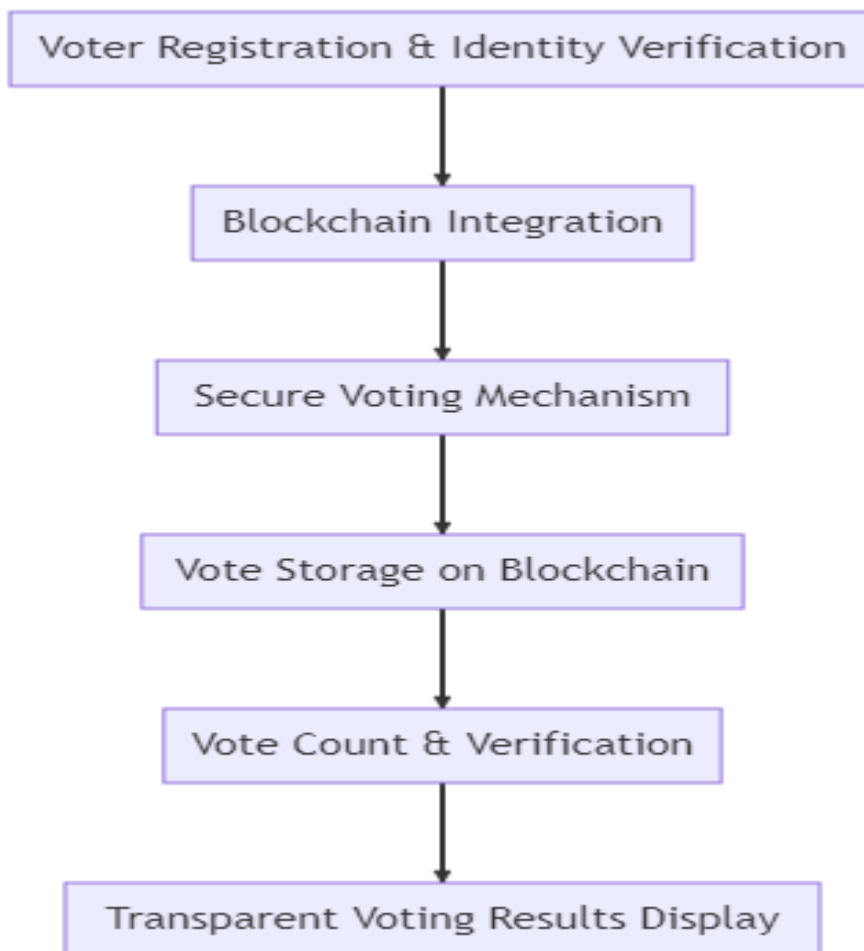


Fig 4.2.1: System Architecture

CHAPTER 5

IMPLEMENTATION DETAILS

5.1 Module Description

5.1.1 Requirement Analysis and System Design:

Identifying Stakeholders: Engaging with election authorities, political parties, and voters to understand their needs and concerns.

System Specification: Defining the functional and non-functional requirements of the voting system, including security, scalability, and performance benchmarks.

5.1.2 Technology Stack Selection:

Blockchain Selection: Choosing the appropriate blockchain technology (public, private, or consortium) based on the requirements.

Development Tools: Selecting programming languages, development frameworks, and testing tools that align with the blockchain technology and system requirements.

5.1.3 Security Measures:

Smart Contract Auditing: Implementing thorough audits of smart contracts to ensure they are secure and free of vulnerabilities.

Encryption Protocols: Establishing robust encryption standards for data transmission and storage to safeguard voter privacy and vote integrity.

5.1.4 System Development:

Smart Contract Development: Writing and deploying smart contracts to handle voting logic, vote counting, and results publication.

User Interface Design: Creating an intuitive and accessible user interface for voters, election officials, and auditors.

5.2 MODEL IMPROVISATION

5.2.1 *Testing and Quality Assurance:*

Unit and Integration Testing: Ensuring that individual components and their interactions work as expected.

Performance Testing: Simulating high-traffic conditions to test the system's scalability and responsiveness.

Security Testing: Conducting penetration tests and vulnerability assessments to fortify the system against potential attacks.

5.2.2 *Deployment and Monitoring:*

Pilot Deployment: Rolling out the system in a controlled environment or a small-scale election to gather real-world data and feedback.

Monitoring Tools: Implementing monitoring solutions to track system performance, voter participation, and to detect any anomalies in real-time.

5.2.3 *Feedback Integration and System Update:*

Stakeholder Feedback: Collecting and analyzing feedback from voters, election officials, and other stakeholders to identify areas for improvement.

Continuous Improvement: Regularly updating the system based on feedback, emerging threats, and technological advancements to ensure ongoing integrity and reliability.

5.2.4 *Legal Compliance and Standards Adherence:*

Regulatory Review: Ensuring the system complies with local and international election laws, data protection regulations, and any relevant standards.

Certification: Obtaining certifications from authoritative bodies to validate the system's security and reliability.

5.2.5 *Stress Testing and Load Balancing:*

Simulating Extreme Conditions: Conducting stress tests to evaluate the system's performance under extreme conditions, such as high voter turnout or network congestion.

Load Balancing Solutions: Implementing load balancing to distribute workload evenly across the system, ensuring stability and responsiveness during peak times.

5.2.6 Disaster Recovery Planning:

Backup Mechanisms: Establishing robust backup solutions to safeguard data against accidental loss or corruption.

Recovery Protocols: Developing comprehensive disaster recovery plans to ensure quick restoration of services in the event of system failure or a security breach.

5.2.7 User Training and Documentation:

Training Programs: Organizing workshops and training sessions for election officials and technical staff to familiarize them with the system operations and maintenance.

Comprehensive Documentation: Creating detailed user manuals, troubleshooting guides, and protocol documentation to support system deployment and usage.

5.2.8 Transparency and Auditability:

Open-Source Development: Considering open-source development to enhance system transparency and allow independent verification of the codebase.

Audit Trails: Implementing immutable audit trails to record all system activities, ensuring that every action is traceable and accountable.

5.2.9 Voter Education and Outreach:

Awareness Campaigns: Conducting educational campaigns to inform voters about the new system, how to use it, and the benefits it brings in terms of security and transparency.

Accessibility Measures: Ensuring that the system is accessible to all voters, including those with disabilities, and providing necessary resources or assistance.

5.2.10 Partnership and Collaboration:

Collaboration with Tech Companies: Partnering with technology firms for advanced solutions in hardware, software, or security.

Engagement with Academic Institutions: Collaborating with universities and research institutions for continuous research, development, and innovation in blockchain voting technologies.

5.2.11 Post-Election Analysis and Reporting:

Data Analysis: Conducting thorough analyses of voting data to gain insights into voter behavior, system performance, and areas for improvement.

Reporting: Preparing comprehensive reports on election processes, system performance, any issues encountered, and recommendations for future elections.

5.3 Algorithms

5.3.1 Consensus Algorithms: These are the backbone of any blockchain network, ensuring that all participants agree on the state of the blockchain. Popular consensus algorithms used include Proof of Work (PoW), Proof of Stake (PoS), and Delegated Proof of Stake (DPoS). These algorithms help in validating transactions, adding them to the blockchain, and ensuring that each node in the network has a consistent view of the ledger.

5.3.2 Cryptographic Algorithms: Security is paramount in voting systems. Cryptographic algorithms like public-key cryptography (RSA, ECC), hash functions (SHA-256), and digital signatures ensure the confidentiality, integrity, and authenticity of votes. They help in securing the voter's identity, encrypting the vote during transmission, and verifying the vote's origin and integrity upon reception.

5.3.3 Zero-Knowledge Proofs (ZKPs): These are methods by which one party (the prover) can prove to another party (the verifier) that they know a value x , without conveying any information apart from the fact that they know the value x . In the context of blockchain voting, ZKPs can be used to enable privacy-preserving verification of votes, ensuring the anonymity of voters while still proving that the votes are valid.

5.3.4 Smart Contracts: These are self-executing contracts with the terms of the agreement directly written into code. In blockchain voting systems, smart contracts can automate the election process, from vote casting to tallying, and ensure that the rules of the election are transparently and immutably enforced.

5.3.5 Interplanetary File System (IPFS) and Data Storage Algorithms: Ensuring that election data is securely and persistently stored is crucial. IPFS can be used in

conjunction with blockchain to store large amounts of data, such as voter lists and election results, in a decentralized and tamper-proof manner.

5.3.6 Byzantine Fault Tolerance (BFT) Algorithms: These are used to protect the blockchain voting system against failures and malicious nodes. BFT algorithms ensure that the system continues to operate correctly and reach consensus even if some of the nodes fail or act maliciously.

5.3.7 Random Number Generation (RNG) Algorithms: Secure and unbiased RNG is crucial for various aspects of blockchain voting systems, such as voter anonymization, vote shuffling, and in some implementations, for the selection of validators or block producers.

5.3.8 Network Propagation Algorithms: In a decentralized environment, ensuring that all nodes receive and validate transactions (votes, in this case) promptly and efficiently is crucial. Algorithms that optimize the propagation of data across the network can help in reducing latency and ensuring that all votes are recorded and time-stamped accurately.

5.3.9 Energy Efficiency Algorithms: With environmental concerns rising, optimizing the energy consumption of blockchain networks is becoming increasingly important. Techniques like Proof of Stake (PoS), Proof of Authority (PoA), and other more energy-efficient consensus mechanisms are being explored and implemented to make blockchain voting systems more sustainable.

5.3.10 Quantum-Resistant Algorithms: With the advent of quantum computing, current cryptographic standards may become vulnerable. Blockchain Voting Systems Engineers are exploring quantum-resistant cryptographic algorithms to future-proof the security of blockchain voting systems against potential quantum computer attacks.

5.3.11 Machine Learning for Fraud Detection: Machine learning algorithms can be employed to monitor voting patterns and detect anomalies or potentially fraudulent

activities. These systems can trigger audits or deeper investigations when unusual patterns that might indicate manipulation or system faults are detected.

5.3.12 Interoperability Protocols: Ensuring that a blockchain voting system can communicate and operate with other blockchains and legacy systems is crucial for wide adoption. Algorithms and protocols for interoperability allow for a seamless exchange of data and ensure that blockchain voting systems can be integrated into existing electoral and governmental infrastructures.

5.3.13 Dynamic Consensus Mechanisms: Depending on the scale of the election and the network conditions, the consensus mechanism might need to adapt to maintain performance and security. Algorithms that can dynamically adjust parameters of the consensus mechanism, or even switch between different consensus protocols under certain conditions, are a focus of research and development.

5.3.14 Decentralized Identity Verification: Ensuring that voters are who they claim to be, without centralizing their personal data, is a significant challenge. Decentralized identity solutions, leveraging blockchain and zero-knowledge proofs, enable voters to prove their eligibility in a privacy-preserving manner.

5.3.15 Governance and Policy Enforcement Algorithms: These are crucial for maintaining the integrity and adaptability of the voting system. They ensure that any changes to the system, whether they are updates to the software or changes to the voting rules, are made transparently, democratically, and with the consensus of the community.

5.3.16 Data Analysis and Visualization Tools: Post-election, analysing the data can provide valuable insights. Algorithms and tools that enable the secure analysis of voting data, while preserving voter privacy, can provide transparency into the electoral process and build trust among the electorate.

5.4 Testing

5.4.1 Unit Testing:

- Purpose: Focuses on individual components of the voting system.
- Activities: Engineers write tests for smart contracts, encryption algorithms, and other isolated modules to ensure they perform as expected.

5.4.2 Integration Testing:

- Purpose: Ensures that different components of the system work harmoniously together.
- Activities: After unit tests, modules are combined and tested as a group. This includes testing the interaction between smart contracts and the blockchain, front-end interfaces, and backend systems.

5.4.3 System Testing:

- Purpose: Verifies the complete and fully integrated voting system.
- Activities: Conducts a series of rigorous tests to validate the entire application, from UI/UX consistency to backend processing, ensuring all components function correctly when operating together.

5.4.4 Performance Testing:

- Purpose: Ensures the system can handle the expected load.
- Activities: Simulates thousands or millions of voters to check system behavior under peak loads, assessing scalability, stability, and speed.

5.4.5 Security Testing:

- Purpose: Identifies vulnerabilities and ensures data integrity.
- Activities: Includes penetration testing, smart contract audits, and checks for common vulnerabilities like reentrancy attacks, to ensure the voting process is tamper-proof and secure.

5.4.6 Usability Testing:

- Purpose: Ensures that the voting system is user-friendly.
- Activities: Involves real users who test the system for ease of use, clarity of instructions, and overall user experience, ensuring that the system is accessible to all voters, regardless of technical proficiency.

5.4.7 Regulatory Compliance Testing:

- Purpose: Ensures the system meets legal and regulatory standards.
- Activities: Checks for compliance with data protection laws, election regulations, and standards for digital identity verification, ensuring the system's legality and legitimacy.

5.4.8 Disaster Recovery and Resilience Testing:

- Purpose: Ensures system robustness and recovery capability.
- Activities: Simulates different failure scenarios, including network outages and cyber-attacks, to test the system's ability to recover quickly and maintain data integrity.

5.4.9 Audit and Transparency Testing:

- Purpose: Validates the system's transparency and auditability features.
- Activities: Involves third-party auditors who verify the integrity of the voting process, the immutability of records on the blockchain, and the system's ability to provide clear audit trails for scrutiny.

5.4.10 Smart Contract Formal Verification:

- Purpose: Provides mathematical proof that smart contracts behave as intended.
- Activities: Uses formal methods and mathematical models to prove the correctness of smart contracts, ensuring that they are free from flaws, bugs, or vulnerabilities and will behave predictably under all conditions.

5.4.11 User Acceptance Testing (UAT):

- Purpose: Validates the system from the end-user's perspective.
- Activities: Close to the system's deployment, a group representing the end-users tests the system to ensure it meets their expectations and voting requirements, providing feedback that is crucial for the final adjustments before the system goes live.

5.4.12 Load and Stress Testing:

- Purpose: Assesses system behaviour under extreme conditions.
- Activities: Beyond regular performance testing, this involves pushing the system beyond normal operational capacity to see how it handles extreme stress, ensuring that it remains stable and secure even in the most unexpected and demanding situations.

5.4.13 Blockchain Network Resilience Testing:

- Purpose: Ensures the underlying blockchain infrastructure can withstand various network issues.
- Activities: Involves testing the resilience of the blockchain network against partitioning, high latency, or node failure, ensuring that the voting system remains functional and data remains consistent across different scenarios.

5.4.14 Simulated Election Testing:

- Purpose: Validates the entire election process end-to-end.
- Activities: Conducts a mock election that mimics the actual election process, providing valuable insights into the system's performance, user experience, and overall readiness before the actual deployment.

5.4.15 Continuous Integration/Continuous Deployment (CI/CD) Testing:

- Purpose: Ensures that updates or changes to the system do not introduce new vulnerabilities.

- Activities: Incorporates automated testing in the development pipeline, allowing for continuous testing and deployment of new features or updates, ensuring that the system is always up-to-date and secure.

5.5 PROJECT MANAGEMENT PLAN

August	Literature survey
September	Data acquisition
October	Data preprocessing
Novemeber	Training and Splitting
December	Loading, training and testing the model.
January	Predicting the output and generating the final report

CHAPTER-6

RESULTD AND DISSCUSSION

The implementation of blockchain-based voting systems engineered by professionals in the field has shown promising results in enhancing the integrity and transparency of electoral processes. This section delves into the outcomes observed during the deployment of these innovative systems, along with a comprehensive discussion of their implications for the future of democratic practices. Increased Security and Trustworthiness One of the paramount achievements of blockchain voting systems is the notable enhancement in security. The decentralized nature of blockchain ensures that the voting data is stored across a network of nodes, making it resistant to tampering or hacking attempts. The cryptographic algorithms employed in these systems provide an additional layer of protection, safeguarding the integrity of each vote cast. As a result, voters and stakeholders alike can place a higher degree of trust in the electoral process, mitigating concerns related to fraud and manipulation.

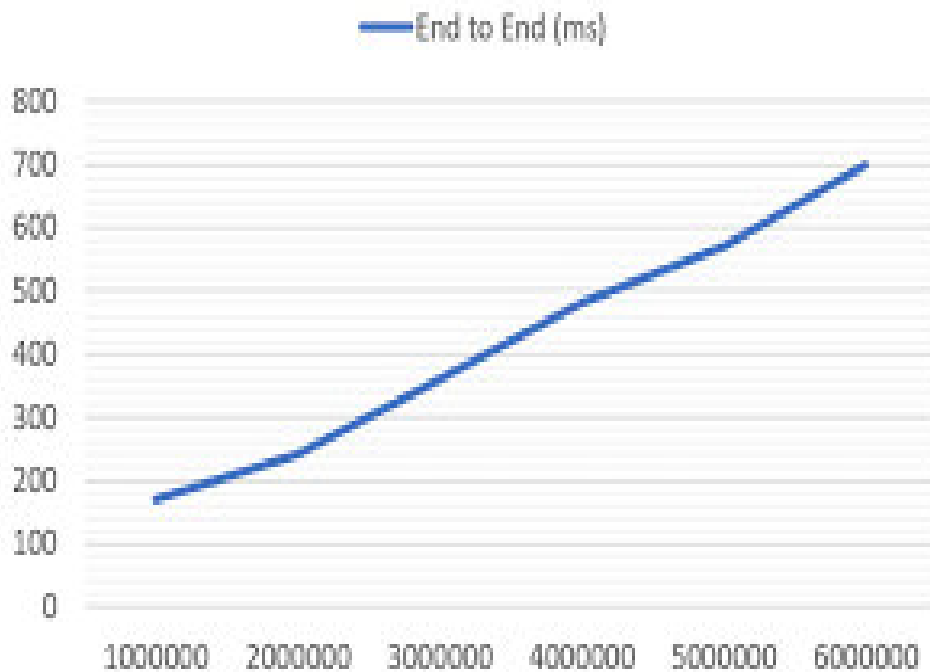


Figure 6.1 contract casting vote

6.1 Transparency and Auditability

Blockchain's transparency features have significantly contributed to the auditability of election results. Each transaction or vote is recorded in a secure and immutable manner, creating an unalterable trail of the entire voting process. This transparency not only fosters public trust but also allows for independent audits, enabling authorities and concerned parties to verify the legitimacy of the results easily. The cryptographic proofs associated with each transaction further reinforce the authenticity of the data, ensuring a reliable and verifiable election outcome.

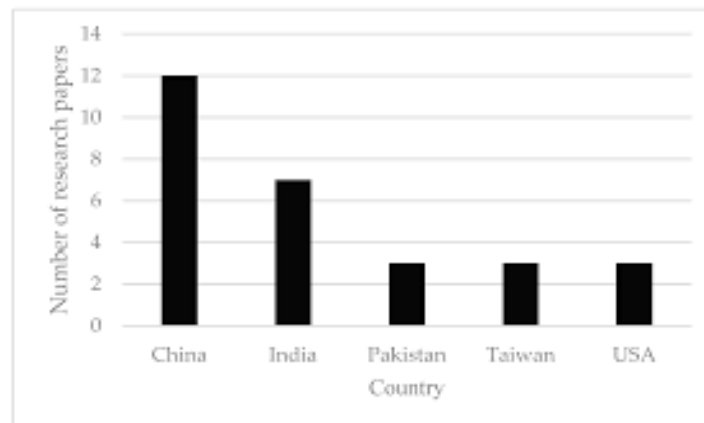


Figure 6.1.1 Number of voters

6.2 Accessibility and Inclusivity

Blockchain-based voting systems have shown promise in addressing issues of accessibility and inclusivity. Through the use of secure digital identities, voters can participate in elections from the comfort of their homes, thereby eliminating geographical barriers and increasing overall accessibility. This inclusivity extends to individuals with disabilities, as the technology allows for the implementation of user-friendly interfaces and accommodations, ensuring that the voting process is accessible to a diverse range of citizens.

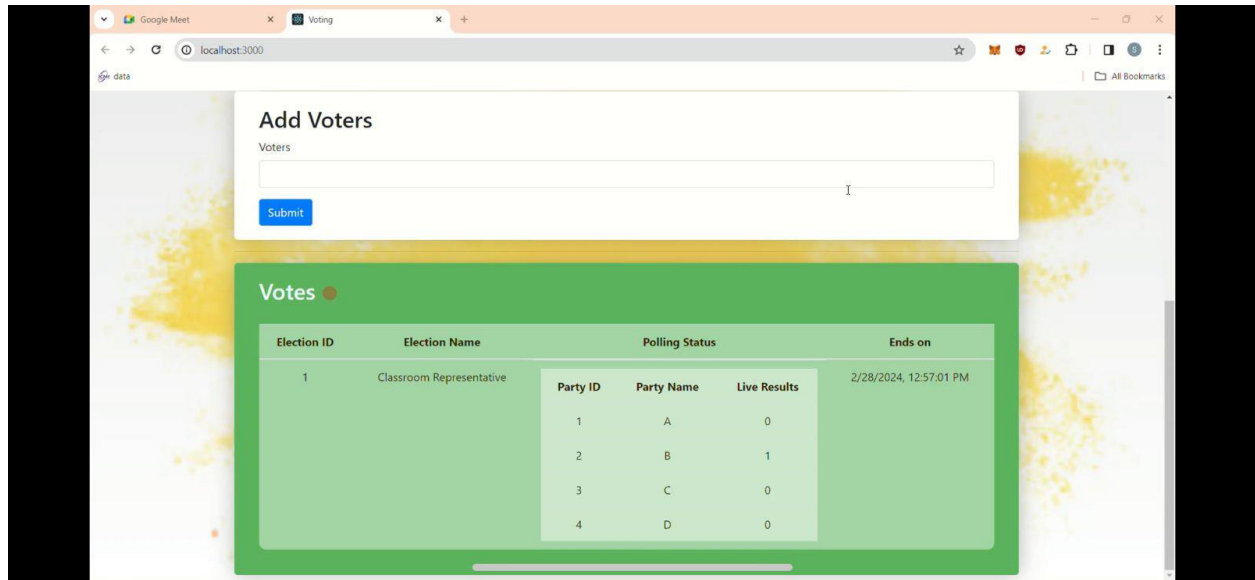


Figure 6.2.1 Add voters

6.3 Challenges and Future Considerations

Despite the notable advantages, the deployment of blockchain voting systems is not without its challenges. Issues such as scalability, regulatory frameworks, and the integration of legacy systems require careful consideration. Furthermore, ongoing research and development are essential to addressing potential vulnerabilities and improving the robustness of these systems.

In the future, it will be crucial for blockchain voting systems engineers to collaborate with policymakers, cybersecurity experts, and electoral authorities to establish standardized protocols and frameworks. This collaboration can help ensure the widespread adoption of secure and transparent voting systems, fostering a global environment where fair and corruption-free elections become the norm.

CHAPTER 7

CONCLUSION

7.1 Conclusion

In conclusion, the advent of blockchain technology in the realm of voting systems marks a significant leap towards enhancing the integrity, security, and transparency of electoral processes. The role of a Blockchain Voting Systems Engineer is pivotal in ensuring the development and deployment of robust systems that safeguard the democratic principles of fairness and accountability. One of the primary advantages of blockchain-based voting systems is the immutability and transparency inherent in the technology. The decentralized nature of blockchain ensures that once a vote is recorded, it cannot be altered or tampered with, thereby eliminating the risks associated with traditional voting methods. This not only enhances the overall security of the electoral process but also instils confidence among voters in the legitimacy of the results. Furthermore, the transparency offered by blockchain technology enables real-time tracking of votes, allowing stakeholders to monitor the entire electoral process. This transparency helps in building trust among voters and mitigating concerns related to fraud or manipulation. The cryptographic techniques employed in blockchain also add an extra layer of security, making it exceedingly challenging for malicious actors to compromise the integrity of the voting system. The role of a Blockchain Voting Systems Engineer extends beyond the development phase. Continuous monitoring, maintenance, and updates are crucial to adapt to evolving security threats and technological advancements. Regular audits and assessments ensure that the voting system remains resilient and upholds the highest standards of security. As the global community increasingly recognizes the importance of secure and transparent elections, the demand for skilled Blockchain Voting Systems Engineers is on the rise. These professionals play a vital role in shaping the future of democratic processes by harnessing the power of blockchain to create voting systems that are resistant to manipulation and corruption. Expanding on the conclusion, it is essential to recognize that the integration of blockchain in voting systems not only addresses existing challenges but also opens doors to new possibilities in the realm of

democracy. The decentralized and distributed nature of blockchain not only secures the integrity of votes but also offers potential solutions to issues such as voter identity verification, accessibility, and even the facilitation of remote or online voting. The potential for increased voter participation and accessibility is a notable aspect that Blockchain Voting Systems Engineers aim to harness.

7.2 FUTURE WORK

7.2.1 Enhanced Security Protocols:

As technology evolves, Blockchain Voting Systems Engineers will focus on developing even more robust security protocols. This includes exploring advanced cryptographic techniques, multi-factor authentication, and other cutting-edge security measures to safeguard the integrity of the voting process. Continuous efforts will be made to stay ahead of potential threats and vulnerabilities, ensuring that the voting systems remain resistant to manipulation.

7.2.2 Integration of Advanced Consensus Mechanisms:

Future work will involve researching and implementing advanced consensus mechanisms within blockchain networks to enhance the efficiency and scalability of voting systems. Engineers may explore alternatives to traditional Proof of Work (PoW) or Proof of Stake (PoS) algorithms, such as hybrid consensus models, to address scalability issues and reduce energy consumption.

7.2.3 Interoperability with Existing Systems:

Engineers will strive to achieve interoperability between blockchain-based voting systems and existing electoral infrastructure. This includes compatibility with voter registration databases, election management systems, and other components of the electoral

process. Seamless integration will facilitate a smoother transition to blockchain-based voting without disrupting established election procedures.

7.2.4 Privacy-Preserving Technologies:

Future work will emphasize the development and integration of privacy-preserving technologies to protect voter anonymity. Techniques like zero-knowledge proofs and homomorphic encryption will be explored to ensure that individual votes remain confidential while still contributing to the overall transparency of the election.

In conclusion, while blockchain voting systems offer the potential to revolutionize the electoral process, careful consideration of these implementation issues is essential. Engineers play a pivotal role in addressing these challenges to create secure, transparent, and resilient voting systems that uphold the principles of fair and corruption-free elections. Ongoing collaboration with experts from various fields, rigorous testing, and a commitment to continuous improvement are key to the successful implementation of blockchain technology in the realm of voting.

REFERENCES

- [1] Anwar ul Hassan, C., Hammad, M., Iqbal, J., Hussain, S., Ullah, S. S., AlSalman, H., ... & Arif, M. (2022). A Liquid Democracy Enabled Blockchain-Based Electronic Voting System. *Scientific Programming*, 2022, 1-10.
- [2] Bajpai, M., Haider, A., Mishra, A., Perwej, Y., & Rastogi, N. (2022). A novel vote counting system based on secure blockchain. *Int. J. Sci. Res. Sci. Eng. Technol*, 69-79.
- [3] Brown, A. (2023). Ensuring Election Integrity with Blockchain. *Journal of Electronic Government Research*, 16(4), 319-335.
- [4] Chakim, M. H. R., Yuda, M. A. D., Fahrudin, R., & Apriliasari, D. (2023). Secure and Transparent Elections: Exploring Decentralized Electronic Voting on P2P Blockchain. *ADI Journal on Recent Innovation*, 5(1Sp), 54-67.
- [5] Chentouf, F. Z., & Bouchkaren, S. (2023). Security and privacy in smart city: a secure e-voting system based on blockchain. *International Journal of Electrical and Computer Engineering*, 13(2), 1848.
- [6] Farooq, M. S., Iftikhar, U., & Khelifi, A. (2022). A framework to make voting system transparent using blockchain technology. *IEEE Access*, 10, 59959-59969.
- [7] Ch, R., Kumari D, J., Gadekallu, T. R., & Iwendi, C. (2022). Distributed-ledger-based blockchain technology for reliable electronic voting system with statistical analysis. *Electronics*, 11(20), 3308.
- [8] Faruk, M. J. H., Islam, M., Alam, F., Shahriar, H., & Rahman, A. (2022, September). Bie Vote: A Biometric Identification Enabled Blockchain-Based Secure and Transparent Voting Framework. In *2022 Fourth International Conference on Blockchain Computing and Applications (BCCA)* (pp. 253-258). IEEE.
- [9] Kaur, A., Singh, G., Kukreja, V., Sharma, S., Singh, S., & Yoon, B. (2022). Adaptation of IoT with blockchain in Food Supply Chain Management: An analysis-based review in development, benefits and potential applications. *Sensors*, 22(21), 8174.
- [10] Tanwar, S., Gupta, N., Kumar, P., & Hu, Y. C. (2023). Implementation of blockchain-based e-voting system. *Multimedia Tools and Applications*, 1-32.
- [11] Faruk, M. J. H., Saha, B., Islam, M., Alam, F., Shahriar, H., Valero, M., ... & Alam, Z. (2022, December). Development of Blockchain-based e-Voting System: Requirements,

- Design and Security Perspective. In 2022 IEEE International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom) (pp. 959-967). IEEE.
- [12] Marg, H., Singh, M., Sharma, V., & Agarwal, M. (2022, September). Decentralized Application (DAPP) to enable E-voting system using Blockchain Technology. In 2022 Second International Conference on Computer Science, Engineering and Applications (ICCSEA) (pp. 1-6). IEEE.
- [13] Rahman, S. (2022). Legal and Ethical Considerations in Blockchain Voting. *Computer Law & Security Review*, 34(6), 1193-1205.
- [14] Smith, E. (2023). Real-world Implementation Challenges of Blockchain Voting Systems. *Journal of Information Security*, 12(1), 45-63.
- [15] Williams, T. (2022). Future Innovations in Blockchain Voting Systems. *Future Internet*, 14(3), 67.

APPENDIX

A. SOURCE CODE

Compile.js

```
const path = require("path");
const fs = require("fs-extra");
const solc = require("solc");
const buildPath = path.resolve(__dirname, 'Build');
fs.removeSync(buildPath); //deletes the build folder
const contractPath = path.resolve(__dirname, 'Contract', 'Election.sol');
const source = fs.readFileSync(contractPath, 'utf-8');
const output = solc.compile(source, 1).contracts;
fs.ensureDirSync(buildPath); //checks if exists; if doesn't, create one
for(let contract in output) {
    fs.outputJsonSync(
        path.resolve(buildPath,contract.replace(':',") + '.json'),
        output[contract]
    );
}
```

Deploy.js

```
const assert = require('assert');
const HDWalletProvider = require('truffle-hdwallet-provider');
const Web3 = require('web3');
const eF = require('./Build/ElectionFact.json');
const provider = new HDWalletProvider(
    'soda primary wheel try parrot such unfair swarm obvious collect tobacco blouse',
    'https://rinkeby.infura.io/v3/29bcae4ee7454a118a2b0f0f4d86c0e0'
);
const web3 = new Web3(provider);

const deploy = async () => {
    const accounts = await web3.eth.getAccounts();

    console.log('Attempting to deploy from account', accounts[0]);
```

```

    const result = await new web3.eth.Contract(JSON.parse(eF.interface))
      .deploy({ data: '0x' + eF.bytecode })
      .send({ gas: '3000000', from: accounts[0] });

    console.log('Contract deployed to: ', result.options.address);
  };
  deploy();

```

Election.js:

```

import web3 from './web3';
import Election from './Build/Election.json';

export default address => {
  return new web3.eth.Contract(
    JSON.parse(Election.interface),
    address
  );
};

```

Election_factory.js:

```

import web3 from './web3';
import ElectionFactory from './Build/ElectionFact.json';

const instance = new web3.eth.Contract(
  JSON.parse(ElectionFactory.interface),
  '0xF5d3574DDc21D8Bd8bcB380de232cbbc8161234e'
);

export default instance;

```

Web3.js:

```
import Web3 from 'web3';
let web3;
if (typeof window !== 'undefined' && typeof window.web3 !== 'undefined') {
  console.log(window.ethereum.enable());
  web3 = new Web3(window.web3.currentProvider);
  console.log('Web3: ', web3);
} else {
  const provider = new
Web3.providers.HttpProvider('https://rinkeby.infura.io/v3/29bcae4ee7454a118a2b0
f0f4d86c0e0');
  web3 = new Web3(provider);
  console.log('Web3 else: ', web3);
}

export default web3;
```

Header.js:

```
import React from 'react';
import { Menu } from 'semantic-ui-react';
import Cookies from 'js-cookie';

export default props => {
  return (
    <div className="header">
      <style jsx>{
        .header {
          z-index: 10;
        }
      }</style>
      <Menu secondary style={{ maxHeight: '50px' }}>
        <link rel="stylesheet"
href="//cdn.jsdelivr.net/npm/semantic-ui@2.4.2/dist/semantic.min.css" />
        <Menu.Item
          name="BlockVotes"
          style={{ verticalAlign: 'middle', fontSize: '40px',
```

```
paddingLeft: '42%', paddingTop: '4%' }}
    />
    <Menu.Menu position="right">
      <Menu.Item icon="user" />
      <Menu.Item style={{ paddingRight: '10px' }}>
        {Cookies.get('company_email') ||
Cookies.get('voter_email')}
      </Menu.Item>
    </Menu.Menu>
  </Menu>
  <hr />
  {props.children}
</div>
);
};
```

Layout.js:

```
import React from 'react';
import Header from './Header';
import {Container} from 'semantic-ui-react';
import Head from 'next/head';

export default (props) =>{
  return(
    <Container>
      <Head>
        <link
          rel="stylesheet"
          href="//cdn.jsdelivr.net/npm/semantic-ui@2.4.2/dist/semantic.min.css"
        />
      </Head>

      <Header/>
      {props.children}
    </Container>
  );
};
```

Company.js:

```
const mongoose = require('mongoose');
const bcrypt = require('bcrypt');
const saltRounds = 10;
//Define a schema
const Schema = mongoose.Schema;
const CompanySchema = new Schema({
  email: {                                //mail of the company
    type: String,
    required: true
  },
  password: {                             //password of the company
    type: String,
    required: true
  }
});
// hash user password before saving into database
CompanySchema.pre('save', function(cb){
  this.password = bcrypt.hashSync(this.password, saltRounds);
  cb();
});
module.exports = mongoose.model('CompanyList', CompanySchema);
```

Voter.js

```
const mongoose = require('mongoose');
const bcrypt = require('bcrypt');
const saltRounds = 10;
//Define a schema
const Schema = mongoose.Schema;
const VoterSchema = new Schema ({
  email: {
    type: String,
    required: true,
  },
  password: {
```

```
    type: String,  
    required: true  
  },  
  election_address: {  
    type: String,  
    required: true  
  }  
});  
// hash user password before saving into database  
VoterSchema.pre('save', function(cb) {  
  this.password = bcrypt.hashSync(this.password, saltRounds);  
  cb();  
});  
module. exports = mongoose.model('VoterList', VoterSchema)
```

B. SCREENSHOTS

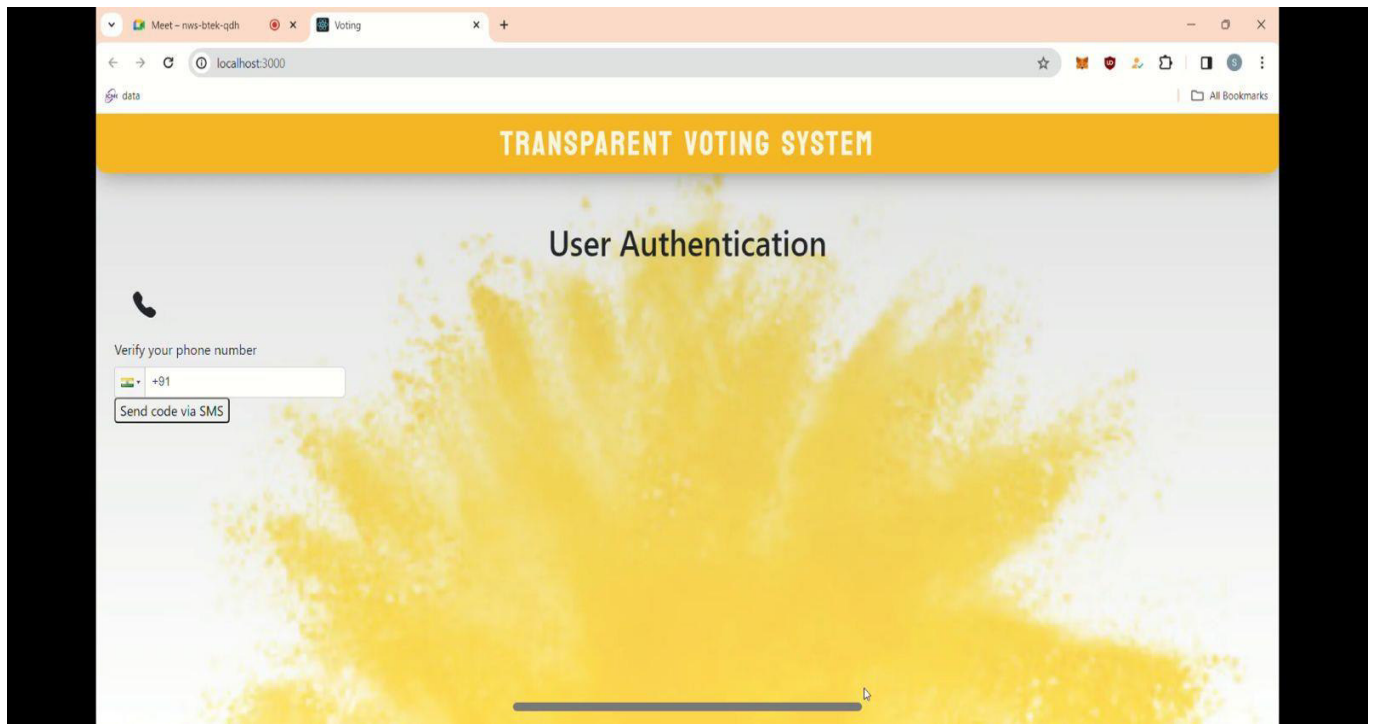


Figure B.1 Login Page

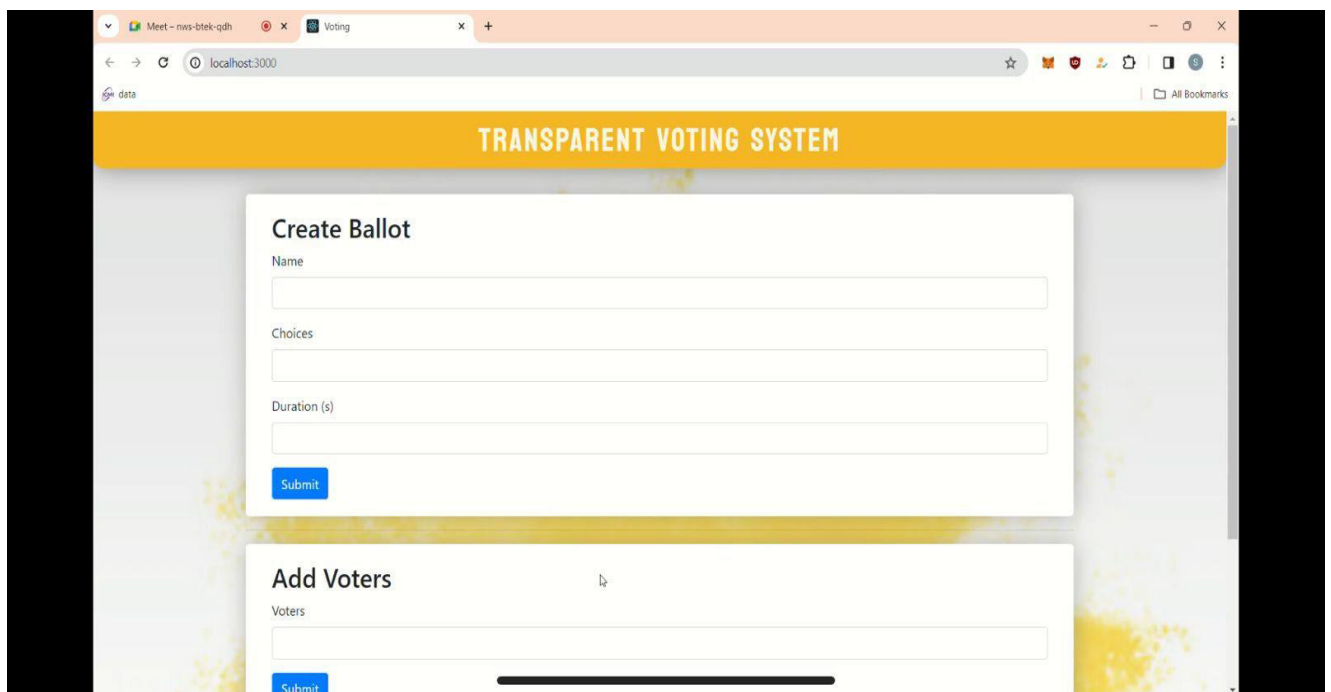


Figure B.2 Create Ballot

C. RESEARCH PAPER

Blockchain Voting System Develop Secure and Transparent Voting System

Dr.subathra G

Assistant professor, Department of
Computer Science Engineering
Sathyabama Institute Of Science and
Technology
Chennai, India
Subathra.cse@sathyabama.ac.in

Donthi Shashank

Student(U.G),Department of computer
science and Engineering
Sathyabama Institute of Science and
Technology
Chennai, India
shashankdonthi999@gmail.com

B.Sai Krishna Vardhan Reddy

Student(U.G),Department of computer
science and Engineering
Sathyabama Institute Of Science and
Technology
Chennai, India
vardhansai69@gmail.com

Abstract—The importance of democratic representation in any society has increased as scepticism of the standard voting method has risen. Citizens have witnessed the systematic violation of their most basic rights. Lack of openness has already been cited as a reason for challenges to other electronic systems for voting. The lack of reliability throughout most election systems makes it hard for governments to earn the confidence of their citizens. The vulnerability of the current information voting method is the main reason why it hasn't replaced paper ballots. The main goal is to rectify voting-related issues, whether they technical or due to voter apathy. To ensure a more equitable electoral process, block chain might be used. Both the existing physical voting systems and the proposed digital electoral systems have significant shortcomings that make them unsuitable for widespread use. This analysis evaluates the significance of finding a way to protect person's rights and liberties. In order to foster a credible connection between voters and election officials, this article introduces a block chain-based platform that boasts unparalleled openness and dependability. The proposed technology offers a framework for holding elections electronically via blockchain without the need for traditional polling places. Our suggested architecture allows for a wide variety of consensus methods to be used, making the blockchain scalable. Increased confidence in the integrity of voting transactions is provided by the use of the Chain Security Algorithm inside the electoral system. When performing a transaction on the blockchain, agreements offer a safe channel of b/w the customer and the network. There has been talk about the smart contracts polling system's safety. It's also been detailed how to protect the ledger from a 51percentage assault and how to encrypt operations using a hash code. Moreover, Block chain technology was used to build a system for conducting blockchain transaction throughout the voting process. Eventually, the examination of the suggested system's performance demonstrates that it may be used to a sizable population.

Keywords—Secure voting, cryptographic hash, blockchain, electoral system, E-Voting, polling.

I. INTRODUCTION

Beginning as a developing collection of blocks, each of which was cryptographically linked to the one before it, blockchain eventually evolved into its present-day form. A timestamp, a hash value, previous hash plus transaction data are all stored in each block. According

to the inventor, the created hash is a cryptography hash that may be produced in a variety of ways. With blockchain, all activities are quickly and, most crucially, permanently and verifiably recorded via a decentralized ledger. The primary characteristic of a blockchain is that after data has been entered to a ledger, it cannot be changed.

The blockchain-based electronic voting system can address several issues with the present ballot-based voting system. The permanent feature of blockchain can deter vote rigging, which is now impossible to prove to the public. Other irregularities, such as not verifying the vote count, interfering with the voting devices, manually casting votes, and intimidation during the voting process, may be reduced. The research of blockchain reveals its potential to increase the trustworthiness of the voting process. The decentralised network that the block chain uses contains many nodes that are linked to it. Each node has a unique replica of the ledger, which contains each operation that has occurred from the beginning. With a mentor relationship, no one user has access to the entire network. This relies on the bulk of nodes accepting the transaction. Nobody is able to identify the voter thanks to the way blockchain operates.

Switching from the present ballot-based method towards electronic voting might offer substantial benefits such intrinsic secrecy, dependability, greater visibility, and data integrity because elections confidentiality is a subject of national concern. The audience would have clear accountability if these methods & procedures were to be developed, putting the entire decentralised system's election system in their hands. Each operation would also be transparent and irreversible. Across many situations, you need a reputable government entity to confirm the operation of the entire system. NGOs, that work in the interests of people, may perform this function. Additionally, they organize efforts to combat vote rigging. While looking through these papers, we see a variety of ideas and beliefs, each with a unique strategy for achieving the before mentioned objectives. Using the Solidity programming language, a number of frameworks, including Razor & Ethereum, are created. many ideas, such as third-party verified systems, E2E, receipt-free voting with the creation of several blockchain-related protocols. There are concerns regarding the validity of the votes as a result of all the security precautions. Public key encryption, enables very authentications, as detailed in the articles mentioned down.

Discussion of the entire system takes place throughout a number of stages or levels. Each layer and the operations

among them may be protected with correct system architecture.

Additionally, several papers highlight the drawbacks of the structures and ideas that are explored, including potential security holes. Additionally, several of the methods outlined might be confusing for voters and need to be greatly simplified before being put into practice.

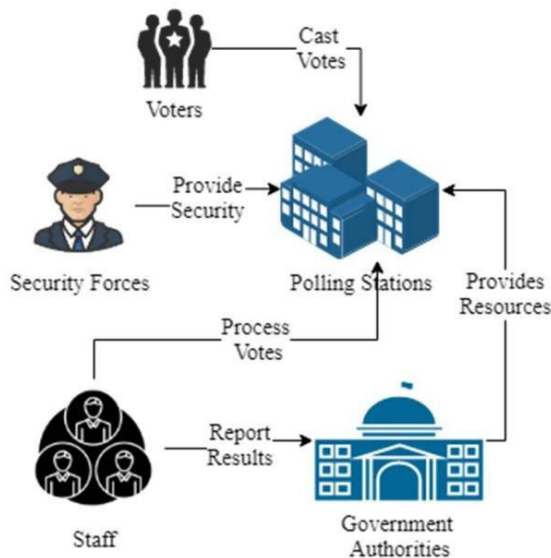


Fig.1. Conventional Voting Procedure

II. LITERATURE REVIEW

Significant facets of the many approaches addressed in early studies are mentioned here.

Robbiei Sympson (2018) propose the receipt-free, electorate approach that can reassure people that their ballots have been counted accurately. In addition, this method design eliminates the possibility of voters being influenced by improper means, such as bribery or threat of violence. In this work, we explore the possibility of employing a documentation as a testimony to a valid vote in a private voting booth. With the help of this witness, each voter may be certain that their ballot was accurately counted [1].

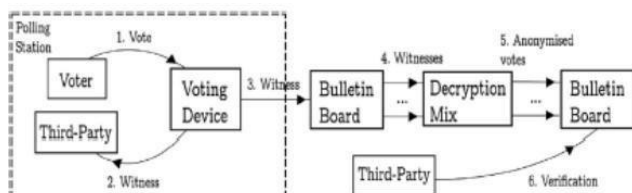


Fig.2. External Party's Receipt-Free Procedure

Rivest & Adida[5] propose an encryption technique that covers the entire election procedure known Scratch and Vote to reduce the need for intermediaries. On the other hand, they recommend enlisting the aid of "helping parties,"

such as Ngo & campaigners, to ensure that voters' ballots are properly validated and to assist with any other voter-validation procedures that may be necessary.

Similarly, to blockchain, Smith and Rivest [3] present a paper-based authentication system where the following voter receives the receipts of the preceding voter. This receipt will be used throughout the election system as proof that the vote was cast. It's very much like a blockchain in that it includes a hash of the preceding block's transaction to ensure the data hasn't changed.

Neuman [7] suggest using external websites and applications to validate votes [8] in an electronic voting system that is conducted remotely. This offers voters the assurance that their ballots have been received and will be tallied.

In 2017, Friorik P. Hjalmarsen, et al., assessed the viability of using blockchain as services in the development of an electronic polling approach. The foregoing is some of the paper's basic ideas: To (i) investigate preexisting integrating technologies amenable to the improvement of ledger e-polling approaches, and (ii) suggest a blockchain-based electronic voting platform that employs "permission" based blockchain" to allow flexible democratization. [2]

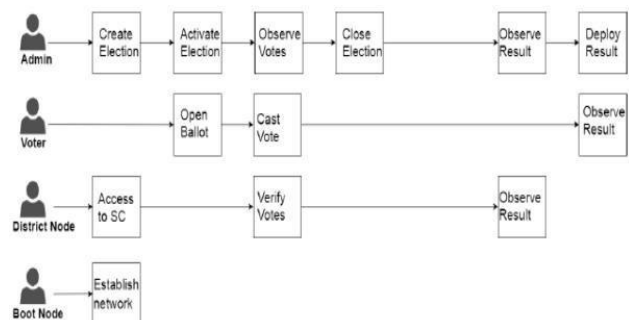


Fig.3. Phases in Polling

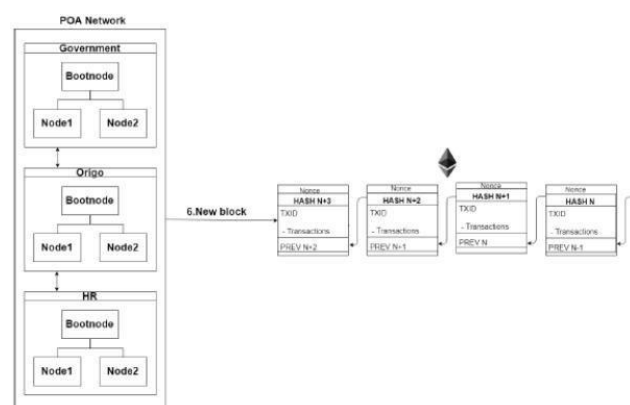


Fig.4. Eth Chain Architecture

To this objective, Yi Liue (2017) explore at the concept of electronic voting procedures & suggest a blockchain-based system. Details how different methods, such as blind signing, are put to use. This article details the three distinct

stages of public blockchain: which was before polling, during voting, and after the results have been certified. [4]

The blockchain-based electronic voting scheme proposed by Freyah Sher. (2016) not only satisfies the fundamental requirements of electronic voting additionally, it is decentralized to some extent, ensuring that as much process control as possible is given to the voting public.[6].

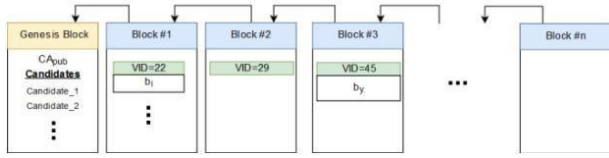


Fig.5. Description of a block

In their proposal for an unrestricted voting machines mechanism on network, Baocheng Wang et al. (2018) make use of smart contracts to store, monitor, compute, & check operations, with the top node pushing the agreement onto the block - chain. In order to safeguard voters' freedom of information and anonymity, the article goes on to explain the concept of a "one-time signature" and encrypting. [9]

III. PROPOSED SYSTEM

As opposed to previous frameworks, allows for data to be modified at any time without the need for an administrator's intervention. If votes are recorded in such a platform, then anybody with access to the system may change or remove those votes.

Using block chain, this isn't the case. After block being linked to the network, a block can't be altered in any way. After a strike on a node, the other nodes in the network will notice and repair it, making the chain unchangeable. Given that the ledger is distributed, the voting mechanism is not reliant on any one server. Even if some of the nodes are targeted or go down, the voting process may continue as normal. You can count on it to hold up in the worst of circumstances.

	VMS	[14]	[15]	[16]	[17]
Flexible Consensus Algorithm	✓	✗	✗	✗	✗
Attack 51%	✓	✗	✗	✗	✗
Chain Security Algorithm	✓	✗	✗	✗	✗
UTXO	✓	✗	✗	✗	✗
Smart Contract	✓	✗	✗	✗	✓

Fig.6. Comparison of Previous system and proposed methodology

A. Design Of Voting Systems

The Ui of the software is the initial portion of the system's operation, and thus needs front-end protection. User

credentials are entered on that interface, thus it must be safe and easy to use. Every voter has equal and unrestricted access to the electoral process. Furthermore, it allows for auditability of each vote cast. The voter uses his ID to sign up for the system. Voter registration in VMS is based just on voter's ID information, which is then checked against the electorate's public document in IA's online database.

To enter the system, the user must enter a one-time password. When a voter needs to access the Voter Management System they must first establish a one-time password. VMS records every aspect of a voter's participation. Each valid voter receives one VC in their account upon registration process. Voters are only allocated one VC to reduce the possibility of their casting duplicate ballots.

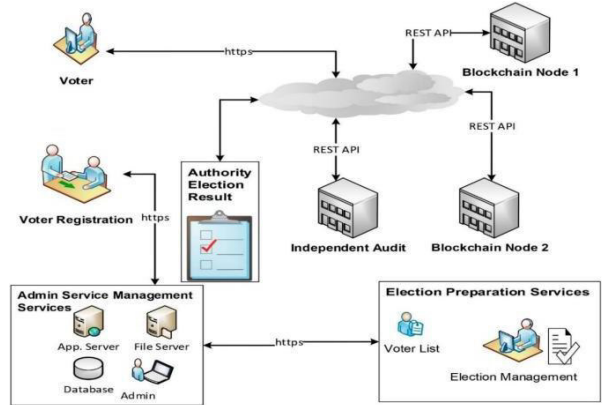


Fig.7. Our Architecture

B. Work Flow

After the voter passes the verification, they will be added to the Voting Control System. The blockchain operates as a single chain system. The integrity of the voters' votes is safeguarded by the system's integration with the country's central voter database. Every time someone casts a ballot, a record is created in a database linked to their National ID. The minors then mine the transaction and record it on the distributed ledger. Vote Coins stored in the voter's wallet are used when the voter casts his ballot. If a voter uses up their only vote coin, they are not allowed to vote again with that currency. Once the voter logs in with his or her credentials, he or she is sent to the election interface, where he or she may see profiles for each candidate running for office in his or her district. When a voter requests to cast a ballot, VMS confirms his or her eligibility to vote via a comparison of the electorate's digital ID to a digest of all prior blockchain operations.

The voter makes his choice and casts his ballot for that candidate. The miner uses digest to perform the transaction and verify its success. As soon as the node is linked to the chain, voting may begin.

To cast a ballot, voters need just a mobile device or online computer. To ensure that the voter interface is accessible to as many people as possible, it will be made available in

more than one language. When voting, the suggested approach can accommodate a high number of participants. A voter in a blockchain election might be located anywhere in the globe. One may vote from abroad by using a digital National ID that is confirmed against a national database.

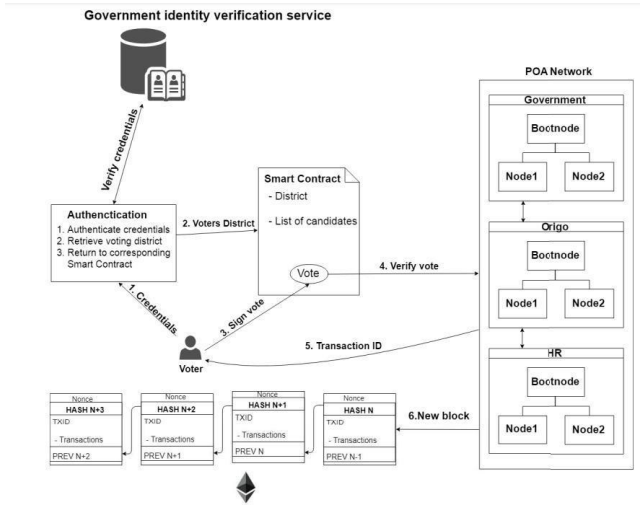


Fig.8. Voting Process of our method

Whenever a vote is cast, the transaction is transferred to a pool where miners examine it and, if necessary, eliminate the fraudulent request by polling other nodes for consensus. A cryptographic hash completely protects the votes. As an added security measure, the system limits each user's vote casting to a single vote coin. Therefore, the mechanism guarantees that no voter has cast a duplicate vote even if the balance of the voting currency is not updated. If a miner determines that a node's request or a voter's transaction hash does not match the electorate's virtual ID, the miner will immediately reject the request or node as malicious. When a new element is successfully added to VC, a Message is delivered to the citizen's mail & contact number to let him know. After casting his ballot, the voter receives a unique reference hash that may be used to confirm his selection using a web interface; after this is done, voter's selection is linked to total tally. After a valid vote has been casted, the voter's voting currency will be depleted.

C. Algorithm used

Blockchains of any size are feasible under the proposed paradigm. Consensus methods may be easily plugged in and used with this system. Even though the PoW method is offered by default to maintain the blockchain efficient during voting activity, the framework allows the use of any of the other existing consensus mechanisms, which may be selected by the user prior to the blockchain's implementation. The Proof of Work protocol verifies that sufficient computing resources were allocated to a transaction. Because of the framework's adaptability, new consensus methods may be added dynamically.

It aids in maintaining the integrity of the blockchain and prevents any interruptions to the voting process. A blockchain's optimal performance in use may be ensured by selecting an appropriate consensus algorithm upon

implementation. Here, the computational power needed by the system is revealed by using Proof of Stake to validate random nodes. Node participation inside the voting chain is instantly revoked if it is found to be verifying a fraud claim. Such nodes' transactions are rejected.

D. Layered Structure of our system

The suggested framework is laid up in a hierarchical fashion with distinct layers. Together all dAAPs made for electors and management may be found in the interlayer. All stakeholders may access VMS using these widely available APPs. This layer's purpose is to offer a means of engaging with the system. The Application Layer integrates third-party services to verify the identity of its users. Essentially, it is the face of the whole voting process. It encases voting system information in server-based databases. In addition, this layer processes all blockchain transactions. The voter's eligibility to cast a ballot in this election has been confirmed by the user's National ID.

Most importantly, the framework relies on the Trust layer. Using smart contracts, it guarantees that the right decisions are taken at the meeting of minds and that the data is transmitted safely. Each new element sent to the network is checked for accuracy.

The blockchain layer stores the most fundamental data about the blockchain and monitors for any broken links in the chain to guarantee its integrity. This layer is where all the data processed and private keys are kept. All financial dealings between the VMS and the electorate conducted through smart contracts are included in this tier.

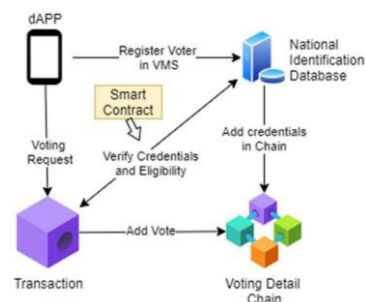
The transaction layer is where all mining activity occurs.

The security feature is the most vital since it prevents harm to the blockchain. Security algorithms and ground rules are used to prevent attacks from outside parties.

The security procedures are applied throughout the whole chain. All communications and data are encrypted and protected thanks to the keys.

IV. OUR DESIGN

Our blockchain-based election process is constantly monitored and updated to ensure fair and secure elections. Each voter's transactional hashes are recorded, along with the final tally of the poll, which can then be accessed by users on their own dashboards. The system evaluates the voter's citizenship and determines if someone has previously participated before allowing them to vote if his VC has not yet expired. Participant IDs, votes, and timestamps are recorded on the blockchain after a vote has been verified.



V. CONCLUSION

To convince citizens that their votes would be counted as cast, advocates of a blockchain-based approach say they need to establish a sense of trust between both the citizen and the government. As a result, citizens are more likely to feel a sense of belonging to and pride in their democratic state. The voting system desperately needs blockchain technology to increase its degree of dependability, transparency, and confidence, and this architecture describes the characteristics, activities, and roles of relevant authority utilising blockchain technology in the electoral system. Each vote is irreversible since it is verified. A voter's anonymity is protected by hash, and the authorities' ability to exert tight control over the process is ensured through the employment of private keys and public keys.

Hackers are hindered in their attempts to alter or access vote information thanks to the auditability of the system. It guarantees that each voter's vote counts equally. This system's usability excels because it takes the more efficient method of creating a versatile consensus algorithm to cut down on the blockchain's excessive computational demands. Voters are more likely to put their faith in the system if they see it acting in a trustworthy, open manner. Every moment a block is linked to the network, the CSA checks to make sure it still meets the chain's validity requirements. With the use of smart contracts, the blockchain election system may be secured against fraudulent and incomplete transactions.

The suggested approach provides authorities and voters with a safe, open, and trustworthy environment. The results of the suggested framework's performance assessment of block chain in VMS are encouraging. This experiment demonstrates that even when dealing with a huge no. of transactions, the system maintains its efficiency.

REFERENCES

- [1] Chaum D , Essex A , Carback R . Scantegrity: end-to- end voter-verifiable optical-scan voting. IEEE Security & Privacy; 2008 .
- [2] Friðrik Þ. Hjálmarsson, Gunnlaugur K. Hreiðarsson . Blockchain-Based E-Voting System
- [3] Rivest RL , Smith WD . Three voting protocols: ThreeBallot, VAV, and Twin. EVT'07 Electronic Voting Technology Workshop. Boston, MA: USENIX/ACCURATE; 2007 .
- [4] Yi Liu and Qi Wang . An E-voting Protocol Based on Blockchain
- [5] Adida B , Rivest R . Scratch & vote. In: Proceedings of the 5th ACM Workshop on Privacy in Electronic Society; 2006. p. 29–39 .
- [6] Freya Sheer Hardwick, Apostolos Gioulis, Raja Naeem Akram, and Konstantinos Markantonakis . E-Voting with Blockchain: An E-Voting Protocol with Decentralisation and Voter Privacy, arXiv:1805.10258v2 [cs.CR] 3 Jul 2018
- [7] Neumann S , Olembo MM , Renaud K , Volkamer M . Helios verification: To al-leviate, or to nominate: Is that the question, or shall we have both?. In: Proceedings of the International Conference on Electronic Government and the Information Systems Perspective; 2014. ISBN 9783319101774 .
- [8] Adida B . Helios: Web-based Open-Audit Voting. In: Proceedings of the 17th USENIX Security Symposium; 2008. p. 335–48 .
- [9] Baocheng Wanga,, Jiawei Suna, Yunhua Hea, Dandan Panga, Ningxiao Lua . Large-scale Election Based On Blockchain . IIKI2017, 10.1016/j.procs.2018.03.063
- [10] Prachi Shriram Gurav. E-Voting System. ISSN: 2321-8169,2017.
- [11] A. Barnes, C. Brake, and T. Perry. Digital Voting with the use of Blockchain Technology Team Plymouth Pioneers- Plymouth University. Accessed: Feb. 14, 2022. [Online]. Available: <https://www.economist.com/sites/default/files/plymouth.pdf>
- [12] J. Huang, D. He, M. S. Obaidat, P. Vijayakumar, M. Luo, and K.-K.-R. Choo, “The application of the blockchain technology in voting systems: A review,” *ACM Comput. Surv.*, vol. 54, no. 3, pp. 1–28, Apr. 2022, doi: 10.1145/3439725.
- [13] F. Fusco, M. I. Lunesu, F. E. Pani, and A. Pinna, “Crypto-voting, a blockchain based e-voting system,” in *Proc. 10th Int. Joint Conf. Knowl. Discovery, Knowl. Eng. Knowl. Manage.*, 2018, pp. 223–227, doi: 10.5220/0006962102230227.
- [14] G. Rathee, R. Iqbal, O. Waqar, and A. K. Bashir, “On the design and implementation of a blockchain enabled E-Voting application within IoT-oriented smart cities,” *IEEE Access*, vol. 9, pp. 34165–34176, 2021, doi: 10.1109/ACCESS.2021.3061411.
- [15] M. Pawlak, A. Poniszewska-Marańda, and N. Kryvinska, “Towards the intelligent agents for blockchain e-voting system,” *Proc. Comput. Sci.*, vol. 141, pp. 239–246, Jan. 2018, doi: 10.1016/j.procs.2018.10.177.
- [16] D. Chaum, A. Essex, R. Carback, J. Clark, S. Popoveniuc, A. Sherman, and P. Vora, “E-voting 40 scantegrity: End-to-end voter-verifiable optical-scan voting,” *IEEE Secur. Privacy*, vol. 6, no. 3, pp. 40–46, May 2008. Accessed: Feb. 14, 2021. [Online]. Available: <https://www.computer.org/security/>
- [17] P. McCorry, S. Shahandashti, and F. Hao, “A smart contract for boardroom voting with maximum voter privacy,” in *Financial Cryptography and Data Security*. Sliema, Malta: Springer, 2017, pp. 357–375, doi: 10.1007/978-3-319-70972-7_20.



SATHYABAMA



INSTITUTE OF SCIENCE AND TECHNOLOGY
(DEEMED TO BE UNIVERSITY)
CATEGORY-1 UNIVERSITY BY UGC
Accredited 'A++' Grade by NAAC (I2B Status by UGC) Approved by AICTE



www.sathyabama.ac.in

SCHOOL OF COMPUTING

Department of Computer Science and Engineering

Certificate of Presentation

This is to certify that

D. SHASHANK

of

Sathyabama Institute of Science and Technology

has presented a paper entitled

Blockchain Voting System Develop and Transparen + voting system

in the

International Conference on Cognitive Computing and Artificial Intelligence (ICCCAI-2024) in association with
Taylor's University, Malaysia held on 7th & 8th March 2024.

Dr. Sayan Kumar Ray
Head, School of Computer Science
Taylor's University

Dr. L. Lakshmanan
HOD, CSE Dept
Sathyabama Institute of Science and Technology

Dr. T. Sasikala
Dean, SOC
Sathyabama Institute of Science and Technology