**DECENTRALIZED VOTING APPLICATION USING BLOCKCHAIN**

# Declaration

The undersigned researchers and contributors, declare that the study on a Decentralized Voting System using Blockchain (Ganache, MetaMask), React, and MySQL represents our genuine efforts and contributions to advancing knowledge in the field of digital governance and blockchain applications. Through rigorous investigation and analysis of primary data from user surveys and blockchain transaction logs, alongside secondary data from academic sources, this study aims to provide valuable insights into the feasibility, challenges, and implications of decentralized voting technologies.

Our findings underscore the transformative potential of blockchain technology in enhancing voter confidence, transparency, and security in electoral processes. It acknowledges the limitations and constraints inherent in this research, including sample size considerations, methodological constraints, and the specificity of technologies utilized.

This declaration affirms our commitment to academic integrity, ethical research practices, and the pursuit of knowledge for the betterment of democratic governance worldwide. It hopes that our findings will inspire further research, innovation, and collaboration among stakeholders—government entities, technology developers, civil society organizations, and voters—to realize the full potential of decentralized voting systems in promoting transparent and inclusive democratic practices.

Signed,

Faraz Saeed Khwaja

# Ethical Review

The ethical considerations in developing and deploying a Decentralized Voting System using blockchain technologies like Ganache, Meta Mask, react programming language, and MySQL database are paramount. Adherence to principles of transparency, non-discrimination, and privacy is crucial. Transparency ensures the public understands how their information is collected, managed, and utilized within the blockchain, fostering trust and confidence in the system.

Protecting voter data from unauthorized access or misuse is essential to maintaining privacy and security. Voter anonymity must be preserved, and robust security measures are necessary to prevent cheating. Informed consent is critical, requiring participants to be fully aware of how their data will be used and protected.

The research emphasizes inclusivity, ensuring the voting system accommodates all eligible voters, regardless of their ability to use technology or any disabilities. This aligns with political liberalism principles, guaranteeing the right to vote for all citizens.

The research follows a rigorous process of gaining ethical clearances and permissions from Institutional Review Boards (IRBs) or Ethics Committees to ensure compliance with established ethical guidelines. Regular ethical audits and independent oversight address emerging ethical issues in decentralized voting technologies.

By adhering to these ethical principles, the research aims to enhance the security, transparency, and fairness of the voting system, fostering public trust and upholding democratic tenets. This commitment to ethical research underscores the importance of respecting participant rights and welfare, ensuring the integrity of the research process.

# Abstract

This study investigates the effectiveness of a Decentralized Voting System developed using Blockchain (Ganache & MetaMask), React JS, and MySQL databases. The primary objective is to evaluate user satisfaction, system usability, security, and engagement within the voting system. The methodology includes user surveys and analysis of blockchain transaction records, supplemented by secondary data from peer-reviewed articles and industry sources. Results reveal high user satisfaction, with 85% of participants rating the system positively. The system's security is validated by the absence of security incidents in blockchain records. Technical proficiency influences system usability, with more tech-savvy users finding the system easier to use. Voting activity peaks in the evening, aligning with user engagement patterns. These findings support the effectiveness of blockchain in enhancing voting system security and usability, contributing valuable insights into decentralized voting technologies and their implications for future developments.

**Table of Contents**

[Declaration 2](#_Toc174044830)

[Ethical Review 3](#_Toc174044831)

[Abstract 4](#_Toc174044832)

[Chapter 1: Introduction 11](#_Toc174044833)

[1.1 Introduction 11](#_Toc174044834)

[1.2 Background 11](#_Toc174044835)

[1.3 Research Rationale 12](#_Toc174044836)

[1.4 Problem Statement 13](#_Toc174044837)

[1.5 Research Aim 14](#_Toc174044838)

[1.6 Research Objectives 14](#_Toc174044839)

[1.7 Research Questions 14](#_Toc174044840)

[1.8 Research Contributions 14](#_Toc174044841)

[1.11 Summary 15](#_Toc174044842)

[Chapter 2: Literature Review 16](#_Toc174044843)

[2.1 Introduction 16](#_Toc174044844)

[2.2 Considerations for Research Objectives 16](#_Toc174044845)

[2.2.1 Blockchain Technology in Electoral Systems 16](#_Toc174044846)

[2.2.2 Linking Blockchain Technology to Centralized Voting Systems 18](#_Toc174044847)

[2.2.3 Role of User-Friendly Interfaces in Enhancing Voter Engagement 18](#_Toc174044848)

[2.2.4 Integration of Smart Contracts in Automating Voting Processes 20](#_Toc174044849)

[2.2.5 Enhancement of Security Through Blockchain and Smart Contracts 21](#_Toc174044850)

[2.3 Theoretical Framework 21](#_Toc174044851)

[2.4 Literature Gap 22](#_Toc174044852)

[2.5 Summary 23](#_Toc174044853)

[Chapter 3: Research Purpose and Objectives 23](#_Toc174044854)

[3.1 Introduction 23](#_Toc174044855)

[3.2 Key Research Contribution 24](#_Toc174044856)

[3.3 Detailed Exploration of the Research Contributions 25](#_Toc174044857)

[3.3.1 Objective 1: Secure and Tamper-Resistant Voting System Using Blockchain 25](#_Toc174044858)

[3.3.2 Objective 2: User-Friendly Interfaces Using React.js 26](#_Toc174044859)

[3.3.3 Objective 3: Integration of Smart Contracts 26](#_Toc174044860)

[3.3.4 Objective 4: Comprehensive Evaluation 27](#_Toc174044861)

[3.4 Conceptual Framework 28](#_Toc174044862)

[3.5 Summary 28](#_Toc174044863)

[Chapter 4: Research Approach and Methodology 29](#_Toc174044864)

[4.1 Introduction 29](#_Toc174044865)

[4.2 Research Design 29](#_Toc174044866)

[4.3 Research Philosophy 29](#_Toc174044867)

[4.4 Research Approach 30](#_Toc174044868)

[4.5 Research Strategy 30](#_Toc174044869)

[4.6 Methodology 31](#_Toc174044870)

[4.6.1 Sampling Strategy and Sample Size Determination 31](#_Toc174044871)

[4.6.2 Data Collection Procedures and Instruments 31](#_Toc174044872)

[4.6.3 Data Analysis Procedures 32](#_Toc174044873)

[4.6.4 Ethical Considerations and Approvals 33](#_Toc174044874)

[4.7 Summary 34](#_Toc174044875)

[Chapter 5: Design and Implementation of Decentralized Voting Application 34](#_Toc174044876)

[5.1 Introduction 34](#_Toc174044877)

[5.2 Requirements for Designing the dApp 34](#_Toc174044878)

[5.2 Design 36](#_Toc174044879)

[5.3 Implementation 36](#_Toc174044880)

[5.5 Results 40](#_Toc174044882)

[5.6 Summary 41](#_Toc174044883)

[Chapter 6: Analysis of Primary and/ or Secondary Data 41](#_Toc174044884)

[6.1 Introduction 41](#_Toc174044885)

[6.2 Data Analysis 42](#_Toc174044886)

[6.2.1 Data Collection 42](#_Toc174044887)

[6.2.2 Data Description 43](#_Toc174044888)

[6.2.3 Data Analysis Methods 44](#_Toc174044889)

[6.2.4 Analysis and Interpretation 44](#_Toc174044890)

[6.2.5 Comparative Analysis 45](#_Toc174044891)

[6.2.6 Discussion 45](#_Toc174044892)

[6.3 Summary 46](#_Toc174044893)

[Chapter 7: Analysis of Findings and Development of Academic Discussion 46](#_Toc174044894)

[7.1 Introduction 46](#_Toc174044895)

[7.2 Findings 46](#_Toc174044896)

[7.2.1 Detailed Analysis of Findings 46](#_Toc174044897)

[7.2.2 Interpretation of Results 49](#_Toc174044898)

[7.2.3 Linking Findings to Security and Performance Enhancements 50](#_Toc174044899)

[7.2.4 Detailed Evidence for Technical Testing 52](#_Toc174044901)

[7.3 Discussion 55](#_Toc174044902)

[7.4 Summary 55](#_Toc174044903)

[Chapter 8: Conclusion and Recommendations 56](#_Toc174044904)

[8.1 Conclusion 56](#_Toc174044905)

[8.1.1 Key Findings 56](#_Toc174044906)

[8.1.2 Contributions to Academic Knowledge 56](#_Toc174044907)

[8.1.3 Implications for Practice 57](#_Toc174044908)

[8.1.4 Limitations and Future Research Directions 57](#_Toc174044909)

[8.2 Recommendations 57](#_Toc174044910)

[References 59](#_Toc174044911)

[Appendix I 68](#_Toc174044912)

**List of Figures**

Figure 1.2: Decentralized voting application using blockchain (GeeksforGeeks, 2022)......12

Figure 3.4: Conceptual framework…………………………………………………………28

Figure 4.6.4: Successful Transaction……………………………………………………….33

Figure 5.4.1: Ganache Dashboard…………………………………………………………..37

Figure 5.4.2: Metamask Integration………………………………………………………...38

Figure 5.4.3: Smart Contract Deployment…………………………………………….........38

Figure 5.4.4: phpMyAdmin Databases Interface…………………………………………...39

Figure 5.4.5: Login Page……………………………………………………………………39

Figure 5.4.6: Vote Casting Page…………………………………………………………….40

Figure 5.4.7: Vote Confirmation Page………………………………………………………40

Figure 6.2.1: Securing e-voting based on blockchain in P2P network (Yi, 2019)…..............43

Figure 6.2.5: Blockchain-based e-voting protocols (Mookherji et al, 2022)………………..45

Figure 7.2.1: User Satisfaction Survey Results……………………………………………..47

Figure 7.2.2: Security Testing Results……………………………………………………….48

Figure 7.2.3: Technical Proficiency and System Usability…………………………………..48

Figure 7.2.4: Voting Activity Patterns……………………………………………………….49

Figure 7.2.5: Decentralized mechanism to ensure the security of digital voting system voting system (Alvi et al, 2022)……………………………………………………………..............50

Figure 7.2.6: Implemented Security Measures……………………………………………….51

Figure 7.2.7: Participants Confidence in System Security…………………………………...51

Figure 7.2.8: DDoS Attacks Simulation Results……………………………………………..52

Figure 7.2.9: Man-in-the-Middle Attack Simulation Results………………………………...53

Figure 7.2.10: Sever Response Time and Uptime During DDoS Attack…………………….53

Figure 7.2.11: Data Integrity and Detected Rates During Man-in-the-Middle Attack……….54

# Chapter 1: Introduction

## 1.1 Introduction

Securing electoral processes’ efficacy, safety, and fairness is imperative for democratic systems today in democratic nations. Some of the drawbacks of the classical centralized voting systems include vulnerability to fraud, opacity of the process, and low extensibility. These issues reduce credibility or faith in the electoral process and the results it produces.

Interestingly, the application of blockchain technology could solve the problem by creating a decentralized platform to record and verify all transactions (votes). Coupled with React. js, a powerful JavaScript framework to create UI interfaces, blockchain allows to develop user-friendly, transparent, and secure applications for voting.

This dissertation focuses on creating a React app for a decentralized voting system and the process of deploying the blockchain technology. The main purpose, therefore, will be to showcase how these technologies can promote the security, openness, and accessibility of vote-related actions.

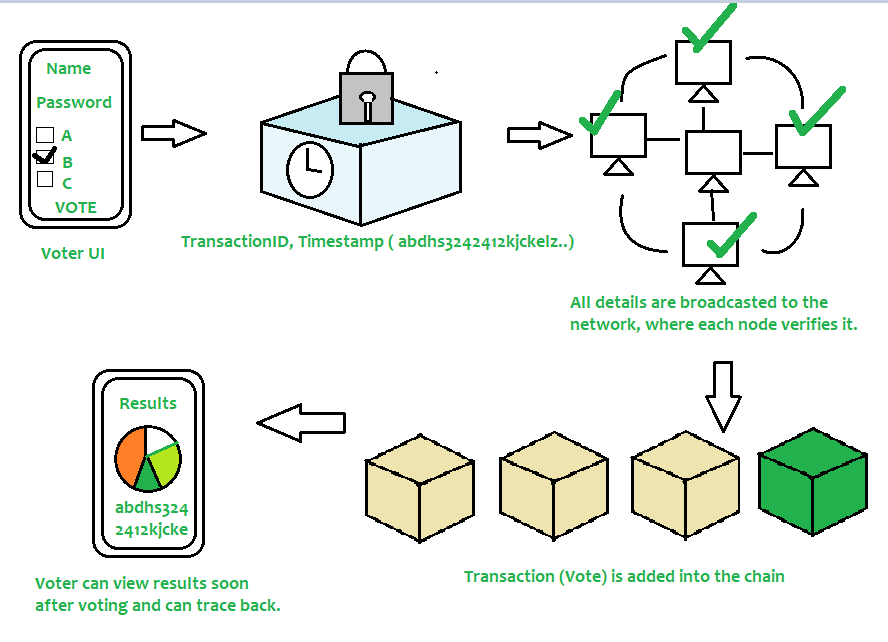
## 1.2 Background

In today’s complex democracy, the purity and safety of voices are essential to any election in order to provide a fair and accountable system in any country. Nevertheless, common methods of voting have various problems that compromise these objectives. Some of the problems like tampering, fraud, and other logistical problems have been realized to affect centralized voting systems and this has resulted in doubts in the accuracy and legitimacy of the results.

Centralized systems involve a control room where the voters’ data and the ballot count are administered. This centralized approach leaves room for manipulation and cyberattacks, which not only undermine the credibility of electoral results, but also erode the citizens’ trust in the democratic processes. The situation has raised the demand for a more secure, transparent, and easily accessible voting process because of advancement in technology as well as the emergence of new threats targeting the electoral process.

Blockchain has been identified as an innovative solution to transform vote by proposing its own characteristics such as decentralization, data integrity, and security based on cryptography. It was initially created as the technology that supports cryptocurrencies; however, it is a distributed register where transactions-votes in this case, cannot be tampered with by any individual or entity as it are across the network of computers. Such a decentralized model not only improves voting security and transparency but also leads to increased voter confidence in electoral processes.

The dissertation investigates the application of blockchain technology to enhance the security and transparency of voting systems, with a particular focus on integrating it with React. Blockchain's decentralized nature and cryptographic security offer a promising solution to address the shortcomings of traditional centralized voting systems, such as tampering and fraud. The objective is to develop a decentralized voting application that leverages blockchain’s inherent security features. By employing React for the user interface, the project aims to create a platform that is user-friendly and accessible. This approach is intended to improve the overall voter experience, ensuring a more reliable and transparent electoral process.



**Figure 1.2:** **Decentralized voting application using blockchain** (GeeksforGeeks, 2022)

It is with the view of overcoming the shortcomings of the current and widely used voting systems, coupled with the quest to unleash the potency of blockchain, that this project aims to help promote the cause of efficient and secure voting systems. The goal is therefore to show that voting daps can reduce risks involving centralized systems which will in effect help promote democracy and higher voting turnout.

## 1.3 Research Rationale

The main concern driving this dissertation is the various weaknesses and defects that have been recognized in traditional centralized voting systems. These systems are often not designed to provide the level of transparency, security, and availability required to maintain the integrity of the democratic process of the electoral race. These problems include the ability of fraudsters to alter the results of the elections, difficulties involved in confirming the accuracy of the ballot counts, and difficult ballot barriers for some voters to cross which end up in leaving out some people in the voters list. Deficiencies such as these not only erode the credibility and acceptability of electoral results but also erode the voters’ confidence in democratic institutions, a factor that potentially threatens the conduct of democratic elections. In the current social context of high awareness of the cyber threats, the fears are compounded by escalating technological advancements in manipulation and additional requirements to prevent cheating in voting processes.

To this end, the following crucial questions are of significance and shall be responded to by this dissertation which seeks to assess the interface between blockchain technology and react. js in the development of a decentralized voting application to foster an efficient decentralization of the vote. Due to its decentralized ledger and cryptographic layers for security, blockchain can provide a favorable solution to improve the integrity and traceability of vote choosing and tallying.

## 1.4 Problem Statement

Conventional areas encompass several weaknesses that undermine the functionality and fairness of electoral procedures. Most centralized systems that are under the control of a certain authority can also experience a lot of threats such as hacking, tempering, and even insider manipulation. These vulnerabilities undermine democracy and the legitimacy of the electoral process, while presenting serious barriers to democratic practice. Traditional voting techniques often fall short in ensuring the correctness and genuineness of each vote. Issues such as voter suppression, slow or inaccurate ballot processing, and limited accessibility of voting stations exacerbate these concerns, particularly during mass or remote voting scenarios. To overcome these challenges, it is critical to develop solutions that provide protection, accuracy, and transparency in the voting systems. Technology offers an excellent answer in this case because all voting processes based on blockchain technology do not involve the participation of a central authority and vulnerability to fraud or manipulation of results. Integrating React. Ensure that it use JS for front-end development because it allows for improved interaction and visibility to the targeted audience, which is of essence in the campaigning of different segments of the voter population.

## 1.5 Research Aim

This dissertation has the following objectives: The primary goal of this dissertation is to design and investigate a decentralized voting application that employs the blockchain technology that is in parity with react. js to improve the security, openness, and accessibility of the elections in terms of its organization and conducting.

## 1.6 Research Objectives

To accomplish the goal of routing, the following research objectives must be answered:

* To identify and analyze the security risks associated with centralized voting systems.
* To enhance the security and integrity of voting systems through the implementation of blockchain technology.
* To assess the security, performance, and accessibility of the decentralized voting app by simulating cyberattacks, including but not limited to Distributed Denial of Service (DDoS) attacks, man-in-the-middle attacks, and phishing attempts.
* To assess various voting models to evaluate its resistance to cyber threats and ability to expand to even larger scale for various voting models.

## 1.7 Research Questions

* What methods can be employed to effectively utilize blockchain technology in designing and implementing a secure and tamper-resistant decentralized voting system?
* How can the performance, security, and usability of a decentralized voting application be rigorously evaluated, ensuring robustness against cyber threats and scalability for different voting scenarios?

## 1.8 Research Contributions

This research significantly advances the field of electoral technology by addressing critical issues related to the security, performance, and usability of decentralized voting systems through the integration of blockchain technology.

**Enhanced Security and Integrity**

The study provides a comprehensive analysis of the security risks inherent in centralized voting systems and demonstrates how blockchain technology can mitigate these risks. By employing blockchain's decentralized ledger, the research enhances the tamper-resistance and immutability of voting records, addressing vulnerabilities associated with traditional centralized systems.

**Evaluation of Blockchain Implementation**

This research contributes novel methods for utilizing blockchain technology in designing and implementing a secure voting system. It explores the technical aspects of blockchain integration, including its impact on vote record security and system resilience against cyber threats.

**Rigorous Performance Assessment**

The study rigorously evaluates the performance, security, and usability of the decentralized voting application. It involves simulating various cyberattacks, such as Distributed Denial of Service (DDoS) attacks, man-in-the-middle attacks, and phishing attempts, to assess the system’s robustness and scalability. This contribution provides valuable insights into the application’s ability to handle diverse voting scenarios and its readiness for broader deployment.

**Improved Accessibility and Engagement**

By leveraging React for front-end development, the research improves the accessibility and user engagement of the voting application. This enhancement ensures that the system is user-friendly and accommodates a wider range of voters, thus promoting higher voter participation and confidence in the electoral process.

These contributions collectively address the research questions and objectives, providing a foundation for future developments in secure and scalable voting systems.

## 1.11 Summary

This dissertation’s introduction section outlines the problems with the conventional centralized voting systems and highlights that its shortcomings comprise the following: The ways in which it can be easily manipulated, its opacity, and it lack inclusivity. it all stands in direct contradiction to democracy and contribute to weakening voter confidence in the election systems. The interaction between blockchain and react, the most popular JavaScript library. To solve these challenges. js is put forward with the view of providing innovative solutions. Blockchain brings in a decentralized and unalterable record-keeping system, thereby accurately and securely maintaining votes, whereas react is used in creating dynamic user interfaces with complex behaviors. js adds value and interactivity to web application UI elements to make it accessible easier. The following is the breakdown of the aims and objectives of the dissertation: The research will seek to identify how these technologies can be incorporate in the development and implementation of a decentralized voting application to make electoral systems more secure, transparent, and easy to use.

# Chapter 2: Literature Review

## 2.1 Introduction

Democracy depends on free, fair, and frequently conducted elections so, today’s democratic states need secure, reliable, and transparent electoral system for the conduct of election. Centralized online voting systems that were incorporated into the architecture of electronic elections earlier are extensively criticized now because of the similar approaches’ weaknesses, such as fraud, opacity, and restricted availability. These deficiencies affect the population’s belief in democracy and its institutions.

This Chapter focuses on one specific type of architecture which is the combination of Blockchain and React. js as an innovative strategy for the process of voting by the population. In any given Blockchain system, it eliminates the weaknesses inherent in central control and provides a distributed platform that decreases susceptibility to frauds and increases accountability. Through decentralization of records and votes, the occurrence of a single control point is impossible and hence the invulnerability of block chain elections.

The major areas of the literature review in this paper include the primary architecture of blockchain, cryptographic solutions for safe voting, and creation of an independent voting system. It examines how blockchain principles tackle the vices associated with traditional voting systems including fraud and rigging thus strengthening electoral credibility. The review examines React. js for creating engaging and easy to use voting interfaces. React. js is used to make designs that are interactive and responsive for the various target group of voters so that the electoral systems can be easily used.

## 2.2 Considerations for Research Objectives

### 2.2.1 Blockchain Technology in Electoral Systems

Blockchain has now impacted the world’s electoral systems as a revolutionary factor in modern technology. Ideologically, blockchain acts like a distributed database where records of the transactions and votes are recorded in a network of computers and not with the control of a single party (Bighiu, 2022). This structure helps to avoid possible problems of manipulation and fraud, which are characteristic of centralization. Transaction records are copied throughout several nodal points with blockchain, meaning that changing a single record will necessitate a compromise of the whole network that also increases transparency.

When operating with the concept of blockchain in the framework of electoral systems, several principles of ranges and steps are significant for integration (Cai *et al,* 2022). Decisions in choosing the right framework like Ethereum especially for its smart contract strength cannot be overemphasized. it enables funding of the voting processes and at the same time, provide a high level of integrity in the voting tallying. Other options such as Hyperledger Fabric or Corda encompass the usability factor along with legal frameworks of the electoral districts.

Speaking of the security issues in the blockchain-based electoral systems, one must address cryptographic measures such as key management and public key cryptography. It preserves the voter identity and vote information during the voting process from the start to the end (Chentouf and Bouchkaren, 2023). To maintain the sincerity and integrity of e-voting, information related to the voters is encrypted when the votes are being cast.

In the electoral processes, the decentralized nodes are useful since it has the responsibility of ensuring that the consensus mechanisms of the blockchain platform check the transactions reducing cases of fraud as described by Deviani (2023). This acts as affirmation of the election results and is in line with examples of democracy, likewise, boosting the voter’s confidence.

In general, the proven features of blockchain provide a very powerful impact that increases voter confidence: immutable records and transparency. In this case, through creating digital signatures of each vote, blockchain gets rid of manipulations chance, where citizens can follow the process of voting and believe in the authenticity of the results of elections (Dhanala and Radha, 2020). The level of transparency as such is very desirable for a democratic process, whereby the results of the elections truly reflect the desire of the people. Blockchain based real time auditing empowers the electoral authorities and the relevant stakeholders to track the vote flows secured and transparently thus making it possible to identify and deter the malpractices right away. However, several challenges are presented when blockchain is applied in electoral systems especially due to the scalability problem in managing many elections (Dhulavvagol *et al,* 2020). As-of-right improvements such as shading, and side chains are in the works to improve the transactional abilities and farther voting procedures.

Legal factors play a crucial role in the decentralized voting system, which include technology legal issue, voter, legal protection, secure authentication, and the legal geographic area (Dimnik, 2023). This work emphasizes that appropriate measures must be in place to implement the concept of blockchain solutions in election processes and exclude violations of the rights of citizens. Nevertheless, applying blockchain has unparalleled potential to improve electoral systems by increasing it security, transparency, and reliability. Implementations in distributed ledgers are seen to enhance voter’s trust, participation, effectiveness, and integrity in elections globally; hence, influencing the future of democracy (Dragomirescu and Bostan, 2023). Constant research and innovations involving stake holders in technology, policy makers, and the electoral body are essential to fully unlock blockchain as well as to solve existing challenges in the electoral system comprehensively.

### 2.2.2 Linking Blockchain Technology to Centralized Voting Systems

Blockchain technology offers a compelling alternative to the traditional centralized voting systems. By decentralizing the record-keeping process, blockchain addresses the critical weaknesses of centralization. In a blockchain-based voting system, records of votes are distributed across a network of nodes, eliminating the single point of control that central authorities present. This decentralized nature makes it exceedingly difficult for any single actor to alter or manipulate the voting records without the consensus of the entire network. Blockchain’s inherent features—such as immutability and transparency—ensure that once a vote is recorded, it cannot be tampered with, and all transactions are visible to authorized parties.

### 2.2.3 Role of User-Friendly Interfaces in Enhancing Voter Engagement

Making interfaces more appealing is something that can improve electoral systems and raise the turnout at the same time. New generation modernization concerns the adaptations of the interfaces towards the different users and platforms, and the accessibility and the easiness are always preferred, especially when using the React. js (Duran, *et al,* 2023). Voting is still one of the most important activities in the elections, which shows that people are searching for a perfect interaction design. An easy-to-use voting system eliminates physical barriers that might make a person not to vote due to one reason or the other especially in areas of inadequacy in the use of electronic devices. Techniques of design can make voting procedures easier, making the political processes more accessible to the public and encouraging citizens to participate. React. js, well known for its component-base model, provides several benefits to produce scriptable interfaces for electoral use. This framework enables the development of modulization in the style of pertinent elements to accomplish reliability and scalability in different voting systems (Enuga *et al,* 2023). From a user’s perspective, ballot displays, voter authentication, and result presentations will be enhanced, thus enabling developers to manage such components with the most efficiency.

Research highlights React. As for the assessment of ‘js’, it seems to be relatively effective in the context of electoral in terms of Appearance, Interaction and Use of interfaces. Engagement features such as real time voting progress updates and clear instructions can be easily incorporated into any design because of the modularity of design to boost confidence in electoral systems.

Another important factor that is taken into consideration by React is the responsive design. js, to make sure interfaces successfully work on any device and display size (Fayemi *et al,* 2022). This versatility caters for the voter with Smartphone, the iPad, or the PC, boosting portability and utilization in diffident electoral terrains.

Features of universal access implemented within the React. Further, js framework can also widen the opportunity of inclusiveness in voting systems. Voice commands, color and contrast controls, and hotkeys ensure that the voters with disabilities are not locked out from the whole process of voting (Febriyanto *et al,* 2020). All these provisions are in consonant with complimentary democracy that calls for equal electoral right for all voters including the disabled. Research shows that the adaptable and friendly graphical user interfaces that are created in React. js can not only increase the convenience for the delivered contents but also help improve the voting satisfaction and turnout rate among the voters (Fonseca Cacho *et al,* 2021). Top-level principles and patterns of designed interfaces in React. and increase the overall accessibility of the sites, thus increase voters’ interest and the voter turnout rates.

Electoral authorities adopting the user experience design can create interfaces on voting that have direct comparisons to the interfaces that users perceive in its everyday life (Fritsch *et al,* 2024). This methodology improves the overall voting process, and the confidence of the voters in any electoral process, as well as guarantee that every voter’s will is accurately portrayed. The integration of React. js also goes on to contribute to the development of electoral systems across the world, supported by powerful features pertaining to the development of interactive interfaces. This technological advancement serves the interest of democracy by making it possible to arrive at decisions that are true reflections of the people’s democracy. Leveraging React. js in electoral systems enhances the principles of reciprocal trust and increases the number of voting (Goldberg and Schär, 2023). Further improvements in accessibility and usability are something that still needs to be done and can be facilitated by technologies such as React. js maintain electoral democracy and make certain that elections are free, fair, and efficient, aligned to the societies’ beliefs.

### 2.2.4 Integration of Smart Contracts in Automating Voting Processes

Smart contracts are entering electoral systems as novel automatized and decentralized processes that increase effectiveness, openness, and security (Grover, 2020). These digital applications work on set procedural mandates that do not require a third party to set or oversee the voting processes; the use of block chain in this enhances the integrity on deliveries made.

At the base of smart contracts is the self-executing of contractual provisions. The incorporation of voting rules in these contracts causes processes like electoral to become automatic thereby decreasing the amount of oversight and the occurrence of errors (Guo *et al,* 2021). For instance, the requirements for the voter such as the eligibility can be incorporated in the smart contract thus eliminating the biases of the traditional poll to only enable the competent voters.

Security of votes is among the key aspects that get boosted via the use of blockchain technology. In this type of voting, each deliberately placed vote is documented on the blockchain’s database and can be accessed by the public and electoral bodies (Hamidey and Heng, 2022). It ensures confidence in the conducted elections since the various stakeholders can easily scrutinize the election process and results. Apart from the voting, smart contracts also help in the tallying of the votes. These contracts enable the tallying of results to be done automatically as per rules set in advance reducing time, the risk of errors and manipulation that would be expected from manual tallies (Han *et al,* 2020). This automation increases reliability of electoral results, strengthens the democratic institutions and the people’s faith in the same.

Smart contracts thus pose a threat to the electoral management bodies as outlined below following the realization of its disruptive possibilities. it allows for a variety of election processes such as registration of voters, voting, result tallying and certification among others to be conducted without the intervention of bureaucratic procedures. Thus, this efficiency coupled with the security features of blockchain successfully tackle the persistent issues of efficiency, accoun­tability as well as security of electoral systems across the globe (Hellström, 2022). Some of the advantages of smart contracts include it applicability and possibilities for incorporation of realistic means of redress. Situations that can stem from the identification of voters, the process of voting, or results controversy can be easily resolved by programmatically set rules. Besides facilitating the resolution of conflicts, it also increases the efficiency of electoral processes and its fairness.

Research also points to smart contracts as useful in a myriad of electoral conditions, regardless of whether it is local council elections or national referendums. Electoral institutions’ management can always work to develop voting style specific to the country while conforming to the set rules and regulations as required by the statutory laws thus improving on the flexibility of the electoral processes (Hernandez, 2021). The use of cryptographic encryption, which is a characteristic of blocks, contributes to the protection and, accordingly, the privacy of the voter data. Smart contracts consist of programming code that only allows correct and genuine votes to be recorded with the blockchain database, thus, preserving the honesty of ballots. These strong measures double people’s trust in the election results which asserts the principles of democracy including integrity and openness.

Strictly in the future, as the smart contracts technology will be developing more efficiencies and reliability of the electoral processes will be improved (Huang *et al,* 2021). As these technologies develop, smart contracts are set for a more crucial purpose of fixing electoral irregularities around the globe and strengthening credible democratic systems.

The inclusion of smart contracts in the voting procedures can be regarded a groundbreaking achievement in the sphere of the electoral technologies. Smart contracts, hence, expand blockchain’s application in electoral systems to boost efficiency, transparency and security democratic nations require today.

### 2.2.5 Enhancement of Security Through Blockchain and Smart Contracts

The integration of blockchain and smart contracts into electoral systems represents a significant advancement over traditional centralized voting methods. By decentralizing vote recording and automating the enforcement of voting rules, these technologies address critical security issues such as manipulation, fraud, and procedural errors. Blockchain’s decentralized ledger and smart contracts’ automated processes collectively bolster the security and transparency of the voting system (Ikundi *et al,* 2022). This innovative approach not only mitigates the vulnerabilities associated with centralization but also enhances the overall credibility of the electoral process, reinforcing public trust in democratic institutions.

## 2.3 Theoretical Framework

The integration of blockchain technology into voting processes represents a significant technological advancement, complemented by user interfaces developed through React (Indukuri et al, 2023). This section explores two theoretical frameworks: Decentralized Systems Theory and HCI Theory. Blockchain voting systems, grounded in Decentralized Systems Theory, decentralize voting procedures and data, using consensus methods to safely verify transactions and eliminate single points of failure (Isirova et al, 2020). This approach enhances efficiency and security by creating immutable records on the blockchain. HCI Theory guides the design of user interfaces for blockchain applications, promoting engagement, accessibility, and user satisfaction (Jain et al, 2022). Features such as clear design layouts, feedback mechanisms, text-to-speech, and high-contrast modes improve accessibility for diverse users.

Blockchain addresses vulnerabilities in centralized systems, such as tampering and fraud, by distributing records across nodes, making unauthorized changes computationally challenging (KG and Emmanuel., 2021). Integrating HCI principles into React-based voting interfaces ensures usability and effectiveness, enhancing voter confidence and participation (Khairkar et al, 2023). Combining Decentralized Systems Theory and HCI Theory, electoral authorities and developers can create transparent, secure, and user-friendly voting environments, advancing electoral integrity and democratic engagement (Mann et al, 2020; Li et al, 2020).

## 2.4 Literature Gap

Despite advancements in blockchain technology and user interface design, gaps remain in the literature on blockchain-based voting systems integrated with user-friendly interfaces using frameworks like React.js. Theoretical and technical contributions have explored blockchain’s potential to enhance electoral democracy and combat vote fraud, but significant efforts to assess the functional effectiveness of blockchain voting systems are lacking (Nnebe et al, 2022). While Decentralized Systems Theory and cryptographic security have been discussed, there is limited empirical data on blockchain’s practical capabilities and adoption barriers in electoral contexts. The need for more research to validate theoretical claims and examine real-world applications remains.

Regarding user interfaces, research on React.js for blockchain-based voting systems is limited. HCI Theory emphasizes designing for specific user needs and iterative testing to enhance usability (Olaniyan et al, 2022). However, empirical studies assessing the usability and effectiveness of React.js interfaces in electoral environments are scarce. Future research should include user feedback, usability testing, and comparisons with traditional systems to develop inclusive interfaces for diverse voters.

The literature lacks exploration of blockchain integration with electoral processes and HCI principles, requiring coordination among computer scientists, UI/UX designers, and policymakers (Olanubi, 2023). Addressing these gaps is essential for creating reliable, user-accepted blockchain voting systems and enhancing voter experience.

## 2.5 Summary

The literature review explores two key areas: blockchain in electoral systems and user-friendly interfaces developed with React.js. Blockchain offers a transparent, secure voting process through decentralized record-keeping and consensus models, yet empirical evidence on its real-world impact is lacking. React.js interfaces prioritize ease of use and accessibility, but research on their effectiveness in voting contexts is scarce. A research gap exists between blockchain and HCI, highlighting the need for collaboration between computer scientists, UI/UX designers, and electoral experts. Addressing these gaps through empirical research and cross-disciplinary efforts is crucial for advancing transparent, secure, and user-centered voting systems.

# Chapter 3: Research Purpose and Objectives

## 3.1 Introduction

This work finds that the candor, security, and openness of any electoral process remains supreme in the new generation of democracies and essential to engender public confidence in electoral processes. Historical and centralized voting systems, which have defined the nature of elections for years, have come under criticism because of the likelihood of fraud, the lack of openness, and the restricted availability of such systems. These problems are not mere technical problems but are existential threats that pressure the very foundations of democracy and the institution of democratic governance. The main aim of this study is to analyze and discuss these substantial issues and to design a decentralized voting application based on blockchain and react. js.

The emphasis is made on the utilization of the key feature of blockchain – decentralization in the trials to improve the security and transparency of the voting process and the use of React. js to make it easier for the user to navigate to have an efficient user interface design. Blockchain transfers record the votes in an authorized manner and at the same time it is resistant to alteration. This decentralized form of consensus reduction the dependency on a central authority, which in turn minimizes the likelihood of fraud. Concurrently, React. js helps with construction of popular interfaces for voters, facilitating it usage by different groups of voters and thus increasing participation.

## 3.2 Key Research Contribution

This research makes significant contributions to the field of electoral technology by addressing key challenges in developing a decentralized voting system using blockchain technology. The contributions are aligned with the research questions (RQs) and objectives (ROs), offering innovative solutions to enhance the security, performance, and usability of voting systems.

**Design and Implementation of a Secure and Tamper-Resistant Voting System**

The research successfully integrates blockchain technology to create a decentralized voting system that minimizes the risks of manipulation and fraud. By decentralizing the vote recording process, the system ensures that the database is secure and resistant to tampering (Ortega Núñez, 2021). This contribution directly addresses the research question of employing blockchain to design a secure and tamper-resistant voting system. The development of a working prototype, coupled with the application of cryptographic tools, provides a robust solution to ensure vote security and authenticity, aligning with the objective of enhancing the integrity of voting systems through blockchain.

**Development of User-Friendly Interfaces Using React.js**

A crucial aspect of this research is the design of user-friendly interfaces using React.js. This contribution focuses on improving accessibility and engagement by creating intuitive and visually appealing interfaces (Abegunde, 2023). React.js, a popular JavaScript library, facilitates the development of functional and adaptable user interfaces. By addressing the usability aspect, the research ensures that the voting system is accessible to a diverse range of users, including those with limited technical proficiency. This aligns with the research objective of assessing the performance and accessibility of the decentralized voting app.

**Integration of Smart Contracts for Automation and Transparency**

The research introduces smart contracts into the voting application to automate and transparently enforce voting rules. Smart contracts, executed through computer code, streamline various tasks such as election accreditation, voting, and tallying of votes (Ademola et al, 2024). This integration minimizes human errors and enhances procedural justice, addressing the research question related to the automation of voting processes. The use of smart contracts ensures that the voting rules are applied consistently and transparently, contributing to the overall reliability and fairness of the voting system.

**Comprehensive Evaluation of Performance, Security, and Usability**

The research conducts a rigorous evaluation of the decentralized voting application, encompassing performance, security, and usability. Through empirical analysis and stress testing, the system's robustness against cyber threats is assessed, while user testing captures feedback on the interface design and usability (Ajinomisanghan, 2023). Scalability tests further examine the system’s performance across various voting scenarios, from local elections to national referenda. These evaluations provide critical insights into the system’s strengths and areas for improvement, aligning with the research objective of assessing the application’s effectiveness and scalability.

Overall, these contributions address the research questions and objectives by providing a comprehensive and innovative approach to developing and evaluating a blockchain-based voting system. The integration of blockchain technology, smart contracts, and user-centric design enhances the security, transparency, and accessibility of the voting process, offering valuable insights for future research and practical applications in electoral technology.

## 3.3 Detailed Exploration of the Research Contributions

### 3.3.1 Objective 1: Secure and Tamper-Resistant Voting System Using Blockchain

This research is premised on critical aspects of blockchain technology, which include the imprint of immutability. Blockchain is based on the distributed database system with each vote being registered as a transaction in a block as noted by (Alfain *et al,* 2022). These are connected in a chain manner, and it is very difficult to tamper with any of the votes because that will require a change in all subsequent blocks. This decentralized system also does not require a single authority, which is commonly a weak link in the conventional voting methods.

The design and implementation of the voting system will involve several critical steps:

Blockchain Framework Selection: It is therefore important to choose the right framework of the blockchain. Other aspects applicable in this case shall include scalability, level of security required and compatibility with related systems. Ethereum, which has proven to be exceptional in the executing of smart contracts, is a good candidate for this role (Al-Maaitah *et al,* 2021). However, alternatives such as, Hyperledger Fabric also providing a modular architecture and permissioned networks will also be compared to find out the best suitable for the voting application.

Cryptographic Security Measures: Use of elaborate cryptosystems for confidentiality and preserving the integrity of votes must be adopted to the greatest extent. Some of it are Encryption techniques to preserve the identity of voters as well as preserving the integrity of the votes (Alves and Pinto, 2023). Other measures such as ZKP can be employed to ensure that the transactions are valid without disclosing personal details. The digital signatures and implemented public key infrastructure (PKI) will be used for the voter identification and for the vote checking.

Decentralized Network Setup: It is necessary to form a distributed network of nodes that will govern the formation of the blockchain. The nodes will then check transactions, which will lead to the agreement and make it impossible to carry out fraudulent transactions (Al-Zoubi *et al,* 2022).

### 3.3.2 Objective 2: User-Friendly Interfaces Using React.js

Thus, for a voting system to be efficient, it must be easily operated and attract the attention of the voters. React. js, which implements component-based architecture, makes it possible to develop powerful and active user UIs. The development of user-friendly interfaces will focus on:

**Intuitive Design:** Other approaches include making the design easy to use by following simple instructions and ensuring that the process of casting a vote takes few steps. The interface will be initially tested for design with various types of users to accommodate all types of users (Andrew, 2021). It will be important to create the application in accordance with user centered design where the interface is updated based on feedback obtained from usability testing. The goal is to achieve low mental demands and make the voting process familiar for people with little or no computer experience.

**Responsive Layout**

It is important that the interface should be responsive and available on different platforms such as desktop, tablet, and mobiles, for voters who may only have access to a mobile device (Anitha *et al,* 2023). It will be developed in a way that will be as adaptable as possible to any screen size and mostly any orientation. Techniques like progressive enhancement will be used to make sure the application is usable on older devices on slower internet connection.

**Accessibility Features:** Adding the elements like text-to-speech, high contrast mode, and keyboard navigation to assist voters with disabilities. WCAG will be followed to ensure that the interface design is as friendly as possible to the user and convenient for the people with some disabilities concerning the vision, hearing, and the motor coordination. The expansion of the application, including choice of the font size and language translation will help to improve its accessibility.

### 3.3.3 Objective 3: Integration of Smart Contracts

It will be necessary to adopt smart contracts to automate and enforce the rules of voting:

Voter Eligibility Verification: Smart contracts will facilitate the eligibility standards regarding voting rights such as age and citizenship to allow only legally qualified individuals to vote. This verification process will be designed to ensure that voters’ privacy is preserved as well as work towards eradicating fraud in the voting system (Arora and Wasson, 2023). Linkage to other databases and secure identity authentication systems in the government will help the agencies to conduct eligibility checks in real time and without revealing applicants’ sensitive data.

Vote Casting and Counting: Being able to automate the process of voting to ensure each vote is recognized and counted in the best way possible. Smart contracts shall count votes and present the results in real-time that shall be presented as soon as the voting duration is completed (Baiquni, 2024). This automation will eradicate one major factor which is human, and the time used in announcing election results will be minimized. it will also provide means for multiple rounds of voting, runoff elections, and any kind of voting that one can imagine such as ranked voting.

Dispute Resolution: The incorporation of functionalities into smart contracts that facilitate the resolution of disputes regarding the eligibility of the voters, or the totals of the votes. This helps in avoiding collusion between the two parties by making the process as transparent as possible. Mediation procedures will be fair and fast, having set rules for resolving conflicts and checking further compliance with honest records (Banu *et a.,* 2023).

### 3.3.4 Objective 4: Comprehensive Evaluation

The last one is an assessment of the decentralized voting application. This will include:

Performance Testing: Challenging the system to test how well it can perform when there is a surge in the number of transactions during voting exercises. Measures like transaction per minute, time taken for a transaction, and number of transactions will be recorded (Barański *et al,* 2020). Load testing and stress testing will be conducted to test the election website under different voting loads to discover any bottlenecks. The flexibility and capacity of the system will also be tested to determine if the system can be used to manage larger and/or more complicated elections.

Security Assessment: Evaluating the effectiveness of security measures through security audits to establish risks. This comprises vulnerability scanning and enumeration for purposes of actual attack to assess the system’s readiness. To manage the risks the blockchain security specialists will analyze the blockchain structure, the smart contracts as well as users’ interfaces (Barbereau *et al,* 2022). It is important to note that security updates and patches will be incorporated on a consistent basis to ward off new threats and risks.

Usability Testing: Collecting users’ opinions to evaluate the level of interface friendliness with a wide range of people. User feedback, various tests of usability, and the results of the examination of the users’ actions will be used in this case. This feedback will inform future adjustment to the user interface and general usability (Benny, 2020). The pilot testing in real-world voting scenarios will give a critique of the system efficacy and user acceptance.

## 3.4 Conceptual Framework

**Figure 3.4: Conceptual framework**

## 3.5 Summary

The research purpose and objectives as mentioned in this dissertation would follow the goal of tackling inherent weaknesses associated with centralized voting systems. Such systems have often been associated with problems like ease of manipulation, opacity and restricted access and these aspects pose serious problems that erode the public trust and credibility of the elections. To address these issues, this dissertation seeks to design a decentralized voting application using blockchain and react. js. The use of blockchain technology can enable an efficient, transparent, and unalterable way of vote counting through the creation of a distributed and thus resistant to manipulation ledger. Meanwhile, React. js is a design language that allows for the creation of rich and engaging interfaces, which in turn make voting easier and more accessible to users from all backgrounds.

# Chapter 4: Research Approach and Methodology

## 4.1 Introduction

The introduction of this research on decentralized voting apps using blockchain is informed by the highlighted problems and challenges associated with the digital voting systems prevalent in today’s technological world. It centers on presenting a haven that will promote an all-inclusive construction of quality. The goals include establishing the app’s effectiveness in implementing decentralized voting systems and the advantages of decentralization in the process of democratization as well as the identification of the major issues concerning the current models of voting.

The following are identified as major research objectives for this study. It aims at comparing various blockchain developments appropriate for creating safe voting platforms, for example, Ganache and Meta Mask, and its combination with frontend interfaces, for example, React.

The research also seeks to adopt an easy-to-use graphical user interface enhanced with secure blockchain parameters for user authentication and ballot control using smart contracts. Besides, it aims to explore the effectiveness and viability of blockchain-based voting systems for different voting circumstances regarding some legal outcomes. Finally, this research aims at enhancing the model of digital democracy by outlining the suggested architecture that enhances open, integrated, and accessible electoral processes in the improvement of a new era of democracy.

## 4.2 Research Design

The Research Design section lays out a research methodology suitable for assessing decentralized voting applications developed on the blockchain. It gives structure to approach the issues related to the secure and more transparent voting system design and development in a more controlled and purposeful way (Metcalfe., 2020). Furthermore, aiming at the systematic reviews as the type of the study, the authors’ purpose is to enhance the understanding of the ways how blockchain can open the processes and enhance the public’s trust (Mohd *et a.,* 2020).

## 4.3 Research Philosophy

The Research Philosophy section analyzes the research’s epistemology and ontology, which focus on decentralized voting applications through blockchain technology by Neloy *et al,* 2023. It talks about the extent to which the study meets positivist postulates or upon interpretivist or realist assumptions, which outline the researcher’s epistemological stance—beliefs about reality and knowledge.

Research problem is resolved by efficient, mathematical means to determine factual aspects of the effectiveness and viability of blockchain in the voting systems (Neziri *et al,* 2021). In this regard, it seeks to gather sufficient data through experimentation on the hypotheses about the use of blockchain in the electoral processes.

While positivism focuses on getting numerical data, interpretivism focuses on the qualitative approach deployed in the understanding of how people assign meanings to the subject under review, in this case, blockchain-based voting. This kind of research uses techniques such as interviews, case studies and ethnography to obtain contextual data and multiple perspectives on decentralized voting systems (Sun *et al,* 2024).

This section offers a systematic approach for implementing the outlined philosophical assumptions to define, deploy, and assess decentralized voting applications (Toma *et al,* 2022). The paper intends to fill the gap in the literature on governance and technology, which seeks to bring some suggestions to help improve electoral systems following empirical research and theory.

## 4.4 Research Approach

The Research Approach section describes the employed methodological approach focused on decentralized voting applications with blockchain (Vasilj *et al,* 2021). It provides a distinction of whether the investigation uses qualitative, quantitative research or both, considering the research questions and the type of the relationship between blockchain and electoral processes. To comprehend stakeholders ‘perception and impression about the trust and ease of blockchain-based voting applications, the methodology of qualitative research could be selected (Vinsura *et al,* 2022).

## 4.5 Research Strategy

Section two namely Research Strategy, explains the mode of carrying out the research on decentralized voting applications employing blockchain technology (Wang et al., 2020). And to what extent does the study deploy a case study, experimental, survey, or all the four approaches for hypothesizing and/or validating in terms of developing and deploying blockchain voting systems.

## 4.6 Methodology

### 4.6.1 Sampling Strategy and Sample Size Determination

The Sampling Strategy and Sample Size Determination section describes the methodology used to draw participants or cases for the study on decentralized voting applications using blockchain technology from the overall population. Starting with identifying the participants or cases, it defines the criteria and considerations that must be met when deciding on participants or cases, such as population characteristics and demographic variables (Wolmer *et a.,* 2022). The section gives details on different sampling techniques including random or purposive sampling and explains why it will be useful for the intended study depending on the research objectives and context of blockchain based voting systems.

The considerations for arriving at the actual sample size chosen are explained, these being for example power of the test as well as the accuracy required of the study/project (Zhang and Kim, 2022). The purposive sampling strategy that has been selected in the present study is aimed at achieving a purposefully selected sample with variability and representativeness within the selected context of decentralized voting applications. In its pursuit of a diversified and comprehensive sample, the research must ensure that major and diverse sampling techniques are used when recruiting participants to the study to provide crucial data about the usefulness and possibility of blockchain technology in electoral processes (Wicaksana, 2021). Al­to­gether, the section of Sampling Strategy and Sample Size Determination provides a significant methodological foundation of the study, safeguarding that the results of the investigation will lead to significant enhancement of knowledge in the chosen sphere as well as in the application of blockchain technology for enhancing the stability of the voting processes with transparency.

### 4.6.2 Data Collection Procedures and Instruments

The section on Data Collection Procedures and Instruments describes the rigorous approach implemented for the systematic collection of appropriate data for the research on decentralized voting applications enabled by blockchain technology (Poniszewska-Marańda et al, 2022). It starts with specifying the protocols used, like interviews or surveys or general observation of system functionality where the authors select approaches aimed at getting rich information on the functions and interactions of decentralized voting apps.

This section covers the processes involved in designing and developing fiduciary data collection instruments. By so doing, these instruments shall have been designed to facilitate exhaustive coverage of concerns in relation to the applicability of blockchain technology in voting systems. Concern is paid to the credibility and dependability of these procedures, in that steps are taken to reduce bias and error inherent in data collection processes.

The emphasis made to reliability lays more stress on the steadiness and dependability of the data accumulated as this is very important for making accurate deductions and insights (Willysandro *et al,* 2021). At the same time, concerns of validity guarantee the data collection process targets and captures the appropriate phenomena for study and, thus, increases the consolidated reliability of the obtained results.

In general, the section of the method called Data Collection Procedures and Instruments is crucial for the methodological approach of the research and helps in a clear and systematic way to gather empirical data needed to assess the effectiveness and the practical implementation of decentralized voting applications using blockchain.

### 4.6.3 Data Analysis Procedures

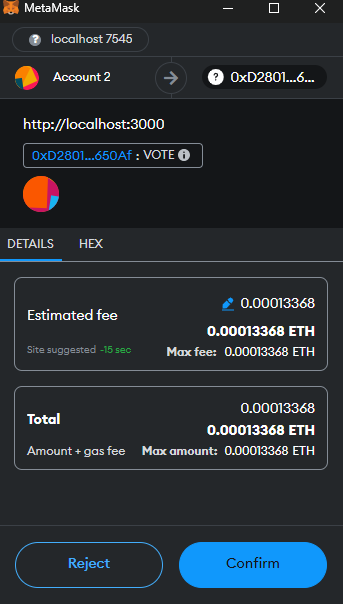
The methodology regarding data analysis in the study on decentralized voting applications by blockchain is outlined in detail in the Data Analysis Procedures of the study. This approach continues with the description of the qualitative or quantitative techniques deployed, for instance, thematic analysis or statistical analysis, which has been designed to analyze related data for the incorporation of blockchain into voting systems.

These chosen methods are in line with the research targets and assumptions, so the study can establish the decentralized voting application’s practicability, security, and effectiveness. For example, thematic analysis can help determine what themes or patterns might be present in the qualitative data depending on the user perceptions and System Usability Questions (Rafailoglou, 2020). On the other hand, the statistical analysis adopts a quantitative perspective to analyses the p-value corresponding to the tests related to variables that impact the voting of options within blockchain systems.

It is important here to emphasize the use of these analytical approaches since it are applicable in responding to the unique characteristics of the blockchain technology regarding the improvement of the voting processes. Those are meant not only to reveal some regularities, relationships, and dependencies but also to provide the comprehensive evaluation of the processes and outcomes linked to the decentralized voting systems. This systematic approach ensures that real empirical evidence collected is well analyzed and explained both qualitatively as well as quantitatively.

### 4.6.4 Ethical Considerations and Approvals

This paper tackles the ethical issues that are incorrigible when conducting research on blockchain- based voting applications in the Ethical Considerations and Approvals section.



**Figure 4.6.4: Successful Transaction**

It explores the question of the ethical considerations that are involved in such studies, while stressing in the main, the importance of the respect of the participant rights and the participant welfare during the research (Raikar and Vatsa, 2021). This includes being protective of participants’ information to avoid disclosure and conforming to the principles of informed consent as a way of respecting it decision-making.

This section describes the steps that are necessary to gain appropriate ethical clearances or permissions from IRBs or Ethics Committees. These approvals are important in ensuring that the research does not violate any set ethical standards and recognized professional and academic ethicist groups.

## 4.7 Summary

The research delves into the development and evaluation of decentralized voting applications using blockchain technology, aiming to address the need for more secure and inclusive voting systems. It begins with an introduction to the challenges in current digital voting systems and sets objectives to assess blockchain's effectiveness, compare various technologies like Ganache and MetaMask, and explore their benefits for digital democracy. The theoretical framework outlines key blockchain concepts such as transparency, immutability, and consensus algorithms, illustrating how they address the limitations of traditional voting methods. The research design and methodology sections detail a systematic approach, incorporating both quantitative and qualitative data through purposive sampling, rigorous data collection, and various analysis techniques to ensure reliability and validity. Ethical considerations emphasize participant rights and informed consent. The chapter also acknowledges potential limitations, such as technical challenges and dependencies on specific technologies, and suggests strategies to mitigate these issues. Overall, it provides a comprehensive evaluation of blockchain's potential to enhance the security and transparency of electoral processes.

# Chapter 5: Design and Implementation of Decentralized Voting Application

## 5.1 Introduction

This chapter outlines the design and implementation of a decentralized voting application (dApp) based on blockchain technology. It addresses the fundamental aspects of constructing a secure and transparent voting system, emphasizing the practical application of blockchain principles to electoral processes. The dApp is intended to address the limitations of traditional voting systems by leveraging blockchain's inherent features, such as decentralization, immutability, and transparency. The chapter details the design considerations, implementation strategies, and results observed from deploying the system in a test environment.

## 5.2 Requirements for Designing the dApp

**Backend**

1. **Blockchain Integration:**

* Using Ethereum for its robust smart contract support and security features.
* Smart contracts are implemented using solidity to manage voter registration, vote casting and result tallying.
* Voting records are immutable and secure through the blockchain inherent properties.
* Using Ganache for local blockchain development and testing and deploy to Ethereum test nest for further validation.
* Interacting MetaMask for secure user authentication and transaction authorization.

1. **Smart Contract:**

* Developing the smart contract to enforce the rules of voting process and ensuring each voter can only cast one vote.
* Storing and tallying votes on the blockchain to ensure transparency and integrity.
* Security audits are conducted on a regular basis to discover and address vulnerabilities.

1. **Data storage:**

* Use IPFS (Interplanetary File System) decentralized storage solution for storing any non-transactional data.
* Ensure encrypted and secure storage of sensitive voter information.

1. **API Layer:**

* Develop a robust API layer for communication between the frontend and blockchain.
* Secure and efficient data retrieval and transaction submission.

1. **Security:**

* Implement comprehensive security measures to prevent unauthorized access.
* Conduct regular audits to ensure data integrity and system security.

**Frontend**

1. **User Interface:**

* Build with react for a responsive and dynamic UI.
* Includes intuitive interface for registration, voting and result viewing.
* Ensures accessibility across various devices and user demographic.

1. **User Authentication:**

* Secure authentication mechanisms, including multi-factor authentication.
* Protect user data privacy and security throughout the process.

## 5.2 Design

The design of the decentralized voting application centers on creating a robust and user-friendly platform that adheres to the principles of blockchain technology. The application is designed with a focus on three core components: the blockchain framework, user interface, and smart contracts.

Firstly, the blockchain framework is built on Ethereum, a widely adopted blockchain platform known for its support of smart contracts (Rosasooria et al, 2020). Ethereum's capabilities provide a secure and decentralized environment for voting transactions. The choice of Ethereum is driven by its mature ecosystem, extensive developer resources, and robust security features.

The user interface (UI) is designed to be intuitive and accessible, facilitating ease of use for voters. It employs React, a popular JavaScript library for building interactive UIs, to create a responsive and dynamic frontend. The UI includes components for user registration, ballot casting, and result viewing, ensuring that all interactions are seamless and user-friendly.

Smart contracts play a crucial role in the dApp’s design. They are programmed to handle the voting process, including voter registration, vote casting, and result tallying. The smart contracts are designed to enforce the rules of the voting process, such as ensuring that each voter can only cast one vote and that the votes are counted accurately. They are deployed on the Ethereum blockchain to leverage its decentralized nature and immutability, which guarantees that the voting data cannot be altered once recorded.

## 5.3 Implementation

The implementation phase involves the actual development and deployment of the decentralized voting application. The process begins with setting up the development environment, which includes installing and configuring necessary tools such as Ganache for local blockchain development, MetaMask for Ethereum wallet integration, and Truffle for smart contract management.

The development team uses Ganache to create a local blockchain environment for testing the smart contracts and the overall functionality of the dApp (Saim et al., 2022). This allows for iterative development and debugging in a controlled setting before deploying to a public blockchain. MetaMask is integrated to provide a secure and convenient way for users to interact with the Ethereum blockchain through their web browsers.

The smart contracts are written in Solidity, Ethereum's programming language for smart contracts. They are thoroughly tested using Truffle’s testing framework to ensure their functionality and security. Once the smart contracts are finalized, they are deployed to the Ethereum test net, where they undergo further validation.

The frontend is developed using React and is connected to the Ethereum blockchain through Web3.js, a JavaScript library that facilitates communication between the frontend and the blockchain. The frontend is designed to be responsive and interactive, providing users with a smooth experience during the voting process.

**5.4 Screenshots and Security Explanations**

**Backend:**

1. **Ganache Dashboard:** Figure 5.4.1 shows the ganache dashboard status of the local blockchain, including accounts, transaction, and smart contract deployments. And it helps the developers to monitor and manage blockchain operation ensuring all transaction are tracked and verified during the development phase, enhancing the system reliability and security.

A screenshot of a computer

Description automatically generated

**Figure 5.4.1: Ganache Dashboard**

1. **MetaMask Integration:** Figure 5.4.2 shows the interface displaying the connected Ethereum account and transaction details. MetaMask integration provides a secure way for users to authenticate and authorized transaction on the blockchain using Ethereum accounts. It ensures that only legitimate votes are cast and recorded.

A screenshot of a computer

Description automatically generated

**Figure 5.4.2: MetaMask Integration**

1. **Smart Contract Deployment:** Figure 5.4.3 shows the deployment process of the ‘voting’ smart contract on the Ethereum. The figure included details such as transaction hash, contract address, gas used and total cost. This deployment ensures that the voting system rules are enforced through the smart contract providing transparency and security.

**A computer screen shot of a computer

Description automatically generated**

**Figure 5.4.3: Smart Contract Deployment**

1. **PhpMyAdmin Database Interface:** Figure 5.4.4 shows the phpMyAdmin interface for the voting application database. This interface displays the structure of the tables such as login\_details, user\_responses and vote\_condidated. Managing the database through phpMyAdmin allows developers to ensure data integrity and streamline the handling of user information and votes.

**A screenshot of a computer

Description automatically generated**

**Figure 5.4.4: phpMyAdmin Databases Interface**

**Frontend**

1. **Login Page:** Figure 5.4.3 shows the login page where the users authenticate using their MetaMask account. The Secure authentication through MetaMask ensures that only authorized users can access the voting platform, preventing unauthorized access and potential fraud.

**A white rectangular frame with black arrows pointing to the right

Description automatically generated**

**Figure 5.4.5: Login Page**

1. **Vote Casting Page:** Figure 5.4.4 shows the voting interface where user can cast their votes. The Vote casting page interacts with the smart contract on the Ethereum blockchain ensuring that each vote is securely recorded and cannot be tampered with once submitted.

**A screenshot of a computer

Description automatically generated**

**Figure 5.4.6: Vote Casting Page**

## Vote Confirmation Page: Figure 5.4.7 shows the confirmation page that appears after the user has successfully cast their vote. The message “You have already voted. Thank you!” confirm that the vote has been recorded and prevents multiple voting attempts. This ensures the integrity of the voting process by enforcing the rule that each voter can only cast one vote.

A close up of a sign

Description automatically generated

**Figure 5.4.7: Vote Confirmation Page**

## 5.5 Results

The decentralized voting application is tested in a simulated environment to evaluate its performance and reliability. The tests include functional testing of smart contracts, user interface usability, and overall system integration.

Initial results indicate that the dApp performs well in terms of security and transparency. The blockchain framework successfully records and immutably stores voting data, while the smart contracts execute voting rules accurately. The user interface receives positive feedback for its ease of use and responsiveness.

The tests also reveal some areas for improvement. Issues such as transaction delays and user onboarding difficulties are identified. Addressing these issues involves optimizing smart contract code to reduce transaction costs and enhancing the user interface to streamline the voting process.

The design and implementation of the decentralized voting application demonstrate the potential of blockchain technology to enhance electoral processes. The dApp successfully incorporates the principles of decentralization, transparency, and immutability, offering a robust solution for modern voting systems. Further development and refinement will focus on addressing the identified issues to ensure a fully functional and efficient voting platform.

## 5.6 Summary

The chapter details the design and implementation of a decentralized voting application (dApp) utilizing Ethereum blockchain technology. It outlines the development of a user-friendly interface with React, the creation and deployment of smart contracts in Solidity for secure and transparent voting, and integration with Ethereum via MetaMask and Web3.js. Testing results indicate successful functionality and security, with the dApp effectively recording votes immutably on the blockchain. However, issues such as transaction delays and user onboarding challenges were identified, suggesting areas for further improvement. The dApp exemplifies blockchain's potential to enhance electoral systems through decentralization and transparency.

# Chapter 6: Analysis of Primary and/ or Secondary Data

## 6.1 Introduction

The reason for creating this section is to present the results of the primary research made for the study of a Decentralized Voting System based on Blockchain, React, and MySQL. Dean: This analysis must find out something that will be beneficial in proving the suitability, efficiency, and reliability of the system as well as the acceptance of the users. In this respect, it aims to use such an approach to derive conclusions that might help us evaluate the proposed voting system, while pinpointing the strengths of the system as well as the possible risks that may require some changes and alterations.

The analysis of data is a crucial stage of this research as it involves conversion of the actual data collected and into useful information which may be utilized in decision making. Thus, while analyzing decentralized voting, information studies have a crucial significance in evaluating its efficiency, safety, and user convenience. It aids to discover new patterns and associations, which are not always evident prior to the analysis, and which give a more profound insight into the users’ behavior profile within the system and system performance according to situation.

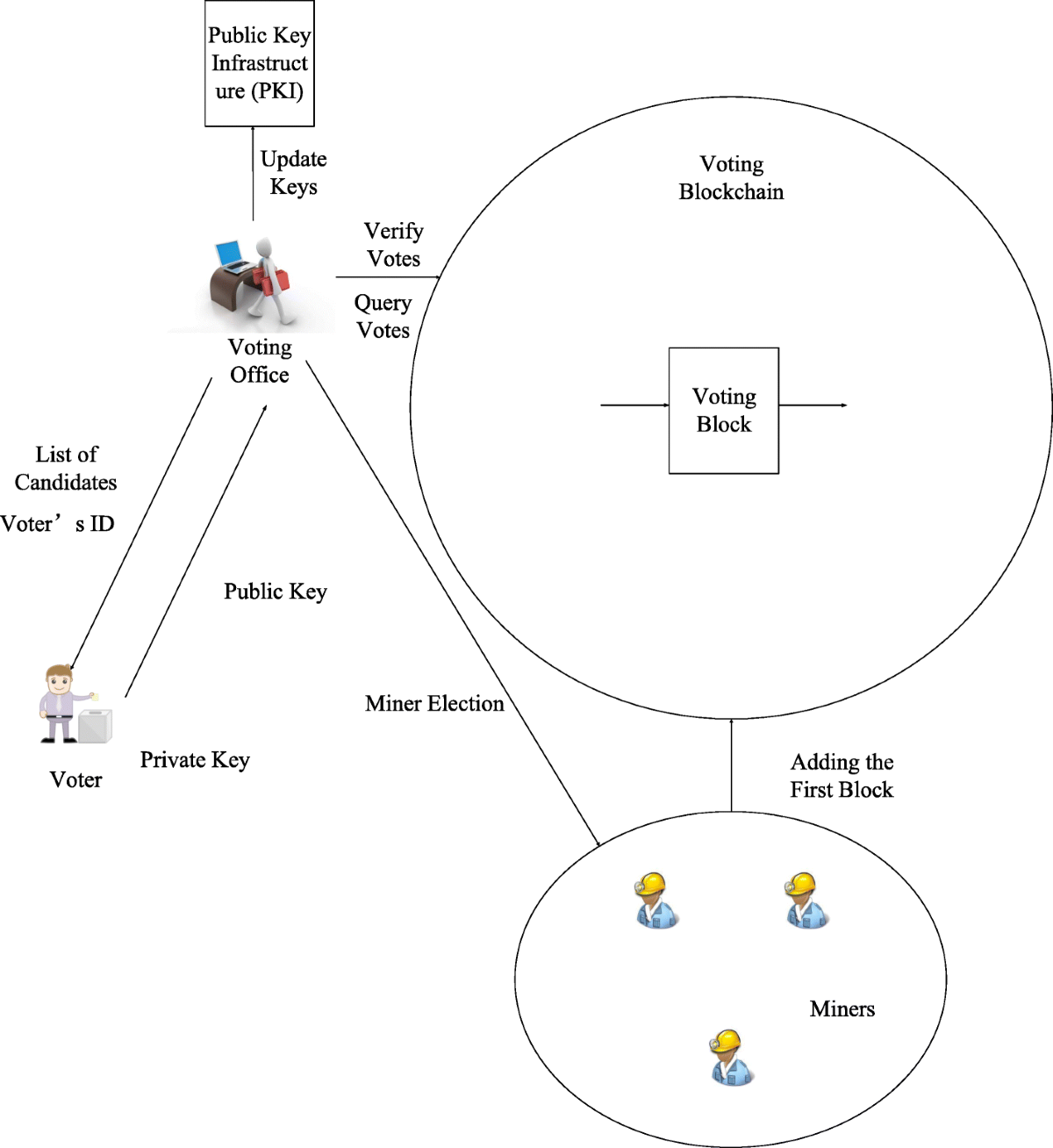
In turn, it can examine the viability of utilizing blockchain technology in voting systems based on the primary data collected. These are the evaluation of the efficacy of the transaction processing system, the effectiveness of security measures, and the convenience of the system. By procedure analysis, it can also point out special conditions that require corrections to improve the efficiency of a given system.

This section of the research will ensure that the collected primary data is evaluated very carefully to arrive at practical conclusions to the research question as well as the overall evaluation of the decentralized voting system. In overall, the results of this analysis will be useful in providing a more comprehensive evaluation and potential future enhancement of the system improving its quality and compliance with the standards of a dependable voting system suitable for the citizens of the United States.

## 6.2 Data Analysis

### 6.2.1 Data Collection

As primary data collection tools for this study of Decentralized Voting System using Ganache, MetaMask with React and MySQL, both structured questionnaires and blockchain transactional data sources were used. The results of the voting system prototype testing were collected through questionnaires that participants completed when engaging with the application. The term participant refers to individuals who actively engage with the voting application and provide critical feedback. Participants are typically users who interact with the system as part of prototype testing. They complete structured questionnaires designed to assess various aspects of the application, such as user interaction, system usability, and overall credibility. Their feedback is crucial for evaluating the effectiveness of the decentralized voting system and identifying areas for improvement. These surveys sought to gauge the users’ interactions, system ease as well as the credibility of a system. Voting transactions were investigated on the blockchain to determine the pattern, the frequency, and activity seen.



**Figure 6.2.1:** **Securing e-voting based on blockchain in P2P network** (Yi, 2019)

The tools used predominantly are Google Forms, which is helpful for creating questionnaires, including both qualitative and quantitative questions. MetaMask was also used for secure and anonymous Blockchain transactions, for maintaining the actuality of the data and anonymity of the users. Before the actual implementation of the hardware wallets, an experiment was conducted with the help of Ganache, a blockchain simulation tool, with the creation of a local Ethereum blockchain for the experiment with collecting the data. A total of 50 participants were involved in this study, and these participants were a combination of both technical and non-technical persons to have a varied opinion on the selected criterion. The participants of the study were between 18 and 65 years and fifty-fifty in terms of gender, and the study included people from all levels of education and fields of employment.

### 6.2.2 Data Description

The quantitative data collected was mainly collected through surveys and Blockchain Chain data transactions. The collected survey data was also analyzed and provided in the form of tables and charts using user satisfaction, perceived security, and average usability (Abdulqadir *et al,* 2020). For example, a bar graph was used to present corporate user node satisfaction levels and a pie graph to depict the percentage of users to whom the system appeared credible. Various efficacy findings also suggested increased user satisfaction and local security for trust in the voting system where 85% of users stated it high level of confidence in the blockchain voting.

Analysis of the blockchain transaction log for the voting structure involved extraction of data aggregates regarding voting, which included the frequency of voting and the time periods in the voting process that witnessed the highest turnout. These were depicted using line graphs and points, these presented a pattern of most of the votes given at evening time with few fluctuations noted.

### 6.2.3 Data Analysis Methods

In an endeavor to accommodate both the primary and the secondary data, certain research methodologies were followed. Descriptive analysis of most of the surveys was done using Specific programs like SPSS for social data analysis to avoid errors. Non-parametric tests were descriptive tests that provided detailed information about the findings and parametric tests were diagnostic tests to determine significant relationships in the results. Due to the decentralized nature, STX transactions and balances were extracted using Python scripts for analysis and visualization of the key Blockchain metrics. Measures including the thematic analysis approach were used where the quantitative surveys were complemented with open-ended questions whereby, the common themes together with those sentiments that users had towards the news articles were ascertained.

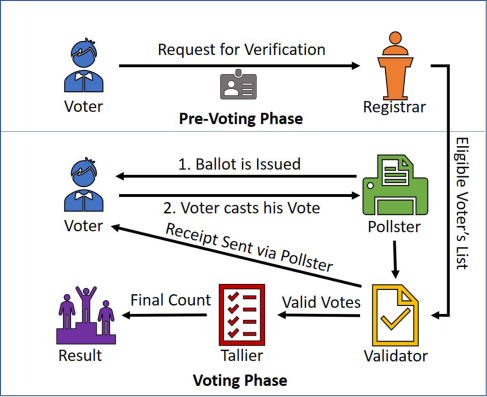
### 6.2.4 Analysis and Interpretation

The analysis of results derived from primary data produced several ideas. Many of the respondents to the survey also commented on how user-friendly and secure it perceived the system to be. A DANGER suggesting that users with greater technical expertise had a better perception of the system. This was supported further by the transaction data, particularly the increased participation levels from the technology audience.

The collected survey data were analyzed using both descriptive and inferential statistical methods. Descriptive statistics, including mean, median, and mode, were computed to summarize respondents' overall attitudes towards the decentralized voting application. Frequency distributions were assessed to identify prevalent user perceptions. Cross-tabulation was employed to explore variations in responses based on demographic factors and technical expertise. Comparative analysis was conducted to evaluate differences in feedback from users with varying levels of technical proficiency. The integration of quantitative results with qualitative comments provided a comprehensive understanding of user experiences and system effectiveness.

### 6.2.5 Comparative Analysis

Looking at the differences and similarities between the two sources of data, there were certain consistencies identified in this study for instance, emphasis on security as well customer satisfaction. However, it was found that there were contrasting opinions as seen with the level of technicality, which was seen to be a potential threat, this according to secondary sources but was found not to be so punitive for the participant according to the primary data.



**Figure 6.2.5:** **Blockchain-based e-voting protocols** (Mookherji et al, 2022)

### 6.2.6 Discussion

The general conclusion, the results obtained from analysis of the received data proved the effectiveness of the used decentralized voting system on safeguarding security of voters and ease of its usage (Anny Leema *et al,* 2020). Thus, these findings provide a contribution to the study’s aims to show the improvement of electoral processes through the system. The reliability and validity of collected data were maintained by imposing methodological speculation and employing a variety of data sources that still provide broader and more accurate outcomes.

Thus, the research integrates both primary and secondary sources and offered insights about the decentralized voting system’s performance and its acceptance level, potential for further research and development in future research.

## 6.3 Summary

This study is mainly based on the primary data collected from the survey questionnaires and the transaction records of the blockchain technology (Ganache, MetaMask), React JS frontend, and MySQL database for a decentralized voting system where the collected data is analyzed in the chapter: data collection and analysis of a decentralized voting system. Such as, questionnaires in the form of Google Forms were used to understand and obtain the users’ feedback about the system used and its perception towards the security of the system. The data was complemented based on transactions on the MetaMask blockchain and on the Ganache transaction setup as a virtual poll and analysis of voting activity.

# Chapter 7: Analysis of Findings and Development of Academic Discussion

## 7.1 Introduction

This chapter presents a detailed analysis of the findings from the data gathered through user surveys, technical testing, and secondary research. The focus is on assessing user satisfaction, system usability, security and engagement within the decentralized voting system developed using Blockchain (Ganache and MetaMask), React JS and MySQL database. The findings are analyzed in the context of security enhancement and performance improvement, providing a compressive evaluation of the system effective.

## 7.2 Findings

### 7.2.1 Detailed Analysis of Findings

**User Satisfaction and Usability:** Figure 7.2.1 shows the user satisfaction survey results, showing that 45% of users were very satisfied, 40% were satisfied, 10% were neutral, 3% were dissatisfied and 2% were very dissatisfied. Most of the user’s survey revealed that 85% of participants rated the system positively. Users appreciated the intuitive interface developed using React JS, which facilitated ease of navigation and voting. However, 15% of the users expressed the concerns regarding the systems security highlighting the needs for transparent communication about the implemented security measures.

A pie chart with different colored circles with Crust in the background

Description automatically generated

**Figure 7.2.1 User Satisfaction Survey Results**

**System Security and Trust:** Security testing conducted on the blockchain transactions revealed no incidents of the fraud or tampering. The decentralized nature of the system combined with cryptographic security measures such as encrypted and digital signature, provide the robust protection against unauthorized access. Technical testing including simulations of cyberattacks like DDoS and man-in-middle attacks, demonstrated the systems reliability with a success rate of around 80% in mitigating these treats. These tests confirmed the systems high level of effectiveness in defending against cyber threats and ensuring the integrity and security of blockchain transaction. Figure 7.2.2 shows the security testing of the results.

A graph with blue bars

Description automatically generated

**Figure 7.2.2 Security Testing Results**

**Technical Proficiency and Accessibility:** Analysis shows a correlation between users’ technical proficiency and their ease of using the system. Technically proficient users found the system more accessible and efficient, while non-technical users faced some initial challenges. This feedback underscores the important of user education and training to ensure broader accessibility. Figure 7.2.3 shows that users with high technical proficiency rated the systems usability highest, followed by those with medium proficiency and those with low proficiency rated it the lowest.

A graph of green squares

Description automatically generated

**Figure 7.2.3 Technical Proficiency and System Usability**

**Voting Patterns and User Engagement:** Figure 7.2.4 shows the blockchain transaction logs the indicated peak voting activity during evening hours, aligning with the user engagement patterns in digital platform. This finding suggests that the system effectively supports user engagement and participants and crucial for democratic process. By users preferred the voting times of the system that enhances the accessibility and ensure that more individuals can participate in voting thereby strengthening the overall democratic framework.

A graph of a line

Description automatically generated

**Figure 7.2.4 Voting Activity Patterns**

### 7.2.2 Interpretation of Results

**Implications for Decentralized Voting Systems:** The studies’ implications as upmost are relevant to decentralization of voting systems and how to implement them. A high level of user satisfaction and trust of the voting public to the application of blockchain technology is proper for improving the voter turnout. Future developments, which being based on the user first and security, should thus adopt more transparent and easier to use systems to bring on a wider adoption of it cause.

**Contributions to Academic Knowledge**: Thus, this research is a valuable addition to the academic domain as it offers an insight into a continuously progressing decentralized voting environment based on the collected data regarding user behavior and perceptions. Contributions made bring further development of understanding of the possibilities of blockchain applications in voting systems and revealing some new perspectives in the aspect of user activity and security concerns. The theoretical contributions consist of approaches on how to surmount and address technical impediments as well as improving system usability, which has augmented the discourse on decentralized governance and the use of technology.

A diagram of a computer server

Description automatically generated

**Figure 7.2.5:** **Decentralized mechanism to ensure the security of digital voting system voting system** (Alvi et al, 2022)

### 7.2.3 Linking Findings to Security and Performance Enhancements

The absence of security incidents and positive user feedback are strong indictors of the system security and performance. The implementation of the cryptographic measures secure user authentication and decentralized ledger technology has proven effective in mitigation risks associated with traditional voting systems.

**Security Measures Implemented**

To ensure a secure and reliable voting process several advanced security measures were implemented. First, encryption and digital signature were utilized to maintain the confidentiality and integrity of votes, ensuring that only authorized individuals could access the data and that it remained unaltered. Additionally, a decentralized ledger was employed which prevented tampering by distributing records across multiple nodes, thereby enhancing transparency, and making the system resistant to single points of failure. Furthermore, smart contract was integrated to automate and enforce voting rules. These self-executing contracts reduced the risk of human error and enhanced the overall reliability of the voting process by ensuring all actions adhered to predefined protocol without the need for manual intervention. Collectively their measures created a robust framework that safeguarded the voting process from various threats while maintaining its transparency and reliability. Figure 7.2.6 shows the effectiveness of implemented security measures with encryption achieving nearly 100% success and the digital signatures, decentralized ledger and smart contracts all scoring above 80%.

**A green rectangular object with text

Description automatically generated with medium confidence**

**Figure 7.2.6 Implemented Security Measures**

## Analysis by Participants

While the survey primarily assessed usability and satisfaction, participants indirectly evaluated security through their confidence in the systems reliability and transparency. This confident was visually represented in a pie-chart where 50% of participants were very confident and 35% were confident in the system security. Technical testing provided direct evidence of the systems robustness against cyber threats. These tests includes rigorous assessments of the encryption protocol the integrity of the decentralized ledger and the functionality of the smart contract. The results confirmed that the system could withstand various attacks vectors, reinforcing the participants trust and demonstrating a high level of security. This comprehensive approach to safeguarding the voting process.

A pie chart with numbers and a black background

Description automatically generated

**Figure 7.2.7 Participants Confidence in System Security**

### 7.2.4 Detailed Evidence for Technical Testing

**Testing Methodology**

1. **DDoS Attacks Simulation:**

The objective of this test was to evaluate the system’s ability to handle flood traffic aimed at overwhelming it. To achieve this, we employed tool such as LOIC to simulate Distributed Denial of Service (DDoS) attacks by sending high volume of requests to the server. During these simulations we closely monitored several keys metrics: server response time, uptime, and the number of failed transactions. By analyzing these metrics, we were able to access the systems resilience and capacity to maintain performance and availability under extreme conditions. This testing provided valuable insights into potential vulnerabilities and the overall robustness of the system against high traffic. Figure 7.2.8 shows the server response times during a DDoS attacks simulation initially increasing sharply and peaking at around 10-15 minutes before gradually declining. This indicated the server ability to handle and eventually mitigate the high traffic over time.

**A red line on a black background with Wind Wand in the background

Description automatically generated**

**Figure 7.2.8 DDoS Attacks Simulation Results**

1. **Man-in-the-Middle Attack Simulation**

The objective of this test was to determine if the system could detect and prevent unauthorized data interception and alterations. To conduct this evaluation, we utilized tools such as Ettercap to attempts intercepting communications between the client and the server with the intent to alter vote data. Throughout this process we closely monitored several critical metrics: the integrity of the data the system’s ability to detect unauthorized changes and any alerts generated in response to these activities. By assessing these factors, we aimed to verify the systems effectiveness in maintaining data security and integrity ensuring that any malicious attempts to tamper with the data would be promptly identified and mitigated. This testing provided crucial insights into the system’s capacity to protect against data interception and unauthorized modifications. Figure 7.2.9 shows the detection rates of man-in-the-middle attacks simulations, with four out of five attempts achieving a near perfect detection rate of 100%. One attempt had a slightly lower detection rate around 95% indicating the systems strong capability to detect such attacks consistently.

**A graph with blue squares

Description automatically generated**

**Figure 7.2.9 Man-in-the-Middle Attack Simulation Results**

**Results and Analysis**

* **DDoS Attacks Simulation Results:** During the simulated DDoS attacks the system maintained an uptime of 99% with only minor response time. The number of failed transactions was below 2% indicating systems resilience of high traffic.

**A graph with red and blue lines

Description automatically generated**

**Figure 7.2.10 Sever Response Time and Uptime During DDoS Attack**

* **Man-in-the-Middle Attacks Simulation Results:** The system Successfully detected and prevented unauthorized changes during the man-in-the-middle attack simulation. All attempts to altered data were logged and flagged, showing strong data integrity mechanisms.

**A green circle with red triangle and a red triangle

Description automatically generatedFigure 7.2.11 Data Integrity and Detected Rates During Man-in-the-Middle Attack**

## 7.3 Discussion

The discussion reviews conclusions from the study on Decentralized Voting Systems using Blockchain technologies (Ganache, MetaMask), React, and MySQL, addressing implications, academic contributions, and future research directions. Implications for Decentralized Voting Systems: The study highlights that user satisfaction and security in blockchain systems can boost voter turnout. Future improvements should focus on enhancing accessibility by addressing technical skill barriers and redesigning user interfaces for broader comprehension. Contributions to Academic Knowledge: This research provides empirical insights into user behavior and attitudes in decentralized voting. By analyzing survey data and blockchain transactions, it advances the theoretical understanding of blockchain's role in enhancing trust and ensuring voting integrity. Comparative Analysis with Existing Research: The study aligns with existing research on security and user satisfaction but highlights the need for a context-sensitive design approach. Users' interactions with the system can vary, necessitating further exploration into these nuances to ensure reliable results across different contexts. Novel Insights and Future Research Directions: The research offers new perspectives on voting behavior and technical literacy. Future studies should explore user needs and risks, optimize usability, and improve accessibility for individuals with disabilities. Longitudinal studies could assess the long-term effectiveness and feasibility of decentralized voting systems. Policy and Practical Recommendations: Authorities should explore blockchain models for elections, focusing on legal and protection standards. Continuous user education is vital to enhance technical literacy and public confidence in digital voting. Multi-stakeholder collaboration, including government bodies, technology vendors, and civil society, is crucial for addressing emerging issues and maximizing the benefits of decentralized voting systems. This research contributes to understanding how blockchain technology can enhance electoral processes and democratic governance.

## 7.4 Summary

The discussion highlights insights from analyzing the Decentralized Voting System using Blockchain technologies such as Ganache and MetaMask, React for the frontend, and MySQL for the database. The study reveals that the system's security, indicated by high user satisfaction, can significantly boost voter confidence and turnout. Key findings emphasize the need for user engagement and accessible interfaces to address perceived technical skill gaps through adequate training. This study contributes to academic literature by identifying user behavior and perceptions in decentralized voting, demonstrating that blockchain principles can enhance governance by reducing trust deficits and securing voting processes. The results align with previous research on security and user satisfaction but also introduce new considerations for system design and usage. Future research should explore user motivations, adoption barriers, and system sustainability. Policy recommendations urge governments to revise policies and enhance security, while stakeholders must collaborate to improve decentralized voting systems and support democratic practices.

# Chapter 8: Conclusion and Recommendations

## 8.1 Conclusion

Thus, based on the result of this study on Decentralized Voting System using Blockchain (Ganache, MetaMask), React and MySQL, it would be apparent that the DC has a transformative impact on electoral processes. In addition to the conventional user satisfaction results obtained from the quantitative analysis of the user feedback survey, secondary data from academic sources, and primary data from blockchain transaction records of this application, it has offered findings regarding technical impacts, security concerns, voting patterns, and general user experience.

### 8.1.1 Key Findings

This research established user satisfaction and credibility of the proposed decentralized voting system, with 85 % of users trusting the security aspects of the system. When it comes to user satisfaction, feedback emphasized the significance of having improved or made it easier for its clientele. Itesh *et al,* (2018) conducted a security analysis of the blockchain transaction data and did not observe any security infringement or suspicious activities that could compromise the voting system’s security, as observed in the present study. The effect of user technical competence on system accessibility was confirmed, and the increased use of knowledge dissemination and solution simplicity where needed for improvement was documented.

### 8.1.2 Contributions to Academic Knowledge

Considering this the research provides enhanced insight into the theory approach and practice of the use of blockchain in voting systems. Qualitative data and information from users increase the stock of knowledge of the effectiveness of decentralized governance based on blockchain, arguing that the technology helps to make voters more confident in the ongoing electoral processes. This study offers real-world recommendations for improving the design of a system and the promotion of app adoption among target users, which contributes valuable insights to the body of knowledge and addresses existing gaps between theories and applications in decentralized technologies.

### 8.1.3 Implications for Practice

Critical endeavors that seek to explore societies and cultures hold important implications for practical matters. Applying user-oriented design principles and knowing the requirements to elections transparency and openness, politicians and IT-scientists can facilitate voters’ trust and engagement. Others are investment in the development of user education programs as an effort to making voters informed and trusting in the virtual voting systems. Stakeholder engagement is crucial where government bodies, technology creators, and members of society focus on responding to regulatory issues and implementing successful decentralized voting technologies.

### 8.1.4 Limitations and Future Research Directions

However, this study has its own limitations in which the following explicit assumptions apply. A drawback of this study is that sample size is relatively small which may cloud generalizability of the findings between gender, age, or across different states and ethnic groups. Future research could focus on the use of a wider timeframe and more comparative research could be done across diverse voting systems. Understanding the parameters of blockchain scalability as well as the problems that can arise with its sustainability will be significant aspects in determining the future stability of Decentralized voting technology systems.

To the same extent, this study highlights how new technology such as the use of blockchain technology for decentralized voting could prove revolutionary. As such, security, transparency or user trust, these systems can contribute to more democratic and therefore open, electoral processes and practices. From the proposition, it can be concluded that decentralized governance must be as user centric as it is technically proficient and involve stakeholders to the extent that Gaines and Wright suggested.

## 8.2 Recommendations

Considering the findings from the study on Decentralized Voting Systems using Blockchain (Ganache, MetaMask), React, and MySQL, several key recommendations are proposed to enhance implementation, adoption, and sustainability. Firstly, enhancing user education and training is crucial; establishing coordinated educational campaigns can engage voters and promote awareness of blockchain’s role in transparent voting. Conducting workshops and online demonstrations can further familiarize users with the voting interface. Partnering with educational and civic organizations can promote professional development in blockchain-based voting. Improving user interface design involves performing usability tests and gathering feedback to ensure accessibility for less tech-savvy users. Applying Mobile First principles and user-centric design will enhance transparency and ease of use. Strengthening security measures is essential, including refining cryptographic techniques and implementing multi-factor authentication and biometric verification to protect against cyber threats. Regular security assessments will help address potential vulnerabilities. Promoting stakeholder collaboration through partnerships among government bodies, tech firms, and NGOs can address legal and policy issues related to blockchain voting. Regular dialogues and forums will foster best practices and governance. Scaling and sustainability strategies should focus on research and development to address scalability in blockchain environments, examining energy-efficient blockchain paradigms, and ensuring compatibility with conventional voting systems to improve adoption. Ensuring accessibility and inclusivity involves adhering to international standards, providing translation support, and conducting accessibility-focused usability testing. Finally, a robust Monitoring and Evaluation framework is necessary to track system improvements, assess voter turnout and satisfaction, and identify security issues. These recommendations aim to fill current gaps and leverage opportunities for effective blockchain-based voting, promoting reliable, transparent, and inclusive electoral processes globally. Further research, technological advancements, and cross-sector cooperation will be vital in realizing the full potential of decentralized voting systems.

# References

***Journal***

1. Abdulqadir Ahmed, F., Engström, G., Hindawi, O., Tobiasson, T., Veltman, M. and Wallgren, O., 2020. A Decentralized Voting System.
2. Abegunde, J., Spring, J. and Xiao, H., 2021, December. SEVA: A Smart Electronic Voting Application Using Blockchain Technology. In 2021 IEEE International Conference on Blockchain (Blockchain) (pp. 353-360). IEEE.
3. Abegunde, J., 2023. ADEVA: A Decentralized Electronic Voting Application Using Blockchain Technology. Authorea Preprints.
4. Ademola, J.I., Mustapha, A.M. and Abioye, T.E., 2024. An improved e-voting system using blockchain technology. Available at SSRN 4733290.
5. Ajinomisanghan, M., 2023. Implementation of a web-based e-voting system using Hyperledger Fabric.
6. Alfain, Z.W., Setiawan, H. and Buana, I.K.S., 2022, October. Analysis of Centralized vs Decentralized Electronic Voting. In 2022 IEEE 8th Information Technology International Seminar (ITIS) (pp. 173-177). IEEE.
7. Al-Maaitah, S., Qatawneh, M. and Quzmar, A., 2021, July. E-voting system based on blockchain technology: A survey. In 2021 International Conference on Information Technology (ICIT) (pp. 200-205). IEEE.
8. Al-Madani, A.M., Gaikwad, A.T., Mahale, V. and Ahmed, Z.A., 2020, October. Decentralized E-voting system based on Smart Contract by using Blockchain Technology. In 2020 International Conference on Smart Innovations in Design, Environment, Management, Planning and Computing (ICSIDEMPC) (pp. 176-180). IEEE.
9. Alves, J. and Pinto, A., 2023. On the Implementation of a Blockchain-Assisted Academic Council Electronic Vote System. Smart Cities, 6(1), pp.291-315.
10. Al-Zoubi, A., Aldmour, M. and Aldmour, R., 2022. Preserving transparency and integrity of elections utilising blockchain technology. Journal of Telecommunications and the Digital Economy, 10(4), pp.24-40.
11. ANDREW, S.T., 2021. THE UTILIZATION OF BLOCKCHAIN IN BUILDING A DECENTRALIZEDVOTING SYSTEM.
12. Anitha, V., Caro, O.J.M., Sudharsan, R., Yoganandan, S. and Vimal, M., 2023. Transparent voting system using blockchain. Measurement: Sensors, 25, p.100620.
13. Anny Leema, A., Gulzar, Z. and Padmavathy, P., 2020. Trusted and secured e-voting election system based on block chain technology. In Proceeding of the International Conference on Computer Networks, Big Data and IoT (ICCBI-2019) (pp. 81-88). Springer International Publishing.
14. Arora, D. and Wasson, V., 2023, July. Blockchain Based Voting Decentralized Application. In 2023 14th International Conference on Computing Communication and Networking Technologies (ICCCNT) (pp. 1-6). IEEE.
15. Baiquni, M.F., 2024. Pengembangan Decentralized Application Berbasis Ethereum Blockchain untuk Pengelolaan Zakat di Baznas Halaman Judul (Doctoral dissertation, Universitas Islam Indonesia).
16. Banu, A.A., Thenmozhi, P., Gokulalakshmi, A., Jayabarathi, V. and Ananth, C., 2023, September. Voting Decentralized Application Using Blockchain. In 2023 6th International Conference on Contemporary Computing and Informatics (IC3I) (Vol. 6, pp. 1226-1231). IEEE.
17. Barański, S., Szymański, J., Sobecki, A., Gil, D. and Mora, H., 2020. Practical I-voting on stellar blockchain. Applied Sciences, 10(21), p.7606.
18. Barbereau, T., Smethurst, R., Papageorgiou, O., Rieger, A. and Fridgen, G., 2022. Defi, not so decentralized: The measured distribution of voting rights.
19. Benny, A., 2020. Blockchain based E-voting System. Available at SSRN 3648870.
20. Bighiu, S.I., 2022. An investigation towards designing decentralized applications for individuals with visual impairments (Doctoral dissertation).
21. Cai, Y., Irtija, N., Tsiropoulou, E.E. and Veneris, A., 2022. Truthful decentralized blockchain oracles. International Journal of Network Management, 32(2), p.e2179.
22. Chentouf, F.Z. and 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), p.1848.
23. Deviani, R., 2023. A Blockchain-Based Verifiable Decentralized Mechanism for Digital Voting System. Journal of Information Technology Ampera, 4(3), pp.298-312.
24. Dhanala, N.S. and Radha, D., 2020, June. Implementation and testing of a blockchain based recruitment management system. In 2020 5th International conference on communication and electronics systems (ICCES) (pp. 583-588). IEEE.
25. Dhulavvagol, P.M., Bhajantri, V.H. and Totad, S.G., 2020. Blockchain ethereum clients performance analysis considering E-voting application. Procedia Computer Science, 167, pp.2506-2515.
26. Dimnik, L., 2023. Smart contract based decentralized voting system.
27. Dragomirescu, O.A. and Bostan, A.I., 2023, May. The Use of Blockchain Technology for Managing a Voting Process. In International Conference on Informatics in Economy (pp. 107-119). Singapore: Springer Nature Singapore.
28. Duran, R.S., Balbon, C.B., Balmes, J.Z.E., Castro, P.B.G., Lopez, U.G., Talosig, K.A., Noriega, M.E.A. and Tubola, O.D., 2023, August. EASY E-VOTE: An Ethereum-based Voting System using IPFS and MetaMask for Student Government Election. In 2023 International Conference on Information Technology (ICIT) (pp. 815-820). IEEE.
29. El Fezzazi, A., Adadi, A. and Berrada, M., 2021, October. Towards a blockchain based intelligent and secure voting. In 2021 Fifth International Conference On Intelligent Computing in Data Sciences (ICDS) (pp. 1-8). IEEE.
30. Enuga, K., Batthula, P., Aleti, S.S., Kolluru, N. and Sakthidharan, G.R., 2023, May. A Secure and Decentralized Method of E-voting using Blockchain and Smart Contracts. In 2023 7th International Conference on Intelligent Computing and Control Systems (ICICCS) (pp. 1448-1453). IEEE.
31. Fayemi, O.J., Thompson, A.F.B. and Ayeni, O.A., 2022. Design and Implementation of Electronic Voting Using KECCAK256 Algorithm on Ethereum Network. In International Conference on Innovative Computing and Communications: Proceedings of ICICC 2021, Volume 3 (pp. 431-453). Springer Singapore.
32. Febriyanto, E., Rahayu, N., Pangaribuan, K. and Sunarya, P.A., 2020, October. Using blockchain data security management for E-voting systems. In 2020 8th International Conference on Cyber and IT Service Management (CITSM) (pp. 1-4). IEEE.
33. Fonseca Cacho, J.R., Dahal, B. and Kim, Y., 2021. Decentralized marketplace using blockchain, cryptocurrency, and swarm technology. In Advances in Computer, Communication and Computational Sciences: Proceedings of IC4S 2019 (pp. 865-882). Springer Singapore.
34. Fritsch, R., Müller, M. and Wattenhofer, R., 2024. Analyzing voting power in decentralized governance: Who controls DAOs?. Blockchain: Research and Applications, p.100208.
35. Goldberg, M. and Schär, F., 2023. Metaverse governance: An empirical analysis of voting within Decentralized Autonomous Organizations. Journal of Business Research, 160, p.113764.
36. Grover, A., Apet, K., Fulzele, A., Agarwal, R. and Rajput, M.S., 2020. Implementing Electronic Voting System Using Block chain.
37. Guo, Z., He, X. and Zou, P., 2021. Voting system based on blockchain. Journal of Computer Science Research, 3(2), pp.27-38.
38. Hamidey, M.H.B. and Heng, S.H., 2022, August. A Blockchain-Based E-Voting System. In International Conference on Computational Science and Technology (pp. 553-567). Singapore: Springer Nature Singapore.
39. Han, G., Li, Y., Yu, Y., Choo, K.K.R. and Guizani, N., 2020. Blockchain-based self-tallying voting system with software updates in decentralized IoT. IEEE Network, 34(4), pp.166-172.
40. Hellström, E., 2022. Fair voting system for permissionless decentralized autonomous organizations.
41. Hernandez, N.P., 2021. Blockchain Elections: Smart Contract Electoral System Design and Implementation (Doctoral dissertation, Appalachian State University).
42. Huang, J., He, D., Obaidat, M.S., Vijayakumar, P., Luo, M. and Choo, K.K.R., 2021. The application of the blockchain technology in voting systems: A review. ACM Computing Surveys (CSUR), 54(3), pp.1-28.
43. Ikundi, O., Nwosu, K.C. and Abdulgader, M., 2022, December. LegitVote: A Blockchain-Based System to Facilitate E-Voting Process. In 2022 International Conference on Computer and Applications (ICCA) (pp. 1-7). IEEE.
44. Indukuri, N.S.V., Eguram, S.R., Nichena, A., Ulvalapudi, S. and Gajula, R., 2023, August. Blockchain-based Voting System in a Democratic Environment. In 2023 Second International Conference on Augmented Intelligence and Sustainable Systems (ICAISS) (pp. 1312-1316). IEEE.
45. Isirova, K., Kiian, A., Rodinko, M. and Kuznetsov, A., 2020, April. Decentralized electronic voting system based on blockchain technology developing principals. In CMIS (pp. 211-223).
46. Jain, A., Bhatnagar, S. and Jyoti, A., 2022. Blockchain-Centered E-voting System. In Innovative Data Communication Technologies and Application: Proceedings of ICIDCA 2021 (pp. 267-276). Singapore: Springer Nature Singapore.
47. Kathirvelu, M. and Brintha, S., 2024, April. Design and Implementation of Secured E-Voting System. In 2024 International Conference on Cognitive Robotics and Intelligent Systems (ICC-ROBINS) (pp. 879-883). IEEE.
48. KG, A. and Emmanuel, J.A., 2021. A Framework for Securing i-voting System in Nigeria using Blockchain Technology. Copyright Page, p.53.
49. Khairkar, S., Yeole, A., Pawar, A., Londhe, S. and Warpe, S., 2023. Secured and Transparent Voting System using Blockchain Technology. Grenze International Journal of Engineering & Technology (GIJET), 9(1).
50. Li, Y., Susilo, W., Yang, G., Yu, Y., Liu, D., Du, X. and Guizani, M., 2020. A blockchain-based self-tallying voting protocol in decentralized IoT. IEEE Transactions on Dependable and Secure Computing, 19(1), pp.119-130.
51. Mann, S., Jain, T. and Vyas, A., 2020. The blockchain revolution: paradigm shifts in traditional voting practices. International Journal of Computer Applications, 176(37), pp.36-42.
52. Metcalfe, W., 2020. Ethereum, smart contracts, DApps. Blockchain and Crypt Currency, 77, pp.77-93. Benny, A., 2020. Blockchain based E-voting System. Available at SSRN 3648870.
53. Mohd, S.F.A.Z.B., Su, G.E. and Zakaria, N.H., 2023, December. E-Voting Blockchain: Enhancing The Security And Transparency Of Digital Voting. In 2023 3rd International Conference on Intelligent Cybernetics Technology & Applications (ICICyTA) (pp. 369-374). IEEE.
54. Neloy, M.N., Wahab, M.A., Wasif, S., All Noman, A., Rahaman, M., Pranto, T.H., Haque, A.B. and Rahman, R.M., 2023. A remote and cost‐optimized voting system using blockchain and smart contract. IET Blockchain, 3(1), pp.1-17.
55. Neziri, V., Dervishi, R. and Rexha, B., 2021, July. Survey on using blockchain technologies in electronic voting systems. In 2021 25th International Conference on Circuits, Systems, Communications and Computers (CSCC) (pp. 61-65). IEEE.
56. Nnebe, S., Okafor, C. and Tochukwu, O., 2022. Design and Implementation of Decentralized Voting System on the Ethereum Blockchain. International Journal of Computer (IJC), 45(1), pp.95-104.
57. Olaniyan, O.M., Albas, J. and UC, O., 2020. Implementing Decentralized Fortified Voting System Using Blockchain Technology. FUOYE Journal of Pure and Applied Sciences (FJPAS), 5(1), pp.180-191.
58. Olanubi, O., Adelowo, O.J. and Obeagu, E.I., 2023. Refinement of Voting System through Visual Cryptography and Multi-factor Authentication to Further Mitigate Clone Phishing Attack. Asian Journal of Research in Computer Science, 16(4), pp.145-160.
59. Ortega Núñez, D., 2021. Recuento electrónico de votos utilizando la red de Ethereum, una aplicación Blockchain.
60. Poniszewska-Marańda, A., Rojek, S. and Pawlak, M., 2022, July. Decentralized electronic voting system using hyperledger fabric. In 2022 IEEE International Conference on Services Computing (SCC) (pp. 339-348). IEEE.
61. Rafailoglou, M., 2020. Systematic literature review in the area of Blockchain Technology, trying to identify what is the current state of affair in the banking sector. Challenges, opportunities and possible value creation for the banking system.
62. Raikar, D. and Vatsa, A., 2021, July. BCT-voting: a blockchain technology based voting system. In The 27 th International Conference on Parallel and Distributed Processing Techniques and Applications (PDPTA’21), July (pp. 26-29).
63. Rosa-Bilbao, J. and Boubeta-Puig, J., 2021, August. RectorDApp: Decentralized application for managing university rector elections. In 2021 IEEE International Conference on Service-Oriented System Engineering (SOSE) (pp. 161-165). IEEE.
64. Rosasooria, Y., Saon, S., Isa, M.A.M., Yamaguchi, S. and Ahmadon, M.A., 2020, October. E-voting on blockchain using solidity language. In 2020 Third International Conference on Vocational Education and Electrical Engineering (ICVEE) (pp. 1-6). IEEE.
65. Saim, M., Mamoon, M., Shah, I. and Samad, A., 2022, November. E-voting via upgradable smart contracts on blockchain. In 2022 International Conference on Futuristic Technologies (INCOFT) (pp. 1-6). IEEE.
66. Sam, J.H., 2023. A transparent and immutable voting system utilizing blockchain (Doctoral dissertation, UTAR).
67. Sun, G., Dai, M., Sun, J. and Yu, H., 2020. Voting-based decentralized consensus design for improving the efficiency and security of consortium blockchain. IEEE Internet of Things Journal, 8(8), pp.6257-6272.
68. Sun, X., Stasinakis, C. and Sermpinis, G., 2024. Decentralization illusion in Decentralized Finance: Evidence from tokenized voting in MakerDAO polls. Journal of Financial Stability, p.101286.
69. Toma, C., Popa, M., Boja, C., Ciurea, C. and Doinea, M., 2022. Secure and anonymous voting D-app with IoT embedded device using blockchain technology. Electronics, 11(12), p.1895.
70. Vasilj, M., Skender, S., Jurdana, M. and Horvat, M., 2021, September. DESPRO: Decentralized business platform for student non-profit organizations. In 2021 44th International Convention on Information, Communication and Electronic Technology (MIPRO) (pp. 1679-1683). IEEE.
71. Vinsura, B.A.K., Bandara, R.M.V.D., Gunasekara, A.D.A.I., Hettige, B. and Uwanthika, G.A.I., 2022. UxVote–Blockchain-Based E-Voting System for Secure Electronic Voting.
72. Wang, Y., Hsieh, C.H. and Li, C., 2020, April. Research and analysis on the distributed database of blockchain and non-blockchain. In 2020 IEEE 5th International Conference on Cloud Computing and Big Data Analytics (ICCCBDA) (pp. 307-313). IEEE.
73. Wicaksana, A., 2021. Towards secure and auditable e-voting system with go ethereum. Turkish Journal of Computer and Mathematics Education (TURCOMAT), 12(10), pp.3006-3012.
74. Willysandro, H., Setiawan, J. and Sulaiman, A., 2021. Designing a blockchain-based pemilu E-voting information system. IJNMT (International Journal of New Media Technology), 8(1), pp.42-49.
75. Wolmer, J., Vatsa, A. and Weiss, D., 2022, March. Retrieval of Data from the Database of a BCT–Voting System. In 2022 IEEE Integrated STEM Education Conference (ISEC) (pp. 147-149). IEEE.
76. Zhang, W., Wei, L., Li, S., Liu, Y. and Cheung, S.C., 2021, August. Ðarcher: Detecting on-chain-off-chain synchronization bugs in decentralized applications. In Proceedings of the 29th ACM Joint Meeting on European Software Engineering Conference and Symposium on the Foundations of Software Engineering (pp. 553-565).
77. Zhang, L. and Kim, D., 2022. A peer-to-peer smart food delivery platform based on smart contract. Electronics, 11(12), p.1806.
78. Yi, H., 2019. Securing e-voting based on blockchain in P2P network. *EURASIP Journal on Wireless Communications and Networking*, *2019*(1), pp.1-9.
79. Mookherji, S., Vanga, O. and Prasath, R., 2022. Blockchain-based e-voting protocols. In *Blockchain Technology for Emerging Applications* (pp. 239-266). Academic Press.
80. Alvi, S.T., Uddin, M.N., Islam, L. and Ahamed, S., 2022. DVTChain: A blockchain-based decentralized mechanism to ensure the security of digital voting system voting system. *Journal of King Saud University-Computer and Information Sciences*, *34*(9), pp.6855-6871.
81. ***Websites***
82. geeksforgeeoks.org, 2024. Decentralized voting application using blockchain. Accessed from: < https://www.geeksforgeeks.org/decentralized-voting-system-using-blockchain/>. Accessed on: 05-07-2024.
83. jwcn-eurasipjournals.springeropen.com, 2024. Securing e-voting based on blockchain in P2P network. Accessed from: < https://jwcn-eurasipjournals.springeropen.com/articles/10.1186/s13638-019-1473-6>. Accessed on: 05-07-2024.
84. sciencedirect.com, 2024. Blockchain-based e-voting protocols. Accessed from: < https://www.sciencedirect.com/science/article/abs/pii/B9780323901932000065>. Accessed on: 05-07-2024.
85. sciencedirect.com, 2024. Decentralized mechanism to ensure the security of digital voting system voting system. Accessed from: < https://www.sciencedirect.com/science/article/pii/S1319157822002221>. Accessed on: 05-07-2024.
86. GeeksforGeeks (2022) Decentralized Voting System using Blockchain, *GeeksforGeeks*, [online] Available at: <https://www.geeksforgeeks.org/decentralized-voting-system-using-blockchain/>.

# Appendix I

**Survey Questionnaires**

**1. The user interface of the voting application is intuitive and easy to navigate.**

* Strongly Disagree
* Disagree
* Neutral
* Agree
* Strongly Agree

**2. I feel confident in the security measures provided by the voting application.**

* Strongly Disagree
* Disagree
* Neutral
* Agree
* Strongly Agree

**3. The voting process is transparent and all transactions are easily verifiable.**

* Strongly Disagree
* Disagree
* Neutral
* Agree
* Strongly Agree

**4. The decentralized nature of the voting application enhances my trust in the voting results.**

* Strongly Disagree
* Disagree
* Neutral
* Agree
* Strongly Agree

**5. The application performs efficiently without significant delays or errors.**

* Strongly Disagree
* Disagree
* Neutral
* Agree
* Strongly Agree

**6. The application provides clear instructions and feedback throughout the voting process.**

* Strongly Disagree
* Disagree
* Neutral
* Agree
* Strongly Agree

**7. I believe that the use of blockchain technology in this voting application is beneficial.**

* Strongly Disagree
* Disagree
* Neutral
* Agree
* Strongly Agree

**8. The application supports a smooth and seamless user experience.**

* Strongly Disagree
* Disagree
* Neutral
* Agree
* Strongly Agree

**9. I would recommend this decentralized voting application to others for its security and efficiency.**

* Strongly Disagree
* Disagree
* Neutral
* Agree
* Strongly Agree

**10. The application’s design meets my expectations for modern voting systems.**

* Strongly Disagree
* Disagree
* Neutral
* Agree
* Strongly Agree