DESIGN AND IMPLEMENT A BLOCK-BASED DECENTRALIZED VOTING SYSTEM TO ENHANCE TRANSPARENCY, SECURITY AND ACCESSIBILITY IN ELECTORIAL PROCESS

ALO JOEL

ENG1603856

DEPARTMENT OF COMPUTER ENGINEERING

FACULTY OF ENGINEERING

UNIVERSITY OF BENIN,

EDO STATE, NIGERIA.

APRIL, 2024

DESIGN AND IMPLEMENT A BLOCK-BASED DECENTRALIZED VOTING SYSTEM TO ENHANCE TRANSPARENCY, SECURITY AND ACCESSIBILITY IN ELECTORIAL PROCESS

ALO JOEL

ENG1603856

DEPARTMENT OF COMPUTER ENGINEERING

FACULTY OF ENGINEERING

UNIVERSITY OF BENIN,

EDO STATE, NIGERIA.

SUPERVISED BY:

PROF S. T. APEH

A PROJECT SUBMITTED IN PARTIAL FULFILMENT FOR THE AWARD OF BACHELOR OF ENGINEERING (B.ENG) DEGREE IN COMPUTER ENGINEERING

APRIL, 2024

CERTIFICATION

This project was carried out by Alo Joel in the Department of Computer Engineering, Faculty of Engineering, University of Benin, Benin City, and is hereby certified.

_____ _____

Prof. S. T. Apeh Date

(Project Supervisor)

_____ _____

Engr. Dr. (Mrs) Okosun Date

Head of Department

DEDICATION

I dedicate this project to my family, whose unwavering support and encouragement have been my greatest source of strength throughout this journey. Thank you for your guidance and knowledge that have shaped my understanding of this field.

ACKNOWLEDGEMENT

I would like to begin by acknowledging God Almighty for his divine guidance and blessings. Without his grace, wisdom and strength this project would not have been possible.

I am deeply grateful to my supervisor, Prof. S. T. Apeh, for his invaluable guidance, unwavering support throughout the course of this project.

I extend my sincere appreciation to the dedicated staff of the Department of Computer Engineering for providing a conducive academic environment and access to resources that facilitated my research.

ABSTRACT

Voting is a fundamental process in a democratic society, but traditional voting systems often suffer from issues such as lack of transparency, security vulnerabilities, and limited accessibility. To address these challenges, this paper presents the design and implementation of a block-based decentralized voting system that leverages blockchain technology to enhance transparency, security, and accessibility in the electoral process.

The proposed system utilizes a block-based architecture to ensure the immutability and transparency of voting records. Each vote is recorded as a transaction in a blockchain, which is distributed across multiple nodes in the network. This decentralized approach eliminates the need for a central authority and reduces the risk of tampering or manipulation of votes.

To enhance security, the system employs advanced cryptographic techniques, such as digital signatures and hash functions, to protect the integrity of the voting process. Voters are required to authenticate themselves using secure methods, such as biometric identification or digital certificates, ensuring that only eligible voters can participate in the election.

The system also aims to improve accessibility by providing multiple channels for voters to cast their ballots, including web-based interfaces, mobile applications, and even physical voting stations equipped with blockchain-enabled devices. This flexibility allows voters to participate in elections from anywhere, reducing barriers to participation and increasing voter turnout.

The paper presents the design and implementation details of the proposed system, including the architecture, protocols, and algorithms used. It also discusses the challenges and limitations encountered during the development process and provides insights into future research directions.

The results of this study demonstrate the potential of blockchain technology in enhancing the transparency, security, and accessibility of electoral processes. The proposed system offers a viable alternative to traditional voting methods and can be adapted to various electoral contexts, contributing to the advancement of democratic practices worldwide.

Contents

Table of Figures

CHAPTER ONE

INTRODUCTION

1.0 BACKGROUND OF STUDY

Ensuring electoral integrity is not only crucial for democratic nations but also for fostering trust and accountability among state voters. The methods employed in political voting play a pivotal role in upholding this integrity. From a governmental perspective, the adoption of electronic voting technologies has the potential to enhance voter engagement, instill confidence, and reignite interest in the electoral process. Elections, as a cornerstone of democratic decision-making, have long been a societal priority. With the increasing volume of votes being cast, citizens are growing more cognizant of the importance of the electoral system (Li et al., 2021), (Shahzad & Crowcroft, 2019). The voting system serves as the mechanism by which individuals are chosen to represent constituents in political and corporate governance. Democracy functions as a system where voters select representatives through the act of voting (Racsko et al., 2019). The effectiveness of this process hinges largely on the level of trust the public places in the electoral procedures. The establishment of legislative bodies to reflect the will of the populace is a well-established practice, spanning from student unions to governmental constituencies. Over time, voting has evolved into the primary means through which citizens express their preferences by electing individuals from the options available to them (Shahzad & Crowcroft, 2019).

Traditional or paper-based polling methods have historically served to bolster public confidence in the majority voting process. This approach has contributed to the perceived legitimacy and value of the democratic process, facilitating the election of representatives and governments in a more democratized manner. According to recent data, out of approximately 200 nations worldwide, 167 were classified as democracies in 2018, although some were considered flawed or hybrid in nature (Cullen & Houghton, 2000). The secret ballot system has been employed since the inception of voting systems as a means of enhancing trust in democratic institutions. Maintaining confidence in the voting process is paramount. A recent study highlighted concerns regarding the hygiene of traditional voting methods, raising significant questions about fairness, equality, and the

accurate representation of people's will within the governmental framework (Schınckus et al., 2020).

Blockchain technology offers a decentralized platform for online voting and electronic voting systems. The recent adoption of distributed ledger technologies, such as blockchain, in electronic voting systems is primarily driven by the benefits of end-to-end verification (Ometov et al., 2020). Blockchain technology presents an attractive alternative to traditional electronic voting systems, characterized by features such as decentralization, non-repudiation, and enhanced security. It has been applied in both boardroom and public voting contexts (Gao et al., 2019). A blockchain is a growing list of blocks, each containing a hash, timestamp, and transaction data from the previous block, linked through cryptographic connections. Designed to be data-resistant, blockchain technology is now being explored in the context of voting, where researchers aim to leverage its benefits, including transparency, secrecy, and non-repudiation, which are crucial for voting applications (Hakak et al., 2020). The utilization of blockchain technology for electronic voting applications has garnered significant attention in recent years, particularly in efforts to secure and rectify elections (Çabuk et al., 2018).

Blockchain technology has emerged as an alternative to traditional methods by ensuring system immutability and transparency. It operates as a structured data arrangement comprised of interconnected blocks, with each block linked to its predecessors, starting with the genesis block. These blocks collectively form a chain known as a blockchain, with each containing data, a hash, and the hash of the previous block. Any modification to the data in a block alters its hash, consequently invalidating the block and all subsequent ones. This preventive measure against tampering necessitates recalculating hashes for subsequent blocks, a process that has become increasingly challenging with advancements in computing power. To mitigate this, blockchain employs the proof-of-work concept, slowing the rate of new block creation.

Furthermore, blockchain utilizes a decentralized peer-to-peer network, devoid of a central authority. Upon creating a new block, it is disseminated to all network nodes, where each node verifies its integrity to prevent tampering. Consensus among network nodes ensures the validity of each block, reinforcing the security, trustworthiness, and reliability of blockchain technology.

A smart contract refers to an autonomously enforced agreement embedded within blockchain-managed computer code. This code delineates a set of rules dictating communication and decision-making between involved parties, with automatic enforcement upon meeting predefined criteria. Smart contracts provide a structured framework for streamlined control over tokenized assets and access rights among multiple parties. Blockchain, as an immutable database, gains enhanced functionality through smart contracts, expanding its utility and capabilities.

Smart contracts facilitate self-verification of conditions through data interpretation. Each network node ensures the proper execution of individual contracts, relieving creators from monitoring contract execution. These contracts are self-executing, with agreement conditions encoded into the code, enabling the automation of legal obligations. Contract execution can be triggered automatically, such as by an expiration date.

In our research, we implement a blockchain-based e-voting system to address challenges encountered in electronic voting, fostering trust among voters in the integrity of the process. Furthermore, this initiative represents a significant stride toward the advancement of smart governance.

1.1 PROBLEM STATEMENT

Despite the increasing use of technology in electoral processes, there are still significant concerns regarding the transparency, security, and accessibility of these systems. Centralized voting systems are vulnerable to data breaches, tampering, and manipulation, which can undermine the integrity of electoral processes and erode public trust in democratic institutions. To address these challenges, there is a need for a more secure and transparent voting system that eliminates the need for a central authority and ensures the privacy and security of voter data. A block-based decentralized voting system has the potential to address these concerns by creating a tamper-proof and verifiable record of votes that can be audited and validated by multiple parties.

However, designing and implementing a block-based decentralized voting system is not without its challenges. There are technical, political, and social factors that need to be considered to ensure the system is accessible, user-friendly, and secure. Therefore, the problem statement for this topic is to design and implement a block-based decentralized voting system that enhances transparency, security, and accessibility in electoral

processes while addressing the technical, political, and social challenges associated with the development and deployment of such a system.

1.2 AIM AND OBJECTIVES

The aim of this report is to design and implement a block-based decentralized voting system that enhances transparency, security, and accessibility in electoral processes.

The Objectives are as follows:

1. **Proposal Management**: Develop a function to allow the chairperson to add proposals to the voting system, enabling the system to accommodate a diverse range of options.
2. **Voting Rights Management**: Implement a feature that allows the chairperson to grant voting rights to specific addresses, ensuring that only authorized participants can participate in the voting process.
3. **Vote Delegation System**: Design a mechanism that enables voters to delegate their voting rights to trusted individuals, enhancing inclusivity and participation in the voting process.
4. **Vote Casting Mechanism**: Create a function that enables voters to cast their votes securely for their preferred proposals, preventing double voting and ensuring the integrity of the voting process.
5. **Winning Proposal Determination**: Develop a method to determine the winning proposal based on the highest number of votes, with provisions to handle tie-break situations transparently and fairly.

1.3 SCOPE OF STUDY

The scope of the study on "Design and Implement a Block-Based Decentralized Voting System to Enhance Transparency, Security and Accessibility in Electoral Process" includes a comprehensive review of the existing literature on blockchain technology and its applications in voting systems. The study will identify the technical, political, and

social challenges associated with the design and implementation of a block-based decentralized voting system.

The study will propose a design for a block-based decentralized voting system that addresses these challenges and enhances transparency, security, and accessibility in electoral processes. The proposed design will be implemented using appropriate programming languages and tools.

The study will evaluate the performance of the implemented system in terms of its security, scalability, and user-friendliness. The evaluation will be based on a set of criteria, including security, integrity, accessibility and availability, privacy, transparency, end-to-end verifiability, affordability, scalability, and coercion resistance.

The study will provide recommendations for future research and development in the area of block-based decentralized voting systems. The recommendations will be based on the findings of the study and the limitations of the proposed system.

The study will focus on the use of blockchain technology to create a decentralized and secure voting system that enhances transparency, security, and accessibility in electoral processes. The study will not cover other applications of blockchain technology, such as cryptocurrencies and smart contracts. The study will also not cover the political and social implications of the proposed system, such as the impact on voter turnout and the potential for voter coercion. These topics may be addressed in future research.

1.4 RELEVANCE

The relevance of designing and implementing a block-based decentralized voting system is significant in enhancing transparency, security, and accessibility in electoral processes. The use of centralized voting systems has been associated with issues such as data breaches, tampering, and manipulation, which can undermine the integrity of electoral processes and erode public trust in democratic institutions.

A block-based decentralized voting system has the potential to address these concerns by creating a tamper-proof and verifiable record of votes that can be audited and validated

by multiple parties. This can enhance transparency and accountability in electoral processes, ensuring that the results accurately reflect the will of the voters.

Furthermore, a decentralized voting system can eliminate the need for a central authority, reducing the risk of data breaches and tampering. This can enhance security and privacy in electoral processes, ensuring that voter data is protected and confidential.

Additionally, a block-based decentralized voting system can enhance accessibility in electoral processes by enabling remote voting and reducing the need for physical polling stations. This can increase voter participation and representation, particularly for marginalized communities who may face barriers to accessing traditional polling stations.

Overall, the relevance of designing and implementing a block-based decentralized voting system lies in its potential to enhance transparency, security, and accessibility in electoral processes, thereby promoting democratic participation and representation. The proposed system has the potential to contribute to the development of secure and transparent voting systems that enhance democratic governance and public trust in democratic institutions.

1.5 OUTLINE OF THESIS

This research proposal work is extensively discussed from Chapter Two through Chapter Five. Chapter Two begins with a theoretical review of the research framework, and is followed by an analytical review of related works. Chapter Three provides the detailed methodology for the research design implementation. Chapter Four presents the results and discussion Finally, Chapter Five concludes the research with a recommendation and summary.

CHAPTER TWO

LITERATURE REVIEW

2.1 VOTING SYSTEM

Voting is a fundamental democratic process by which individuals or groups collectively express their preferences, opinions, or choices on a particular matter, such as electing representatives or making decisions. It involves the act of casting a ballot, voice, or other means to indicate one's will or preference. Voting is a key mechanism for ensuring that the will of the people is reflected in the decisions made by their representatives or governing bodies. It is a cornerstone of democracy, providing citizens with the right and opportunity to participate in the decision-making process and hold their elected officials accountable. The integrity, fairness, and accessibility of voting systems are crucial for maintaining public trust in democratic institutions and ensuring that the electoral process accurately represents the will of the electorate.

Despite the existence of laws governing the electoral process in many countries, these legal frameworks have been consistently disregarded, thereby creating an environment conducive to electoral manipulation. This has allowed unscrupulous candidates, often in collusion with corrupt election officials and voters, to exploit these breaches to secure an unfair advantage in the electoral process.

2.1.1 Types of voting systems

a) Internet Voting

Internet voting, also known as online voting, is an electoral system that enables voters to cast their ballots remotely using a computer or mobile device connected to the internet. This innovative approach to voting offers several potential benefits, such as increased accessibility, convenience, and voter participation. However, it also raises significant concerns regarding the security and integrity of the electoral process.

The internet, serving as the medium for transmitting votes, introduces vulnerabilities that could be exploited by malicious actors, such as hackers attempting to disrupt the system or tamper with the results. Ensuring the confidentiality, integrity, and authenticity of votes cast through an internet voting

system is a critical challenge that must be addressed to maintain public trust in the electoral process.

Despite these concerns, several countries, including Canada and Estonia, have experimented with internet voting in various capacities. These pilot projects have provided valuable insights into the potential benefits and risks associated with this emerging voting method. As technology continues to advance, it is crucial that policymakers and election officials work collaboratively with cybersecurity experts to develop robust security measures and protocols to safeguard the integrity of internet voting systems.

b) **Short Message Service Voting**

Mobile voting, a form of electronic voting, enables voters to cast their ballots using their mobile phones, typically through text messaging. This innovative approach to voting has been implemented in select countries as an alternative to traditional in-person or internet-based voting methods.

One of the primary advantages of mobile voting is its potential to reach a wider segment of the electorate. Given the widespread adoption of mobile phones, even among populations with limited internet access, mobile voting can help bridge the "digital divide" and provide more voters with the opportunity to participate in the electoral process.

However, like other forms of electronic voting, mobile voting systems also face challenges related to security and integrity. Ensuring the confidentiality, authenticity, and verifiability of votes cast via mobile devices requires robust security measures and protocols to mitigate the risks of fraud, manipulation, or unauthorized access.

As countries continue to explore and experiment with mobile voting, it is crucial that policymakers, election officials, and technology experts work collaboratively to develop and implement best practices for secure and accessible mobile voting systems. This includes ongoing monitoring, evaluation, and adaptation of security measures to keep pace with evolving threats and technological advancements.

c) **Paper Based Voting System**

Paper-based voting, a traditional and widely used electoral system, involves the use of physical ballots that are manually counted by election officials. This method has been employed for centuries and remains a prevalent choice in many countries worldwide.

In a paper-based voting system, all voting-related documents, including ballots, are paper-based and designed to be interpreted by human readers rather than machines (Mohammed et al., 2010). This approach offers a tangible and transparent record of the voting process, allowing for manual verification and recounts if necessary.

Despite the longevity and familiarity of paper-based voting, it is not without its challenges. The manual nature of the process can be time-consuming and labour-intensive, potentially leading to delays in reporting results. Additionally, the reliance on physical ballots introduces logistical challenges related to ballot printing, distribution, and secure storage.

As technology continues to advance, some jurisdictions have explored the integration of paper-based voting with electronic systems, such as ballot-marking devices or optical scan machines, to streamline the process while maintaining the benefits of a paper trail. However, the fundamental reliance on paper ballots and manual counting remains a defining characteristic of this traditional voting method.

Within this system, a ballot paper containing the names of candidates alongside their respective parties is provided to each eligible voter. Utilizing either a pen or an inked finger, voters indicate their choices on the ballot paper before depositing it into a designated box. Despite its widespread use, this method presents challenges, including time consumption and susceptibility to errors. Instances of miscounting, ballot loss, or damage are not uncommon. Moreover, the necessity for a substantial number of election officials to manage the counting process contributes to its considerable financial burden.

d) **Mechanical Lever Voting System**

A mechanical voting system, once prevalent in 20th-century United States elections, represents a traditional paper-based approach that has since become obsolete. This antiquated system involved the use of paper ballots inserted into voting machines. Upon approaching the machine, a voter would activate a curtain closure, ensuring privacy, before manually pulling a lever to cast their vote. Not reliant on electricity, this system offered the advantage of manual recounting capabilities if necessary. However, it presented notable challenges, including the potential for recording errors and the risk of paper jams within the machine. Furthermore, its maintenance costs were significant, and extensive storage space was required, contributing to its phased-out status in modern electoral practices.

e) **Punch-card Voting System**

This particular voting system is characterized by the use of paper ballots featuring perforated holes. Voters indicate their preferred candidates by punching out the corresponding holes on the ballot. Subsequently, election officials utilize a machine to tally the votes by reading the punched-out holes. Widely adopted in 20th-century United States elections, this system was regarded as relatively efficient and cost-effective (Gelman, 1997). Nonetheless, it was susceptible to errors, including instances of incorrect ballot punching (Gelman, 1997; U.S Election Assistance Commission, 2018). Notably, controversies arose during the 2000 presidential election, particularly in Florida, where issues with punch card voting systems cast doubt on the election outcome (Gelman, 1997; U.S. Election Assistance Commission, 2018). Consequently, the popularity of punch-card voting systems experienced a notable decline in the United States post-2000 (Lori, 2016).

S/N	Types	Benefits	Limitations
1	Mechanical lever voting system	i. Accessibility. ii.Security. iii.Simplicity iv.Speed	i. Expensive to maintain and requires a large space. ii.insecurity of votes
2	Paper-based voting system	i. Cost. ii.Transparency. iii.Sustainability.	i. Susceptible to human error ii. Attacks on voter sand theft of ballot papers.
3	Punch-card voting system	i. Efficiency ii. Accuracy. iii.Reliability	i. Attacks on voters and theft of ballot papers. ii. Since the votes are counted by humans, the system is susceptible to human errors.
4	Short message service (SMS)voting system	i. Security ii. Transparency iii. Real-Time Results.	i. SMS can be interrupted ii. Easy to gather people and bribe them to vote for a particular candidate
5	Internet voting system	i. Reduced error ii. Increased Transparency iii. Increased VotersTurnout.	i. Possibility of under-age voting ii. Susceptible to hackers attacks.

Table 2. 1: Benefits and limitations of voting systems

2.1.2 Electronic Voting System concept

Electronic voting, also known as e-voting, is a system that enables voters to cast their ballots using electronic devices such as mobile phones, computers, and smart devices.

This innovative approach to voting has been adopted in various contexts, including political elections, corporate meetings, and other decision-making processes.

Electronic voting systems can be implemented in either controlled or uncontrolled environments. Controlled environment elections refer to the use of electronic voting systems in a supervised and secured setting, such as a polling station. These systems are often audited and secured by vetted government officials to ensure the integrity of the election. Examples of electronic voting systems used in controlled environments include punch-card voting systems and direct-recording electronic (DRE) machines.

In contrast, uncontrolled environment elections involve the use of electronic voting systems in unsecured settings, such as internet voting or voting by mail. In these cases, the vote is typically transmitted over the internet or mobile phone network, which introduces additional security risks and challenges related to voter authentication, ballot secrecy, and the prevention of unauthorized access or tampering.

As electronic voting systems continue to evolve and gain popularity, it is crucial that policymakers, election officials, and technology experts work collaboratively to develop and implement robust security measures and protocols to safeguard the integrity of the electoral process. This includes ongoing monitoring, evaluation, and adaptation of security measures to keep pace with evolving threats and technological advancements.

2.1.3 Advantages and disadvantages of electronic voting

a. **Advantages**

1. **Enhanced Efficiency**: Electronic voting systems streamline the voting process by eliminating manual counting of paper ballots. Votes can be tabulated almost instantly, accelerating result announcements and reducing post-election delays. The simplified logistics save time, resources, and minimize errors, leading to a smoother voting experience for citizens.

2. **Improved Accuracy**: Electronic voting minimizes human errors like miscounting by automating the tabulation process. Built-in validation mechanisms prevent invalid votes, detecting and rejecting overvotes and undervotes. Robust audit trails and encryption techniques ensure the integrity of the voting process, enhancing accuracy and enabling post-election audits.

3. **Increased Accessibility**: Electronic voting systems bridge accessibility gaps by accommodating individuals with disabilities through features like screen readers and alternative input methods. Remote and overseas citizens can participate in elections through secure online portals or mobile applications, enhancing inclusivity. Multilingual interfaces cater to diverse populations, ensuring language barriers do not hinder voter participation.

4. **Enhanced Security**: Electronic voting platforms offer advanced security features like token-based authentication, voter verification, and bank-grade data encryption. These measures ensure transparent, auditable voting data and provide a level of security surpassing traditional paper-based methods. The integrity of the voting process is maintained through secure data transmission and protection against unauthorized access or tampering.

5. **Convenience and Increased Turnout**: Electronic voting offers improved convenience for eligible voters, making the process more accessible and user-friendly. Compared to paper-based methods, electronic voting is more convenient, leading to increased voter turnout. Simplified processes and secure platforms empower voters to cast their ballots easily, contributing to higher participation rates and achieving quorum efficiently.

b. **Disadvantages**

Disadvantages of Electronic Voting:

1. **Vulnerability to Hacking**: Electronic voting systems are susceptible to hacking, potentially compromising the integrity and security of the electoral process. Attackers may exploit weaknesses in the system to manipulate votes or disrupt election results, raising concerns about the reliability of electronic voting systems.

2. **Lack of Voter Verified Paper Audit Trails**: Fully-electronic voting systems may lack voter-verified paper audit trails, making it challenging to independently verify that all votes have been accurately recorded and counted. Without a paper trail, there is a risk of undetected errors or tampering with election outcomes, undermining transparency and accountability.

3. **Susceptibility to Fraud**: Electronic voting systems can be vulnerable to various forms of fraud, including malicious tampering with voting machines or software. The potential for large-scale fraud, such as the manipulation of millions of votes through compromised systems, poses a significant threat to the fairness and accuracy of elections.

4. **Accuracy in Capturing Voters' Intent**: Touch screen devices used in electronic voting may experience calibration issues, leading to misinterpretation of voters' choices. Inaccuracies in touch screen sensors can result in unintended selections, potentially affecting the outcome of an election and compromising the accuracy of voter intent.

5. **Political Influence on Manufacturers**: The involvement of manufacturers in the development of electronic voting systems raises concerns about potential political bias or influence. Manufacturers may tailor voting machines to align with the preferences of a particular political party, leading to distrust and scrutiny from other political entities and voters.

6. **Malicious Software Programming**: The programming and coding of electronic voting software can be susceptible to tampering by individuals with knowledge of the source code. Malicious coding inserted into the software can alter election results, making it challenging to detect and prevent unauthorized changes that could impact the outcome of an election.

7. **Physical Security of Machines**: Direct recording electronic voting machines may exhibit weaknesses in physical hardware controls, potentially compromising

the security and integrity of the system. Inadequate safeguards to protect voting machines from tampering or unauthorized access raise concerns about the reliability and trustworthiness of electronic voting systems.

2.1.4 Electronic Voting System Phases

The electronic voting system encompasses multiple components or units and typically undergoes several stages throughout the voting process. According to Abdalla and Samani (2013) and Sayali et al. (2018), e-voting is generally categorized into three phases:

i. Pre-voting phase:
   a) Candidate nomination process: The candidate nomination process refers to the procedure through which individuals or political entities formally present their candidacies for an election. This process can vary depending on the regulations set by the national legislature. Eligibility criteria for candidates typically include factors such as party membership status and minimum educational qualifications.
   b) Voter registration process: In most elections, depending on the local laws, voters have to register for voting explicitly. In some elections, citizens of the society, environment, or country are registered for voting automatically.

ii. Voting phase:

   The voting phase is the culmination of the electronic voting process, where all eligible voters are empowered to exercise their democratic right to participate in the election. This phase is triggered by the outcome of the pre-voting phase, which ensures that the necessary preparations and checks have been completed to facilitate a smooth and secure voting process.

   During this phase, voters are presented with the options and candidates, and they are able to cast their ballots electronically. The voting process is designed to be user-friendly and accessible, ensuring that all eligible voters can participate in the election without any barriers or obstacles.

iii. Post-voting phase:

a) Transmission of votes: Following the voting phase, the electronic voting system transmits the votes either over the internet or through a network to a centralized remote location for counting. This process often employs secure communication protocols to ensure the integrity and confidentiality of the vote.

b) Vote counting: This stage represents one of the pivotal aspects of the electoral process. It is commonly conducted through specialized software designed specifically for the purpose of tallying votes.

c) Results and reporting: Following the tallying of votes, the results are transmitted to designated election officials who are duly authorized to receive them. In accordance with predetermined regulations, the total number of votes garnered by each candidate is presented and officially confirmed by the authorized election personnel through their signatures.

d) Result announcement: A designated election official, typically the chairperson of the electoral body, publicly announces the conclusive outcome and formally declares the victor of the election based on the accumulated votes garnered by each candidate.

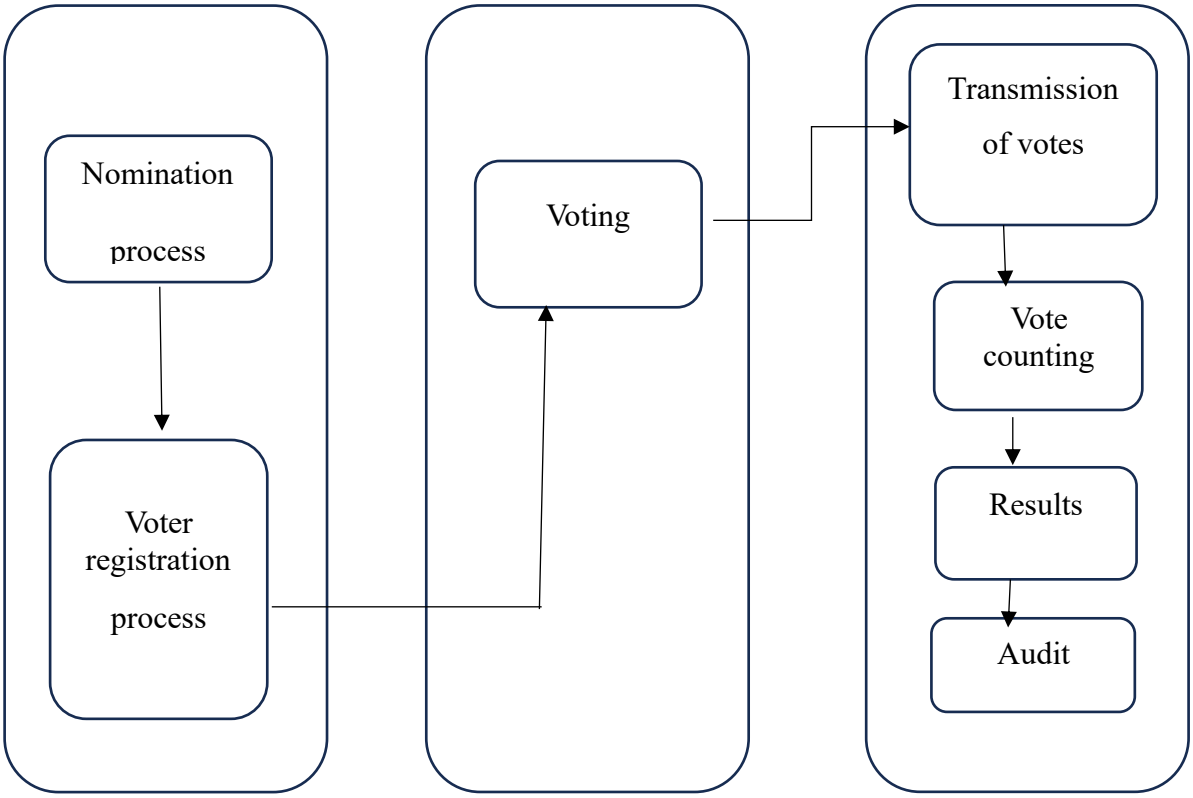

Figure 2. 1: E-voting phases

2.2 RELATED WORKS

In recent years, there has been a growing body of research examining the security and privacy challenges associated with blockchain-based electronic voting systems. These studies have provided critical insights into the potential vulnerabilities and limitations of employing blockchain technology in the context of electronic voting. A number of articles have been published that compare and contrast various blockchain-based electronic voting schemes, evaluating their effectiveness in addressing security and privacy concerns. These comparative analyses have shed light on the strengths and weaknesses of different approaches, helping to identify best practices and areas for improvement in the design and implementation of blockchain-based voting systems.

By examining the security and privacy implications of blockchain-based voting systems through a comparative lens, researchers have been able to develop a more nuanced understanding of the trade-offs and challenges involved in leveraging this emerging technology for electoral processes. This knowledge is crucial for informing the development of robust, secure, and privacy-preserving blockchain-based voting solutions that can be deployed with confidence in real-world settings.

The introduction of the Open Vote Network (OVN) was introduced in a study by (McCorry et al., 2017), marking the initial implementation of a transparent and self-tallying internet voting protocol that prioritizes user privacy through the utilization of Ethereum blockchain technology. Within the OVN framework, the voting capacity was constrained to a range of 50 to 60 electors, ensuring a manageable scale for the voting process.

Despite its innovative approach, the OVN system faces challenges in preventing fraudulent activities, particularly from malicious miners who could potentially compromise the integrity of the voting system. Additionally, there are vulnerabilities that allow fraudulent voters to manipulate the voting process by submitting invalid votes, undermining the accuracy and reliability of the electoral outcomes.

Furthermore, the OVN protocol lacks mechanisms to ensure resistance to coercion or violence, raising concerns about the system's ability to withstand external pressures that may influence the voting results. This highlights the importance of addressing security

and trust issues within the electoral administration to uphold the integrity and credibility of the voting process (Zhang et al., 2019).

In addition to its limitations, the Open Vote Network (OVN) faced an additional challenge due to the constraints of the Solidity programming language, which does not natively support elliptic curve cryptography. To overcome this limitation, the developers utilized an external library to perform the necessary computations (Woda & Huzaini, 2021). However, this addition resulted in the voting contract becoming too large to be efficiently stored on the blockchain, a common issue that has been observed in the history of the Bitcoin network.

Furthermore, the OVN system is vulnerable to denial-of-service (DoS) attacks, which can significantly impact its performance and availability (Hjalmarsson et al., 2018). This is a critical concern, as DoS attacks can be used to disrupt the voting process and undermine the integrity of the electoral outcomes.

Lai et al., 2018 proposed a decentralized anonymous transparent electronic voting system (DATE) with the aim of ensuring a minimal degree of confidence among participants. They contend that for extensive electronic elections, the current DATE methodology is suitable. However, their proposed system lacks robustness against Denial of Service (DoS) attacks due to the absence of a third-party authority responsible for post-election vote auditing. The objectives of the research were to design and implement an efficient and effective decentralized, anonymous and transparent e-voting system that ensures the transparency of voting by putting all messages on 21the Ethereum blockchain and the privacy of each voter through an efficient and effective ring signature mechanism.

The research was implemented using an Ethereum smart contract and storing all the necessary information on it. Due to the fact that the gas limit of the Ethereum blockchain cannot afford too complex operations and all the information about the blockchain history need not be calculated in the smart contract, only pointers on a ballot are stored. The proposed system (DATE) has three phases including:

a) Setup phase: During this phase, election-related data such as the voter list, candidate list, key management scheme, setup time, voting duration, and tallying period are openly disclosed on an Ethereum smart contract.

b) Voting phase: Every eligible voter is assigned a private key corresponding to one of the public keys listed on the voter registry, and they possess awareness of the publicly available information.
c) Tallying phase: During the setup phase of the key management scheme, key managers are required to disclose their individual secrets to retrieve their deposits. Following this phase, the smart contract ceases to accept any ballots once the voting period concludes.

Khan, K.M. (2020) introduced a block-based e-voting architecture (BEA) which underwent rigorous experimentation encompassing both permissioned and permissionless blockchain frameworks across various scenarios, including variations in the voting population, block size, block generation rate, and block transaction speed. Their experiments yielded valuable insights into how these parameters impact the scalability and reliability of the electronic voting model, as well as the interplay between different parameters and the efficacy of protection and performance measures within the system. In their proposed scheme, the electoral process involves the generation of unique addresses for both voters and candidates. These addresses are utilized for the transmission of votes from voters to candidates. A designated mining group is tasked with updating the main blockchain ledger to record the votes cast and the corresponding status of each vote. The voting status remains pending until a miner updates the main ledger, following which the vote is officially cast using the voting machine located at the polling station. However, this model exhibits several identified shortcomings. Firstly, there lacks a regulatory authority to prevent ineligible voters from casting their ballots, leaving the system vulnerable to exploitation. Additionally, it remains susceptible to quantum attacks, thereby compromising its overall security. Furthermore, the model fails to adequately address concerns regarding voter integrity. Moreover, their utilization of Distributed Consensus introduces the risk of collusion among participants, potentially enabling the formation of cartels and facilitating a "51%" attack, particularly problematic due to the reduced number of active network participants. Notably, the model overlooks crucial considerations such as scalability and potential delays inherent in electronic voting systems based on blockchain technology. Additionally, the choice of the Multichain framework, a private blockchain derivative from Bitcoin, proves unsuitable for

nationwide voting processes. As acknowledged by the authors themselves, the efficacy of their system is confined to small and medium-scale voting environments exclusively.

Guo, He, and Zou (2021) introduced a Blockchain-based Voting System in response to identified vulnerabilities within traditional voting methodologies, which exhibited susceptibility to issues such as inaccurate tallying, voter impersonation, and electronic voting machine tampering, thus necessitating the exploration of alternative solutions. The primary aim of this project is the development of a novel electronic voting system leveraging blockchain technology to eradicate manipulation possibilities and empower voters to authenticate and monitor their votes securely. The overarching objective is to devise a voting mechanism characterized by fairness, impartiality, and transparency, underpinned by blockchain's capabilities to safeguard, trace, and anonymize voting data, thereby mitigating data manipulation risks, ensuring verifiability, and preserving voter confidentiality. Central to this endeavor are two key mechanisms: the Consensus mechanism, governing the blockchain's integration and determining the addition of new blocks to the existing chain, and the Data Verification mechanism, tasked with verifying data integrity across network nodes through initial validation, digital signature verification, and adherence to predefined criteria for data acceptance. To bolster data integrity, cryptographic hash functions are employed to condense input data into fixed-length outputs, while asymmetric encryption, timestamps, and Merkle trees are leveraged to reinforce data security without compromising integrity. Despite the utilization of electronic devices, a notable concern persists regarding voter trust, which remains a focal point for ongoing refinement and assurance within the proposed system.

Bhabendu KM, Debasish J, Soumyashree S.P, and Srichandan S (2019) conducted a comprehensive study addressing the privacy and security challenges associated with implementing blockchain technology. Their research delves into the architecture of blockchain and its diverse applications, aiming to map out research areas and pinpoint any existing gaps. The decentralized nature of blockchain ensures robust security, transparency, and resistance to tampering. Transactions executed on the blockchain are systematically recorded in blocks, sequentially linked to form an immutable chain, hence the term "blockchain". Cryptography safeguards transaction security, restricting access solely to authorized users. Each block within the chain encompasses a series of transactions and a unique hash code linking it to its predecessor, rendering alteration or

tampering exceedingly difficult. This inherent feature establishes the security and integrity of blockchain technology. Moreover, the distributed structure of blockchain eradicates single points of failure, bolstering system resilience and reducing susceptibility to attacks. The blockchain architecture comprises multiple interconnected nodes, each maintaining an updated copy of the blockchain ledger. Various tasks, such as initiating and validating transactions or engaging in mining activities, can be performed by these nodes. Research findings suggest that blockchain holds potential as a solution for existing legal frameworks governing cross-jurisdictional contracts, offering a decentralized digital ledger devoid of third-party intervention. Furthermore, integrating blockchain architecture into digital rights management systems can foster transparency among stakeholders while safeguarding the security and privacy of individuals.

Yi (2019) introduced the Blockchain-based Electronic Voting Scheme (BES), aimed at enhancing electronic voting security within peer-to-peer networks through the utilization of blockchain technology. BES, grounded in distributed ledger technology (DLT), offers mechanisms to mitigate vote falsification. The system underwent testing and development on Linux platforms within a peer-to-peer network environment. However, countermeasures against potential attacks pose notable challenges. Effective implementation often requires the involvement of trusted third parties and may not be ideally suited for centralized use within systems featuring numerous agents. A distributed approach, involving secure multipart computation, presents a potential solution to this issue. Nevertheless, this approach may incur substantial computational expenses, particularly if complex computational functions and a large number of participants are involved (Torra et al., 2019).

Armin Krishnan's article, titled "Blockchain Empowers Social Resistance and Terrorism through Decentralized Autonomous Organizations," examines the potential utilization of blockchain technology (BT) by various social movements, resistance groups, and even criminal organizations to pursue diverse objectives. The decentralized nature of BT fundamentally alters the landscape of resistance organization and practice, enabling coordinated efforts without centralized leadership. Through the utilization of smart contracts and decentralized autonomous organizations (DAOs), collective actions can be organized and resources distributed efficiently. Moreover, BT provides anonymity and

security, shielding the identities and activities of participants from government surveillance and repression.

However, leveraging BT for resistance purposes carries inherent risks, including the potential exploitation by malicious entities for illicit activities. This necessitates policymakers and researchers to carefully consider the ramifications of BT on resistance movements and democracy, and to formulate regulations and strategies that harness its positive aspects while mitigating negative consequences. One illustrative application of BT in social movements is the establishment of decentralized fundraising and financial management platforms, fostering transparency in transactions and bolstering resistance against governmental attempts to impede funding channels. Additionally, BT can facilitate the creation of secure and anonymous communication channels for activists and organizers, complicating government surveillance and disruption efforts.

Further research is imperative to comprehensively grasp the implications of BT on social and civil resistance movements, and to devise effective strategies for addressing potential negative outcomes. The article underscores the significance of evaluating the impact of BT on resistance and democracy, advocating for responsible and ethical utilization of the technology.

Xiaoyu et al. (2020) introduced a blockchain-based voting system incorporating a feedback mechanism and Wilson score algorithm. Voting serves as a fundamental mechanism in various contexts, spanning public elections in democratic nations, audience polls to determine rankings in talent shows, and assessments of movie popularity among others. The proposed system aims to detect and mitigate malicious voting behavior, particularly users attempting to artificially boost the approval ratings of non-mainstream candidates by casting excessive votes.

The system employs a points-weighted voting approach, wherein each candidate receives both positive (yes) and negative (no) votes. The Wilson score ranking algorithm adjusts the support rates of candidates based on voter feedback. Additionally, a feedback mechanism is integrated into the blockchain voting process, facilitated by a smart contract built on the Ethereum private chain. Each vote necessitates a new smart contract creation.

Within the smart contract, a conversion rate coefficient (α) converts ether into voting points, customizable based on specific voting circumstances. Notably, only positive votes are considered, with voters receiving negative votes equivalent to the positive votes they cast. To deter malicious behavior, the authors propose a mechanism wherein users incur deductions—referred to as commissions—from their initial voting points if their preferred candidate emerges victorious. This ensures users consider both the value of their voting points and the eventual voting outcomes when casting their ballots.

To implement this mechanism, all voting points are locked within the smart contract, with commissions calculated as the product of total voting points and a factor (β) linked to voting outcomes. This approach enhances the integrity of the voting process and discourages fraudulent behavior, reinforcing the reliability and fairness of the blockchain-based voting system.

CHAPTER THREE

METHODOLOGY

This chapter presents the methodology used to design and implement a secure blockchain-based electronic voting system with respect to the drawbacks of traditional and electronic voting systems.

3.1 Functional Requirements

The functional requirements delineate the fundamental operations of an electronic voting system based on blockchain technology. The subsequent functional requirements are taken into account for the system's functionality.

a) **User friendly interface**: The envisioned blockchain-based electronic voting system is designed with a user-centric interface aimed at facilitating seamless interaction for voters. By leveraging intuitive design principles, the system ensures accessibility and ease of use, enabling individuals to navigate the voting process effortlessly. Through intuitive features and clear instructions, voters can engage with the platform confidently, enhancing overall participation and fostering trust in the electoral process.

b) **Security**: The proposed system is engineered with robust security measures meticulously crafted to safeguard against hacking and other malicious attacks. By employing state-of-the-art encryption techniques, stringent access controls, and distributed ledger technology inherent in blockchain, the integrity of the voting process is fortified, mitigating the risks of manipulation or unauthorized interference. These comprehensive security protocols ensure the integrity and reliability of the system, thereby upholding the sanctity of democratic principles and preserving voter confidence in the electoral process.

c) **Anonymity**: The proposed system prioritizes the privacy and anonymity of voters by implementing robust measures to safeguard their identities. Through advanced cryptographic techniques and decentralized architecture inherent in blockchain technology, the system ensures that voter identities remain confidential and untraceable, thereby protecting individual privacy rights. By affording anonymity

to voters, the system fosters trust and confidence in the electoral process, empowering individuals to exercise their democratic rights without fear of repercussions or compromise of personal information.

d) **Identity management**: The proposed system would have a secured identity management process to ensure that each vote is cast by a verified voter.
e) **Transparency**: To instill trust in the election process among voters, the suggested system aims to achieve transparency through decentralization, eliminating a central authority's control over the voting process.

3.2 Security Requirements

The election process is expected to be secured from attacks, unlawful interception, and any illegal modification. The following requirements were considered to secure the election process from the beginning to the end against attacks.

1. **Enrollment**: Only eligible voters would be allowed to vote.
2. **Voter's authentication:** Voting eligibility is restricted to individuals who have completed the registration process and undergone authentication procedures.
3. **Results authentication:** Only validated ballots cast by authenticated voters would be considered in determining the outcome for the candidates.
4. **Results integrity:** The utilization of blockchain technology guarantees the reliability of the election outcome.

3.3 Design of proposed Blockchain-Based Electronic Voting Model

In the design of the proposed model, some developing tools were used which are:

1. Solidity: Solidity is a contract-focused programming language characterized by its high-level nature, tailored for the implementation of smart contracts. It possesses Turing completeness, offering a robust set of features suitable for targeting the Ethereum Virtual Machine (EVM). Drawing inspiration from languages like C++, JavaScript, and Python, Solidity supports libraries, inheritance, and advanced user-defined types, all within a statically typed framework. With its versatility, Solidity empowers developers to craft contracts for diverse applications such as crowdfunding, blind auctions, voting systems, multi-signature wallets, and beyond.

2. NPM: The Node.js Package Manager, or npm, boasts a vast repository of no less than 1.7 million packages, contributing to one of the most extensive developer ecosystems globally. Central to the JavaScript community, npm plays a pivotal role. Given that each package often relies on numerous others, developers benefit from a rich array of libraries and functionalities, sparing them the need to develop solutions from scratch. One of npm's standout attributes is its capacity to not only install multiple versions of a package but also utilize various versions concurrently within a single execution run.
3. Remix IDE: For JavaScript-based smart contracts, Remix IDE (Integrated Development Environment) represents a well-liked browserbased IDE.
4. Web3.js: With the use of HTTP, WebSocket, or IPC, you can communicate with a remote or local Ethereum node utilizing the web3.js library collection.

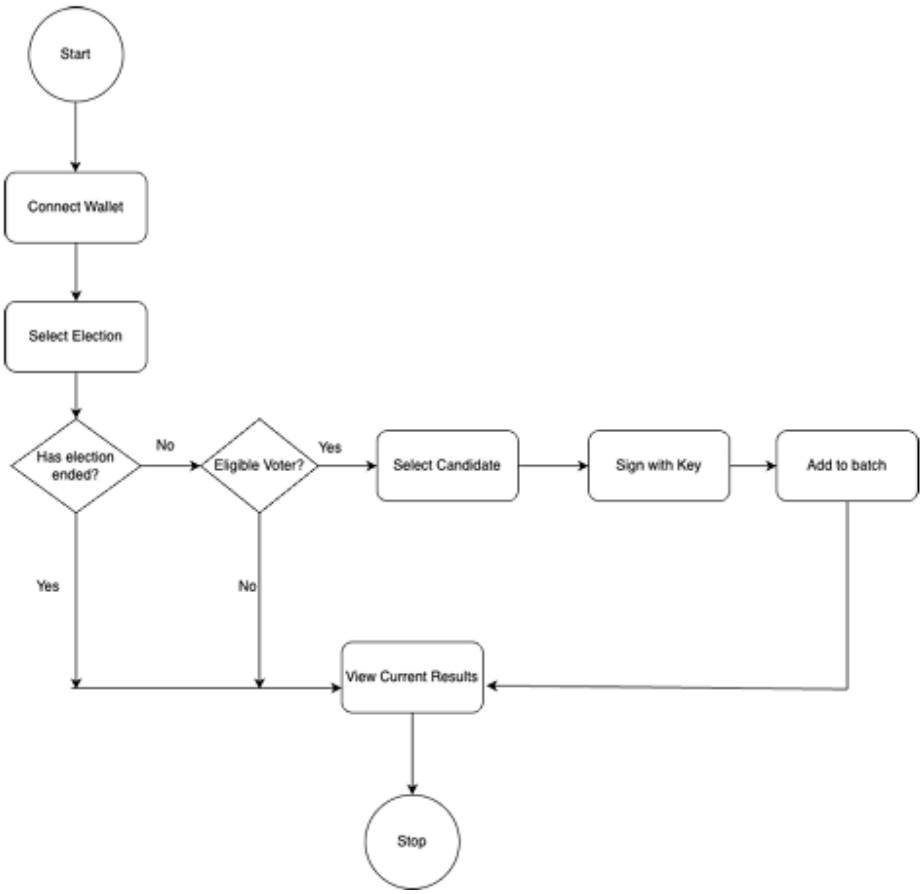

Figure 3. 1: Blockchain e-voting flowchart

3.3.1 BlockChain Technology

Blockchain serves as the foundational layer of the proposed system, offering a secure, decentralized, and immutable ledger to record votes cast by verified voters throughout the election process. Its decentralized nature ensures that no single entity, whether individual or authority, wields unilateral control over the voting mechanism, thereby enhancing trust among participants.

Within this framework, votes are recorded in hexadecimal format and encapsulated into blockchain transactions. These transactions are subsequently organized into blocks, forming an immutable chain. This structural design prevents the alteration of recorded data, safeguarding the integrity and transparency of the voting process. By leveraging blockchain technology, the proposed system establishes a robust foundation that not only

secures voting data but also fosters confidence in the legitimacy and fairness of electoral outcomes.

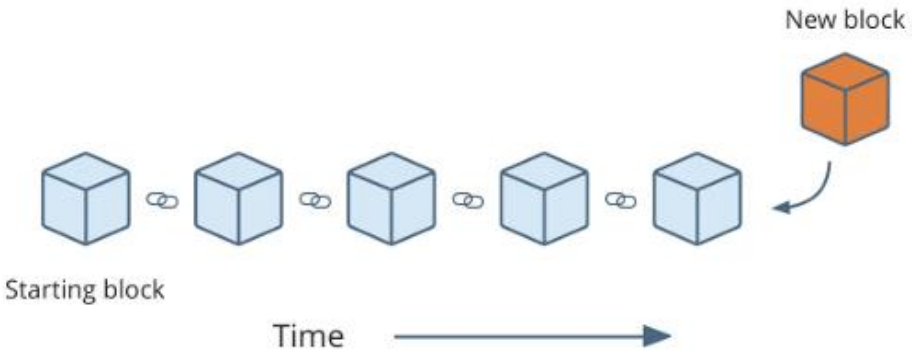

Figure 3. 2: Pictorial representation of BlockChain

Within the blockchain architecture, each block encapsulates three distinct types of information essential to its functionality:

1. **Data on Transactions**: This component comprises the primary content of the block, encompassing the details of transactions executed within a specified timeframe. These transactions typically include information such as the sender, recipient, amount, and any additional metadata relevant to the transaction.

2. **The Block's Hash**: Representing a unique alphanumeric string, the block's hash is automatically generated based on the entirety of information stored within the block. This hash serves as a digital fingerprint, uniquely identifying the block and its contents. Any alteration to the data within the block would result in a significant change in the hash, thereby detecting tampering attempts.

3. **The Hash of the Previous Block**: Each block within the blockchain is intricately linked to its predecessor through the inclusion of the previous block's hash. This linkage creates a sequential chain of blocks, with each block's hash serving as a reference to the preceding block. By maintaining this chronological order, the integrity and continuity of

the blockchain are preserved, ensuring that any attempt to modify earlier blocks would be immediately apparent due to the subsequent hash discrepancies.

Given that every block within the blockchain incorporates the hash of its antecedent, any modification to the data within a preceding block result in a change to its hash. Consequently, this alteration invalidates the hash of the prior block stored within the current block. Hence, it can be inferred that blockchains possess a fundamental resilience to tampering and fraudulent activities.

Utilizing blockchain technology as the underlying infrastructure of an electronic voting system yields several notable advantages, stemming from its attributes as an immutable public digital ledger with robust encryption capabilities:

Security: Blockchains, by nature, are decentralized, meaning there is no singular access point to the database. As all blockchain activities are transparent and once information is recorded, it cannot be altered, hackers face formidable obstacles in attempting to manipulate the voting process or tamper with vote counts within an electronic voting system.

Transparency: The transparent nature of blockchain allows for anyone to access and review all recorded transactions. When integrated with an electronic voting system, this transparency empowers voters to independently verify the inclusion of their votes in the tally and confirm the accuracy of the overall vote count.

3.3.2 Smart Contract

Smart contracts represent deterministic programs stored on the blockchain, executing upon the fulfillment of specified conditions, typically structured around "if/when … then…" statements. They serve as integral components in decentralized application (dApp) development, offering a secure and transparent framework for interaction between multiple parties, even in the absence of mutual trust or familiarity. Smart contracts strictly adhere to their predetermined actions, ensuring they only execute when the requisite conditions are met.

To facilitate on-chain interactions, storage, and verification of voter identities, a smart contract is authored using the Solidity programming language. Subsequently, it is compiled into Ethereum Virtual Machine bytecode and deployed onto a test network for

engagement. Upon a voter casting their ballot, their signature, along with those of fellow voters, is aggregated and submitted to the deployed smart contract for verification prior to recording the vote on-chain. This process ensures the integrity and authenticity of each voter's participation within the system.

3.3.3 Elliptic Curve Digital Signature Algorithm

The Elliptic Curve Digital Signature Algorithm (ECDSA) is a cryptographic method utilized for generating digital signatures, leveraging elliptic curve cryptography keys. It finds extensive application in ensuring the security of digital transactions within blockchain ecosystems like Ethereum and Bitcoin. ECDSA operates as a public-private key algorithm, wherein each user possesses two distinct keys: a public key and a private key. The public key serves the purpose of verifying digital signatures, while the private key is employed in their creation. This dual-key system contributes to the robustness and confidentiality of cryptographic operations within blockchain networks.

1. ECDSA Digital Signature Generation: To sign a given message m, Entity A, possessing domain attributes D comprising (q, FR, a, b, G, n, h), and associated key pair (d, Q), conducts the following steps:

a) 1 Select a random integer k within the range from 1 to n (exclusive).
b) Transform k into an integer x_1 by computing $kG = (x_1, y_1)$.
c) Compute $r = x_1 \mod n$, proceeding to step 1 if $r = 0$.
d) Calculate $k^{-1} \mod n$.
e) Compute $s = (k^{-1})(e + dr) \mod n$, repeating step 1 if $s = 0$.
f) The message m now bears Entity A's signature, represented as (r, s).

2. ECDSA Digital Signature Verification: Entity B, to validate the signature (r, s) on message m attributed to Entity A, obtains an authenticated version of $A's$ domain parameters $D = (q, FR, a, b, G, n, h)$, alongside $A's$ associated public key Q. Entity B executes the following steps:

a. Check if the integers r and s fall within the range $[1, n-1]$.
b. Transform the bit string into a number e by performing SHA-1(m).
c. Compute $w = s^{-1} \mod n$.

d. Calculate $u_1 = (ew) \mod n$ and $u_2 = (rw) \mod n$.
e. Compute $X = u_1G + u_2Q$.
f. Reject the signature if $X = O$; otherwise, proceed.
g. Calculate $v = x_1 \mod n$ and convert the x-coordinate of X, denoted as x_1, into an integer.
h. Accept the signature if and only if $v = r$.

In a blockchain-based election system, ECDSA enables voters to sign their votes without necessitating on-chain transactions. Each voter generates their public-private key pair and utilizes their private key to sign their vote. The signed vote, along with the voter's public key, is submitted to the election authority for verification. This approach offers various advantages over traditional voting systems, including heightened security and transparency. Since votes are signed using the voter's private key, they remain immutable post-casting. Additionally, as votes are stored on the blockchain, they are publicly accessible for straightforward auditing and verification of the election results.

CHAPTER FOUR

IMPLEMENTATION AND RESULTS

This chapter presents the implementation details and results of the system as discussed in chapter 3.

4.1 Platform of the proposed system

The proposed system can be run on Remix IDE.

4.2 System setup

Within the voting framework, the integration of smart contracts facilitated an unchangeable and openly verifiable method to guarantee the secure, reliable, and precise documentation of votes. These smart contracts, formulated in Solidity, a language centered on contract logic (utilizing constructs such as 'if...when', 'if...then'), managed pivotal tasks including voter authentication, preservation of electoral outcomes on the blockchain, and initiation of the electoral process.

Eligible voters can vote for a particular candidate in a particular election using their private key provided they registered for the election. The use of private keys ensures that only authorized voters are allowed to vote and that their votes are secure and cannot be tampered with. Listed below are the Hardware, Software and Service Requirements of the System:

1. Smart device
2. Web browser
3. Remix IDE
4. BlockChain smart contract
5. Web3.js framework

4.3 Model Creation

Exclusive authorization for creating elections rests solely with the platform administrator, as entry to the administrative dashboard necessitates a validated message using the administrator's private cryptographic key. The administrator assumes the responsibility of furnishing essential details such as the election title and candidates' identifiers, along with importing voter information. Unauthorized individuals are precluded from accessing the

administrative dashboard, thereby fortifying the security protocols governing the election initiation procedures.

a. **Contract setup and initialization**

Contract Definitioin

contract Ballot {: This line declares a smart contract named Ballot. Smart contracts are self-executing programs stored on the blockchain that can hold and manage data according to predefined rules.

```
4
5   /**
6    * @title Ballot
7    * @dev Implements voting process along with vote delegation
8    */
9   contract Ballot {
10
11      struct Voter {
12          uint weight; // weight is accumulated by delegation
13          bool voted;  // if true, that person already voted
14          address delegate; // person delegated to
15          uint vote;   // index of the voted proposal
16      }
17
```

Figure 4. 1: Contract ballot

Data Structures:

Voter struct: This defines a structure to store information about each voter.

unit weight: This variable represents the voting weight of the voter. It accumulates with delegation (explained later).

bool voted: This Boolean indicates if the voter has already cast their vote.

address delegate: This variable stores the address of another voter this voter has delegated their vote to (optional).

uint vote: This variable holds the index of the proposal the voter has chosen (0-based indexing).

Proposal struct: This defines a structure to store information about each proposal in the ballot.

bytes32 name: This variable stores the short name of the proposal (limited to 32 bytes for efficiency).

uint voteCount: This variable keeps track of the total number of votes received by the proposal.

```
34      */
35      constructor(bytes32[] memory proposalNames) {   infinite gas 798400 gas
36          chairperson = msg.sender;
37          voters[chairperson].weight = 1;
38
39          for (uint i = 0; i < proposalNames.length; i++) {
40              // 'Proposal({...})' creates a temporary
41              // Proposal object and 'proposals.push(...)'
42              // appends it to the end of 'proposals'.
43              proposals.push(Proposal({
44                  name: proposalNames[i],
45                  voteCount: 0
46              }));
47          }
48      }
49
50      /**
51       * @dev Give 'voter' the right to vote on this ballot. May only be called by 'chairperson'.
52       * @param voter address of voter
53       */
54      function giveRightToVote(address voter) public {   29325 gas
55          require(
```

Figure 4. 2: Data structure

b. Voter Eligibility and Delegation

This code snippet in Figure 4.3 defines three functions within the Ballot contract, allowing voters to interact with the voting system.

```
54      function giveRightToVote(address voter) public {   29325 gas
55          require(
56              msg.sender == chairperson,
57              "Only chairperson can give right to vote."
58          );
59          require(
60              !voters[voter].voted,
61              "The voter already voted."
62          );
63          require(voters[voter].weight == 0);
64          voters[voter].weight = 1;
65      }
66
67      /**
68       * @dev Delegate your vote to the voter 'to'.
69       * @param to address to which vote is delegated
70       */
71      function delegate(address to) public {   infinite gas
72          Voter storage sender = voters[msg.sender];
73          require(!sender.voted, "You already voted.");
74          require(to != msg.sender, "Self-delegation is disallowed.");
75
76          while (voters[to].delegate != address(0)) {
```

Figure 4. 3: Voter delegation and interaction

1. giveRightToVote Function:

- This function allows the chairperson (chairperson variable) to grant voting rights to an address (voter).
- It performs the following checks:
    - Only the chairperson can call this function (require statement with msg.sender == chairperson).
    - The voter hasn't already voted (require statement with !voters[voter].voted).
    - The voter doesn't have any voting weight yet (require statement with voters[voter].weight == 0).
- If all checks pass, it assigns a voting weight of 1 to the voter (voters[voter].weight = 1).

2. delegate Function:

- This function allows a voter (msg.sender) to delegate their vote to another voter (to).
- It performs the following checks:
    - The voter hasn't already voted themselves (require statement with !sender.voted).
    - The voter isn't trying to delegate to themself (require statement with to != msg.sender).
- It then iterates through a loop, checking if the delegate (to) has further delegated their vote.
    - It follows the chain of delegation until it reaches someone who hasn't delegated (voters[to].delegate != address(0)).
    - It prevents loops in delegation (require statement with to != msg.sender).
- Once a valid delegate is found, the function:

- Marks the original voter as having voted (sender.voted = true).
- Sets the original voter's delegate to the chosen address (sender.delegate = to).
- Updates the voting weight of the delegate:
  - If the delegate has already voted (delegate_.voted), it directly adds the original voter's weight to the chosen proposal's vote count (proposals[delegate_.vote].voteCount).
  - If the delegate hasn't voted yet, it adds the original voter's weight to their own weight (delegate_.weight).

3. vote Function:

- This function allows a voter (msg.sender) to cast their vote (including any delegated votes) for a specific proposal (proposal).
- It performs the following checks:
  - The voter has the right to vote (voting weight greater than 0, require statement with sender.weight != 0).
  - The voter hasn't already voted (require statement with !sender.voted).
- Once checks pass, the function:
  - Marks the voter as having voted (sender.voted = true).
  - Sets the voter's chosen proposal (sender.vote = proposal).
  - Increments the vote count for the chosen proposal by the voter's weight (proposals[proposal].voteCount).

c. **Winning Functions**

These code snippets define two functions within the Ballot contract for determining the winning proposal.

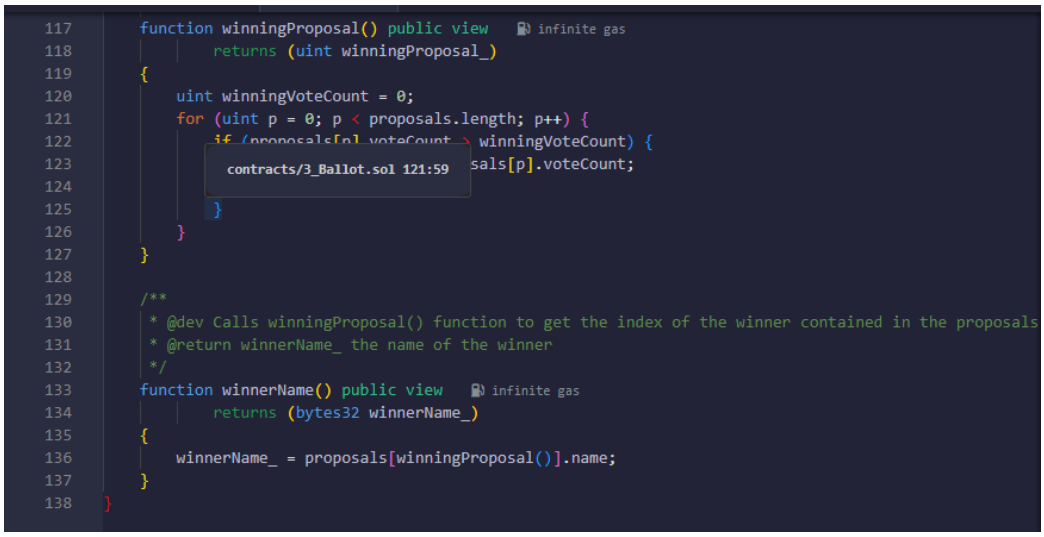

Figure 4. 4: Winning function

1. winningProposal Function:

- This function calculates the proposal with the most votes and returns its index in the proposals array.
- It's marked as public view, meaning anyone can call it to see the current leader without modifying any data.
- Here's how it works:
    - It initializes a variable winningVoteCount to 0, which will store the highest vote count encountered so far.
    - It iterates through all proposals in the proposals array using a loop (for loop).
        - For each proposal (p), it checks if its vote count (proposals[p].voteCount) is greater than the current winningVoteCount.
            - If it is, the function updates winningVoteCount with the higher value and sets winningProposal_ to the current proposal's index (p).
- After iterating through all proposals, the function returns the index of the proposal with the most votes stored in winningProposal_.

2. winnerName Function:

- This function retrieves the name of the winning proposal based on the index returned by the winningProposal function.
- It's also marked as public view, allowing anyone to call it and see the winner's name.
- Here's how it works:
    - It initializes a variable winnerName_ of type bytes32 to store the winning proposal's name.
    - It calls the winningProposal function (presumably within the same contract) to get the index of the winning proposal.
    - It retrieves the name of the proposal at the winning index from the proposals array using proposals[winningProposal()].name. This assumes winningProposal has already been calculated.
    - Finally, the function returns the retrieved name stored in winnerName_.

These functions work together to determine the winning proposal by first calculating the index and then using it to retrieve the corresponding name from the proposals array. Both functions being public view allow anyone to see the current leader without affecting the contract's state.

4.4 Model Deployment and Testing

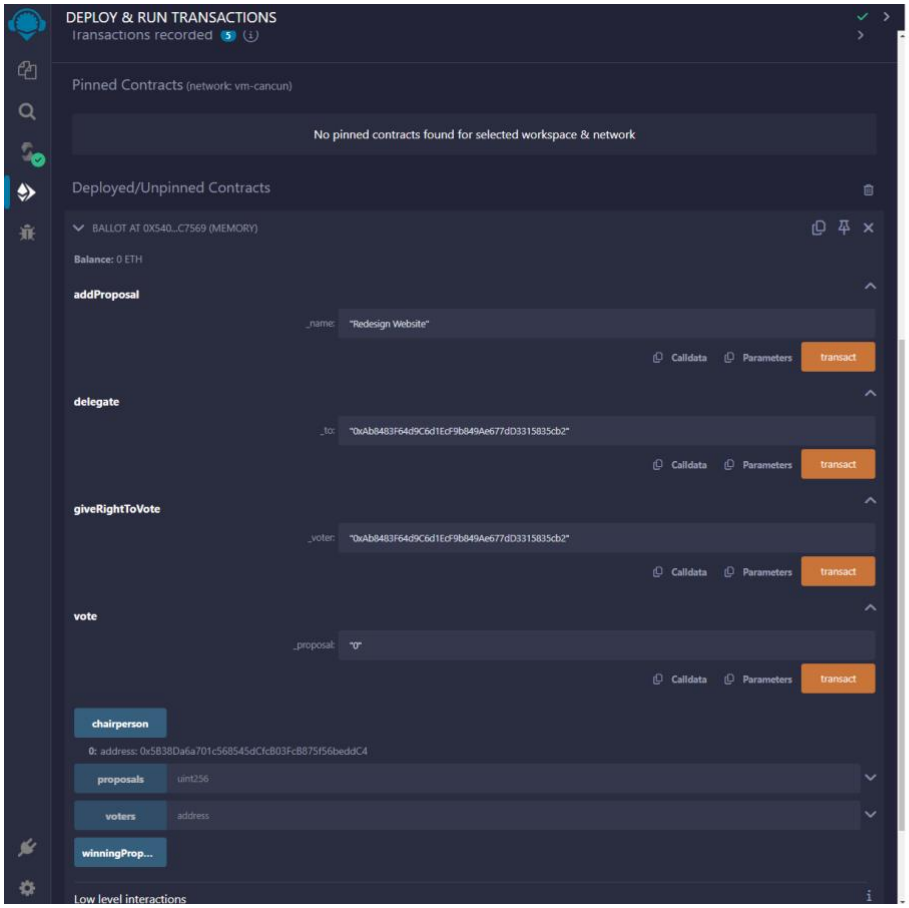

Figure 4. 5: Deployment and run transaction

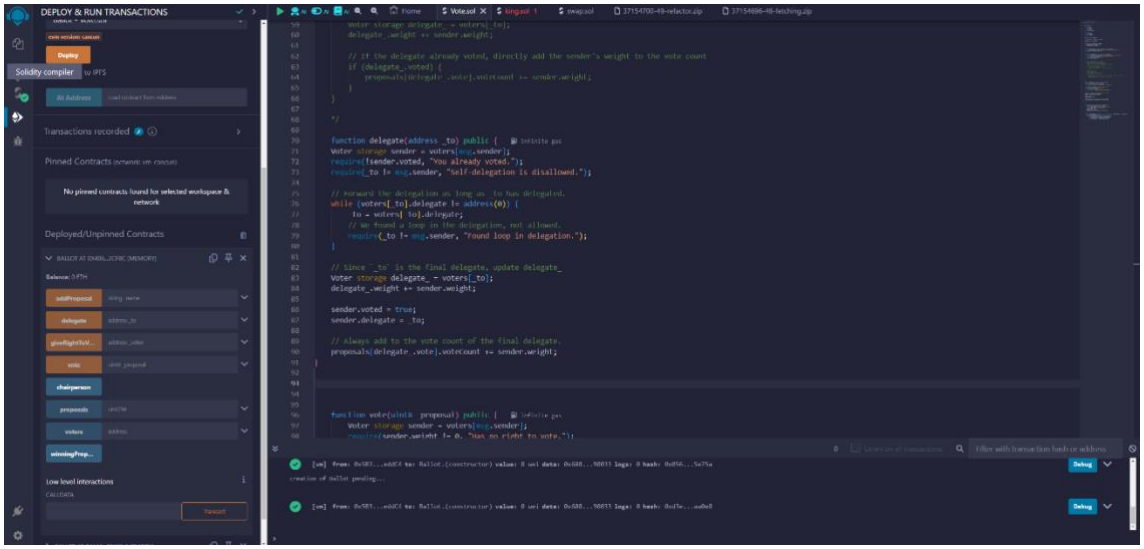

Figure 4. 6: Gas Efficiency

The delegate() function currently adds the sender's weight to the voteCount of the delegate's chosen proposal only if the delegate has already voted. However, this can be optimized. Instead of adding the weight only if the delegate has already voted, we can always add it to the voteCount of the final delegate in the delegation chain. This way, regardless of when the delegate votes, the weight is always accounted for.

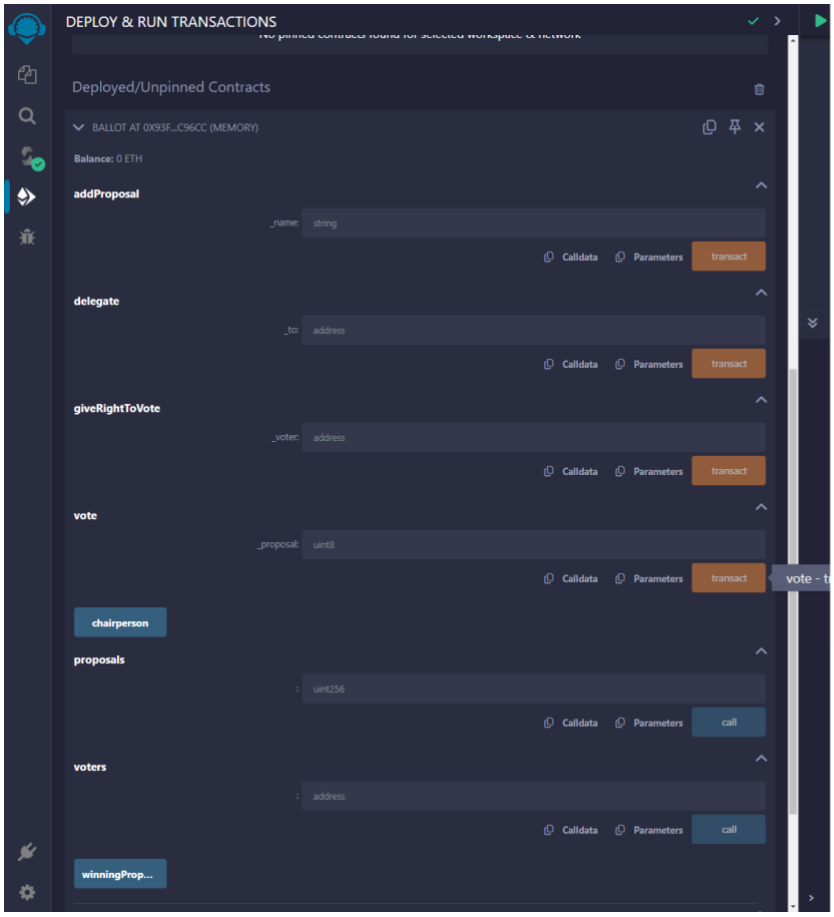

Figure 4. 7: contract deployment

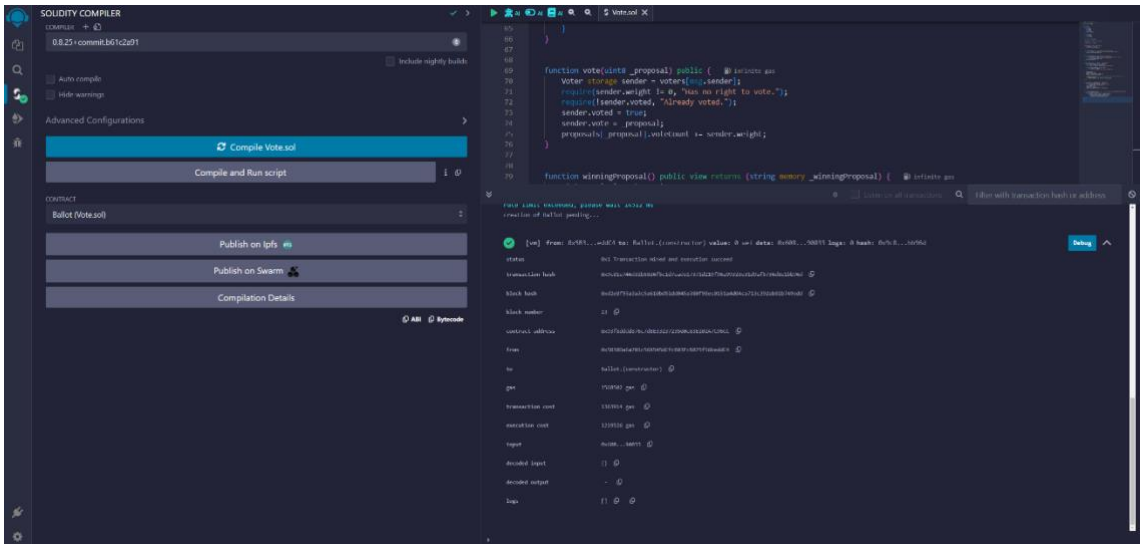

Figure 4. 8: Voting process

Figure 4.8 describes the voting process and compilation, once it is compiled the transaction is mined and the status is updated and ready to be deployed in the blockchain.

CHAPTER FIVE

CONCLUSION

In conclusion, the implementation of a blockchain-based electronic voting system holds immense potential for transforming the way elections are conducted around the world. By providing a secure, transparent, and tamper-proof platform for voters to cast their ballots, this innovative technology can effectively address many of the challenges that have plagued traditional voting methods in different countries, such as voter intimidation, ballot box snatching, and vote rigging.

Addressing Challenges and Promoting Democracy

Adopting a blockchain-based e-voting system can significantly enhance the integrity and transparency in electoral processes. By leveraging the decentralized and immutable nature of blockchain technology, this system can ensure that every vote is securely recorded and that the results are verifiable by all stakeholders. This level of transparency can help to build public trust in the electoral process and promote democratic values, as citizens can be confident that their votes are being counted and that the outcomes accurately reflect the will of the people.

Overcoming Implementation Hurdles

However, implementing a blockchain-based e-voting system will require a substantial investment in technology infrastructure and a concerted effort to build public trust and confidence in the system. Ensuring that all eligible voters have access to the necessary technology and are able to use it effectively will be a significant challenge. Additionally, there will be a need for robust regulations and safeguards to ensure the proper functioning of the system and to protect against potential misuse or abuse.

Embracing the Future of Elections

Despite these challenges, the benefits of a blockchain-based electronic voting system cannot be ignored. By improving the integrity and transparency of the electoral process, such a system can help to protect the rights of voters and ensure that elections in Nigeria are free, fair, and credible. As the world continues to embrace digital technologies, it is essential to stay at the forefront of these advancements and to leverage them to strengthen its democratic institutions.

Recommendations and Way Forward

Therefore, it is recommended that the government and relevant stakeholders around the world should take proactive measures to adopt blockchain-based e-voting technology in the country's electoral process. This will require a comprehensive approach that includes investment in infrastructure, public education and awareness campaigns, and the development of appropriate legal and regulatory frameworks. By embracing this transformative technology, Nigeria can set an example for other African nations and demonstrate its commitment to democratic principles and good governance.

REFERENCES

Li, H., Li, Y., Yu, Y., Wang, B., & Chen, K. (2021). A Blockchain-Based Traceable Self-Tallying E-Voting protocol in AI era. *IEEE Transactions on Network Science and Engineering*, *8*(2), 1019–1032. https://doi.org/10.1109/tnse.2020.3011928

Shahzad, B., & Crowcroft, J. (2019). Trustworthy electronic voting using adjusted blockchain technology. *IEEE Access*, *7*, 24477–24488. https://doi.org/10.1109/access.2019.2895670

Racsko, P. (2019). Blockchain and democracy. *Society and Economy*, *41*(3), 353–369. https://doi.org/10.1556/204.2019.007

Cullen, R., & Houghton, C. (2000). Democracy online: an assessment of New Zealand government web sites. *Government Information Quarterly*, *17*(3), 243–267. https://doi.org/10.1016/s0740-624x(00)00033-2

Schınckus, C. (2020). The good, the bad and the ugly: An overview of the sustainability of blockchain technology. *Energy Research & Social Science*, *69*, 101614. https://doi.org/10.1016/j.erss.2020.101614

Ometov, A., Bardinova, Y., Afanasyeva, A., Mašek, P., Zhidanov, K., Vanurin, S., Sayfullin, M., Shubina, V., Komarov, M., & Bezzateev, S. (2020). An overview on blockchain for smartphones: State-of-the-Art, consensus, implementation, challenges and future trends. *IEEE Access*, *8*, 103994–104015. https://doi.org/10.1109/access.2020.2998951

Gao, S., Zheng, D., Guo, R., Jing, C., & Hu, C. (2019). An Anti-Quantum E-Voting protocol in blockchain with audit function. *IEEE Access*, *7*, 115304–115316. https://doi.org/10.1109/access.2019.2935895

Hakak, S., Khan, W. Z., Gilkar, G. A., Imran, M., & Guizani, N. (2020). Securing Smart Cities through Blockchain Technology: Architecture, Requirements, and Challenges. *IEEE Network*, *34*(1), 8–14. https://doi.org/10.1109/mnet.001.1900178

Çabuk, U. C., Adıgüzel, E., & Karaarslan, E. (2018). A survey on Feasibility and Suitability of blockchain Techniques for the E-Voting Systems. *International Journal of Advanced Research in Computer and Communication Engineering*, *7*(3), 124–134. https://doi.org/10.17148/ijarcce.2018.7324