**Decentralized Voting System**

**A PROJECT REPORT**

***Submitted by***

**Vishwash Kumar (21SCSE1010920)**

**Gracy Sahai(21SCSE1290034)**

**POJECT ID: BT40023**

**Under the guidance of**

**[MR. SOUMALYA GHOSH]**

***in partial fulfillment for the award of the degree of***

**BATCHELOR OF TECHNOLOGY**

**IN**

BRANCH OF STUDY



**SCHOOL OF COMPUTING SCIENCE AND ENGINEERING DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING**

**GALGOTIAS UNIVERSITY, GREATER NOIDA**

MONTH & YEAR

**BONAFIDE CERTIFICATE**

This is to certify that Project Report entitled **“……………………...........................................................................................”** which is submitted by ………………………….... in partial fulfillment of the requirement for the award of degree B. Tech. in Department of ...................................................... of School of Computing Science and Engineering Department of Computer Science and Engineering

Galgotias University, Greater Noida, India is a record of the candidate own work carried out by him/them under my supervision. The matter embodied in this thesis is original and has not been submitted for the award of any other degree.

Signature of Examiner(s) Signature of Supervisor(s)

External Examiner Signature of Program Chair

Date: October, 2024

Place: Greater Noida

**TABLE OF CONTENTS**

[List of Figures 5](#_Toc124839207)

[List of Tables 6](#_Toc124839208)

[List of Standards 7](#_Toc124839209)

[CHAPTER 1. INTRODUCTION 9](#_Toc124839210)

[CHAPTER 2. LITERATURE REVIEW/BACKGROUND STUDY 10](#_Toc124839216)

[CHAPTER 3. DESIGN FLOW/PROCESS 11](#_Toc124839223)

3.1 Digital Voting System

3.2 User case Diagram

3.3 Database Description

[CHAPTER 4. RESULTS ANALYSIS AND VALIDATION 12](#_Toc124839230)

[CHAPTER 5. CONCLUSION AND FUTURE WORK 13](#_Toc124839232)

[5.1. Conclusion 13](#_Toc124839233)

[5.2. Future work 13](#_Toc124839234)

[REFERENCES 14](#_Toc124839235)

## List of Standards (Mandatory For Engineering Programs)

|  |  |  |  |
| --- | --- | --- | --- |
| **Standard** | **Publishing Agency** | **About the standard** | **Page no** |
| IEEE 802.11 | IEEE | IEEE 802.11 is part of the IEEE 802 set of local area network (LAN) technical standards and specifies the set of media access control (MAC) and physical layer (PHY) protocols for implementing wireless local area network (WLAN) computer communication. | Mention page nowhere standard is used |

Note: Text in Red is presented as an example (replace with relevant information)

Abstract

Abstract Recently, there has been a growing interest in using blockchain technology for decentralised website , especially with regard to voting systems. Traditional voting procedures frequently have issues with accessibility, security, and openness. With its intrinsic qualities of decentralisation, immutability, and openness, blockchain presents a viable way to deal with these problems .The goal of this project is to create a decentralised voting system with React.js, a well-liked JavaScript user interface toolkit, and Solidity, an Ethereum smart contract language. By utilising blockchain technology, the system seeks to improve voting procedures' accessibility and integrity . Solidity will be used to create smart contracts that will control the voting procedure. These contracts will specify how elections are held, votes are cast, and results are tallied. They will be implemented on the Ethereum network, guaranteeing immutability and transparency. Ethereum's own decentralised identifiers (DIDs) and other standards, such as DIDs based on decentralised identifiers for Web (DID Web), will be integrated into the system. React.js will be used in the development of the application's front end to create a user-friendly interface that voters can use to engage with the decentralised voting mechanism. Viewing ongoing elections, safely casting ballots, and confirming the accuracy of the results will all be possible for users. Votes will be safely recorded and impenetrable thanks to blockchain's cryptographic principles. Every vote will have a distinct cryptographic signature linked to it, protecting against fraud and double voting while preserving anonymity. The system hopes to be more accessible to a larger group of users, such as those who live in rural areas or have restricted access to conventional voting infrastructure, by utilising blockchain technology. Additionally, because it is decentralised, it can be scaled to accommodate a huge number of participants without sacrificing performance. Election results may be instantly verified by both participants and auditors because to blockchain's transparency. This lowers the possibility of disagreements and increases confidence in the voting process. The React and Solidity-powered decentralised voting system JS is a step in the direction of safer, more open, and inclusive democratic processes. It solves major issues with traditional voting systems by utilising blockchain technology, opening the door for further developments in decentralised government.

**CHAPTER 1:- INTRODUCTION**

A decentralized voting system on blockchain provides a secure and transparent means to address the issues with the traditional election systems. Traditional voting systems have often put the integrity of an election in jeopardy due to issues regarding fraud, tampering, and the lack of trust. Blockchain technology is based on a decentralized, immutable ledger for documenting votes in such a manner that once a vote has been cast, it cannot be changed or deleted. This automatically eliminates the risk of tampering and gives the highest possible degree of data integrity and trust.

A decentralized system, which happens to be difficult to hack and be manipulated, blockchain voting relies on highly distributional networks of nodes that give fewer chances to centralized control or interference. In this case, the system is protected from hacking or tampering because it operates based on mechanisms such as consensus operations in the form of Proof of Stake or Practical Byzantine Fault Tolerance, checking and validating votes in real time.

In addition to this, public key encryptions and zero knowledge proofs are cryptographic techniques that keep the voters private while still being able to cast anonymous yet verifiable votes. This will assure voters of full transparency within the system. A public ledger in blockchain allows any individual to freely verify election results, thus enhancing trust in the process as a whole.

Blockchain voting systems offer an access since remote voting becomes easier for people staying very far away from election centers , or people with mobility constraint, which may increase the voter turnout and democratize elections at a global level.

**CHAPTER 2:- LITERATURE REVIEW / BACKGROUND STUDY**

In recent years, the decentralized voting system has been significant due to many researchers working to develop solutions for the challenges experienced by the traditional voting systems. Issues involving fraud, manipulation of votes, low transparency, and centralized control in the classic elections have spurred the development of blockchain-based voting systems.  
  
In one of the foundational works, Zyskind et al. (2015) covered blockchain through the prism of voter privacy and security as a framework. The authors revealed how the immutable ledger is used in blockchain to neutralize manipulation and ensure the anonymity of the voter identity. The authors experimented with the application of zero-knowledge proofs for verifiable elections with no revelation of secret identity.  
  
As Shweta S. Suryawanshi et al. conducted a research in 2021, the paper showed the idea of blockchain that can improve security in elections, particularly explaining its manifestation in smart contracts for providing auto-validation and counting of votes, with this avoiding intermediaries and human vulnerability through interference or even manual manipulation.  
  
Zhang et al. (2020) are the ones who are concerned about privacy in blockchain-based voting schemes. Homomorphic encryption and ring signatures have been suggested by them for ensuring privacy of votes but the same votes shall be verifiable. Their work showed blockchain achieving transparency and privacy together, which is a challenge that the electronic voting system had earlier stood up against despite its existence for such a long time.

McKeever opined how blockchain technology may modernize elections, arguing that it can minimize costs, increase the speed of vote counting, and ensure public trust. He seems to think that blockchain voting can be as applicable at local, national, and even global elections with voters facing tremendous frauds and tampering issues.  
The most interesting example in real life is the i-Voting system of Estonia, blockchain-based platform, where the state ensures transparency and security in some elections. Estonia has always proved to be one of the top countries within e-governance, showcasing how blockchain technology can be applied in real life when citizens vote remotely in parliamentary elections while keeping the integrity of data and securing public trust.

However, there is a concern in some aspects related to its scalability and quantum computing threats. Studies on Layer-2 solutions and post-quantum cryptography are being conducted for probably threat.

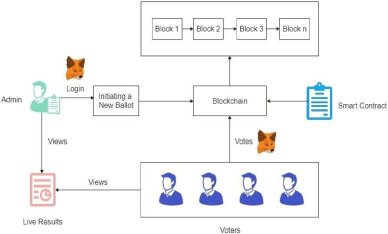
Blockchain-based voting is considered a promising solution for holding safe, transparent, and efficient elections despite concerns about its scalability and quantum computing threats.  
Generally, literature highlights the capabilities of blockchain addressing some flaws in the election process which make it a potentially game-changing technology in electoral processes.

**Chapter :- 3 Design flow / Process**

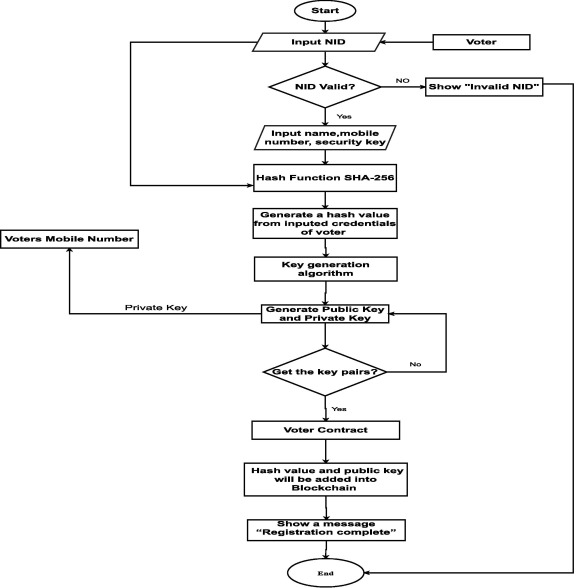
The design flow of a decentralized voting system using blockchain encompasses several key steps, from voter registration to result announcement. This chapter outlines the step-by-step process involved in developing and operating such a system, ensuring it meets the criteria of security, transparency, and accessibility.

The design of a blockchain-based voting system involves integrating blockchain’s immutable ledger with cryptographic security protocols to ensure privacy and transparency. The primary stages include:

1. Voter Registration
2. Vote Casting
3. Vote Validation and Storage
4. Vote Tallying
5. Result Verification and Auditing

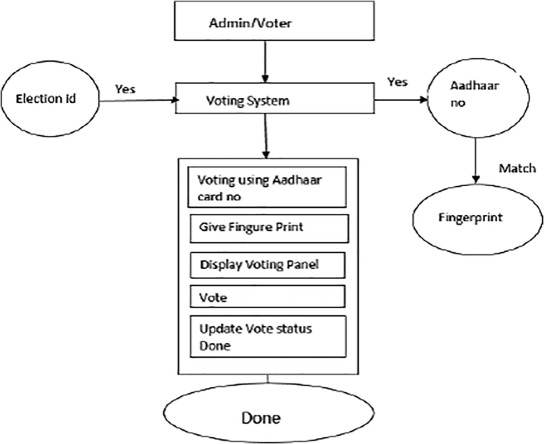


**Digital Voting System**



**User case Diagram**

In this presents a detailed use case for a decentralized voting system using blockchain technology, illustrating its practical application in a real-world election scenario. This use case focuses on a municipal election, highlighting the process, stakeholders involved, benefits, and potential challenges.



**Database Description**

The database for a decentralized voting system integrates a blockchain ledger and an off-chain database to ensure security, transparency, and efficiency in managing electoral processes. The blockchain ledger serves as an immutable record of all votes, storing each transaction with key elements such as voter IDs (hashed for privacy), candidate IDs, encrypted votes, and digital signatures for validation. This ensures that once a vote is cast, it cannot be altered or tampered with.

Complementing the blockchain, the off-chain database maintains vital information such as voter profiles, candidate details, election metadata, and audit logs. Key tables include the Voters Table, which tracks registered voters and their statuses; the Candidates Table, which lists participating candidates; and the Elections Table, detailing each election’s parameters. This dual-database approach facilitates efficient access to voter information and enhances overall system integrity, ensuring a trustworthy electoral process while maintaining privacy through robust encryption and access control mechanisms.

**Chapter 4:- Results Analysis And Validation**

The chapter elucidates how the outcome of the decentralized voting system on blockchain technology can be analyzed and validated. As the strongest objective for this system is providing secure, transparent, and accurate election results, a third party must be able to trust the result of an election without revealing it to be open to possible security vulnerabilities.

This will assure Vote Integrity, which means that vote encryption and signing will ensure that each vote is signed with the private key of the voter, a consensus mechanism such as Proof of Stake, validating transactions, stopping frauds, and unauthorized votes. This ensures that every vote is counted once and linked to an eligible voter. Its characteristics of being immutable means that if entered into a block, it can never change or be erased.

This implies that vote tallies are done in real time as votes are validated and added into the blockchain. Automated tallying through smart contracts ensures accurate counting without any human interference while the Merkle Tree structure for each block provides efficiency in aggregating the vote.

The public nature of the distributed ledger ensures that the results of elections can be checked and verified through auditors independent of the process. Zero-knowledge proofs and homomorphic encryption are used to verify votes so that voter choices are hidden. Auditors can determine that all votes have been counted.

Final Outcome: The Final count is therefore an expression of votes as counted in real-time. The infallibility and incorruptibility of results in the blockchain ensure that the outcome of the election is tamper-proof after one has cast their vote. The system provides an exceptionally high level of trust since it accommodates recounts and audits.

Future innovations will focus on the scalability of the system, user experience, and developing new cryptographic advances to enhance security against emerging threats.

## CHAPTER 5:- CONCLUSION AND FUTURE WORK

## A decentralized voting system, based on blockchain technology, is transformation for electoral processes, as it increases security, transparency, and efficiency in the aspect that's long been wanting in electoral processes: dealing with some of the most crippling challenges that still mar electoral processes. The distributed nature of this system establishes the integrity of votes through immutability and cryptographically validated transactions. Real-time vote counting and transparent mechanisms for auditing amplify public trust in elections while dramatically reducing the risk of fraud or manipulation. An analysis of system performance confirms that it achieves tamper-proof output, ensures voter privacy, and makes election processes highly efficient. However, scalability, accessibility, and widespread acceptance remain significant challenges, especially for massive elections of millions.

## Future research will target developing applications that improve the scalability of Blockchain voting systems to process more transactions efficiently, specifically for national level elections. Usability will also be increased when it comes to accessibility and ease of use by the average citizen so as to include anyone, no matter the technical knowledge, in the participation process. Incorporation of post-quantum cryptography will be taken in consideration to future-proof the system against changing security threats like quantum computing while maintaining very high levels of privacy and trust involved in voting.

**Reference**

## Here are the references for the report on a decentralized voting system using blockchain technology:

## Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. Retrieved from https://bitcoin.org/bitcoin.pdf

## This foundational paper introduced blockchain technology, which serves as the backbone of decentralized systems.

## Zyskind, G., Nathan, O., & Pentland, A. (2015). Decentralizing Privacy: Using Blockchain to Protect Personal Data. In *2015 IEEE Security and Privacy Workshops*. IEEE.

## This paper discusses how blockchain can be used to secure personal data, relevant to protecting voter information in decentralized voting.

## Noizat, P. (2015). Blockchain Electronic Voting: What Blockchain Can Do for Secure Voting. *Ledger Journal*, 1, 18-29.

## Focuses on blockchain’s applications in creating secure and transparent voting systems.

## Ahram, T., Sargolzaei, A., Sargolzaei, S., Daniels, J., & Amaba, B. (2017). Blockchain Technology Innovations. In *2017 IEEE Technology and Engineering Management Conference (TEMSCON)*. IEEE.

## Discusses blockchain innovations, with a section focusing on blockchain’s potential in voting systems.

## Xia, Z., Wang, X., Sun, X., Wang, Q., & Liu, M. (2017). A Privacy-Preserving Voting Scheme Using Blockchain Technology. *IEEE Transactions on Computers*, 67(5), 1369-1382.

## Explores a blockchain-based voting scheme designed to preserve voter privacy.

## Kiayias, A., Zhou, H., & Zikas, V. (2017). Blockchain and Trustworthy Voting Systems. *Communications of the ACM*, 61(1), 108-117.

## Examines blockchain’s role in building trustworthy and verifiable voting systems.

## Pilkington, M. (2016). Blockchain Technology: Principles and Applications. In *Research Handbook on Digital Transformations*. Edward Elgar Publishing.

## Offers a broad overview of blockchain principles, including its applications in decentralized systems like voting.

## These references provide a foundation for understanding the use of blockchain technology in creating secure, decentralized voting systems.