SAVONIA

THESIS – BACHELOR'S DEGREE
TECHNOLOGY, COMMUNICATION AND TRANSPORT

ASSESSING THE ROLE OF BLOCKCHAIN-BASED VOTING SYSTEMS IN ELECTORAL PROCESSES

AUTHOR ISMAILA JIMOH

SAVONIA UNIVERSITY OF APPLIED SCIENCES

THESIS
Abstract

Field of Study Technology, Communication and Transport	
Degree Programme Degree Programme in Incormation Technology, Internet of Things	
Author ISMAILA JIMOH	
Title of Thesis Assessing The Role of Blockchain-Based Voting Systems In Electoral Processes	
Date 18.12.2024	Pages/Appendices 47/
Client Organisation /Partners Savonia University of Applied Sciences	

This thesis examines the function of blockchain-based voting systems in improving electoral processes. Electoral processes worldwide face challenges such as vote tampering, electoral fraud, and administrative inefficiencies, particularly in developing countries. Blockchain technology, defined by decentralization, transparency, and unchangeability, has surfaced as a superior solution to the above challenges. This study analyzes blockchain principles, encompassing cryptographic security, consensus mechanisms, and smart contracts, assessing their relevance to voting systems. Multiple international case studies, such as blockchain-based elections in Sierra Leone, Norway, and Estonia, illustrate the integration of blockchain technology into electoral processes with differing levels of efficacy. Also discusses the implementation of blockchain-based voting architectures using concorduim blockchain testnet, focusing on system authorization, election processes, and delegation mechanisms.
Major findings highlight blockchain's ability to secure electoral data through cryptographic protocols and decentralized networks, reducing the likelihood of vote manipulation and unauthorized access. Limitations including scalability, privacy issues, and possible backdoor vulnerabilities still remain a challenge for the technology. The study also notes that while blockchain can enhance the technical aspects of elections, socio-political issues such as vote-buying and coercion remain unresolved.

Keywords
Blockchain Technology, Voting system, Smart Contract, Electoral process

CONTENTS

LIST OF FIGURES

LIST OF TABLES

1 INTRODUCTION

1.1 Background and Justification of the Study

The fundamental worth of democratic administration depends on the integrity of electoral procedures. Voting techniques, whether digital or manual, are susceptible to various problems, including vote manipulation, ballot stuffing, electoral fraud, and sabotage. Technological solutions are being evaluated as possible methods to address the issues faced by governments in improving election accountability and transparency (Yiaga Africa Report, 2023).

Blockchain technology is a sophisticated breakthrough capable of drastically altering voting procedures. Tripathi et al. (2023) contend that blockchain is a digital distributed ledger that secures and interlinks digital documents, known as blocks, via cryptographic techniques. Every data block is cryptographically connected to its predecessor, making modifications or manipulation highly unlikely. While now employed in industries including banking, supply chain management, and healthcare, researchers are exploring its potential to enhance election processes (Tripathi et al., 2023).

Blockchain-based voting systems seek to address numerous issues inherent in traditional voting methods. Decentralizing election processes via blockchain technology may diminish dependence on centralized authority, which are frequently viewed as susceptible to manipulation or corruption (Benabdallah et al., 2022). This would mitigate issues such as double voting, unauthorized access, and election manipulation. The transparency of blockchain enables all participants to verify the authenticity of their ballots, hence diminishing post-election disputes and maintaining voter confidence in the election results (Wendl et al., 2023).

Blockchain-based voting systems remain comparatively novel in terms of their implementation. Countries include Russia, Switzerland (Zug), Japan (Tsukuba), Estonia, the United States (in specific instances), and Sierra Leone have engaged in trials of blockchain voting (Beedham, 2018; Buldas et al., 2013; Huang et al., 2022; Perper, 2018).

In developing nations such as Nigeria, where electoral and administrative inefficiencies prevail, blockchain voting may provide a remedy to guarantee free, fair, and credible elections. However, the full implementation of these systems would be significantly constrained by shortcomings in infrastructure and technological adoption in these regions. Blockchain-based voting systems possess the potential to profoundly transform Africa, particularly in regions with a history of electoral violence, vote manipulation, and delayed election outcomes (Patil et al., 2018).

1.2 Problem Statement

The integrity breaches in electoral processes have led to substantial voter disengagement and diminished public confidence in democratic institutions, which are fundamental to a democratic government (Almeida et al., 2023). This thesis examines the distinct challenges encountered by conventional voting systems in developing nations, with a focus on Nigeria, and evaluates the potential of blockchain technology to offer viable solutions. In Nigeria, there were notable assaults on the electoral body (INEC) both prior to and following the 2023 election (Yiaga Africa Report, 2023), as illustrated in Figure 1.

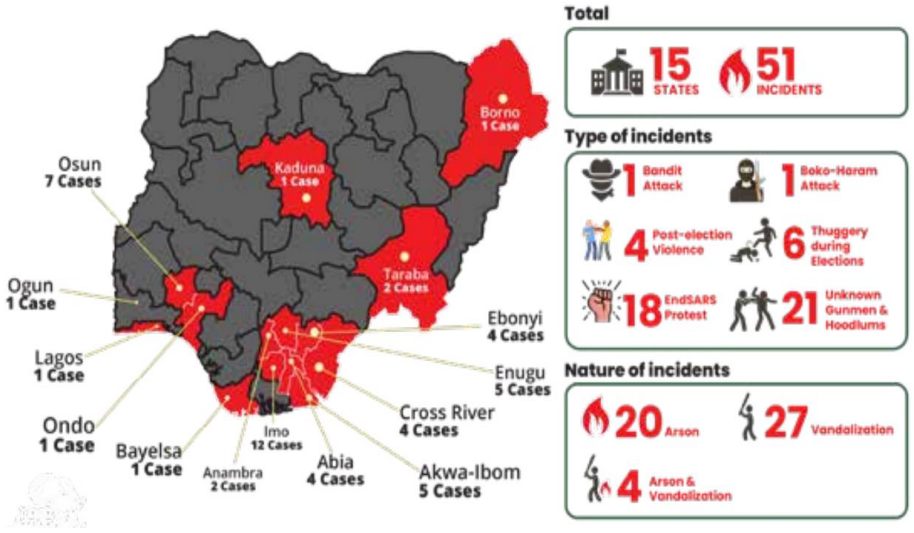

Figure 1. Attack on INEC offices in 2023 election (Yiaga Africa Report, 2023)

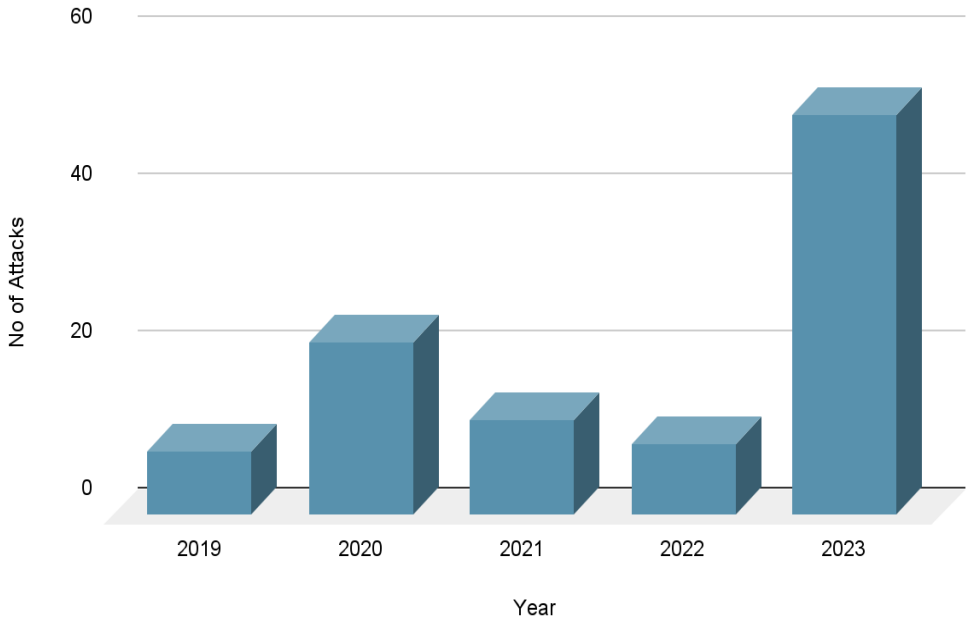

Figure 2. Chart showing the number of attacks on INEC office (Yiaga Africa Report, 2023)

Further electoral challenges faced during the election include electoral fraud and manipulation, including ballot stuffing, multiple voting, and result altering by unscrupulous authorities. The belief that the voting process could be manipulated discourages civic participation and diminishes voter turnout (van Baalen, 2024). The manual electoral processes sometimes encounter bureaucratic inefficiencies, including logistical challenges in ballot distribution, counting, and reporting.

A multitude of voters face challenges in accessing polling places, especially those residing in rural or disadvantaged areas. These challenges may include significant distances, inadequate transportation, and a lack of understanding of voting procedures. The physical infrastructure required for traditional voting methods is sometimes inadequate, leading to reduced voter participation and worries about the representativeness of electoral results (Yiaga Africa Report, 2023).

1.3 Objectives and Scope of the Study

The aim of this project is to assess the role and feasibility of blockchain-based voting systems in enhancing the integrity, transparency, security, and efficiency of electoral processes. The specific objectives are:

1. To examine the ways in which voting systems can be secured using blockchain technology.
2. To compare blockchain voting systems' integrity and transparency with other usual methods.
3. To examine issues with blockchain voting, such as scalability and accessibility.

The Nigerian democracy has major consideration for this thesis on assessing the function of blockchain-based voting systems in the context of electoral processes. The study's focus is on Nigeria's electoral setting, assessing the infrastructure, obstacles, and current election-related processes. Nigeria being one of the biggest democracies in Africa, presents an excellent argument for investigating blockchain solutions due to the country's electoral fraud, inefficiencies in government, and widespread public mistrust of the electoral process.

1.4 Research Approach

This study will review the use of smart contract programs in blockchain-based voting systems. An evaluation of the blockchain network and its features, where the smart contract was deployed, will be conducted. The availability, accessibility, and scalability of smart contracts will depend on the blockchain network where the voting system's smart contract was deployed. Furthermore, smart contracts for the voting system will be examined and evaluated according to authorization components (which aid access control to establish and manage a roster of eligible voters, administrators, and other roles), election components (which are accountable for designing and executing election processes),

and delegation components (which provide mechanisms for the electorate to assign votes to delegates who may vote on their behalf). This study will also clarify the merits and demerits of blockchain-based voting systems.

1.5 Overview of Report Structure

The introductory section of this study provides background information on the subject and establishes context for the research. The second section will elucidate the selected themes in greater detail and provide the reader with essential knowledge. The final section will discuss smart contracts, including their characteristics, scalability, accessibility, and availability. The fourth segment will examine case studies of blockchain-based voting in various nations. The fifth section will evaluate the impact of blockchain-based voting systems, including their benefits and drawbacks. The sixth section analyzes the blockchain authorization, delegation mechanism, and the architecture of the electoral process within the system. Ultimately, conclusions and suggestions will be derived from the review findings.

2 THEORETICAL FRAMEWORK

2.1 Overview of Voting Systems

What makes up an electoral system are the rules, guidelines, and procedures that specify how an election's final tally and consensus are to be reached. There are three parts to an electoral system: the ballot, the alternatives, and the algorithm for tallying votes (Reynolds et al., 2005).

1. Choices**:** This are the candidates in an election, as represented by the options given to voters in an electoral system. Primary elections, general elections, write-in candidates, debates, and other procedures or mixes thereof can all be used to ascertain the potential outcomes (N. P. Hernandez, 2021).
2. District Magnitude: An important factor in an election is the number of choices that are declared winners. The number of seats available to votes in a representative democracy is called the district size (André & Depauw, 2014). An SMD, or single-winner district, is an election with a district magnitude of one that only allows for the election of one candidate or choice. According to N. P. Hernandez (2021), a multi-member district (MMD) or multi-winner district is a voting system where the district magnitude is greater than one, resulting in the election of many candidates.
3. Ballot: Voters express their preferences through the use of a ballot. How many votes each person is allowed to cast and how they can indicate their preference for one or more choices are both determined by the layout of the ballot. The method of tallying has an immediate impact on this (Lu et al., 2024). When used in this sense, the word "ballot" includes not only the voting process itself but also the medium (paper, punch card, electronic machine, etc.) via which a voter indicates their choice and the regulations governing the marking of that medium. According to Lu et al. (2024), the ballot is the primary data structure that the tallying method is based on.
4. Electoral Formula: In order to turn votes into results, the electoral formula is used. The counting method and proportionality, in districts with more than one member, are the main components of the electoral formula (N. P. Hernandez, 2021).

In general, these factors are used to classify electoral systems into one of three broad groups. According to N. P. Hernandez (2021), there are three groups of representational styles: plurality/majority, proportional, and hybrid (combining the two).

The theory behind plurality and majority election systems is simple, but the practice may be more complicated. The choices that received the most votes will be proclaimed the winners once the tallying of votes is complete. In a plurality voting system, the options with the most votes are considered the winners, rather than those with a simple majority. The majority of American elections are held with a plurality ballot (N. P. Hernandez, 2021).

The primary objective of a Proportional Representation (PR) voting system is to deliver election outcomes that accurately reflect the preferences of the electorate. This is achieved by reducing the gap between the amount of votes received by candidates and the percentage of seats they secure. This is especially important within the framework of representative governance frameworks. Proportional representation functions by delivering a cross-section of electoral victors that corresponds proportionally to the votes allocated for each option (N. P. Hernandez, 2021).

Similar to the Alternative Vote (AV), the Single Transferable Vote (STV) is a voting system that uses proportional representation for numerous members. Similar to AV, STV makes use of preference-annotated ballots. STV is based on the idea that voters should rank their selections ordinally on the ballot, and then tallying all of the votes (N. P. Hernandez, 2021).

2.2 Fundamentals of Blockchain Technology

Similar to a traditional public ledger, blockchain technology is a distributed and decentralized series of blocks that include an exhaustive list of transaction data (Cheun, 2015). An example of a blockchain is shown in Figure 3. The genesis block, the first block to be added to a blockchain, does not have a parent block; in contrast, every block in a blockchain has exactly one.

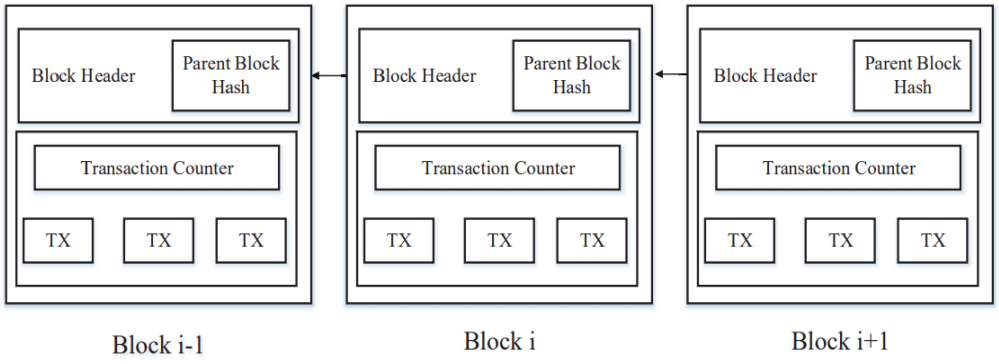

Figure 3. An example of a blockchain, which consists of a continuous sequence of blocks (Zheng et al., 2017).

Blockchain technology is a decentralized and distributed chain of blocks that contains a comprehensive record of transactions, similar to a traditional public ledger (Cheun, 2015). Figure 3 depicts a representation of a blockchain. In blockchain technology, each block possesses a unique parent block, and the first block established in a blockchain is known as the genesis block, which does not have a parent block.

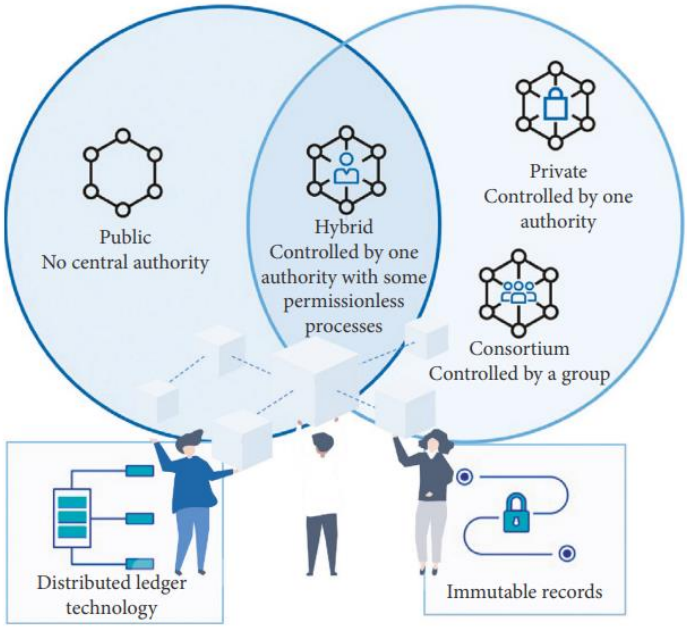

Figure 4. Types of blockchain (Anwar ul Hassan et al., 2022).

The four types of blockchains identified by Anwar-ul Hassan et al. (2022) are public, hybrid, consortium, and private. Because of their decentralized nature, public blockchains are available to anybody. Centralization is at the heart of private blockchains. One style of private permissioned blockchain that stands out is the consortium, which consists of multiple corporations working together to establish a centralized governance system. According to Pawar et al. (2018), a hybrid blockchain combines public and private blockchains. Since blockchain-based voting systems restrict participation to individuals above the age of 18, a permissioned blockchain is utilized. To ensure security and permanence, access is allowed only to those who match specific conditions.

TABLE 1. Overview of different blockchain types

Block-chain Type	Description	Transparency	Scalability	Security
Public Block-chain	Accessible to all, any individual may join and engage in the consensus process. For instance, Bitcoin and Ethereum.	High transparency. All transactions are accessible and can be authenticated by all individuals.	Limited scalability resulting from a substantial number of participants and resource-intensive consensus mechanisms (e.g., Proof of Work).	High security. Robust security via decentralization, yet theoretically susceptible to 51% attacks if an adversary commands the majority of the network.
Private Block-chain	Access is limited; only designated participants may join, regulated by a singular organization or entity.	Low transparency. Data access is limited to authorized individuals.	Enhanced scalability, reduced participants, and regulated environments facilitate expedited processing.	Moderate security, offering greater protection than public systems due to limited access, yet exhibiting reduced decentralization, which may result in trust concerns.
Permissioned Block-chain	A hybrid model permitting exclusively authorized participants, characterized by differing levels of transparency and control.	Moderate transparency, configurable for authorized participants only, not accessible to the public.	Designed for specific applications, it has moderate to high scalability and allows for customization of consensus algorithms.	Security can be robust with regulated participation and hybrid consensus mechanisms (e.g., Proof of Authority).

2.2.1 Decentralization and Data Integrity

Each node in the distributed network stores a full copy of the blockchain, which allows the network to function. Because of decentralization, the network is not controlled by a single entity. Developers work autonomously to distribute data among numerous nodes. This decentralization guarantees that no one entity has complete control over a distributed-control intersecting network. This feature strengthens the network by reducing the likelihood of a single point of failure (Wendl et al., 2023).

With blockchain technology, records of traffic data, intersection control decisions, and other important data may be created in a safe and unchangeable manner. Time stamps and links to previous transactions create a chronological series of blocks of data on the blockchain (Pawar et al., 2018). This ensures that any change to a block may be easily detected, as it would break the chain and alert the developers. Important for keeping the intersecting network secure and efficient, this ensures the data is consistent and reliable (Wendl et al., 2023) as well.

2.2.2 Cryptographic Security and Hash Functions

Hashing is a process that converts an original data set into a digest or hash through cryptographic hash functions, allowing the irreversible transformation of the message, as

illustrated in Figure 5 (Cryptographic Hash Functions in Blockchain, 2023). The cryptographic hash function in blockchain safeguards the message block and interconnects the blocks in a chain. Every block contains its own block hash and a hash of the preceding block. It assists them in establishing a cryptographically secure linear chain of blocks (Komalavalli et al., 2020).

Figure 5. Illustrations showing cryptographic security of messages using hash function (Cryptographic Hash Functions in Blockchain, 2023)

2.2.3 Consensus Mechanisms (Proof of Work, Proof of Stake)

According to Andrew et al. (2023), nodes in a blockchain network can experience Byzantine failures, which can lead to malfunctions, arbitrary or malevolent actions, or the possession of disinformation caused by connection latency. In trustless situations, the consensus mechanism is the backbone of a blockchain network, making sure that all members agree on the state of the network. According to Nguyen et al. (2019), the consensus technique controls several network operations, such as the addition of transactions and the motivation of players to behave responsibly. "Proof-of-Work" and "Proof-of-Stake" are the two most common consensus methods used by blockchains. Various consensus procedures are compared in Table 2.

TABLE 2. Comparisons of consensus mechanism in blockchain technology (Nguyen et al., 2019)

	Proof-of-Work	Proof-of-Stake	Hybrid
Leader selection	Based on hash rate	Based on stake	Depends on variant
Energy consumption	Significant	Negligible	Medium to negligible
Hardware requirement	High	None	Medium to none
Block generation speed	Slow	Fast	Medium to high
Transaction confirmation speed	Slow	Fast	Medium to high
Applications	Bitcoin, Ethereum, etc.	Cardano, Algorand, etc.	Casper, Peercoin, etc.

2.2.3.1 Proof of Work

In initially, Proof-of-Work (PoW) mechanisms were used to build blockchain networks. Each node in a Proof of Work (PoW) blockchain network is responsible for finding a unique identifier, or nonce, for the new block it proposes to create, and this process is repeated until the network reaches consensus (N. P. Hernandez, 2021). For a block to

be legitimate, the hash algorithm, which takes as inputs the nonce, the hash of the previous block, and the transactions in the new block, must produce an output within a specified target range. Cryptographic Hash Functions in Blockchain (2023) state that in order to find the nonce, one must repeatedly try various nonce values until one of them falls within the given range. Once a participant finds the nonce, they will share the block and all of the transactions related to it with other nodes. Upon authentication, the new block will be integrated into the existing chain, becoming the most recent block in the series, if it is acknowledged as the first block mined after the final block in the chain (Nguyen et al., 2019).In initially, Proof-of-Work (PoW) mechanisms were used to build blockchain networks. Each node in a Proof of Work (PoW) blockchain network is responsible for finding a unique identifier, or nonce, for the new block it proposes to create, and this process is repeated until the network reaches consensus (N. P. Hernandez, 2021). For a block to be legitimate, the hash algorithm, which takes as inputs the nonce, the hash of the previous block, and the transactions in the new block, must produce an output within a specified target range. Cryptographic Hash Functions in Blockchain (2023) state that in order to find the nonce, one must repeatedly try various nonce values until one of them falls within the given range. Once a participant finds the nonce, they will share the block and all of the transactions related to it with other nodes. Upon authentication, the new block will be integrated into the existing chain, becoming the most recent block in the series, if it is acknowledged as the first block mined after the final block in the chain (Nguyen et al., 2019).

2.2.3.2 Proof of Stake

Proof-of-Stake (PoS) was developed to reduce the computing requirements of Proof-of-Work (PoW) (King & Nadal, 2012). Recent Proof of Stake networks entirely abolish solution searching and no longer choose block leaders based on compute capability. Figure 6 illustrates how "Proof of Stake" designates block leaders according to the stakes they possess. The stake-based leader selection method reduces a node's probability of being selected as a leader based on its computational capacity, hence markedly decreasing the energy consumption of Proof of Stake mechanisms relative to Proof of Work. Furthermore, PoW networks sustain relatively modest and consistent rates for block production and transaction confirmation to guarantee security, while miners present a diverse array of blocks (Nguyen et al., 2019).

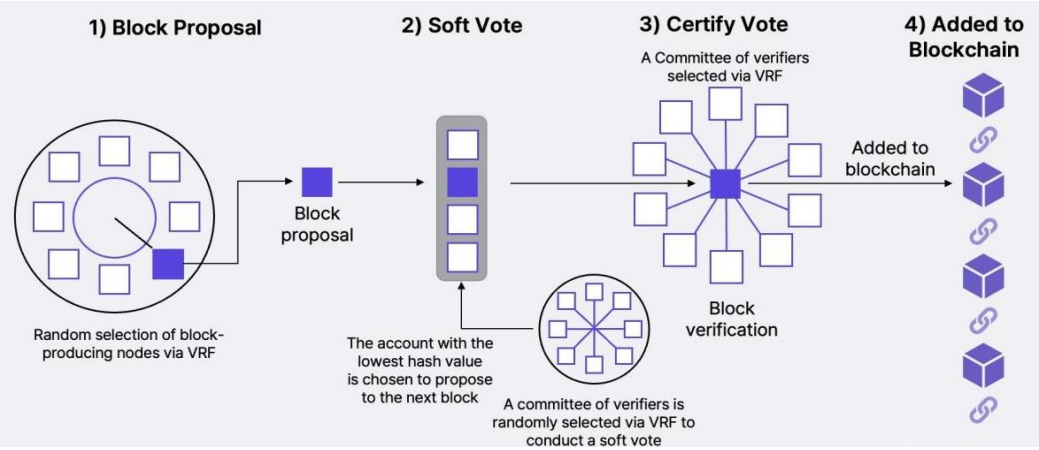

Figure 6. Illustration showing the selection approach in Proof-of-Stake algorithm (Tarasenko, 2022)

2.2.3.3 Delegated Proof of Stake (DPoS)

This version of the previous technique uses the identical staking principle. It is used to obtain voting power, which is then employed to elect block verifiers tasked with generating new blocks. Nodes proficiently assign their power, which is based on their stake in the network, hence the term (Zhang & Lee, 2020).

2.2.3.4 Practical Byzantine Fault Tolerance (PBFT)

A node submits a block proposal to a primary node. This primary node operates as a network administrator and distributes the block proposal to many backup nodes. Should a sufficient number of backup nodes agree with the proposed block, it gets integrated into the chain. If not, it is removed (Xiao et al., 2020).

3 REVIEW ON SMART CONTRACT PROGRAMS IN BLOCKCHAIN

3.1 Overview of Smart Contracts

A smart contract is a digital software that regulates transaction protocols (contractual norms) based on the consensus framework of blockchain technology. A smart contract is implemented within a computer system that uses blockchain technology as a virtual machine (Maksymyuk et al., 2019). The protocol is implemented on the blockchain and can autonomously execute upon completion of the agreement (Alshahrani et al., 2023). The implementation of a smart contract generally determines the specific virtual machine or network employed, such as Ethereum or Cardano. Criteria for evaluating smart contracts include privacy, security, performance, scalability, and speed (Maksymyuk et al., 2019).

A smart contract may independently do calculations, retain information, and facilitate transactions, among other capabilities (Alshahrani et al., 2023). Data authorization regulations, functionalities, and procedures can also be integrated into smart contracts. Thus, decentralization can be implemented via smart contracts, significantly reducing operational expenses (Alshahrani et al., 2023). Ethereum designated Solidity as a programming language, encompassing code instructions and event states (data) such as initial, intermediate, and final, for the implementation of smart contracts (Blockchain Developer's Guide, 2022).

In the Ethereum virtual machine, smart contracts were first introduced by Dannen (Blockchain Developer's Guide, 2022). Virtual machines on Ethereum run in a sandbox setting, with smart contracts having limited access to data. The results of the smart contract code are part of the transactions. In the next steps, the Ethereum Virtual Machine processes the transaction codes. Data collecting, analysis, and solution implementation are all tasks that a smart contract can carry out. According to Maksymyuk et al. (2019), a programming language is used to build smart contracts that are built on blockchain technology. According to the Blockchain Developer's Guide (2022), once a smart contract is created, it is sent to a blockchain and will automatically execute when the conditions are met. The execution of smart contracts is typically unblockable by third parties. A smart contract is a computer program that, when sent to a certain address on the blockchain, automatically carries out predefined tasks. After the smart contract accepts the transaction and the required event occurs, the code is executed by the blockchain-distributed virtual machine. Upon completion of the process, an additional participant can join a smart contract and trigger its automatic execution upon meeting specific predetermined conditions (Zheng et al., 2020).

The whole life cycle of smart contracts consists of four consecutive phases, as illustrated in Figure 7.

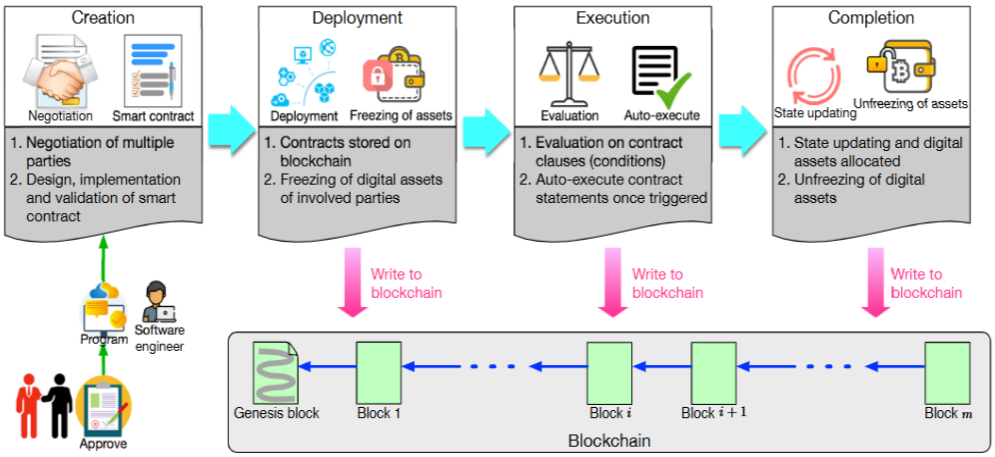

Figure 7. The life cycle of a smart contract (Jani, 2020)

3.1.1 Creation of smart contracts

At the outset, the many parties involved deliberate about the rights, responsibilities, and restrictions imposed by the contract (Idelberger et al., 2016). Reaching a consensus may need several iterations of talks and compromises. In order to help parties come up with a preliminary contract, consultants or attorneys will be present. After the agreement is expressed in regular English, software developers use languages like declarative and logic-based rule languages to build smart contracts (Idelberger et al., 2016). Converting to smart contracts entails the same three steps as developing software: planning, coding, and testing. According to Zheng et al. (2020), smart contract development is an iterative process that involves several optimization and refinement sessions.

3.1.2 Deployment of smart contracts

Soon after their development, platforms built on blockchains will be able to install the validated smart contracts. The contracts kept on blockchains cannot be changed, according to Sillaber and Waltl (2017). There must be a new contract drawn out for each change. All parties involved in a smart contract can access it after it is deployed on a blockchain. In addition, by freezing their digital wallets, the smart contract participants safeguard their digital assets (Sillaber & Waltl, 2017). Digital wallets allow the parties to be recognized.

3.1.3 Execution of smart contracts

Following the implementation of smart contracts, the contractual terms have been examined and evaluated. Upon completion of the contractual criteria (e.g., receipt of the product), the contractual processes will be implemented automatically. A smart contract consists of multiple declarative statements linked by logical relationships. The associated statement is executed automatically upon the fulfillment of a condition, leading to a transaction being conducted and validated by blockchain miners (Koulu, 2016). The blockchains subsequently retain the finalized transactions and the revised states.

3.1.4 Completion of smart contracts

After execution of a smart contract, the statuses of all participating parties are revised. Transactions conducted using smart contracts and their modified statuses are documented on blockchains. Concurrently, the digital assets have been conveyed from one entity to another (e.g., financial transfer from the purchaser to the vendor). Consequently, the parties concerned have liberated their digital assets. The smart contract has thus completed its whole life cycle (Zheng et al., 2020).

3.2 Attributes of Smart Contracts in Blockchain Voting

A smart contract possesses several significant attributes, including autonomy (it operates independently), transparency (the code is accessible on the blockchain), immutability (once deployed, it cannot be altered), the absence of intermediaries, determinism (predefined conditions initiate execution), and distribution (replicas of the contract are present throughout the network). These characteristics indicate that a smart contract adheres to predetermined rules autonomously, is immutable after deployment, and is accessible to all participants in the network. This implies that a trustworthy third party is not required to monitor the agreement.

3.3 Availability, Accessibility, and Scalability of Smart Contracts

Smart contracts function independently of conventional business hours, allowing blockchain users to execute transactions at any time, including outside typical operational periods. This contrasts with traditional working hours, which may limit accessibility and influence timelines (Bogner et al., 2016). The availability of smart contracts pertains to their continuous functionality on blockchain networks, whereas the accessibility of smart contracts assesses the ease with which developers and consumers can engage with them.

On-chain smart contracts may be restricted by the restrictions of the blockchain network, such as the speed of transactions (Zheng et al., 2020). Therefore, scalability is essential for these blockchain networks. Scalability refers to a blockchain network's ability to effectively handle a growing number of transactions and users, hence directly impacting the execution of smart contracts (Bogner et al., 2016). In certain instances, an external solution for scalability is necessary in blockchain. These external solutions are referred to as layer 2.

3.4 Comparison of Blockchain Networks for Voting Systems

Different blockchain networks have varying features that make them suitable for implementing voting applications. As seen in Table 3, some blockchain networks are considered and compared in this section.

Ethereum: Ethereum is a decentralized platform capable of executing smart contracts. In contrast to Bitcoin's Turing-incomplete scripting system, Ethereum has developed Turing-complete languages such as Solidity, Serpent, Low-level Lisp-like Language (LLL), and Mutan, enabling a broader range of user applications beyond bitcoin (Bogner et al., 2016; Dai et al., 2019).

Hyperledger Fabric: A distributed ledger system developed for the purpose of executing smart contracts is known as Hyperledger Fabric (Cachin, 2016). Hyperledger executes code inside a Docker container, as opposed to Ethereum's smart contracts running on virtual machines (EVM). The use of containers allows smart contract applications to run with less overhead than virtual machines (VMs), but this comes at the expense of operating system isolation (Zheng et al., 2020). Fabric does not support Ethereum-specific smart contract languages but rather more traditional, high-level ones like Java and Go (Golang). There is Turing completeness in fabric.

Corda: This blockchain network operates as a decentralized ledger system for the preservation and processing of historical digital asset information. Consensus in Corda can be achieved by leader selection, log replication, and safety guarantees. Corda employs a point-to-point communications system rather than worldwide broadcasting in blockchains. Users must specify the recipients of their communications and the particular information they intend to convey (Zheng et al., 2020).

Stellar: Stellar is easier to use and understand than Ethereum. Stellar is compatible with a wide range of languages, such as PHP, Golang, Python, and JavaScript. Stellar contracts, however, are not Turing complete. Stellar, like Fabric, runs code within Docker containers, which further reduces overhead. In addition, according to Mazières (2015), Ethereum takes about 3.5 minutes to execute a transaction, whereas Stellar takes about 5 seconds.

Rootstock: Rootstock operates on Bitcoin, allowing expedited transaction execution. Simultaneously, Rootstock is compatible with Ethereum, using Solidity for contract implementation (Zheng et al., 2020).

EOS: Built from the ground up, EOS makes decentralized apps more scalable. By not relying on just one consensus algorithm, EOS is able to leverage the benefits of both Byzantine Fault Tolerance (BFT) and Delegated Proof of Stake (DPOS) (Yaqoob et al., 2017).

(47)

TABLE 3. Comparison of Smart Contract Networks for Voting Systems (Zheng et al., 2020)

	Ethereum	Fabric	Corda	Stellar	Root-stock	EOS
Execution environ-ment	EVM	Docker	JVM	Docker	VM	Web As-sembly
Language	Solidity, Ser-pent, LLL, Mu-tan	Java, Go-lang	Java, Ko-tlin	Python, JavaS-cript, Golang and PHP, etc	Solidity	C++
Turing Complete-ness	Turing com-plete	Turing complete	Turing in-complete	Turing incomplete	Turing complete	Turing complete
Data model	Account based	Key-value pair	Transac-tion based	Account based	Account based	Account based
Consensus	PoW	PBFT	Raft	Stellar Consensus Protocol (SCP)	PoW	BFT-DPOS
Permission	Public	Private	Private	Consortium	Public	Public
Application	General	General	Digital currency	Digital currency	Digital currency	General

4 CASE STUDIES ON BLOCKCHAIN-BASED VOTING IN OTHER COUNTRIES

4.1 The role of blockchain technology in voting in various countries

Some countries have already taken the initiative to experiment and improve their voting system by using blockchain technology and a decentralized peer-to-peer network accompanied by a public ledger. Only a limited number of countries have effectively integrated blockchain technology into their voting systems, typically in pilot programs or specific use cases (Srivastava et al., 2018). This section presents case studies of blockchain technology utilized in the voting processes of various countries where this technology has been implemented.

4.2 Sierra Leone

In March 2018, the first blockchain-based elections occurred in Freetown, the capital and largest city of Sierra Leone. The importance of this presidential election lay in the blockchain-based framework of the voting procedure (Patil et al., 2018). The blockchain project in Sierra Leone's Western District, the nation's most populous area, relied on manual vote documentation by Agora, a Swiss organization that offers digital voting solutions. The integration of a blockchain analogy ensures transparency by documenting each vote on a blockchain, thereby allowing Agora to verify the transparency of the votes cast inside the district. While entries on permissioned blockchains are available to all users, their validation is confined to authorized personnel. The supervision of these authorized individuals is an important additional phase in Sierra Leone's blockchain-based voting procedure.

A notable advantage of blockchain-based electronic voting is the reduction of long-term expenses for developing countries, since it eliminates the costs related to producing paper ballots. Furthermore, they are significantly more inclined to mitigate electoral violence. Chohan (2018) asserts that this blockchain technique signifies an advancement towards the total automation of the electoral process. Citizens may vote electronically via biometric data and unique cryptographic keys, with vote validation conducted through blockchain technology.

4.3 Morocco

The use of blockchain technology in Moroccan elections has been the subject of a recent research. The research team came up with a hybrid approach that combines online and in-person voting to accommodate different kinds of elections. The Solana blockchain (Chafiq et al., 2024) is the basis for the election system's layered design, as seen in Figure 8. Two basic levels make up this design. Data validation and verification is handled by a Distributed Permission Ledger Technology (DPLT) layer, while data immutability and decentralization are ensured by a Solana blockchain layer. According to Chafiq et al. (2024), the combination of the two layers ensures a trustworthy and safe voting environment throughout the election process.

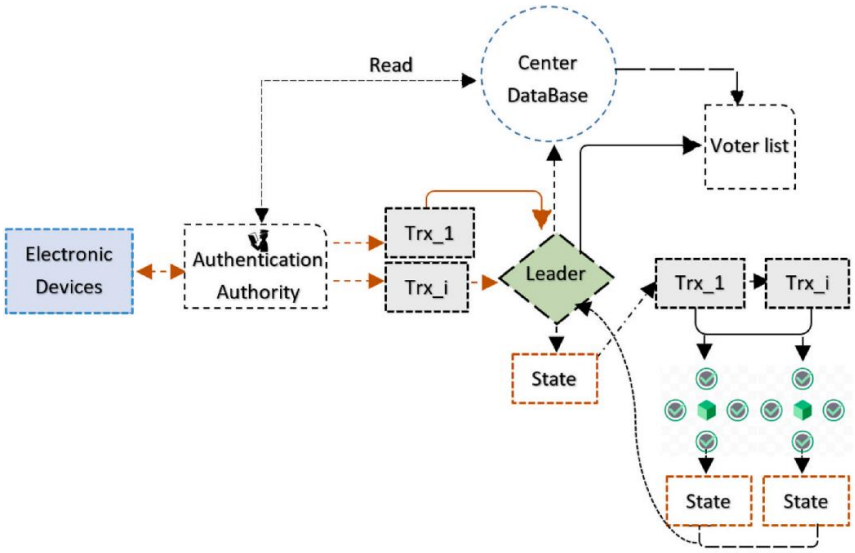

Figure 8. Transaction Flow in Moroccan's Blockchain system (Chafiq et al., 2024)

The system begins when the user initiates the voting procedure. The system retrieves essential electoral information, containing candidate lists, from the database. The system later offers the user a selection of candidates for consideration. This measure allows voters to make educated choices. Upon completion of voter selections, the system processes the choices and produces an encrypted ballot, thereby safeguarding the security and confidentiality of the vote. The system evaluates the operational capability of the user's device, verifying its capacity to securely send the encrypted ballot. This measure ensures the precise recording of the vote (Maksymyuk et al., 2019). The third phase entails a verification of ballot accuracy, confirming that the voter's choices are correctly documented prior to the official casting of the vote.

The study suggests that blockchain can effectively prevent electoral fraud and manipulation if designed and implemented correctly (Chafiq et al., 2024).

4.4 Norway

Smartmatic conducted a case study on blockchain technology for Norway's voting systems. Smartmatic, a premier provider of safe, transparent, accessible, and verifiable voting solutions, establishes the benchmark for election integrity and inclusivity globally, incorporating encrypted result transmission, paper ballot backup, comprehensive auditing, and online voting (Smartmatic, 2018). Smartmatic focuses on the design and implementation of electoral system technologies.

Citizens might choose to vote online or use conventional paper ballots at polling locations. The voting period lasted eight days. Smartmatic (2018) reported that a significant online participation rate of 85.5% demonstrated voters' confidence in technology and their preference for convenience. Online voters were permitted to cast their votes many times via the internet, but only the last submission was considered valid. Voters who engaged online could modify their digital vote by presenting a paper ballot at a polling location. This technique allowed authorities to eliminate any criminal incentive for voter coercion or the transaction of online votes (Smartmatic 2018).

TIVI, an online voting system developed by Smartmatic, was fully linked with Norway's ID-Porten to improve participation and keep voters informed. ID-Porten is often used by residents to access online Norwegian government services. Automated SMS-based electronic poll cards were sent to remind voters of the referendum and to inform them upon the reception of their online vote. To enhance security and transparency, the system employed a permissioned, private blockchain to safeguard and verify ballot box integrity (Smartmatic, 2018).

4.5 Estonia

Estonia has implemented electronic voting via blockchain technology (Almeida et al., 2023). Estonia's achievement in electronic voting depends on (i) improving technical infrastructure and public trust and (ii) creating a strong legal framework (Organization for Economic Co-operation and Development, 2019). Estonia's effective electronic voting depends on its technical framework, particularly the X-Road data exchange middleware and an effective national public key infrastructure (PKI) backed by a solid encryption scheme, namely the electronic identification card (ID card). The ID card, which effectively integrates digital and physical identities, has enabled the seamless provision of online public services in Estonia. The ID card can be used in public key infrastructure for authentication, safeguarding specific data (e.g., electronic ballot data) (Almeida et al., 2023), and signature verification (Organization for Economic Co-operation and Development, 2019).

From Estonia's practical experience, multiple insights regarding the factors that contribute to the successful implementation of electronic voting can be outlined as follows: Estonia has established an adequate foundation for its e-government model and established public trust in electronic services. Secondly, the nation has established reasonably extensive legal frameworks governing election management (both traditional and electronic) and technical advancement (Organization for Economic Co-operation and Development, 2019). These characteristics have established the fundamental prerequisites for the effective execution of blockchain-based electronic voting (Cong et al., 2024).

4.6 Other Case studies

American nonprofit "Follow My Vote" has developed a blockchain-based electronic voting system with an emphasis on voter mobility; the group is non-partisan and serves the public good. The application showcases the implementation of their solution on the BitShares blockchain, a public blockchain that offers smart contract capabilities, through a comprehensive web site (Long & Ernest, 2020; BitShares Whitepaper). The "Voting Booth" decentralized application (dApp) is the main means by which users interact with this blockchain. Users are required to generate two sets of Elliptic Curve Cryptography (ECC) keys when they register for the system (Kapor & Pandya, 2009). To guarantee voter anonymity, one pair is utilized to validate voters' identities through a reliable third party; this permits individuals to cast their votes using their registered key as an identifier rather than their real identity (BitShares Whitepaper). Authentication of transactions storing encrypted vote data onto the blockchain requires the second pair in addition to the

identification key. An attacker can't impersonate a person successfully until they obtain both keys linked to that person, which is why the two-pair technique is so effective at improving system security. Votes are securely recorded on a blockchain, which guarantees transparency while keeping voters' anonymity intact. This is because only the voters themselves own the private key that is needed to decrypt the contents of their votes from the identity pair (Almeida et al., 2023).

Based in Boston, Massachusetts, Voatz is a venture capital-funded business that focuses on mobile-first electronic voting solutions. Using blockchain technology to incorporate the public bulletin board feature common to centralized systems, Voatz developed an electronic voting solution that was indistinguishable from TiVi's. Not only that, but Voatz took a more cautious approach and ended up with a more centrally planned system than the others we've looked at (Voatz, 2020). Its smartphone app for voting is the heart of the Voatz solution. Similar to desktop PC virus and malware detection software, the program safeguards itself from various mobile-centric intrusions through a Mobile Threat Defense service. Numerous references to "smartphone-to-server" and "server-to-smartphone" interactions show that Voatz's methodology is mainly centralized, despite the fact that it uses HTTPS and end-to-end encryption to protect connections at the network level (Almeida et al., 2023). Only data storage was conducted via blockchain in this particular case study.

5 EFFECTS OF BLOCKCHAIN-BASED VOTING SYSTEMS

5.1 Advantages of Blockchain in Voting System

Implementing blockchain technology in a voting system offers numerous benefits. This section discusses the followings.

5.1.1 Security

This represents a significant advantage of blockchain-based e-voting systems, with sub-categories emphasizing the following distinct viewpoint:

1. Integrity: Comprehensive security assurances are aligned with the architecture (Harley & Cooper, 2022).
2. Immutability: Once a vote is cast, it cannot be altered, ensuring the conclusiveness of the voting procedure (Cabuk et al., 2020).
3. Durability: Resistant to data loss and ensures the persistence of stored information.
4. Stability: The ability to endure disturbances or alterations, including hacking. Robust encryption systems, typically embedded in blockchain technology, augment stability (Kugusheva & Yanovich, 2019).
5. Non-repudiation: A voter is unable to contest the legitimacy of their submitted vote (Haiyan et al., 2020).

5.1.2 Transparency

There is more openness in the voting, recording, administration, and tallying processes with the blockchain-based electronic voting system's design. As a result, audits may be conducted by third parties with confidence, and the blockchain's transactions (votes) can be easily confirmed (Hjalmarsson et al., 2018).

5.1.3 Privacy

This refers to the capacity of blockchain-based e-voting systems to protect voters' personal information and ensure the confidentiality of their voting choices..

1. Anonymity: safeguarding a voter’s identity (Kumar et al., 2017).
2. Confidentiality: The selections of voters are private, and results are not disclosed in advance (Russo et al., 2021).
3. Untraceability: Inhibit the identification of a vote's origin to its specific voter (Kumar et al., 2017).
4. Pseudo anonymity: The true identities of voters are concealed, yet their voting actions are associated with unique identifiers aligned to pseudonyms or addresses (Ikundi et al., 2022).

5.1.4 Verifiability

This pertains to the ability to confirm that votes have been cast as intended, maintained, and counted.

1. Public verifiability: The capacity for all individuals to authenticate the complete electoral process (Vivek et al., 2020).
2. Individual verifiability: The ability of each voter to ascertain that their vote was correctly recorded and counted (Vivek et al., 2020).
3. Auditability: Guarantee the precision and veracity of the voting process (Mello-Stark & Lamagna, 2017).

5.1.5 Accessibility

This provides each eligible voter with an equitable opportunity to engage in the voting process.

1. Availability: Blockchains often guarantee that voters can submit their ballots at any time during the designated timeframe without facing any complications.
2. Significant participation: This technology facilitates considerable engagement of eligible voters (Benabdallah et al., 2022).
3. Universal accessibility: All qualified voters can use the system efficiently.

5.1.6 Decentralization tart with capital

This pertains to the allocation of voting system authority, accountability, and operations throughout a network, rather than a centralized institution. This characteristic is crucial to blockchain technology and is vital for bolstering public trust by reducing the influence of a potentially corrupt intermediary (Benabdallah et al., 2022).

5.1.7 Usability

This enables a substantial number of voters to cast their votes effectively while ensuring satisfaction with the process (Hsu & Bronson, 2018).

1. Usability: The ease and directness with which the system can be operated.
2. Comprehensibility: Transparency in system functionality guarantees that voters execute their votes as intended.

5.1.8 Efficiency

This relates to the capacity of an e-voting system to enable voters to cast their votes efficiently and cost-effectively.

1. Cost efficiency: The system's capacity to execute voting procedures at a minimal expense. This could include reduced spending for installation and repair, material allocation, and labor charges (Ikundi et al., 2022).
2. Temporal efficiency: The system's capacity to expedite the voting process and the tabulation of votes.
3. Performance efficiency: The ability to handle large quantities of data (votes), process, and accurately count votes with security and rapidity (Kumar et al., 2017).

5.1.9 Trustworthiness

This includes a secure, transparent, and equitable system that guarantees the precise monitoring and integrity of each vote. It is an equilibrium of stringent security protocols, fast outcomes, and scalability, all of which are essential for maintaining confidence in the electoral process (Shahzad & Crowcroft, 2019).

1. Participation is restricted to eligible voters (Shahzad & Crowcroft, 2019).
2. Equity: Election results are not revealed until after the voting process has concluded (Sheer Hardwick et al., 2018).
3. Accountability: The blockchain enables the verification of the accuracy of the official vote record (Küsters & Müller, 2017).
4. Uniqueness: Each qualified voter is permitted one and only one vote.
5. Precision: Every vote is scrupulously documented, ensuring no modification, exclusion, or illicit inclusion occurs (Anane et al., 2007).
6. Credibility: The degree to which voters, legislators, and the general public believe and have confidence in the e-voting system.
7. Reliability: The system's consistent performance over time guarantees accurate, error-free functionality and availability (Taş & Tanrıöver, 2021).

5.1.10 Compatibility

This relates to the ability of the blockchain-based voting system to operate in conjunction with various hardware, software, protocols, and legal frameworks.

1. Adaptability: The ability of an e-voting system to alter or adjust in response to various situations or requirements that may emerge.
2. Flexibility: The ability to adapt to diverse frameworks, electoral systems, voting methods, and voter interactions.

5.2 Disadvantages of Blockchain in Voting System

Although blockchain technology's intrinsic qualities offer a potential solution to the ongoing problems with electronic voting systems, Khudoykulov et al. (2021) stress that there are substantial risks associated with using this technology. The fact that these vulnerabilities go beyond common problems like malware injection suggests that blockchain technology could not be the answer to all of the problems with electronic voting (Kumar et al., 2017). One major issue with electronic voting on blockchain networks, according to an EU Parliament study, is that there isn't yet a publicly accessible blockchain that can quickly and efficiently process millions of transactions, or votes (Skotnica et al., 2021).

5.2.1 Scalability

Because of their architectural restrictions, blockchain-based voting systems are not suited for national adoption due to scalability issues; nevertheless, they are suitable for smaller applications (Jafar et al., 2021). The blockchain network is stressed during large-scale elections, according to Pawlak and Poniszewska-Maranda (2021). The growing computing costs and length of the storage chain are to blame for this, as they threaten to

render the system unusable and limit its scalability. In order to handle a high number of voters with simultaneous processing needs, a national voting framework faces a significant problem (Dogo et al., 2018). Network congestion, delays in vote verification and recording, and undermining of the integrity and timeliness of election results (termed latency and throughput) are all consequences of blockchain architecture's scalability issues, according to Yang et al. (2020). The costs of developing a blockchain network were also highlighted by Apeh et al. (2021). Infrastructure, maintenance, and operations all add up to a significant financial burden for a country like Nigeria, which is already struggling to make ends meet.

1. Throughput: This refers to the rate at which transactions are processed and confirmed within the blockchain network. Unlike traditional databases, blockchain networks face throughput constraints due to the need to combine block size, block production time, and network security (Sanka & Cheung, 2021; Xie et al., 2019). The creation of substantial voting transactions in a brief timeframe during a national election is a difficulty, necessitating a high throughput that current blockchain platforms are unable to deliver (Huang et al., 2022).
2. Latency: This denotes the processing length, signifying the time needed for each transaction to be completed on the blockchain. Sallal et al. (2023) contend that this characteristic is essential as it directly reflects the operational velocity of a blockchain network. Tang et al. (2023) imply that an increase in network latency jeopardizes the consensus process of a blockchain network, potentially causing delays in the real-time voting experience and the recording of voting transactions. Latency difficulties are exacerbated with more transactions, potentially resulting in election delays (Wan et al., 2019). This matter is especially relevant when contemplating the potential application of blockchain technology in Nigeria's voting systems.

5.2.2 Issues on Privacy and Security

The blockchain network is vulnerable as all members can see the details and balances associated with every public key, thereby compromising transactional privacy (Prashanth Joshi et al., 2018). The network associates each transaction with a pair of pseudonyms that distinguish the sender and receiver. Nonetheless, de-anonymization facilitates the implementation of static analysis on the blockchain or the active surveillance of network data to identify users, thereby rendering the blockchain network vulnerable to numerous attacks (Bernal Bernabe et al., 2019; Feng et al., 2019), such as address clustering, transaction fingerprinting, denial-of-service (DoS) attacks, and Sybil attacks, which jeopardize the security of voters. In contrast to paper ballots submitted at a real polling location, the method does not ensure voter confidentiality by linking specific ballots to their respective voters. Notwithstanding the adoption of multiple protocols (Henry et al., 2018) designed to improve blockchain privacy, none of the proposed methods effectively obscure user identities from attackers functioning at the network level. According to Dasgupta et al. (2019), the commonly used cryptographic hash algorithm SHA-256 is susceptible to birthday attacks and length extension attacks. Moreover, these vulnerabilities

let unauthorized modifications to signed message hashes without the necessity of the shared secret. This jeopardizes the security and integrity of the Nigerian electoral process (Bellare & Kohno, 2004). Furthermore, encryption algorithms now considered secure may face problems with the rise of quantum computing. Current encryption technologies considered secure may be compromised by future quantum computing wielded by individuals with illicit purposes (Dasgupta et al., 2019).

5.2.3 Backdoor Vulnerabilities/Loopholes in Network Architecture

The endpoints of a blockchain system, where interactions among computers, humans, and the blockchain network occur, are the most susceptible places. User authentication and authorization are the sole security procedures at this point in time (Prewett et al., 2020). This is because hackers pose a threat to the voting process by posing as voters, casting ballots in their stead, or otherwise disrupting the process using the credentials needed to access a shared distributed ledger (Abuidris et al., 2019).Because blockchain technology only guarantees the security of system data within the blockchain, it is insufficient. Inadequate border protection is a consequence of the absence of distinct boundaries in the architectural layers of blockchain. Because of this, the system is more susceptible to cyber-attacks from inside and outside the organization (Lee et al., 2019). Shrivas et al. (2020) assert that blockchain systems, functioning as a service at the application level, are susceptible to hacking due to vulnerabilities in the hardware, operating system, and language runtime environment. These may manifest in diverse forms, including concealed access points, clandestine codes, or purposeful vulnerabilities embedded into the system's design or execution. Blockchain depends on a decentralized consensus method to establish trust among its participants. Nonetheless, the consensus system is vulnerable to a 51% attack, enabling attackers to seize control of the entire blockchain (Feng et al., 2019). This presents an added risk to the voting system, wherein attackers, including hackers, user groups, or organizations like the electoral commission, may exploit the system for their advantage (Kumar et al., 2017).

5.2.4 Blockchain does not prevent vote-buying or coercion

Although blockchain technology can substantially improve the security and transparency of e-voting systems, it cannot entirely eliminate coercion or vote-buying, which remain concerns in a democratic society (Abuidris et al., 2019). Suwito and Dutta (2019) noted that despite the implementation of cryptographic safeguards and a decentralized framework, many electronic voting protocols are developed without addressing two pivotal concerns: vote-buying and coercion, which may subject voters to pressure or manipulation to vote in specific ways, regardless of the blockchain system in place (Abuidris et al., 2019). The research suggested that although individual votes remain confidential, this confidentiality may unintentionally heighten coercion. The transparency of the blockchain allows coercers to monitor voters through their wallet addresses and potentially determine if a voter adhered to their instructions. This completely jeopardizes the confidentiality of the voting process. Eghe-Ikurhe et al. (2023) assert that coercion within a blockchain-based e-voting system will compromise the integrity of transparent, free, and fair

(47)

elections. If the suggested method does not inhibit fraudulent activities, it requires a reevaluation of its effectiveness in election processes.

6 SYSTEM DESIGN

6.1 Architecture of Blockchain-Based Voting System

The system's architecture has various components interacting to meet both functional and non-functional requirements. Three steps, authorization, election, and delegation, make up the system's design execution. Each stage focuses on a different part of the system's design, and each part is responsible for completing a unique set of duties.

6.1.1 Functional Requirements

Certain subcategories of the functional requirements are considered essential to this research:

1. All implementations of electoral systems seek to examine and comprehensively fulfill multi-vote capability.
2. To a large extent, the features of blockchain technology that guarantee "a voter's ballot and the act of casting a ballot are recorded and retained as anticipated" bring to this confidence. When a voter sends a transaction to the network along with their ballot, but miners fail to include it in any blocks, this property is lacking.
3. The inherent characteristics of blockchain partially satisfy the necessity for preserving voter privacy. Although it is practicable to transmit privacy-preserving transactions that retain anonymity on the network, it is probably beyond the capacity of most voting participants and would be difficult to ensure in any significant manner.

6.1.2 Non-Functional Requirements

The study asserts that entities external to the system must fulfill the non-functional demands. While many of these demands are beyond the purview of this study, this section of the thesis does address several of them to a limited extent; these needs include flexibility, maintenance, and assurance.

6.2 System Authorization

The goal of the authorization components is to set up access control by making and keeping a variety of administrators, eligible voters, and any other roles needed to run election systems. The authorization components are responsible for controlling who can access sensitive contract function calls that change the contract's state, including setting up elections or casting ballots. The design is flexible enough to meet the evolving needs of different groups and organizations, while still maintaining a consistent enough interface to offer support. System design is informed by principles obtained from authorization procedures and traditional operating system access control frameworks. The fundamental authentication mechanisms are managed using the asymmetric cryptography offered by the fundamental blockchain framework.

6.3 System Election Processes

The election components are tasked with the construction and operation of electoral procedures. Among these responsibilities are the following: handling votes, tallying ballots, determining election winners, and ensuring the integrity and privacy of the election. Typically, an online election will go through the following steps: planning, distribution, voting, submission, counting, and verification. Authorization components are anticipated to regulate responsibilities linked to voter registration, which are typically addressed during the setup process. The dissemination phase, which mostly involves sending election information to voters, is not included in this research because it is considered to be outside its scope. We anticipate that the built-in features of the blockchain network will handle and facilitate the auditing phase, which involves examining the integrity and results of the election.

6.4 System Delegation Mechanisms

The voters can designate delegates to vote on their behalf by using the delegation components. One way to visualize a delegation structure is as a graph. N. Hernandez (2021) describes a directed acyclic graph (DAG) forest structure in which all vertices represent delegates and all voters are separated and inactive. A sink vertex represents a representative who has not yet assigned their vote to anyone else. Edges that are directed denote delegations. By repeatedly counting the incoming edges to each vertex, we may find a voter's cumulative weight, which is a measure of their voting power.

7 RESULTS

7.1 Test Results

The implementation of the voting system thesis was executed on the Concordium Testnet blockchain. Concordium is a scientifically grounded proof-of-stake blockchain, the first globally to incorporate identity within its protocol, tailored to fulfill regulatory standards. The Concordium blockchain aims to address the quadrilemma of scalability, security, decentralization, and regulation. Blockchain stakeholders assert that addressing compliance and regulatory standards is essential to facilitate trillions of possible commercial transactions via blockchain technology (Concordium, 2020).

A blockchain testnet is a supplementary network to the mainnet, explicitly intended for testing and development activities. It replicates the functionality of the mainnet while functioning in a sandbox environment, allowing developers to experiment without the hazards linked to actual assets (Trust Wallet, 2024). The subsequent section outlines significant milestones in the execution of the voting system.

voting setup interface: First, the election has to be created before any vote can be made. Figure 9 shows a screenshot of the election creation page. This voting setup is platform running on Concordium Testnet, as seen in Figure 10, while Figure 11 shows a screenshot of the voting poll creation page.

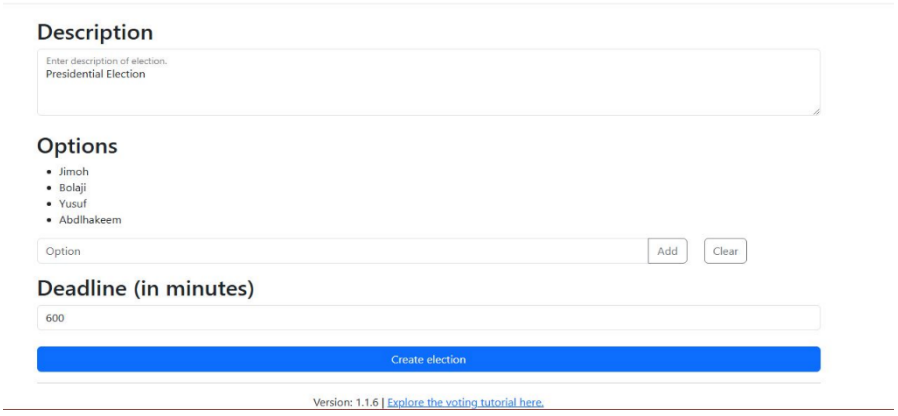

Figure 9. Screenshot of election creation page on Concordium testnet

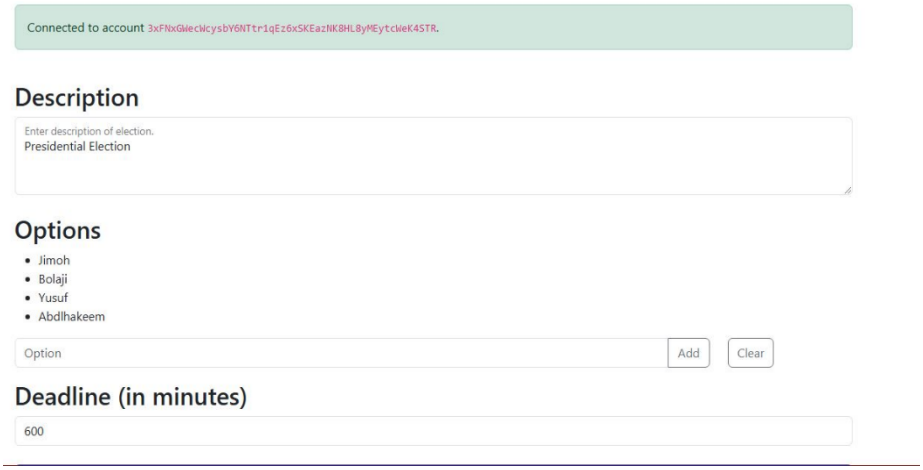

Figure 10. Screenshot of voting setup platform with a connected Concordium blockchain

The upper section exhibits a linked wallet against a green backdrop, revealing the address 3xFNxGWe...K4STR. This wallet facilitates interaction with the blockchain for voting purposes. The term "Presidential Election" is inscribed in the "Description" field. The purpose of the election is being established. Jimoh, Bolaji, Yusuf, and Abdilhakeem are the candidates in the election. The "deadline" is set as 600, signifying that the voting session will last for 600 minutes (10 hours). Additionally, there are input areas and buttons to add or remove voting options.

Figure 11. Screenshot of voting poll creation page

From Figure 12 is a Chrome Extension setup for Concordium Wallet. The wallet setup is being done to interact with the Concordium blockchain for activities like voting, identity verification, or other decentralized applications.

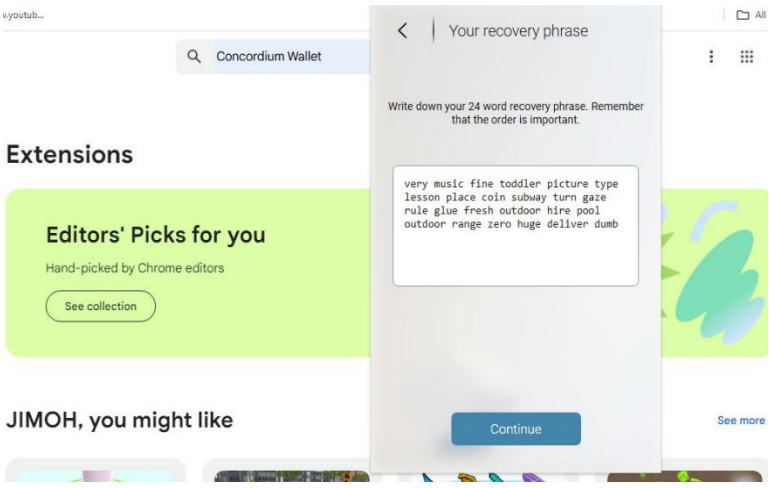

Figure 12. Chrome Extension setup for Concordium Wallet

Figure 13 shows an identity verification interface related to Concordium blockchain. This feature ensures that the user can request and verify their identity before engaging in blockchain transactions or applications. If the wallet is disconnected, it means further operations are paused until reconnected.

Concordium integrates identity verification at the protocol level, meaning every user must verify their identity to participate in the network. Hence, to start using the Concordium blockchain, you must first request an identity from one of the identity providers.

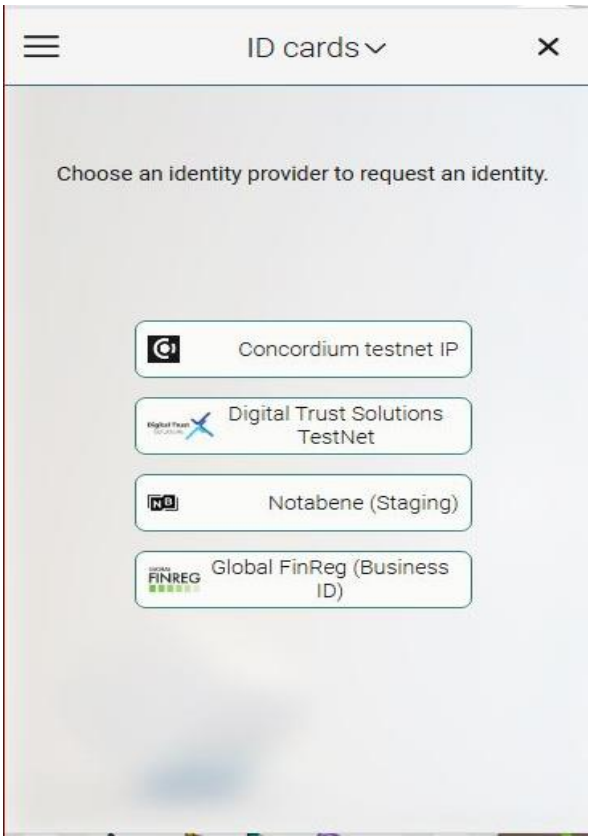

Figure 13. Identity verification interface on Concordium blockchain

User Interface of a Digital Wallet: The wallet interface emphasizes account management, pending actions, and balance tracking. The major components, as seen in Figure 14, include:

1. Accounts Dropdown: Allows users to choose between various wallet accounts.
2. Pending Section: Exhibits transactions or actions awaiting validation.
3. Balance Information: Displays details across three categories: (i) Public Balance Total: Comprehensive visible balance. (ii) Public Amount: Capital accessible for public transactions. (iii) Stake/Delegation Amount: Capital allocated for rewards or governance involvement. All values are displayed as CØ.00, signifying zero balances, which represent placeholder values or an unutilized wallet.
4. Establish New Account: Users may establish a new account at their discretion.
5. Concordium identification: Emphasizes identification verification, featuring a card called "Identity 1" as the identity designation, accompanied by a badge indicating verification by a reputable authority.

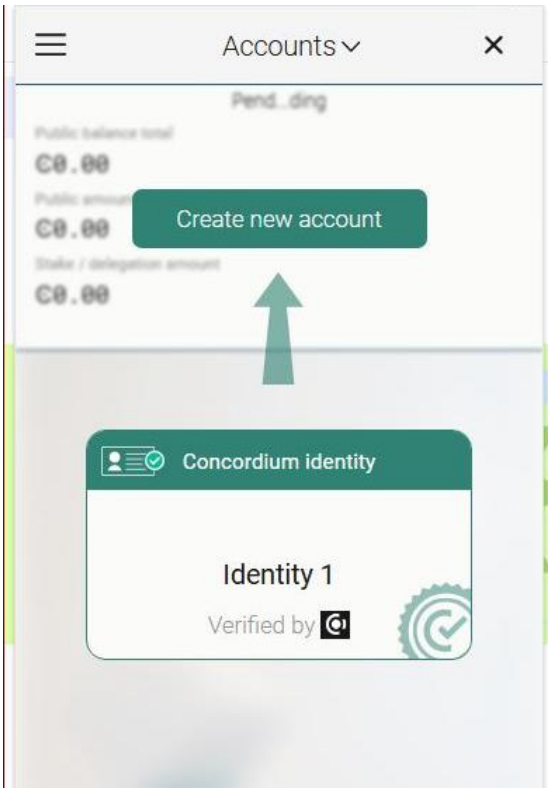

Figure 14. User interface of a digital wallet used for voting

Election Results Interface: The screenshot from Figure 15 represents a live election status page, showcasing ongoing results for a presidential election hosted on the Concordium blockchain.

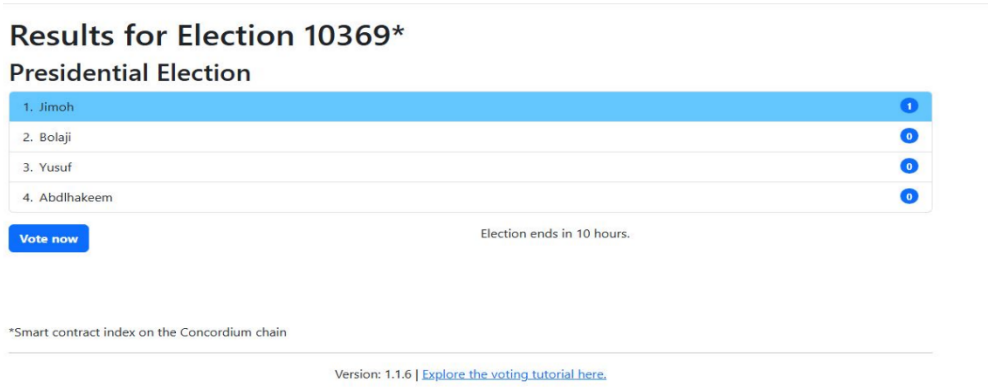

Figure 15. Screenshot showing the election result

7.2 Analysis and Discussion

Certain requirements must be satisfied in order to address digital voting machines, internet voting systems, or traditional paper-based voting:

1. Eligibility: Participation in voting should be restricted to bona fide voters;
2. Non-reusability: Each voter is permitted to cast a single vote.
3. Confidentiality: Only the voter is permitted to access information regarding their selection;

(47)

4. Equity: Intermediate vote results are inaccessible to all.
5. Soundness: Invalid ballots must be identified and excluded from the tallying process;
6. Comprehensiveness: All legitimate ballots must be accurately counted.

Discussed below is a brief discussion for satisfying these properties in online voting systems.

7.2.1 Eligibility

The resolution to the matter of eligibility is quite evident. Voters must authenticate their identity through a recognized identification mechanism to engage in online voting. All legitimate voter identities must be incorporated in the participant list. Nevertheless, dangers exist: Before any changes are made to the list of participants, it needs to be double-checked to make sure no unauthorized people are added. Then, after that, the system for identifying voters needs to be solid and safe to avoid theft or illegal access to voter accounts. The development of an identification system is fundamentally a difficult undertaking (Oliver, 2019). However, considering the importance of this system in different settings, especially with regard to digital government services, it would be wise to utilize an existing identification system instead of developing a new one, as it would go beyond the scope of the project.

7.2.2 Non-reusability

Enforcing non-reusability may seem straightforward first; a voter merely needs to indicate their vote on the participation list and be prohibited from voting again. Regardless, privacy must be prioritized; so, guaranteeing both non-reusability and voter anonymity is a challenge. Furthermore, permitting the voter to cast a second ballot may complicate the process further (Ziegler, 2015).

7.2.3 Privacy

When casting an online ballot, "privacy" means that no one other than the voter knows how they voted. According to Gao et al. (2022), blind signatures, homomorphic encryption, and mix-networks are the main strategies that are needed to achieve this characteristic. The signer of a blind signature does not see the actual data that is being signed. To do this, a blinding function is employed, which ensures that the blinding and signing functions are commutative.

$$Blind(Sign(message)) = Sign(Blind(message))$$ (Gao et al., 2022)

Before sending their message for signature, the requester keeps it secret. To create a signature for an unblinded message, they use what they know about blinding parameters in conjunction with the signature they obtained for a blinded transmission. A mathematically sound blind signature prevents anybody other than the requester from linking a blindfolded communication to its corresponding signature pair and an unblinded version (Wang et al., 2022).

Fujioka, Okamoto, and Ohta's 1992 voting system employed a blind signature (Fujioka et al., 1993). Each eligible voter is required to sign and return their ballot to the validator. The voter's eligibility is confirmed, the blind ballot is endorsed, and then it is returned to the voter by the validator. Before accepting the ballot, the tallier verifies the validator's signature, which the voter generates and sends to them for the unblinded vote.

7.2.4 Fairness

Voters encrypt their choices before submitting them and decode them once the voting process is complete to ensure fairness and avoid the acquisition of temporary results. Crucially, in order to access encrypted verdicts, one must have a decryption key. Only then can intermediate findings be retrieved. The solution is to have many keyholders handle the key distribution (Fujioka et al., 1993). Decryption becomes impossible in a system that demands participation from every key holder; this makes the system unstable. This leads to the use of threshold approaches, which mandate a minimum number of key holders in order to decode data. Secret sharing and distributed key generation are the two main ways to achieve key sharing. According to Jafar et al. (2021), secret sharing and distributed key generation are two different approaches to generating keys. In secret sharing, a trusted dealer splits the generated key into segments and distributes them to key holders. On the other hand, in distributed key generation, all participants work together to derive the key.

8 CONCLUSION

This thesis examined the feasibility of blockchain-based voting systems, the potential issues they may present, and the advantages they could offer in the political process. Blockchain technology offers a better answer to certain electoral difficulties, such as vote tampering, electoral fraud, and insufficient transparency. The immutability, decentralization, and transparency of blockchain can enhance trust in electoral systems by guaranteeing secure and verifiable voting procedures.

The results demonstrate that blockchain's ability to improve election security is evident, since its cryptographic protocols ensure that votes are immutable and irretrievable. Decentralized governance minimizes the potential for centralized manipulation, while transparent public ledgers enable independent verification of results. Blockchain voting can decrease election expenses by obviating the need for paper ballots and minimizing administrative overhead.

Nonetheless, the thesis also uncovered substantial problems. Scalability difficulties remain a critical issue due to blockchain's limited transaction processing capability, especially in large election processes. Privacy concerns persist, as the transparency of public ledgers could expose voter identities if insufficiently safeguarded. The thesis also addressed potential vulnerabilities in the blockchain architecture, such as exploitable backdoors and network attacks, which might compromise the integrity of the election.

Furthermore, although blockchain can guarantee the technological integrity of the voting process, it is incapable of mitigating socio-political challenges such as vote-buying and voter coercion. These difficulties require a balanced strategy that includes technical advancement, regulatory structures, and voter education.

REFERENCES

Abuidris, Y., Hassan, A., Hadabi, A., & Elfadul, I. (2019). Risks and opportunities of block chain based on E-voting systems. *2019 16th International Computer Conference on Wavelet Active Media Technology and Information Processing*. https://doi.org/10.1109/iccwamtip47768.2019.9067529

Almeida, R. L., Baiardi, F., Di Francesco Maesa, D., & Ricci, L. (2023). Impact of decentralization on electronic voting systems: A systematic literature survey. *IEEE Access: Practical Innovations, Open Solutions*, *11*, 132389–132423.

Alshahrani, N. M., Kiah, M. L. M., Zaidan, B. B., Alamoodi, A. H., & Saif, A. (2023). A review of smart contract blockchain based on multi-criteria analysis: Challenges and motivations. In *arXiv [cs.DC]*. https://doi.org/10.48550/ARXIV.2302.08496

Anane, R., Freeland, R., & Theodoropoulos, G. (2007). E-voting requirements and implementation. *The 9th IEEE International Conference on E-Commerce Technology and The 4th IEEE International Conference on Enterprise Computing, E-Commerce and E-Services (CEC-EEE 2007)*. https://doi.org/10.1109/cec-eee.2007.42

André, A., & Depauw, S. (2014). District magnitude and the personal vote. *Electoral Studies*, *35*, 102–114.

Andrew, Isravel, D. P., Sagayam, K. M., Bhushan, B., Sei, Y., & Eunice, J. (2023). Blockchain for healthcare systems: Architecture, security challenges, trends and future directions. *Journal of Network and Computer Applications*, *215*(103633), 103633.

Anwar ul Hassan, C., Hammad, M., Iqbal, J., Hussain, S., Ullah, S. S., AlSalman, H., Mosleh, M. A. A., & Arif, M. (2022). A liquid democracy enabled blockchain-based electronic voting system. *Scientific Programming*, *2022*, 1–10.

Apeh, A. J., Ayo, C. K., & Adebiyi, A. (2021). A scalable blockchain implementation model for nation-wide electronic voting system. In *Lecture Notes in Computer Science* (pp. 84–100). Springer International Publishing.

Beedham, M. (2018, September 3). *Japan is experimenting with a blockchain-powered voting system*. The Next Web. https://thenextweb.com/news/japan-city-blockchain-voting

Bellare, M., & Kohno, T. (2004). Hash function balance and its impact on birthday attacks. In *Advances in Cryptology - EUROCRYPT 2004* (pp. 401–418). Springer Berlin Heidelberg.

Benabdallah, A., Audras, A., Coudert, L., El Madhoun, N., & Badra, M. (2022). Analysis of blockchain solutions for E-voting: A systematic literature review. *IEEE Access: Practical Innovations, Open Solutions*, *10*, 70746–70759.

Bernal Bernabe, J., Canovas, J. L., Hernandez-Ramos, J. L., Torres Moreno, R., & Skarmeta, A. (2019). Privacy-preserving solutions for blockchain: Review and challenges. *IEEE Access: Practical Innovations, Open Solutions*, *7*, 164908–164940.

BitShares Whitepaper. Retrieved November 30, 2024, from https://docs.bitshares.build/docs/get-started/bitshares-whitepaper/

Blockchain Developer's Guide: Develop smart applications with Blockchain technologies - Ethereum, JavaScript, Hyperledger Fabric, and Corda 9781789954722, 178995472X.

Bogner, A., Chanson, M., & Meeuw, A. (2016). A decentralised sharing app running a sm art contract on the ethereum blockchain. *Proceedings of the 6th International Conference on the Internet of Things*. IoT'16: The 6th International Conference on the Internet of Thi ngs, Stuttgart Germany. https://doi.org/10.1145/2991561.2998465

Buldas, A., Kroonmaa, A., & Laanoja, R. (2013). Keyless signatures' infrastructure: How t o build global distributed hash-trees. In *Secure IT Systems* (pp. 313–320). Springer Berlin Heidelberg.

Cabuk, U. C., Adiguzel, E., & Karaarslan, E. (2020). A survey on feasibility and suitability of blockchain techniques for the E-voting systems. *arXiv [cs.CR]*. https://doi.org/10.48550/ARXIV.2002.07175

Cachin, C. (2016). *Architecture of the Hyperledger Blockchain Fabric*.

Chafiq, T., Azmi, R., & Mohammed, O. (2024). Blockchain-based electronic voting systems: A case study in Morocco. *International Journal of Intelli gent Networks*, *5*, 38–48.

Cheun, D. L. K. (Ed.). (2015). *Handbook of digital currency: Bitcoin, innovation, financial i nstruments, and big data*. Academic Press.

Chohan, U. (2018). Blockchain enhancing political accountability? Sierra Leone 2018 cas e. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3147006

Concordium: Secure Blockchain & CCD Token Solutions. (2020). Retrieved December 9, 2024, from https://www.concordium.com/

Cong, L. T. Q., Thuy, N. D. P., Nhi, H. T. N., & Van Anh, T. (2024). Blockchain-based electronic voting: Lessons from Estonia. *Vietnamese Journal of Legal Sciences*, *1 1*(2), 27–39.

Dai, H.-N., Zheng, Z., & Zhang, Y. (2019). Blockchain for internet of things: A survey. *IEEE Intern et of Things Journal*, *6*(5), 8076–8094.

Dasgupta, D., Shrein, J. M., & Gupta, K. D. (2019). A survey of blockchain from security p erspective. *Journal of Banking and Financial Technology*, *3*(1), 1–17.

Dogo, Nwulu, Olaniyi, Aigbavboa, Nkonyana, (2018). Blockchain 3.0: Towards a secure ballotcoin democracy through a digitized public ledger in developing countries. *I-Manager S Journal on Digital Signal Processing*, *6*(2), 24.

Eghe-Ikhurhe, G. O., Roni, N., Bonsu, M. O.-A., & Chen, X. (2023). The relevance of blockchain based voting adoption in governance structure : evidence from Nigeria. *International Journal of Economics, Commerce and Ma nagement*, *11*(1), 1–21.

Feng, Q., He, D., Zeadally, S., Khan, M. K., & Kumar, N. (2019). A survey on privacy prot ection in blockchain system. *Journal of Network and Computer Applications*, *126*, 45–58.

Fujioka, A., Okamoto, T., & Ohta, K. (1993). A practical secret voting scheme for large sc ale elections. In *Advances in Cryptology — AUSCRYPT '92* (pp. 244–251). Springer Berlin Heidelberg.

Gao, W., Chen, L., Rong, C., Liang, K., Zheng, X., & Yu, J. (2022). Security analysis and i mprovement of a redactable consortium blockchain for industrial internet-of-things. *The Computer Journal*, *65*(9), 2430–2438.

Haiyan, X., Lifang, W., & Yuechuan, W. (2020). A new fair electronic contract signing prot ocol. In *Advances in Intelligent Networking and Collaborative Systems* (pp. 289–295). Springer International Publishing.

Harley, K., & Cooper, R. (2022). Information integrity. *ACM Computing Surveys*, *54*(2), 1 –35.

Henry, R., Herzberg, A., & Kate, A. (2018). Blockchain Access Privacy: Challenges and Directions. *IEEE Security & Privacy*, *16*(4), 38–45.

Hernandez, N. (2021). *Nathanph/election-contracts*. GitHub. https://github. com/nathanph/election-contracts.

Hernandez, N. P. (2021). *Blockchain Elections: Smart Contract Electoral System Design And Implementation*. https://libres.uncg.edu/ir/listing.aspx?id=35832

Hjalmarsson, F. P., Hreioarsson, G. K., Hamdaqa, M., & Hjalmtysson, G. (2018). Blockch ain-Based E-Voting System. *2018 IEEE 11th International Conference on Cloud Computing (CLOUD)*. https://doi.org/10.1109/cloud.2018.00151

Home - Voatz secure and convenient voting anywhere. (2020, May 20). Voatz. https://voatz.com /

Hsu, J., & Bronson, G. (2018). E-voting technologies usability: A critical element for enabling successful elections. In *Emer ging Challenges in Business, Optimization, Technology, and Industry* (pp. 61–78). Springer International Publishing.

Huang, J., He, D., Obaidat, M. S., Vijayakumar, P., Luo, M., & Choo, K.-K. R. (2022). The application of the blockchain technology in voting systems. *ACM Comp uting Surveys*, *54*(3), 1–28.

Idelberger, F., Governatori, G., Riveret, R., & Sartor, G. (2016). Evaluation of logic-based smart contracts for blockchain systems. In *Rule Technologies. Research, Tools, a nd Applications* (pp. 167–183). Springer International Publishing.

Ikundi, O., Nwosu, K. C., & Abdulgader, M. (2022). LegitVote: A blockchain-based system to facilitate E-voting process. *2022 International Conference on Computer and Applications (ICCA)*. 20 22 International Conference on Computer and Applications (ICCA), Cairo, Egypt. https:// doi.org/10.1109/icca56443.2022.10039527

Jafar, U., Aziz, M. J. A., & Shukur, Z. (2021). Blockchain for Electronic Voting System—Review and Open Research Challenges. *Sensors (Basel, Switzerland)*, *21*(17), 5874.

Jani, S. (2020). *Smart Contracts: Building Blocks for Digital Transformation*. Unpublished . https://doi.org/10.13140/RG.2.2.33316.83847

Kapor, B., & Pandya, P. (2009). Data Encryption. In *Computer and Information Security Handbook* (pp. 395–421). Elsevier.

Khudoykulov, Z., Tojiakbarova, U., Bozorov, S., & Ourbonalieva, D. (2021). Blockchain b ased E-voting system: Open issues and challenges. *2021 International Conference on Informatio*

n Science and Communications Technologies (ICISCT). https://doi.org/10.1109/icisct52966.2021.9670245

King, S., & Nadal, S. (2012). *Peercoin — The Pioneer of Proof-of-Stake*. https://www.peercoin.net/read/papers/peercoin-paper.pdf

Komalavalli, C., Saxena, D., & Laroiya, C. (2020). Overview of blockchain technology concepts. In *Handbook of Research on Blockchain Technology* (pp. 349–371). Elsevier.

Koulu, R. (2016). Blockchains and online dispute resolution: Smart contracts as an alternative to enforcement. *SCRIPT-Ed*, *13*(1), 40–69.

Kugusheva, A., & Yanovich, Y. (2019). Ring Signature-Based Voting on Blockchain. *Proceedings of the 2019 2nd International Conference on Blockchain Technology and Applications*. https://doi.org/10.1145/3376044.3376054

Kumar, M., Katti, C. P., & Saxena, P. C. (2017). A secure anonymous E-voting system using identity-based blind signature scheme. In *Information Systems Security* (pp. 29–49). Springer International Publishing.

Küsters, R., & Müller, J. (2017). Cryptographic security analysis of E-voting systems: Achievements, misconceptions, and limitations. In *Electronic Voting* (pp. 21–41). Springer International Publishing.

Lee, Hyung, J., & S. M. Massachusetts Institute of Technology. (2019). *Systematic approach to analyzing security and vulnerabilities of blockchain systems* [Massachusetts Institute of Technology]. https://hdl.handle.net/1721.1/121793

Long, W., & Ernest, A. (2020). *Secure Decentralized Application Development*. Follow My Vote. https://followmyvote.com/

Lu, Y., Li, H., Gao, L., Yu, J., Yu, Y., & Su, H. (2024). Self-tallying e-voting with public traceability based on blockchain. *Computer Standards & Interfaces*, *88* (103795), 103795.

Maksymyuk, T., Gazda, J., Han, L., & Jo, M. (2019, July). Blockchain-based intelligent network management for 5G and beyond. *2019 3rd International Conference on Advanced Information and Communications Technologies (AICT)*. https://doi.org/10.1109/aiact.2019.8847762

Mazières, D. (2015). *The Stellar Consensus Protocol: A Federated Model for Internet-level Consensus*.

Mello-Stark, S., & Lamagna, E. A. (2017, March). The need for audit-capable E-voting systems. *2017 31st International Conference on Advanced Information Networking and Applications Workshops (WAINA)*. https://doi.org/10.1109/waina.2017.87

Nguyen, C. T., Hoang, D. T., Nguyen, D. N., Niyato, D., Nguyen, H. T., & Dutkiewicz, E. (2019). Proof-of-stake consensus mechanisms for future blockchain networks: Fundamentals, applications and opportunities. *IEEE Access: Practical Innovations, Open Solutions*, *7*, 85727–85745.

Oliver, J. E. (2019). The effects of eligibility restrictions and party activity on absentee voting and overall turnout. *American Journal of Political Science*, *40*(2), 498.

Organisation for Economic Co-operation and Development. (2019). *Digital opportunities for better agricultural policies*. Organization for Economic Co-operation and Development (OECD).

Patil, H. V., Rathi, K. G., & Tribhuwan, M. V. (2018). A Study on Decentralized E-Voting System Using Blockchain Technology. *International Research Journal of Engineering and Technology (IRJET)*, *5*(11). https://www.irjet.net/archives/V5/i11/IRJET-V5I1109.pdf

Pawar, S., Saraf, A., Parade, S., & Sharma, S. (2018). Review on Blockchain Technology. *International Journal of Computer Applications*, *182*(31), 40–41.

Pawlak, M., & Poniszewska-Marańda, A. (2021). Trends in blockchain-based electronic voting systems. *Information Processing & Management*, *58*(4), 102595.

Perper, R. (2018, March 14). *Sierra Leone just became the first country in the world to use blockchain during an election*. Business Insider. https://www.businessinsider.com/sierra-leone-blockchain-elections-2018-3

Prashanth Joshi, A., ,Kennesaw State University, Marietta, GA 30060, USA, Han, M., & Wang, Y. (2018). A survey on security and privacy issues of blockchain technology. *Mathematical Foundations of Computing*, *1*(2), 121–147.

Prewett, K. W., Prescott, G. L., & Phillips, K. (2020). Blockchain adoption is inevitable—Barriers and risks remain. *Journal of Corporate Accounting & Finance*, *31*(2), 21–28.

Reynolds, A., Reilly, B., & Ellis, A. (2005). *Electoral System Design: The New International IDEA Handbook*. International Institute for Democracy and Electoral Assistance.

Russo, A., Anta, A. F., Vasco, M. I. G., & Romano, S. P. (2021). Chirotonia: A scalable and secure e-voting framework based on blockchains and linkable ring signatures. *2021 IEEE International Conference on Blockchain (Blockchain)*. https://doi.org/10.1109/blockchain53845.2021.00065

Sallal, M., de Fréin, R., & Malik, A. (2023). PVPBC: Privacy- and verifiability-preserving E-voting based on permissioned blockchain. *Future Internet*, *15*(4), 121.

Sanka, A. I., & Cheung, R. C. C. (2021). A systematic review of blockchain scalability: Issues, solutions, analysis and future research. *Journal of Network and Computer Applications*, *195*(103232), 103232.

Shahzad, B., & Crowcroft, J. (2019). Trustworthy electronic voting using adjusted blockchain technology. *IEEE Access: Practical Innovations, Open Solutions*, *7*, 24477–24488.

Sheer Hardwick, F., Gioulis, A., Naeem Akram, R., & Markantonakis, K. (2018). E-voting with blockchain: An E-voting protocol with decentralisation and voter privacy. *2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*. https://doi.org/10.1109/cybermatics_2018.2018.00262

Shiksha (2023). *Cryptographic Hash Functions in Blockchain*.

Shrivas, M. K., Dean, T. Y., & Brunda, S. S. (2020). The disruptive blockchain security threats and threat categorization. *2020 First International Conference on Power, Control and Computing Technologies (ICPC2T)*. https://doi.org/10.1109/icpc2t48082.2020.9071475

Sillaber, C., & Waltl, B. (2017). Life cycle of smart contracts in blockchain ecosystems. *Datenschutz Und Datensicherheit - DuD*, *41*(8), 497–500.

Skotnica, M., Aparício, M., Pergl, R., & Guerreiro, S. (2021). Process digitalization using blockchain: EU parliament elections case study. *Proceedings of the 9th International Con*

ference on Model-
Driven Engineering and Software Development. https://doi.org/10.5220/0010229000650075

Smartmatic. (2018). *Norway: Online voting to facilitate democratic participation for citizens*.

Srivastava, G., Dhar Dwivedi, A., & Singh, R. (2018). Crypto-democracy: A decentralized voting scheme using blockchain technology. *Proceedings of the 15th International Joint Conference on E-Business and Telecommunications*, 508–513.

Suwito, M. H., & Dutta, S. (2019). Verifiable E-voting with resistance against physical forced abstention attack. *2019 International Workshop on Big Data and Information Security (IWBIS)*. https://doi.org/10.1109/iwbis.2019.8935763

Tang, W., Kiffer, L., Fanti, G., & Juels, A. (2023). Strategic latency reduction in blockchain peer-to-peer networks. *Proceedings of the ACM on Measurement and Analysis of Computing Systems*, *7*(2), 1–33.

Tarasenko, E. (2022). *Consensus Algorithms - Proof of Work (PoW) vs Proof of Stake (PoS)*. Merehead. Retrieved November 26, 2024, from https://merehead.com/blog/proof-of-stake-vs-proof-of-work/

Taş, R., & Tanrıöver, Ö. Ö. (2021). A manipulation prevention model for blockchain-based E-voting systems. *Security and Communication Networks*, *2021*, 1–16.

Tripathi, G., Ahad, M. A., & Casalino, G. (2023). A comprehensive review of blockchain technology: Underlying principles and historical background with future challenges. *Decision Analytics Journal*, *9*(100344), 100344.

Trust Wallet. (2024, August 9). *Blockchain Mainnet vs Testnet: What's the Difference?* Trust Blog; Trust Wallet. https://trustwallet.com/blog/blockchain-mainnet-vs-testnet

van Baalen, S. (2024). Polls of fear? Electoral violence, incumbent strength, and voter turnout in Côte d'Ivoire. *Journal of Peace Research*, *61*(4), 595–611.

Vivek, S. K., Yashank, R. S., Prashanth, Y., Yashas, N., & Namratha, M. (2020, July). E-voting systems using blockchain: An exploratory literature survey. *2020 Second International Conference on Inventive Research in Computing Applications (ICIRCA)*. https://doi.org/10.1109/icirca48905.2020.9183185

Wan, L., Eyers, D., & Zhang, H. (2019, July). Evaluating the impact of network latency on the safety of blockchain transactions. *2019 IEEE International Conference on Blockchain (Blockchain)*. https://doi.org/10.1109/blockchain.2019.00033

Wang, W., Xu, H., Alazab, M., Gadekallu, T. R., Han, Z., & Su, C. (2022). Blockchain-based reliable and efficient certificateless signature for IIoT devices. *IEEE Transactions on Industrial Informatics*, *18*(10), 7059–7067.

Wendl, M., Doan, M. H., & Sassen, R. (2023). The environmental impact of cryptocurrencies using proof of work and proof of stake consensus algorithms: A systematic review. *Journal of Environmental Management*, *326*(Pt A), 116530.

Xiao, Y., Zhang, N., Lou, W., & Hou, Y. T. (2020). A survey of distributed consensus protocols for blockchain networks. *IEEE Communications Surveys & Tutorials*, *22*(2), 1432–1465.

Xie, J., Yu, F. R., Huang, T., Xie, R., Liu, J., & Liu, Y. (2019). A survey on the scalability of blockchain systems. *IEEE Network*, *33*(5), 166–173.

Yang, D., Long, C., Xu, H., & Peng, S. (2020, March 12). A Review on Scalability of Block chain. *Proceedings of the 2020 2nd International Conference on Blockchain Technology*. https://doi.org/10.1145/3390566.3391665

Yaqoob, I., Ahmed, E., Rehman, M. H. ur, Ahmed, A. I. A., Al-garadi, M. A., Imran, M., & Guizani, M. (2017). The rise of ransomware and emerging sec urity challenges in the Internet of Things. *Computer Networks*, *129*, 444–458.

Yiaga Africa Report, (2023). Dashed Hopes? Yiaga Africa Report on the 2023 General El ection. (2023). Yiaga Africa. https://yiaga.org/publications/dashed-hopes-yiaga-africa-report-on-the-2023-general-election/

Zhang, S., & Lee, J.-H. (2020). Analysis of the main consensus protocols of blockchain. *ICT Express*, *6*(2), 93 –97.

Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017, June). An overview of blockchain technology: Architecture, consensus, and future trends. *2017 IEEE International Congre ss on Big Data (BigData Congress)*. https://doi.org/10.1109/bigdatacongress.2017.85

Zheng, Z., Xie, S., Dai, H.-N., Chen, W., Chen, X., Weng, J., & Imran, M. (2020). An overview on smart contracts: C hallenges, advances and platforms. *Future Generations Computer Systems: FGCS*, *105*, 475–491.

Ziegler, R. (2015). *the UK and European Human Rights: A Strained Relationship*. Blooms bury Publishing; London, UK.