TRUST SYSTEM FRAMEWORK FOR INTEGRITY CONTROLS IN ELECTORAL VOTE COUNTING AND VALIDATION

By

PATRICK MWANSA

Thesis submitted in fulfilment of the requirements for the degree of

Doctor of Philosophy: Informatics

Discipline: Information Technology

in the Faculty of Informatics and Design

at the Cape Peninsula University of Technology

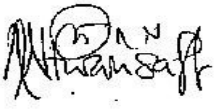
Supervisor: Dr Boniface Kabaso

District Six, Cape Town.

Date submitted: 30 November 2023

DECLARATION

I, Patrick Mwansa, declare that the content of this thesis represents my own independent work, and that the thesis has not previously been submitted for academic examination for any qualification. Furthermore, it reflects my own views and not necessarily those of Cape Peninsula University of Technology.

Signed  Date: 30/11/2023.

ABSTRACT

The integrity and transparency of electoral processes are essential for the legitimacy of democratic systems. This study addresses the challenges faced by traditional and electronic voting systems, including mistrust, security flaws and lack of transparency. Traditional paper-based voting methods carry the risk of losses, miscounts, and fraud, while electronic voting systems represent a significant advance but have not fully solved these problems. The introduction of blockchain technology in voting systems is seen as a potential solution to these problems, as it offers greater security, reliability, and anonymity. However, blockchain applications in elections are not unproblematic. In response to these challenges, this study proposes the development of a blockchain-based vote counting and validation (BBVV) artefact using symmetric cryptography and edge computing. The aim is to create an artefact that ensures transparent, secure, and trustworthy vote counting and validation processes. The research is driven by the need to increase trust in voting systems, especially in the context of increasing complexity and technological advances in voting mechanisms.

On a theoretical level, the scope of the research is limited to the vote counting and validation phase of elections, with a focus on the integration of blockchain technology and edge computing. The study draws on the literature on blockchain platforms such as Ethereum and Algorand and reflects the perspective of election stakeholders in African countries. However, it recognises limitations, including possible biases and the regional specificity of the results. The methodology combines quantitative and qualitative approaches within a pragmatic research philosophy and uses Design Science Research (DSR) to create and evaluate the artefact. Data collection methods include questionnaires for system specifications and historical election results used as experimental data for performance evaluation.

The thesis also offers policy recommendations, arguing in favour of integrating blockchain technology into African electoral systems, with a focus on infrastructure development, legal frameworks, stakeholder engagement and further research. The study highlights three key contributions: the practical contribution of the BBVV artefact in electoral challenges, its practical advances, and the potential of blockchain technology in e-voting systems; theoretical insights from the Byzantine General Problem (BGP) and Byzantine Binary Agreement (BBA) protocol in consensus algorithms for blockchain applications; and methodological advances

in computer science through a novel approach that combines pragmatism and DSR. This methodology, which incorporates iterative testing and expert input, has the potential to improve the efficiency, security, and transparency of real-world elections, with implications for digital governance and cybersecurity.

In conclusion, future research directions include improving scalability and energy efficiency, integrating advanced security measures, exploring IoT integration, conducting empirical studies, and educating the public about these technologies to strengthen the democratic process through technological innovation.

ACKNOWLEDGEMENTS

I would like to thank God, my Creator, for giving me the strength, health, and life to persevere in my studies.

I would also like to wholeheartedly thank my supervisor, **Dr Boniface Kabaso**, for his unfailing patience, unwavering commitment, all-round support, and constant motivation which he generously extended to me from the very beginning.

I am also grateful for the financial support from Kwame Nkrumah University. The opinions and conclusions expressed in this thesis are those of the author and are not necessarily attributed to Kwame Nkrumah University and Cape Peninsula University of Technology.

DEDICATION

I dedicate this work to the honourable memory of my parents Laban Musalula Mwansa and Josephine Kombe Mwansa and with love to my fiancée Rudo Himakuni and our two sons Luthlelo Chapesha Mwansa and Bwalya Mwansa.

PUBLICATIONS FROM THIS RESEARCH

1. Mwansa, P. and Kabaso, B., 2024. Improving Election Integrity: Blockchain and Byzantine Generals Problem Theory in Vote Systems. *Electronics,* 13(10), p.1853. Available at: https://doi.org/10.3390/electronics13101853
2. Mwansa, P. and Kabaso, B., 2023, August. Blockchain Electoral Vote Counting Solutions: A Comparative Analysis of Methods, Constraints, and Approaches. In 2023 *International Conference on Artificial Intelligence, Big Data, Computing and Data Communication Systems (icABCD)* (pp. 1-10). IEEE.
3. Mwansa, P. and Kabaso, B., 2023, August. Perception and Expectations of Vote Counting and Validation Systems: A Survey of Electoral Stakeholders. In 2023 *International Conference on Artificial Intelligence, Big Data, Computing and Data Communication Systems (icABCD)* (pp. 1-10). IEEE.
4. Mwansa, P. and Kabaso, B. 2023, An Exploration of Blockchain Protocols for Trusted Vote Aggregation: A Consensus Algorithm Approach. *In 2023 International Conference on Artificial Intelligence and its Applications (ICARTI) published in the conference proceedings with ISBN 978-99949-984-0-1 (pp 1-7).*

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

ABBREVIATIONS AND ACRONYMS

Algos: The native cryptocurrency of the Algorand blockchain. It is not an acronym, but a specific term for the Algorand network.

BBVV: Blockchain Based Vote counting and Validation artefact.

EPOS: Electoral Proof of Stake

n: Stands for "Officials in consensus" It is a variable used to denote the number of officials who are in consensus.

N: Stands for "total number of officers". It is used as a variable to represent the total number in the analysis.

SLR: Systematic Literature Review.

X-axis: A term that refers to the horizontal axis in the graph.

Y-axis: A term that refers to the vertical axis in the graph.

CLARIFICATION OF TERMS

Confirmed rounds: This term could refer to the consensus rounds of the blockchain network in which transactions are confirmed.

Consensus algorithm: A process used in blockchain networks to reach agreement on a single data value between distributed processes or systems.

Election data insights: This likely refers to analysing data related to elections held on the blockchain, such as vote counts, candidate information and polling station data.

Latency analysis: This refers to analysing the time it takes for transactions to be confirmed on the blockchain network.

Officials in consensus: This term refers to the number of officials who agree with a particular vote count or decision.

Saturation analysis: This analysis could look at transaction fees over time to determine the demand and capacity of the network.

Sharding: A database architecture in which larger databases are split into smaller, faster and easier to manage parts, known as data shards.

Total number of officials (N): The total number of officials involved in the vote or decision-making process.

Traffic analysis: This involves analysing the flow of transactions and the number of transactions over time to identify trends or anomalies.

Transaction fee in Algos: Algos are likely the unit of cryptocurrency used in the Algorand network, and this term refers to the fee charged for each transaction.

Transaction Performance Metric Analysis: This involves analysing the performance of transactions on a blockchain network, which can include metrics such as confirmation time and throughput.

Transaction Throughput: The number of transactions processed by the network in a given period of time.

CHAPTER ONE: INTRODUCTION

This thesis discusses designing a blockchain-based vote-counting and validation (BBVV) artefact using Symmetric Cryptography and Edge Computing. The research was initiated after performing a Systematic Literature Review (SLR) on existing evidence of blockchain vote counting and validation solutions. This problem was identified as one of the findings of that SLR. The detailed description of the SLR is discussed in Chapter 2.

1.1 Introduction and Background

Inconsistencies, unclear processes, and procedures in most democratic countries' election management, particularly vote counting, cause mistrust and dispute in election results. Generally, politicians do not trust each other. An environment where politicians contending in an election agree on a single true value as an election outcome hardly exists. Devising an environment where consensus is reached among competing parties could change the way we deliver and conduct vote-counting in elections.

In this research, the study focuses on the development of a blockchain-based vote counting and validation (BBVV) artefact using the most efficient consensus protocols that can be implemented at a lower cost. The BBVV contributes to knowledge creation through practical, theoretical, methodological, and improved software artefacts that increase confidence in vote counting and validation. The study also attempts to clarify how trustworthy the vote count can be despite the irregularities and unclear procedures and processes. This raises the question of whether the vote count can be trusted.

Elections are an imperative portion of democratic processes, political advances and transitions, execution of harmonious understandings and strengthening of majority rule in any democratic government (Houngnikpo, 2016). This is achieved through a vote-based system by counting and verification of a casted ballot. On a basic level, these guidelines may call for a majority vote, which just requires that the victor receive the most votes. Individual votes are converted into aggregate choices by a wide assortment of principles of tallying that voters and pioneers have acknowledged as genuine preceding the race.

Elections in developing nations frequently neglect to satisfy worthy guidelines of fairness, and this in turn can result in protest, violence, and fragility (Buril, 2020). Regardless of all stipulated policies to demand legitimately accountable representations, government officials now and

again shorten genuine constituent practices through corrupt manipulation control of the vote (Allen, 2015). This often weakens the purpose of elections as a tool for accountability and destroys self-assurance in the electoral and democratic institutions (Keefer & Vlaicu, 2017). In most cases, the electorate is influenced by promises or threats that are dependent on how they vote and result in patronage-based politics. patronage-based politics alludes to the act of giving individual favours—employments, contracts, welfare backing, cash, etc—in return for electoral support (Berenschot, 2018).

Numerous flaws in the vote count, ballot box packing and lack of transparency are at the helm of African elections, with (Kalu & Gberevbie, 2018) listing miscounting or non-counting of ballots and false tallying of votes amid other causes of electoral violence in 2011 and 2015 general elections in Lagos State, Nigeria. Furthermore, security agents (police) in certain instances might try to support a particular party to rig an election in a polling station and leads to the feeling of grievance from other contesting parties thus resulting in violence. Therefore, this can attribute to controversy and mistrust in the vote-counting process which is bad for democratic nations.

In Africa, manual or paper-based and electronic voting systems are the two main voting systems. In the manual system, also known as hand counting, the ballot papers are physically checked and analysed at several polling stations in different constituencies. These ballot papers are then transported or transferred to a central counting centre to obtain a uniform result. In contrast, electronic voting systems count votes electronically and transmit the results to a central counting centre via public telecommunications networks, resulting in a more efficient and shorter timeframe.

Although both systems have clearly defined processes for counting votes, there are still challenges to the results in most general elections. To address concerns about the credibility and reliability of automated counting systems, manual counting is often used for recounts and election audits in conjunction with the Voter Verified Paper Audit Trail (VVPAT) (Solanki & Meva, 2019) . A popular method of manual counting is sorting ballots into piles by candidate and counting the number in each pile. This method is widely used in countries such as Zambia, Zimbabwe, Nigeria, Indonesia, South Africa, Kenya and Tanzania and is usually carried out in

the presence of observers and party representatives (The Commonwealth Observer Group, 2015; COG, 2016; COG, 2018; The Carter Center, 2018; Seftyanto *et al.*, 2019).

In their 2017 paper, Bennett Moses *et al.* (2017) use a case study on the Schulze vote to show that it is possible to check and verify the results in practise. The authors argue that there is no reason to implement vote counting software that cannot be validated or verified. This assertion is supported by a comparison of the eVACS system in the Australian Capital Territory, where the vote counting software is available as open-source software, and in the state of New South Wales, where the vote counting software is available as closed source software and allows only limited verification and validation of the vote count. Furthermore, Sheranova (2020) discusses the use of automatic vote counting through biometric identification and scanning in Kyrgyzstan. However, instead of promoting an open and fair electoral environment, the author argues that the history of electronic voting and counting in Kyrgyzstan has perpetuated, adapted, and reinforced existing methods of electoral fraud, as demonstrated by the 2016 local elections in Osh, Kyrgyzstan.

Other countries such as the USA, Estonia, Switzerland, Germany and Ireland have also introduced electronic vote counting. Among these countries, Estonia has achieved the greatest success in this area (Reznik *et al.*, 2021). Estonia has been the sole nation in Europe to implement remote internet voting since 2005. Despite its success within the Estonian community, further development of the system must ensure consistency with recent security and usability guidelines, as highlighted by Vinkel and Krimmer (2017).

India has also experienced success in electronic voting, resulting in an increase in voter participation and a decrease in the number of disqualified votes. However, Desai and Lee (2021) state that there is little evidence to suggest that electronic voting machines have had an impact on fraud, either positively or negatively. The success of e-voting has also been observed in other nations, including Finland, Switzerland, the United States, and the Philippines, where voters have responded positively to e-voting, as reported by Olusadum and Anulika (2018). Hao and Ryan (2016b) indicate that e-voting is being utilised or explored in various countries worldwide. However, despite the positive experiences, Springall *et al.* (2014) argue that the I-voting system in Estonia may be susceptible to state-level terrorist, advanced

suspect, or unethical insider attacks, and recommend discontinuing the system due to potential vulnerabilities in the electoral process.

The Brazilian e-voting system has been found to have multiple vulnerabilities that compromise the security properties of voting software, specifically ballot secrecy and software integrity. It was discovered that cryptographic keys used to secure data were stored insecurely directly in source code, allowing for full inspection of memory cards containing installation files. Additionally, two shared libraries lacked authentication signatures, enabling arbitrary code injection into machines, both of which violations compromise voter privacy and machine integrity (Aranha *et al.*, 2019). Despite conducting a feasibility study and passing a law on its use in 2000, the e-voting system in Brazil has faced public concerns regarding data security, resulting in Germany's prohibition of electronic voting devices for elections (Risnanto *et al.*, 2020).. This highlights that while some countries may have successfully implemented electronic voting systems, there are potential issues and risks associated with its use.

According to Seftyanto *et al.* (2019), inconsistencies in the control of ballot calculations at polling stations in Indonesia are caused by manual vote counting validations. The study found that ballots that have been tallied more than once are often deemed null but are considered accurate or legitimate in subsequent calculations. This has led to public outrage and the implementation of legislation as a result. Additionally, the study also found that the ballot counting process takes long hours, with the fastest duration taking 10 hours. In the 2016 Austrian presidential election, Potrafke and Roesel (2019) report that postal ballots were tallied carelessly in individual electoral districts, leading to the need for the ballot to be redone in what was labelled as "scandal districts". Conway *et al.* (2017) highlights that in Australia, many votes are counted electronically, but the computerised count is difficult to audit. The authors also mention that most electoral commissions have complete preference data accessible for impartial audits, though the process can take several months.

E-voting systems are faced with various challenges related to vote verification and validation. Haines and Roenne (2021) argue that the goal of software-independence is to provide evidence that the election outcome is correct, regardless of any defects in the software used during the election. However, it is important to note that the concept of "software-independence" is somewhat misleading, as it still relies on software to examine the evidence.

This has led to issues in vote count verification and validation. Several examples of this include: the Swiss Post system (Lewis *et al.*, 2019), the iVoting system implemented in the state of New South Wales, Australia (Halderman & Teague, 2015), the Moscow voting system, Voatz, the I-voting system in Estonia and Democracy Live (Teague, 2020).

Infrastructure plays a fundamental role in the implementation of electronic/Internet voting systems. However, many developing nations lack the necessary framework to support its use. In recent years, the widespread availability of mobile devices such as smartphones, wearable devices, and other computing and communication devices has provided an alternative solution. With the help of cloud computing, these devices have the capability to perform complex computations. Additionally, addressing the issue of receiving timely electronic responses is essential in order to facilitate quicker decision-making. Latency is a significant concern when it comes to cloud computing. Additionally, electronic devices can be constrained by their computing power, processing capacity, and memory. Edge computing has emerged as a solution to these limitations, allowing for complex computations on mobile devices without being constrained by power consumption (Purkayastha & Roy, 2021).

1.2 Research Problem

The integrity of the election results is compromised by the problematic processes of counting, collating, and tabulating votes from the polling stations to the central counting centres. These processes are characterised by inconsistencies and a lack of clarity, leading to widespread mistrust and controversy. The subsequent stages of election verification and validation are also not free from criticism, as they are often seen as susceptible to manipulation and fraud. The introduction of electronic voting systems, which have been extensively researched and trialled in various countries, has not completely solved these problems. Despite their potential, electronic voting systems are still embroiled in debates about their susceptibility to irregularities and controversies (Al Barghuthi *et al.*, 2019). Blockchain technology was introduced to overcome these challenges by providing a secure, reliable and anonymous voting mechanism. However, it struggles with a number of issues, including scalability, resistance to coercion and dependence on unreliable technologies (Jafar *et al.*, 2021; Vivek *et al.*, 2020).

1.3 Statement of the Problem

The lack of security and privacy in traditional paper voting, with the risk of loss or miscounting of votes, necessitates a revision to ensure the integrity of elections. While electronic voting is a significant area of research and application, it is also not immune to these challenges. Blockchain-based electronic voting systems have been recognised for their potential to improve the security, reliability, decentralisation, and anonymity of the voting process. These systems promise to provide a robust solution for identity verification and maintain the sanctity of the electoral process (Vivek *et al.*, 2020). However, the implementation of blockchain technology in elections is not straightforward and is accompanied by concerns regarding scalability, resistance to coercion and reliance on potentially untrustworthy technology (Jafar *et al.*, 2021).

It is imperative to conduct research to develop a blockchain-based vote counting and validation artefact that incorporates symmetric cryptography and edge computing. Such innovation aims to improve the current technology and ensure that vote counting, and validation processes are transparent, secure, and trustworthy.

1.4 Research Aim

This research aims to design a Blockchain-based Vote-counting and Validation (BBVV) artefact using symmetric cryptography, blockchain and edge computing to engender trust in the electoral vote counting and validating process.

1.5 Research Objectives

In view of the above, the aim is further subdivided into four objectives. These are:

1. To review and identify existing blockchain solutions that have been used in the electoral vote systems.
2. To elicit the necessary system specifications for developing a BBVV artefact that exhibits high-performance features and engenders user trust.
3. To identify an appropriate blockchain protocol that supports trusted vote aggregation and includes a suitable consensus algorithm for vote count validation.

4. Develop the BBVV artefact for vote counting and validation and evaluate its performance features to handle maximum load, minimise delays, process high transaction volumes, and foster user trust through traffic analysis.

1.6 Research Questions

This section outlines the specific research questions that this study aims to address.

1.6.1 Main research question

What approach can be used to design a blockchain-based vote-counting and validation artefact that engender trust in an electoral voting process?

1.6.2 Sub-questions

1. What are the existing blockchain solutions adopted in electoral vote systems, and how have they addressed their respective challenges?
2. What are the critical specifications and features required for a BBVV artefact to achieve high performance and secure user trust?
3. Which blockchain protocol best supports trusted vote aggregation and offers an optimal consensus algorithm for vote count validation?
4. How effective is the developed BBVV artefact in vote counting and validation, and to what extent do its performance features engender trust among users?

1.7 Scope and Limitations

The scope of this work is limited to the vote counting and validation phase of the election process. It specifically addresses the integration of blockchain technology and edge computing in this phase, focussing on the recording and collation of physically counted votes. The study will explore the use of smart ballots by election observers to write the vote count at polling stations on to the blockchain. These counts will then be validated on edge computing devices before being consolidated on the blockchain for final national aggregation. The system will be deployed on edge devices equipped with at least 16GB of RAM and an Intel(R) Core (TM) i3-6006U CPU @ 2.00GHz processor to ensure fast processing.

The research assumes that the literature on platforms such as Ethereum and Algorand reflects the current landscape of blockchain solutions for vote counting and validation. It also assumes that the perspectives of election stakeholders in African countries reflect the general sentiment and that the thematic analysis conducted, together with the consensus algorithms studied, thoroughly captures the relevant data. Furthermore, it is assumed that the performance and behaviour of the consensus algorithms are consistent across the different implementations and use cases.

The study acknowledges several limitations that may affect the scope and applicability of the results. First, the literature review may not include all blockchain solutions, especially those that are proprietary, new, or insufficiently documented. Second, the challenges identified, such as inadequate network coverage in some African regions, may not reflect conditions in other countries and therefore may not be universally relevant.

The practical effectiveness of novel algorithm proposed for aggregating and validating votes has been experimentally tested, which introduces an element of certainty regarding their performance in practise. However, the results may be subject to regional biases influenced by the unique cultural, political and social dynamics of the African countries studied, limiting the generalisability of the results to other blockchain networks with different characteristics or operational requirements.

Finally, the use of self-reported or publicly available data carries the risk of bias or inaccuracy. Such data may not represent all facets of the electoral process and may miss important insights into the complexity of the electoral system. These limitations must be considered when interpreting the results of the study and considering its contribution to the field of blockchain-based voting systems.

1.8 Preliminary Review of Literature

1.8.1 Introduction

The integrity of electoral systems is a fundamental aspect of democratic governance, and the emergence of blockchain technology has opened new possibilities for improving the security and reliability of electronic elections. The decentralisation, immutability, and transparency of

blockchain are particularly well suited to addressing the vulnerabilities of traditional voting mechanisms, such as susceptibility to fraud and coercion, as well as the challenges of ensuring privacy and accessibility. A look at existing blockchain solutions for voting systems reveals a variety of approaches that aim to overcome these problems.

1.9 Election Process

The electoral process is a structured series of activities that ensure the selection of representatives or decision-making on specific issues through voting. It usually comprises several phases, each of which has its own procedures and significance (Hao & Ryan, 2016a).

- **Pre-Election Stage:**

Potential voters must register, often presenting an identity card and proof of residence. Individuals or parties declare their intention to run for office during the nomination phase, which may include collecting signatures or paying fees. This is followed by the election campaign, in which candidates and parties attempt to persuade voters through public appearances, debates, advertising and other forms of publicity. The electoral authorities organise the logistics, e.g., the polling stations, train the staff and ensure that the voting equipment is ready and secure.

- **Voting Stage:**

On Election Day or during early voting, registered voters cast their ballots, which can be done in a variety of ways, including paper ballots, electronic voting machines or absentee ballots. Election officials verify voter eligibility by frequently checking names against a voter list and ensuring that voters have not already voted. Measures are taken to ensure that votes are cast in secret and that the privacy of voters is protected.

- **Post-Voting Stage:**

After the polling stations close, the votes are counted, which can be done manually or electronically depending on the voting method. The results of the individual polling stations

are summarised to determine the overall result of the election. The election officials check the accuracy of the results and officially certify them.

- **Post-Election Stage:**

The official election results are announced to the public. There is often a period during which the results can be legally challenged if irregularities are alleged. Any challenges or disputes are resolved through pre-established legal procedures, which may include recounts or court hearings. The elected candidates are sworn into office and begin their term of office.

- **Election Review:**

Electoral bodies, observers and political authorities can analyse the electoral process to identify successes and areas for improvement. Based on the analysis, recommendations can be made for changes to laws, procedures, or technologies to improve future elections.

Each phase is critical to the integrity and legitimacy of the election. The process is designed to be transparent, fair and inclusive to ensure that the outcome accurately reflects the will of the voters.

The study focuses on the post-election phase, particularly the critical phases of "counting and tabulation of votes" and "announcement of results" It proposes a novel integration of edge computing with blockchain technology to improve the accuracy, security and speed of these processes. By using edge computing, the study offers a solution for efficient local processing of votes, which is particularly beneficial in African regions with limited centralised data infrastructure. This reduces the dependency on a large bandwidth and ensures that votes are counted quickly.

For the "announcement of results"," the study utilises the immutable nature of blockchain to ensure a secure and transparent record of election results. This approach guarantees that once the votes are counted and validated on the ground, the results are recorded in a tamper-proof ledger, strengthening the integrity and trust in the electoral process. The application of this technology addresses the key challenges in the post-election phase and represents a scalable model that could significantly improve electoral systems in Africa.

1.10 Types Of Blockchain Platforms

Blockchain technology is a distributed database that enables secure, transparent, and tamper-proof transactions. It consists of a chain of blocks, each of which contains a timestamp and transaction data and is secured by cryptographic principles (nakamoto, 2008). Blockchain platforms can be roughly categorised into public, private and consortium blockchains.

- **Public blockchains**, such as Bitcoin and Ethereum, are open source and allow anyone to participate in the network. They are characterised by a high degree of security and transparency, but often have problems with scalability (Holotescu & Vasiu, 2020).
- **Private blockchains** are restricted and only accessible to authorised participants. They offer faster transaction speeds and better data protection. Examples include Hyperledger Fabric and R3 Corda (Androulaki *et al.*, 2018).
- **Consortium blockchains** are managed by a group of organisations rather than a single company and combine the advantages of public and private blockchains. One example is the Energy Web Foundation (EW Chain) (Zheng *et al.*, 2018).

1.10.1 Edge Computing

Edge computing refers to the processing of data at the periphery of the network, i.e., closer to the source of the data. This paradigm shift aims to reduce latency, increase the speed of data processing, and reduce the load on centralised servers (Shi *et al.*, 2016). By integrating edge computing with blockchain, it is possible to create a distributed and efficient infrastructure for electronic voting systems.

1.10.2 Blockchain Solutions in Election and Voting Systems.

OnurCeyhun & YurdakulArda (2023) have proposed ElectAnon, a protocol that prioritises voter anonymity through zero-knowledge proofs and increases robustness by decentralising authority control with timed machines. This approach not only addresses privacy concerns, but also provides a scalable solution that significantly reduces operational costs, as evidenced by lower gas consumption compared to previous systems. Similarly, Bartolucci *et al.* (2018) developed SHARVOT, which uses Shamir's secret sharing and a circle shuffle technique to

ensure the confidentiality and anonymity of votes. This secret share-based voting system utilises the blockchain's ability to maintain a transparent and irrevocable record of votes.

The work of Kazi Sadia and colleagues (2019) presents a fully decentralised e-voting system that uses smart contracts to increase security and maintain voter privacy. Their system aims to establish a transparent and tamper-proof voting mechanism that minimises the role of intermediaries and thus reduces the potential for voter fraud. Spanos & Kantzavelou (2023) have contributed to this topic with EtherVote, a system that runs entirely on the Ethereum blockchain and dispenses with centralised databases and authority servers to increase security and reduce election costs.

In addition, Stančíková & Homoliak (2023) introduced SBvote, a scalable, self-tuning voting protocol that can be customised for large-scale elections. The protocol is designed to process a large number of voters and is limited only by the capacity of the underlying blockchain platform. This scalability is crucial for the adoption of blockchain in larger electoral contexts, such as national elections. The integration of blockchain technology into electoral systems has been sought to mitigate the risks associated with traditional voting methods and reap the benefits of digital transformation. However, this integration is not without its challenges. The literature identifies several key issues that need to be resolved to ensure the successful implementation of blockchain in electoral systems.

One of the biggest challenges is to preserve the privacy and anonymity of voters while ensuring the irrevocability of the vote and transparency during the vote count. Bartolucci *et al.* (2018) discuss the use of blockchain technology to implement a secure and fair voting system and present the SHARVOT protocol, which uses Shamir's Secret Sharing to enable on-chain voting and determination of the winner. Despite the protocol's innovative approach of decoupling voters from their inputs, the balance between transparency and voter privacy remains a delicate issue.

Another challenge is the scalability of blockchain systems to handle the volume of transactions involved in elections. Faour (2018) provides a comprehensive comparison between current election systems and analyses their structure and the drawbacks that should be considered for future improvements. Faour points out the limitations of current blockchain platforms such

as Ethereum, which can only process a limited number of votes per minute, raising concerns about the feasibility of blockchain for large-scale elections.

The security of blockchain voting systems is also a cause for concern, particularly with regard to possible attacks by quantum computers. Mishra *et al.* (2022) proposes an anonymous voting system with quantum-assisted blockchain to improve the security features of blockchain with quantum resources. This approach aims to fulfil the requirements of a good voting system while being auditable and implementable with current technology. In addition, the existing infrastructure for conducting elections with electronic voting machines (EVMs) has numerous loopholes that could be exploited to cast false votes or distort the results. Mukherjee *et al.* (2023) propose a blockchain-based e-voting system that eliminates these security risks and preserves voter anonymity. Their prototype, developed on the Ethereum platform, demonstrates the power of the system and its potential to enable a more reliable and fairer voting process.

Lastly, the time it takes to count the votes and the overall efficiency of the voting process are also important. Bulut *et al.*, (2019) suggest that blockchain can significantly reduce the waiting time for election results and improve the security and data integrity of votes. They emphasise that the protection of voters' privacy and the transparency of the election process are important requirements that their proposed system ensures. While blockchain offers a promising way to reform voting systems, there are still significant challenges to overcome in terms of privacy, scalability, security, and efficiency. The literature suggests that ongoing research and development is crucial to overcoming these challenges and realising the full potential of blockchain in electoral systems.

1.10.3 Conclusion

The literature shows that blockchain technology holds great promise for reforming electronic voting systems. The analysed blockchain solutions are designed to protect voter privacy, ensure the integrity of the voting process, and offer scalability. However, implementing these systems on a larger scale still requires further research to overcome the limitations of current technology and ensure that these systems are trustworthy and can be used in elections around the world. The references to the work of Onur and Yurdakul, Bartolucci et al, Sadia et al, Spanos and Kantzavelou, and Stančíková and Homoliak provide a comprehensive overview

of the state of blockchain in electronic elections and lay the groundwork for future progress in this area.

1.11 Theoretical Framework

1.11.1 Overview of Byzantine Theory

The Byzantine General Problem (BGP) serve as fundamental concept in the development of consensus algorithms that are critical to blockchain technology, especially in applications such as blockchain-based vote counting and validation (BBVV) artefact. The BGP illustrates the difficulties associated with achieving consensus in distributed systems with potentially treacherous components. This is similar to ensuring trust in the vote counting and validation process in elections (Kuo *et al.*, 2020a). An underlying theoretical paradigm in distributed computing is the Byzantine General Problem (Abraham *et al.*, 2017). It describes the difficulty in reaching agreement amongst a variety of organizations, particularly when some of these entities “like generals in a Byzantine army” act treacherously by disseminating inaccurate or misleading information. Ultimately, the issue is how to create a framework where compliant generals can come to a consensus despite the traitors' cunning tactics. This issue emphasises the intricacy of distributed systems as well as the value of dependability and trust in cooperative settings.

1.11.2 Applying The BGP Theory to BBVV Artefact

Kuo *et al.* (2020b) contribute to this area by proposing a fair Byzantine agreement protocol that addresses the fairness and performance issues in blockchain consensus. Their work is particularly relevant to BBVV as it ensures that each participant's value has an equal probability of being selected, which is essential for trust in voting processes. The protocol they propose is responsive and partition-proof. It tolerates up to one-third corruption, meaning it can maintain security even if the network is partitioned, and it can resume normal operation once the partitioning is resolved. This resilience is critical for BBVV artefact that need to operate reliably under various network conditions and possible attacks.

In addition, the work of Chang *et al.* (2023) on the Practical Byzantine Fault Tolerance (PBFT) protocol with repairable voting nodes provides insights into the reliability and performance of

blockchain systems. Their analysis using a multi-dimensional Markov process and the first-passage time method provides a framework for understanding the throughput, availability, and reliability of PBFT-based blockchain systems. This analysis can guide the development of BBVV artefact by ensuring that the system remains functional and fair even when nodes fail and recover, reflecting the dynamic nature of real-world voting systems.

In summary, the theoretical framework established by BGP with the advances in fair, responsive and partition-resistant Byzantine agreement protocols, provides a solid foundation for the development of a BBVV artefact. By leveraging these concepts, a BBVV system can be created that utilises symmetric cryptography, blockchain and edge computing to ensure a trustworthy and reliable vote counting and validation process in elections. The Byzantine General Problem (BGP) serve as fundamental concepts in the development of consensus algorithms that are critical to blockchain technology, especially in applications such as blockchain-based vote counting and validation (BBVV) artefact.

1.12 Conceptual Framework

Figure 1.1 outlines the four-stage conceptual framework of the research. First, the project collects data and requirements from election officials (EPoS) and selects stakeholders and data collection methods for system development. In the second phase, consensus algorithms based on Byzantine theory and the BBVV protocol will be applied to authenticate and record legitimate votes on the edge network and later consolidate them on the blockchain. This process, secured by cryptographic keys, allows EPOS to verify their votes at the national count, which increases confidence in the accuracy of the vote. In the third phase, the accuracy of the output and the scalability of the system will be tested in different environments. In the final phase, the system will be compared with current voting systems. Phases one and two correspond to the Design Science Research (DSR) phase 'setup", while phases three and four correspond to the phase 'evaluation".

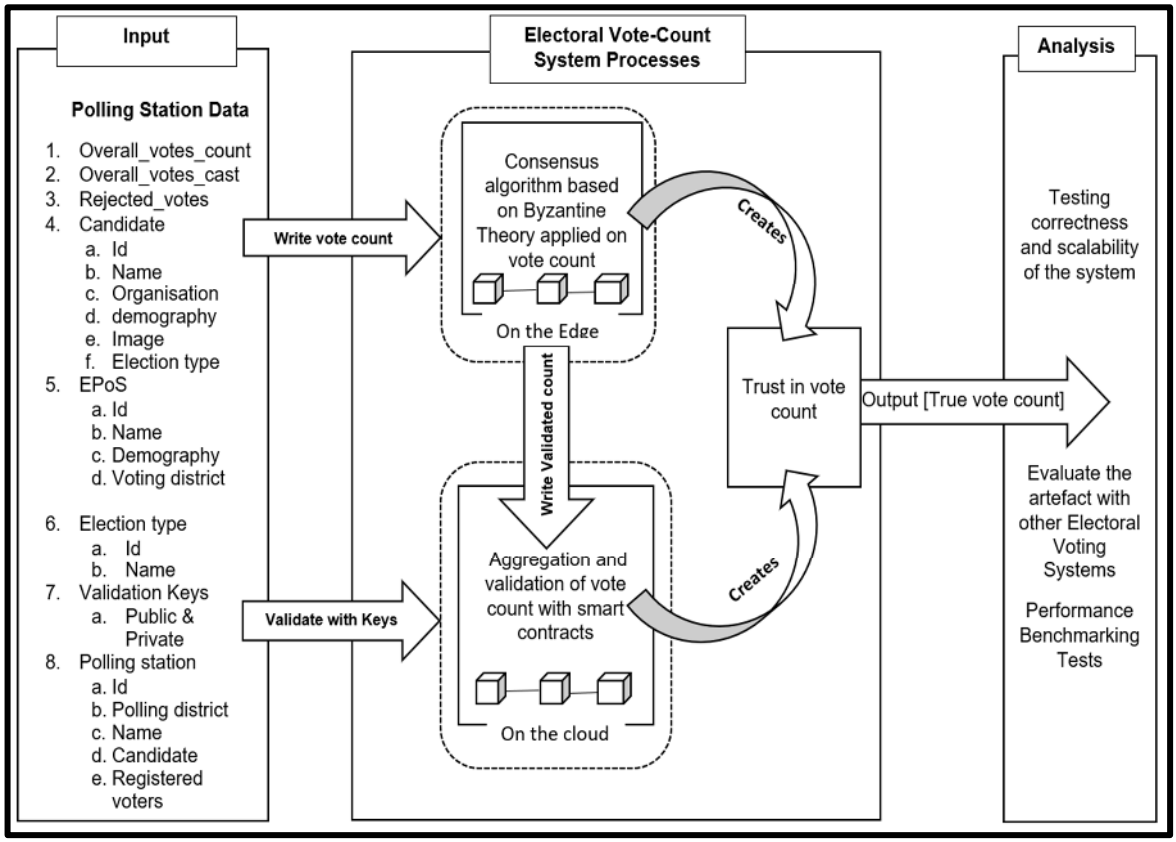


Figure 1-1: Conceptual Framework of the Research

1.13 Methodology

The goal of this section is to lay out the research design, methodology, and ethical guidelines that will be followed throughout the study. Mouton (2001: 56) depicts the research design as an architectural design or roadmap for a research undertaking, as well as the implementation of the design, and the research process or methodology as the methodological building process. In this research, the aim of investigating and designing a Blockchain-based Vote-counting and Validation (BBVV) artefact using symmetric cryptography, blockchain, and edge computing is sought. In trying to find solutions towards the aim, the study will employ a quantitative and qualitative design approach based on the underlying philosophies.

1.14 Research Philosophy

The assumptions of pragmatism are well-suited to this study. As a research paradigm, pragmatism avoids debating controversial philosophical notions like truth and reality. Instead, it acknowledges that there may be single or numerous realities that may be investigated empirically (Creswell & Plano-Clark, 2011). In addition, pragmatism is based on the idea that researchers should choose the philosophical and/or methodological approach that works best for the research question at hand (Tashakkori & Teddlie, 1998 as cited in Kaushik & Walsh, 2019). It is frequently linked to mixed-methods or multiple-methods research where reality can exist in singularity and plurality and may therefore be classified between positivism and constructivism.

The pragmatist approach was used in this study. Artefacts were created and analysed, with quantitative results from practical system tests used to arrive at a single truth: an election's aggregated vote count is always singular in nature. In addition, the qualitative approach was employed to gather information on the system specifications and requirements from customer/stakeholders before and during the actual development using an iterative design approach. As a result, the research used a combination of inductive and deductive approaches.

1.14.1 Design Science Research (DSR)

DSR is pragmatic. This study employed build-and-evaluate-through-test-driven design science. Under the Design-Science Research paradigm (DSR), creating and deploying a designed artefact gains knowledge about a problem domain and its solution. Design science creates and evaluates business-related artefacts (Hevner *et al.*, 2004). According to Gregor & Hevner (2013), “In IS, DSR involves the construction of a wide range of socio-technical artefacts such as decision support systems, modelling tools, governance strategies, methods for IS evaluation, and IS change interventions.”. The design-science paradigm extends human and organisational boundaries by developing new and inventive artefacts.

1.14.2 Data Collection

In this study, we used a questionnaire to obtain the required system specifications from stakeholders. We used a multi-stage sampling procedure to collect the required data and designed a comprehensive questionnaire as our primary data collection. Requirements elicitation is a comprehensive technique for collecting information from all stakeholders. This includes meetings, interviews, surveys, brainstorming and prototyping (Ramdhani *et al.*, 2018). Functional and non-functional requirements must be formulated in the creation phase of the DSR approach. The data for system initialisation such as ID, name, organisation, and type of election (ID, name, demographic data, constituency, etc.) were collected randomly from simulated candidates (randomly selected eligible election officials/presidents). The type of election was captured by ID, name, and polling place information (ID, precinct, candidates, registered voters). Quantitative data for accuracy and scalability was required from a laboratory simulation and a real election event. The quantitative data were obtained from validated real elections vote count. Saturation, latency, traffic, and artefact performance analysis were tested through benchmarking. This was used to evaluate future improvements or changes to the artefact.

1.14.3 Evaluation

According to Chen & Kim (2014), artefact evaluation is seen as being vital for Design Science Research (DSR) to thoroughly prove an artefact's applicability for implementation. Despite the existence of guidelines for structuring DSR processes, the prevailing body of evidence only generates fundamental tools for a design researcher to identify and clarify acceptable artefact evaluation procedures in a particular circumstance (Sonnenberg & Vom Brocke, 2012). Furthermore, Hevner *et al.*, (2004), presents a set of criteria for evaluating artefacts, including functionality, completeness, consistency, correctness, performance, dependability, usability, organizational fit, and other characteristics. The data collected was used for testing, performance analysis, saturation, transaction and measuring of latency was done to evaluate the completeness and functionality of the artefact. The overall aim was to attain one true vote count from the complete artefact.

1.14.4 Ethical Consideration

For this research, data was collected from human subjects. It is therefore necessary to obtain ethics approval from the Cape Peninsula University of Technology (CPUT) Ethics Committee. The human subjects will be registered in the systems. In addition, the consent process was carefully explained to them to ensure their full participation and co-operation. All data collected was used exclusively in this project. The collected data was stored as blind data. (Without the identity of the respondent).

1.15 Outcomes, Contributions and Significance

1.15.1 Outcomes

It is expected that the implementation of the blockchain-based vote counting, and validation artefact (BBVV) will significantly increase trust of all stakeholders involved in the elections in the accuracy of the vote count. It is also anticipated that this innovative approach be measured by contributing academic knowledge through the publication of scientific articles by analysing its impact and methodology.

1.15.2 Contributions

The study is expected to considerably contribute as follows:

1.15.2.1 Practical

The practical contribution of this study is the development of a Blockchain-Based Vote Counting and Validation (BBVV) artefact using the Design Science Research (DSR) methodology. The BBVV system addresses critical challenges in vote counting and validation. By incorporating strategic design and advanced technology, the BBVV system ensures accuracy, speed, efficiency, transparency, and security in elections. The implementation of the Algorand blockchain is a key feature that offers low transaction fees and promotes a reliable and transparent election process. This approach not only improves the election process, but also creates a credible election atmosphere, as the immutable record of the blockchain strengthens the integrity of the elections.

1.15.2.2 Theoretical

Our research advances blockchain-based voting by applying the theory of the Byzantine Generals Problem and Binary Byzantine to secure the integrity of the BBVV artefact against dishonesty. We explore blockchain protocols, cryptography, and develop a secure, transparent artefact and propose a BBVV protocol for vote aggregations.

1.15.2.3 Methodological

This research represents a significant advancement in the field of computer science, particularly in the application of blockchain technology to electoral processes. It addresses the limitations of traditional methods by developing a new methodology that combines pragmatism with Design Science Research (DSR). This innovative approach, developed through iterative testing and refined with expert input, effectively combines practical problem solving with the rigorous development of artefacts. The implementation involved extensive data collection and validation through real-world experimental testing to ensure a comprehensive understanding of blockchain in elections. Beyond academia, this methodology has practical implications for improving efficiency, security, and transparency in real-world election systems, impacting digital governance and cybersecurity. Although the methodology is groundbreaking, it faces challenges in terms of scalability and adaptability to different electoral environments, pointing to future research directions for broader applicability in digital governance and cybersecurity.

1.15.3 Significance

This work has significant implications for the practical application of blockchain in elections, for theoretical blockchain security concepts and for the methodological development of consensus algorithms. The development of a blockchain-based Vote Counting and Validation (BBVV) artefact using the Design Science Research methodology practically addresses the major challenges in election processes by increasing accuracy, speed and security and utilising the Algorand blockchain for its cost-effectiveness and transparency.

Theoretically, the study applies the General Byzantine Problem to the BBVV model and strengthens its protection against fraud by exploring blockchain protocols and cryptography. This contributes to a more secure and transparent framework for digital voting.

Methodologically, the research contributes to a new, experimentally tested BBVV protocol for vote aggregation and validation, which represents an advance in the study of consensus algorithms. Furthermore, the performance of the protocol will be compared with other algorithms to guide the future application of blockchain in voting systems and set a precedent for research in this area.

1.16 Policy Recommendations

The policy recommendation urges the integration of blockchain into electoral systems to improve integrity and solve problems such as electoral manipulation or corruption practises. It emphasises the need to invest in infrastructure, training, legal support, stakeholder engagement and voter education. It emphasises the need for continuous development, testing and updating of blockchain voting technologies.

1.17 Structure of the thesis

This dissertation comprises six chapters. **Chapter 1** provides an overview of the

research.

Chapter 2 examines both the history of the research as well as the research itself, focusing on Objective 1 of the study, which is to review and identify existing evidence in blockchain electoral vote counting solutions that have been used in the electoral vote systems. The chapter compares the existing solutions to each other concerning methods, constraints, and approaches. This is to Identify the strength of the evidence in support of the different solutions and how best they can be used to create a reliable blockchain artefact that engenders trust electoral vote counting and validation in developing countries.

Chapter 3 discusses the philosophical stance and research methodology.

Chapter 4 explains the research Objective 3 & 4, which is to identify an appropriate blockchain protocol for trusted vote aggregation and assess and implement a suitable consensus algorithm for vote count validation. This also includes development of the BBVV artefact.

Chapter 5 Provides the findings and discusses the results obtained using the protocol identified in Chapter 4. This chapter evaluates the artefact performance features that engender trust in the users in terms of performance (saturation, traffic latency).

Chapter 6 concludes the thesis by briefly discussing the research objectives and future directions.

CHAPTER TWO: LITERATURE REVIEW

2.1 Organisation of the Chapter

The review is systematically organised and begins with an introduction to the literature review (section 2.2). It then provides an overview (Section 2.3) and history (Section 2.4) of electronic voting with blockchain, followed by an examination of the key concepts (Section 2.5). Section 2.6 looks at the security measures and consensus algorithms of blockchain-based electronic voting systems, while Section 2.7 discusses the limitations and considerations of blockchain technology in electronic voting. The theoretical foundations are explained in more detail in section 2.8. A comprehensive systematic literature review (SLR), including methodology, main conclusions, and literature trends, is discussed in Section 2.9. The review concludes with a reflection on the SLR (Section 2.10) and a summary of the literature (Section 2.11).

2.2 Introduction to the Literature Review

Chapter two, as mentioned in section 1.14.5 of chapter one, provides the reader with the necessary background information to understand some of the ideas, knowledge and techniques that are shaping and influencing the use of blockchain technology in the counting and validation of votes today. It defines and explains in detail key terms and demonstrates the researcher's deep understanding of the topic and the goal of the research to develop a blockchain-based vote counting and validation (BBVV) artefact. This system utilises symmetric cryptography, blockchain and edge computing to strengthen trust in the voting process.

The chapter covers the history and content of the research and focuses on the first objective of the study: the investigation and identification of existing blockchain solutions for voting systems. It conducts a comparative analysis of these solutions and evaluates their methods, limitations and strategies to assess the robustness of the evidence supporting the different solutions. The aim is to identify the most effective practises for building a trustworthy blockchain artefact for vote counting and validation, with a focus on applicability in developing countries.

2.3 Overview of Blockchain Electronic Voting

Blockchain technology improves the security and efficiency of electronic voting by decentralising the process, removing central authority, and using smart contracts for transparency and voter identification, as demonstrated by systems such as EtherVote (Spanos & Kantzavelou, 2023). The integration of homomorphic encryption with blockchain secures the analysis of voter data while preserving the integrity and confidentiality of the voting process.

Spanos & Kantzavelou (2023) research on EtherVote and other studies emphasise the ability of blockchain to mitigate voter fraud, protect voter anonymity and ensure vote verifiability of voting. These advances, supported by empirical research and prototypes, indicate the suitability of blockchain for electronic voting, although further research is needed to improve scalability and the balance between transparency and voter data ((Sadia *et al.*, 2019; Kim *et al.*, 2021; Cabuk *et al.*, 2020; Mukherjee *et al.*, 2023b).

2.4 History of Blockchain Electronic Voting

The history of electronic voting with blockchain is intertwined with the broader development of blockchain technology, which gained prominence with the emergence of Bitcoin in 2009. The application of blockchain to electronic voting systems has been proposed to utilise the inherent strengths of the technology — immutability, transparency, and security — to solve persistent problems associated with electronic voting such as fraud, complexity, and voter privacy concerns. Early theoretical research on electronic voting with blockchain hypothesised that a public ledger could serve as a robust basis for recording votes to ensure that each vote is tamper-proof and verifiable (Vinet & Zhedanov, 2011a).

In the mid-2010s, practical implementations began to take shape with the emergence of smart contract platforms such as Ethereum. These platforms enabled the creation of decentralised voting protocols where voting rules were enforced by code and the blockchain acted as a neutral arbiter that could be verified by anyone. During this time, various blockchain prototypes for electronic voting were designed and developed, aiming to automate the voting process and guarantee the authenticity of each vote cast (Hjalmarsson *et al.*, 2018a).

However, the development of blockchain e-voting is not without its challenges. Concerns remain about the security of the new systems, the complexity of maintaining voter anonymity and the legal and regulatory changes required for implementation. Researchers have been actively addressed these concerns, balancing optimism about the potential of blockchain with a cautious approach to its application in sensitive voting environments (Hardwick *et al.*, 2018a).

Recent pilot projects have provided valuable insights into the practicality of blockchain e-voting systems. These projects have tested the systems in various electoral contexts, from organisational to public elections, and provide empirical evidence of the systems' performance. The results of these trials are critical to refining blockchain e-voting technology and understanding its implications for the future of democratic processes. These efforts collectively contribute to a cautious but progressive narrative of blockchain adoption in e-voting and point to a future where elections could be conducted with unprecedented levels of trust and efficiency.

2.5 Key Concepts of Blockchain Electronic Voting

2.5.1 Blockchain

Blockchain is an open, distributed, and self-auditing ledger that can efficiently, permanently, and legitimately record transactions between nodes. Fundamentally, it offers a dispersed record of exchanges that are put away on numerous nodes, all of which should keep a refreshed and genuine adaptation of the record continually, without a focal node controlling or maintaining the operation (Abuelhija *et al.*, 2020). This is accomplished through cryptographic conventions and agreement calculations, which suggests that nodes demonstrate the honesty of the information they hold without having to believe any other third party. In contrast, some nodes might be faulty and send differing records to other nodes, leading to the question under which conditions such intelligently inconsistency might be accomplished (Aljosha *et al.*, 2017). This was demonstrated in the Byzantine Generals Problem theory (Lamport *et al.*, 1982).

In a democracy, voting is a necessary practice. To make the voting process easier, many attempts have been made to propose an electronic voting system in which the voting and tallying procedures can be completed quickly and the results made public (Angsuchotmetee

et al., 2019). Most systems are currently centralised (including voting schemes based on the mix-net, blind signature FOO, and homomorphic encryption technology), with the central agency recording, managing, calculating, and verifying them (Wang *et al.*, 2018). Nevertheless, it is important to presume the existence of a reliable bulletin board and the associated reliable counting methods. The prompt, trustworthy and validated results can be achieved by recommending an electronic voting system using blockchain (Febriyanto *et al.*, 2020).

2.5.2 Blockchain Architecture

In terms of use cases, various blockchain frameworks can take a variety of approaches (Valenta & Sandner, 2017). The blockchain architecture allows for its use in a variety of sectors, such as banking and supply chains, while the motivation behind the development of others is more narrowly focused. Nonetheless, the most important blockchain platforms can be divided into four distinct categories (Ellervee *et al.*, 2017) as shown in Table 2.1.

Table 2.1: Classification of Frameworks adopted (Ellervee *et al.*, 2017)

(Group I)	**(Group II)**
Permissionless Transactions only (Bitcoin)	Permissionless With Smart Contracts (Ethereum, Solana, Algorand e.tc)
(Group III)	**(Group IV)**
Permissioned Transactions only (Chain Core, Ripple, Quorum e.t.c)	Permissioned With Smart Contracts (Hyperledger Fabric, Cardano, Tron, e.tc)

Applications that are built on top of blockchains may be developed using blockchain technology. The most well-known blockchain frameworks are R3 Corda, Ethereum, and Hyperledger with Bitcoin as another popular option (Taş & Tanrıöver, 2020a). Blockchain is a shared, decentralised, and distributed state machine that is essentially a chain shaped data structure in which a chain of blocks is linked to each other via an address pointer based on a hash value. This means that each node has its own copy of the blockchain, and the current known "condition" is determined by analysing each transaction (Jayasinghe *et al.*, 2019; Jalalzai & Busch, 2018). Figure 2.1 shows a typical structure of a blockchain.

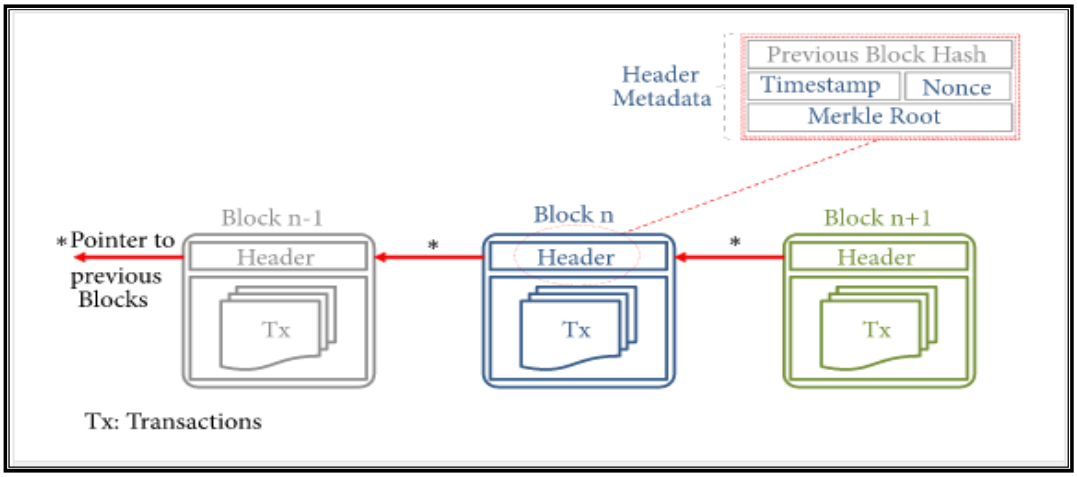


Figure 2-1: Typical structure of a Blockchain ((Jayasinghe *et al.*, 2019)

2.5.3 Smart Contracts on the Blockchain

In this research Smart Contracts are used to self-execute and validate the vote count using a consensus algorithm called Electoral Proof of Stake (EPOS). When certain criteria are met, a "smart contract" will automatically carry out its terms, which are written as computer programs. Essentially, distributed blockchains are used to store, duplicate, and update smart contracts, which are made up of transactions (Zheng *et al.*, 2020). The use of smart contracts on blockchain, as an additional feature, has been getting a lot of buzz of late. To put it simply, smart contracts are blockchain-stored executable programs. As a result, smart contracts and blockchain allow for a reliable, auditable, and irreversible protocol to be established without the usual need of central, trusted third parties (Kemmoe *et al.*, 2020). Figure 2.2 shows an adopted basic framework using smart contracts on the BBVV voting system.

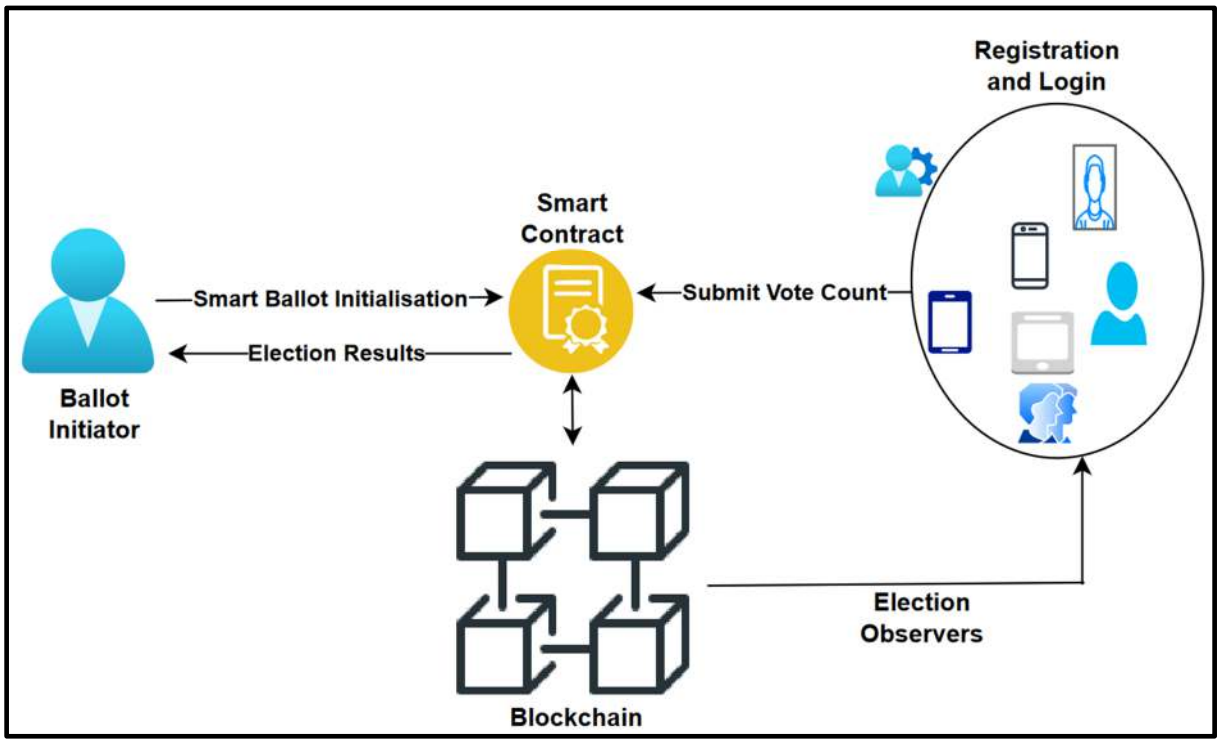


Figure 2-2: Adapted Basic framework of Smart Contract on the BBVV voting system(Ma *et al.*, 2020)

2.5.4 Edge Computing

The Internet of Things (IoT) is producing massive quantities of data that existing cloud infrastructures will struggle to handle. Edge computing has developed as a new model for dealing with the challenges of massive volumes of IoT data by pushing computing to the network's edge, minimising cloud connectivity latency and freeing networks from the bottleneck that would result from that bandwidth (Martin Fernandez *et al.*, 2018; Mao *et al.*, 2017). Edge computing brings the cloud closer to end-users by making ultra-low latency and high bandwidth to the network edge. As a result, there is a movement toward offloading computation to the edge. Computation offloading is the use of powerful infrastructures (such as remote servers) to supplement the computational capabilities of less powerful computers e.g., mobile devices (Lin *et al.*, 2019). The architecture of Edge computing is shown in Figure 2.3.

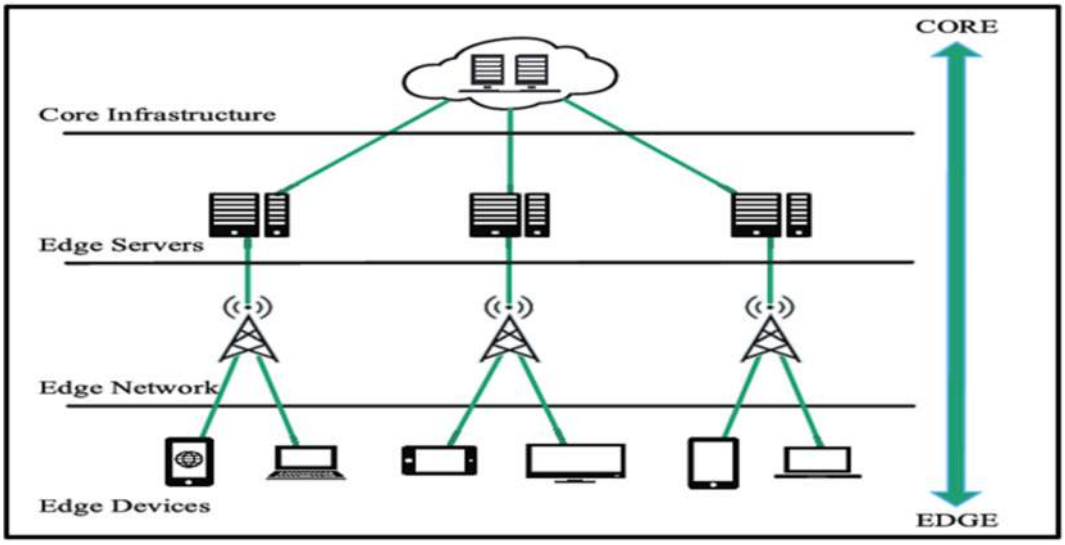


Figure 2-3:Architecture of Edge Computing (Zhang *et al.*, 2018)

Bhattacharya *et al.* (2020) describe Mobile Edge Computing as a dispersed data management structure bordering the main systems, consequently minimising the dormancy of the user on the end-to-end connectivity by incorporating software and hardware platforms. In Figure 2.4, the hardware in the form of edge devices is depicted as being contained within private blockchains, commonly referred to as permissioned blockchains. The data that has been finalised within the private blockchain is then transmitted to a public blockchain, referred to as a permissionless blockchain, for further analysis and consolidation. According to Wust & Gervais (2018), a permissionless blockchain is where a reader and writer can enlist on a blockchain at any time unlike permissioned which requires only authorised participants. Helliar *et al.* (2020) claim that Permissionless blockchains have evolved into a market-driven currency exchange solution. While Permissioned blockchains are getting to be an institutional-driven arrangement for the conduct of commerce with value-based proficiency, cost-cutting and the administration of the provenance and traceability of products in worldwide supply chains like the wine industry.

In this research, a secure electoral vote-counting system was designed using a combination of edge computing and blockchain architecture. Specifically, the processing and validation of the vote count was performed on the edge, in order to facilitate faster processing closer to the voter. This approach was implemented at polling stations and relied on the use of a private or

permissioned blockchain. The final aggregated vote count was then written private or permissioned blockchain, in order to facilitate the national aggregated vote count result.

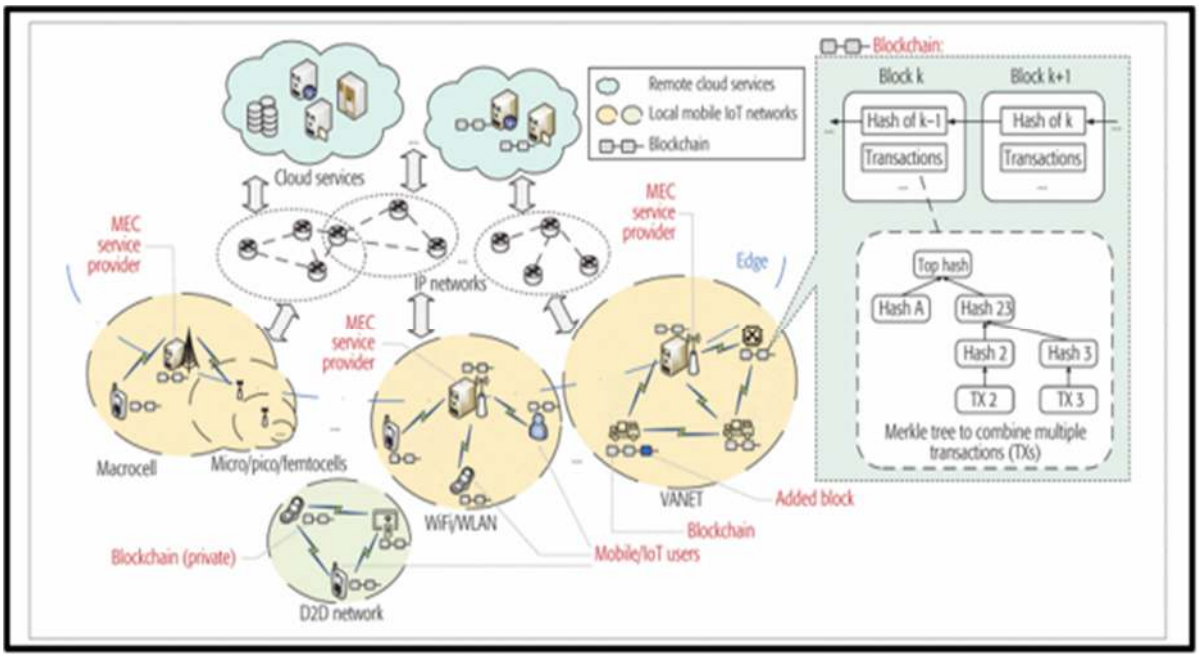


Figure 2-4: Mobile edge computing (MEC) Enabled blockchain (Xiong *et al.*, 2018)

2.5.5 Main features of Blockchain Electronic Voting Systems

Electronic blockchain voting systems have several important features that utilise the unique properties of blockchain technology to improve the voting process. These features make blockchain e-voting a compelling proposition for modernising the electoral process. However, when implementing such systems, these features must be carefully balanced with challenges such as voter verification, ballot secrecy, legal frameworks, and the digital divide (Gandhi *et al.*, 2023).

a) **Decentralisation:** unlike traditional voting systems that rely on a central authority to manage the election, blockchain voting systems are decentralised. This means that the recording of votes is distributed across multiple nodes in the network, making the system less vulnerable to single points of failure or centralised attacks.

b) **Transparency:** Blockchain systems are inherently transparent, as all transactions (in this case, votes) are recorded in a public ledger. This transparency ensures that any participant or observer can verify the integrity of the voting process and vote count.
c) **Immutability:** Once a transaction has been recorded in a blockchain, it can no longer be changed or deleted. This immutability provides a verifiable and permanent record of each vote, which is critical to maintaining the integrity of election results.
d) **Anonymity and data:** In addition to transparency, voter privacy is also of paramount importance. Blockchain e-voting systems can utilise various cryptographic techniques to protect the identity of voters. This ensures that a vote is recorded and verifiable but cannot be traced back to an individual voter.
e) **Security:** The use of cryptographic algorithms for transactions makes blockchain networks extremely secure. The votes cast in a blockchain network are encrypted, which prevents tampering and unauthorised access.
f) **Verifiability:** The combination of transparency and immutability makes blockchain-based e-voting systems fully verifiable. Any discrepancies can be reconciled with the blockchain ledger, which serves as the final record of all votes cast.
g) **Accessibility:** Blockchain-based e-voting can potentially be used by any voter with an internet connection, making voting possible from any location. This convenience could increase voter turnout and make it easier for those who cannot reach a polling station.
h) **Cost efficiency:** By eliminating the need for physical infrastructure, staff and paper-based processes, blockchain e-voting systems can reduce election costs for governments and organisations.
i) **Efficiency:** Electronic voting with blockchain can streamline the election process, allowing votes to be counted almost instantly and results to be announced faster than with traditional voting methods.
j) **Scalability:** Although scalability can be a challenge for blockchain networks, modern blockchain e-voting systems are being designed to process large numbers of transactions to enable widespread adoption in large elections.

2.6 Blockchain-based Electronic Voting Systems: Security Measures and Consensus Algorithms

In their paper, Shahzad & Crowcroft (2019), indicate the security and irreversibility of the blockchain are ensured by the SHA-256 algorithm. They utilised the blockchain electronic voting idea in a private or consortium blockchain, in which transactions, block formation and sealing are all done in a supervised environment, and entries and block creation may only be done by the users' approved members. Ramalingam *et al.*, (2021) employed End-to-end verification, voter confidentiality, and vote consistency with blockchain using the SHA-1 hashing algorithm. This hash algorithm is used to protect the data connected with each vote and behaves as a one-way hash technique with no proven reversal. To avoid information vulnerability, as well as a high number of data breaches, Jingzhong *et al.*, (2020) uses cryptography-based multi-party computing and blockchain ring signature technology, this is a cryptography protocol that allows anonymity among different users. In a blockchain, however, reaching a consensus among users through consensus algorithms is important for new block creation and authentications.

Yi (2019), introduced the blockchain-based electronic voting Scheme which proposed improved electronic voting security solutions in a peer-to-peer network. To prevent voter fraud, a Distributed Ledger Technology (DLT)-based voting scheme was used. This was accomplished via the development of a user credential model based on elliptic curve cryptography, which provides authentication and non-repudiation capabilities. nevertheless, Lai *et al.* (2019) proposed a decentralized anonymous transparent electronic voting system (DATE), needing just a minimum level of trust between participants. This was achieved by putting all election communications on Ethereum's blockchain to ensure openness, while also safeguarding individual voters' anonymity with the use of an efficient ring signature technique.

Liu & Wang (2017), came up with a blockchain-based electronic voting system protocol. This protocol is global and does not rely on any blockchain platform or the requirement for a trusted third party. Each voter must have two sets of public and private keys: one to sign, and one to be revealed to others. To further preserve voter anonymity, a second method involves casting votes through blockchain and requires the voter to keep their public key private.

Hjalmarsson *et al.* (2018) utilised a smart contract between the district node and the boot node that runs the proposed system. To increase transaction speeds, one should use Exonium, Quorum, and Geth, which are all framework options. Additionally, Fernandes *et al.*, (2021) study suggests an e-voting system with secret contracts that are based on blockchain technology. The secret contracts were created using the Enigma platform. Furthermore, Damle *et al.* (2021) work uses the distributed trust mechanism of the blockchain to design a smart contract system, called FASTEN. There are many ways to use smart contracts for voting. We note that these systems are either not scalable or fail to keep the vote count hidden, thus they cannot be used for secret voting.

Consensus algorithms are core blockchain functionality, there are hundreds of different consensus algorithms available today for various application settings, such as Proof of Work (PoW), Proof of Stake (PoS), Delegate Proof of Stake (DPoS), Proof of Reputation (PoR), and so on. However, the speed, security, and stability of public or private blockchains make it impossible to sustain certain projects (Tan & Xiong, 2020).

2.7 Blockchain Technology in Electronic Voting: Limitations and Considerations

Securing electronic voting is a pressing issue that has emerged as a prominent subject in the field of communications and networking (Yi, 2019). A safe and practical e-voting system that overcomes vote fraud is critical. Practical blockchain-based e-voting systems are suitable for a wide range of networking applications. Huang *et al.* (2021) define blockchain as a digital ledger whose data is distributed over a peer-to-peer network, where each member maintains a copy of the append-only ledger, which consists of digitally signed and encrypted transactions.

Blockchain electronic voting systems have shown success evidence by providing security, dependability, decentralisation, and anonymity. A blockchain solution is well-suited to meet the requirements of e-voting systems, particularly since it allows for the easy and universal verification of the identity of both the public and the individuals involved in the system (Vivek *et al.*, 2020a). However, many risks must be dealt with, including susceptibility to scalability

attacks, dependence on untrustworthy technology, and refusal to obey regulations (Jafar *et al.*, 2021). The trust systems reviewed in Sections 2.3 among others showed limitations.

Blockchain technology has been touted for its transparency and immutability, which has the potential to revolutionize various industries. However, this transparency also poses a risk as it can be used for malicious purposes. To overcome this risk, Liu and Wang (2017) proposed the use of permissioned blockchains, which enforce access restrictions. This ensures that only authorized individuals can access the information on the blockchain, thereby reducing the risk of malicious actors gaining access to sensitive information. However, it is important to note that blockchain technology still has a vulnerability. The use of a Public Key Infrastructure (PKI) database in blockchain technology can be a point of failure, as the revelation of this database may undermine the security of the whole process (Hjalmarsson *et al.*, 2018a). Additionally, the cost and scalability of blockchain systems are also a concern. For example, Exonium is a costly system that uses bitcoin and is difficult to deploy on large scales (Yi, 2019). However, there are several free and powerful systems available that can address these issues, making blockchain technology more accessible for practical use.

In conclusion, while blockchain technology has the potential to revolutionize various industries, it is important to consider the potential risks and limitations of the technology. Permissioned blockchains and the use of cost-effective and scalable systems can address some of these concerns and make blockchain technology more secure and accessible. Despite the potential of blockchain technology to address issues in the voting system, it does not fully solve the concerns. Blockchain technology has several limitations that need to be addressed, and there are still technological hurdles to overcome. Considering this, the focus of this research is on the application of blockchain technology for electoral vote counting on the edge.

2.8 Theoretical Foundations

The theoretical underpinnings of our research are covered in this section. It provides an explanation of the key theories, models, or concepts that are pertinent to our study and illustrates the relationship between these theoretical underpinnings and the goals or research questions.

2.8.1 Main Theories

2.8.1.1 The Byzantine Generals Problem Theory (BGP)

Lamport *et al.*, (1982) introduced the name Byzantine Generals to characterise a defective node that could behave maliciously, and the word Byzantine general was devised. Aside from the significant influence, this work has had on the field of fault-tolerant systems science, the word "Byzantine" has since become a descriptor for arbitrary or malicious behaviour. Handling malfunctioning components that give conflicting information to different parts of a system is paramount in reliable computer systems. The Byzantine Generals Problem expresses this situation abstractly in terms of a group of generals of the Byzantine army surrounding an enemy city as shown in Figure 2.5. Their communication is dependent on sending a messenger from one group of the army to the other to agree on a common battle plan of attack.

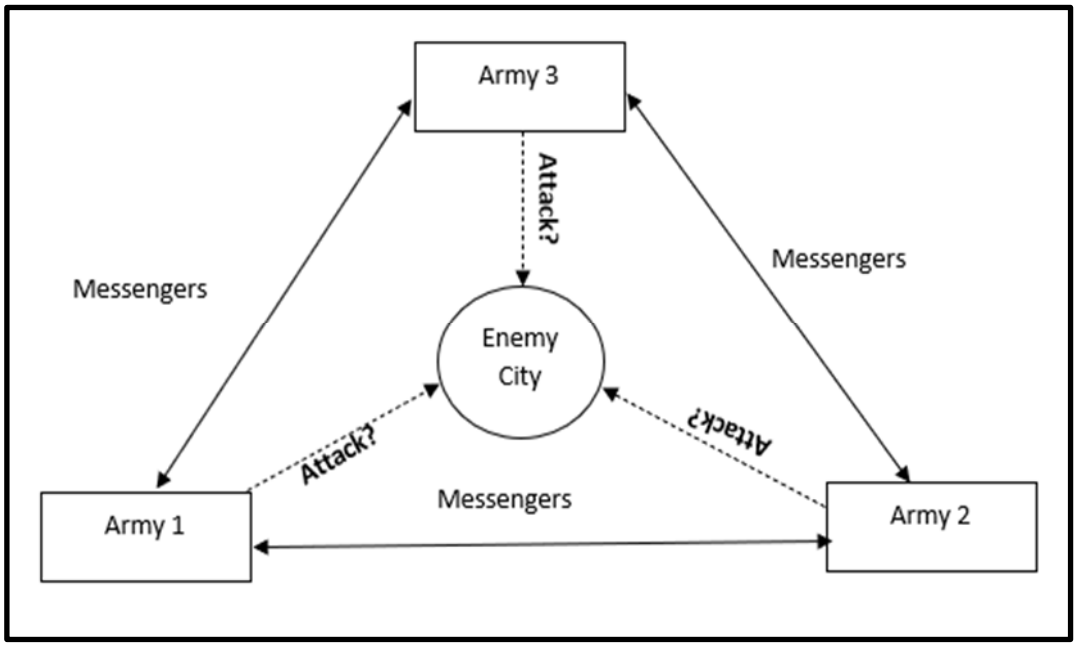


Figure 2-5:The Byzantine Generals Problem

The attack should be instituted at the same time to defeat the enemy city. Nevertheless, the enemy city might capture/kill or exchange the messenger with another one thereby altering the message about the plan of attack and hence having the ability to send false information. In addition, there may be generals or commanders who may try to confuse others by being

traitorous (Lamport *et al.*, 1982). Figure 2.6 illustrates how General 2 modifies the original message sent to General 3 from “Attack” to “Retreat”, thus General 2 communicates “General 1 said retreat”. General 3 will, therefore, receive “Attack” and “Retreat”. Figure 2.7 shows a traitorous General 1 sending “Retreat” to General 2 and attack to General 3. This explains how difficult it is to come to a consensus with unsigned messages when one of the three is a traitor.

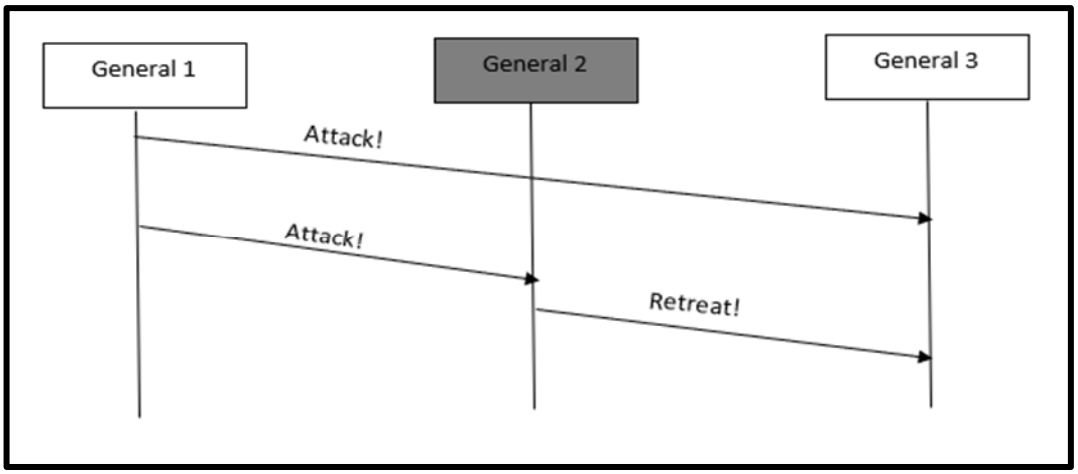


Figure 2-6: Malicious General 2

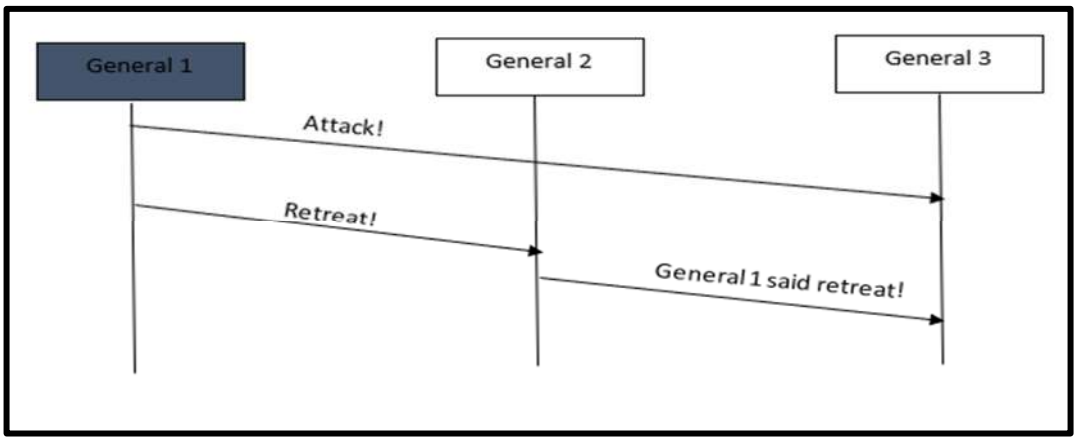


Figure 2-7: Malicious General 1

Attacking at the same time is core to the surrounding army defeating the enemy city, if they attack at different times the enemy city wins. However, if two-thirds of the surrounding army notwithstanding the malicious ones agree on one value which is the time of the attack, then

they can still defeat the enemy city. In this study, the Byzantine general problem theoretical solution will be used to solve a social practical problem in the electoral vote count. Solving the byzantine generals' problem is synonymous to vote count in elections where electoral observers must agree on one value to declare a contending participant as a winner. The Byzantine Generals Problem raises the question of trust. Generally, politicians do not trust each other and yet they must agree on one value in an election to determine the winner.

The Byzantine Generals Problem solution depends on an algorithm to guarantee that all the loyal generals agree upon the same plan of action that a small number of traitorous generals cannot influence. Reaching a consensus needs a communication channel that can be trusted, and messages validated for integrity. Blockchain can be used to reach consensus in distributed networks using two classes of protocols namely: Proof of Work (PoW), Proof of Stake (PoS) and Byzantine Fault Tolerant (BFT) (Jalalzai & Busch, 2018). Blockchain provides a solution to the Byzantine Generals Problem theory for instance to have a two-thirds consensus, it is therefore assumed that:

- f general might be malicious.
- The loyal generals do not know who the malicious ones are.
- Malicious generals might collude.
- Nevertheless, the loyal generals must agree on a plan thus ;

The theorem: Need $3f+1$ generals in total to tolerate f malicious generals i.e <1/3 may be malicious.

2.8.1.2 Mathematical Representation of the Byzantine Generals Problem

Definitions:

Nodes (G):

- Represent the generals in the problem.
- G is the set of all generals.
- G_i represents the i-th General.
- Example: G_1 is General 1, G_2 is General 2, and so on.

Edges (E):

- Represent the communication channels between the generals.
- E is the set of all communication channels.
- An edge (G_i, G_j) indicates that General G_i can directly communicate with General G_j.

Messages (M):

- Represent the messages exchanged between generals.
- M is the set of all messages exchanged.
- A message m_ij = (i, j, v_ij) denotes that General G_i sends a message to General G_j with a value v_ij.

Faulty Node Function (f):

- Indicates whether a node (general) is faulty.
- f is a function that maps each general to a binary value indicating if they are faulty.
- f(G_i) = 1 if General G_i is faulty.
- f(G_i) = 0 if General G_i is non-faulty.

Threshold Condition:

- Determines the maximum number of faulty generals the system can tolerate.
- For n generals, the system can tolerate up to (n-1)/3 faulty generals.
- Example: With 4 generals, the system can tolerate (4-1)/3 = 1 faulty general.

Decision Function (D):

- A function used by each general to determine their decision based on the received messages.
- D_i(M) is the decision function for General G_i.
- D_i(M) takes the set of received messages M and outputs the decision v_i.

Algorithm 2.1 shows the mathematical representation of the BGP:

Algorithm 2.1 The Byzantine Generals Problem

Input: Set of generals G, set of communication channels E, set of messages M, faulty node function f, threshold condition T, decision function D.

Start Algorithm

1. Initialise:

   1.1 $G = \{G\_1, G\_2, \ldots G\_n\}$

   1.2 $E = \{(G\_i, G\_j) | i, j \in \{1,2,\ldots,n\}, i \neq j\}$

   1.3 $M = \emptyset$

2. Send Messages:

   2.1 $for\ each\ General\ G\_i$ in $G\ do$

   2.2 $for\ each\ General\ G\_j$ in G , $j \neq i$ do

   2.3 $if\ (G\_i, G\_j)\ in\ E\ then$

   2.4 $Send\ message\ m\_ij = (i, j, v\_ij)\ from\ G\_i\ to\ G\_j$

   2.5 $M = M \cup \{m\_ij\}$

3. Identify Faulty Generals:

   3.1 $for\ each\ General\ G\_i\ in\ G\ do$

   3.2 $if\ f(G\_i) == 1\ then$

   3.3 $Mark\ G\_i\ as\ faulty$

   3.3 else

   3.5 $Mark\ G\_i\ as\ non - faulty$

4. Check Threshold Condition:

   4.1 max_faulty = (n − 1) / 3

   4.2 $faulty\_count = number\ of\ generals\ G\_i\ such\ that\ f(G\_i) == 1$

4.3 $if\ faulty\_count\ > max\_faulty\ then$

4.4 $Report\ "Too\ many\ faulty\ generals, cannot\ reach\ consensus"$

4.5 $Exit$

5. **Decision Making:**

5.1 $for\ each\ General\ G\_i\ in\ G\ do$

5.2 $received\_messages\ = \{m\_ji \mid m\_ji\ \in\ M, j\ \neq\ i\}$

5.3 $v\_i\ =\ D\_i(received\_messages)$

5.4 $Output\ decision\ v\_i\ for\ General\ G\_i$

End Algorithm

Cryptography using digital signatures helps to solve the Byzantine Generals Problem . Users can use digital signatures to authenticate information without having to provide any secret keys. Three quick algorithms make up a digital signature scheme: a probabilistic key generator G, a signing algorithm S, and a verification algorithm V (Gilad *et al.*, 2017). This study proposes the Binary Byzantine Agreement Protocol.

2.8.1.3 The Binary Byzantine Agreement Protocol (BBA)

The BBA is reasonably fast and relies on the honesty of more than two-thirds of the players: regardless of what the malicious players do, each execution of its main loop brings the players into an agreement with a probability 1/3 (Gilad *et al.*, 2017). Hence:

Each participant has a public key that satisfies the unique signature characteristic of a digital signature scheme.

Step 3 uses digital signatures to create a sufficiently common random bit.

The protocol only requires a simple set-up: a shared random string r that is unrelated to the participants' keys.

Protocol BBA is a three-step loop in which the participants exchange Boolean values repeatedly, with different players exiting the loop at various times. This is as shown in protocol 2.1:

Protocol 2.1: The BBA (Chen and Micali, 2016)

STEP1. $[\mathbf{Coin-Fixed-To-0\ Step}]\boldsymbol{Each\ player\ i\ sends\ b_i}.$

1.1 $if\ \#\frac{1}{i}(0) \geq 2t+1, then\ i\ sets\ b_i = 0, sends\ 0_*, outputs\ out_i = 0, \quad and\ HALTS.$

1.2 $if\ \#\frac{1}{i}(1) \geq 2t+1, then, then\ \ i\ sets\ b_i = 1.$

1.3 $Else, i\ sets\ b_i = 0.$

STEP 2. $[\mathbf{Coin-Fixed-To-1\ Step}]\boldsymbol{Each\ player\ i\ sends\ b_i}.$

2.1 $if\ \#\frac{2}{i}(1) \geq 2t+1, then\ i\ sets\ b_i = 1, sends\ 1_*, outputs\ out_i = 1, and\ HALTS.$

2.2 $if\ \#\frac{2}{i}(0) \geq 2t+1, then\ \ i\ sets\ b_i = 0.$

2.3 $Else, i\ sets\ b_i = 1.$

STEP 3. $[\mathbf{Coin-Genuinely-Flipped\ Step}]\boldsymbol{Each\ player\ i\ sends\ b_i.\ and\ SIG_i}\ (\boldsymbol{r}, \boldsymbol{y}).$

3.1 $if\ \#\frac{3}{i}(0) \geq 2t+1, then\ \ i\ sets\ b_i = 0.$

3.2 $if\ \#\frac{3}{i}(1) \geq 2t+1, then\ i\ sets\ b_i = 1.$

$3.3\ Else, letting\ S_i$

$= \{j \in\ N\ who\ have\ set\ i\ a\ proper\ message\ in\ this\ step\ 3\}, i\ sets\ b_i$

$= c \triangleq lsb(min_{j \in S_i} H(\ SIG_i 1\ (r, y)));\ increase\ \gamma_i\ by\ 1;\ and\ returns\ to\ Step\ 1.$

$Theorem$: $whenever\ n \geq 3t + 1, BBA^{*} is\ a\ binary(n, t) - BA\ protocol\ with\ soundness\ 1.$

The concept of dynamic PBFT, introduced by Chang *et al.* (2022), extends the applicability of BGP and BBA to blockchain voting systems. By considering the changing number of voting nodes in a PBFT blockchain network, their large-scale Markov modelling technique enables the analysis of dynamic voting processes, which is directly applicable to the design of BBVV artefact. This approach can help create a BBVV system that supports decentralisation and distributed structures and ensures that the system can adapt to the entry and exit of voting nodes, thus maintaining the integrity and trustworthiness of the vote counting process.

Finally, the lightweight BFT consensus protocol for blockchains presented by Hackfeld (2019) and the generalised Byzantine quorums presented by Alpos & Cachin (2020) provide additional theoretical foundations for BBVV systems. Hackfeld's protocol fits into existing mechanisms for block proposals and is designed to be simple and efficient, which is beneficial for BBVV systems that require a balance between security and performance. Alpos and Cachin's work on consensus with generalised quorums provides a way to implement more sophisticated trust assumptions in blockchain consensus that can be tailored to the specific needs of a BBVV system to handle different trust scenarios and failure modes.

2.8.2 The Proposed BBVV protocol

EMB in this case represents Elections Management Board and EPoS, Electoral Proof of Stake being officials or political agents with the right to write to the blockchain. The abstract protocol is given in section 2.8.2.1.

2.8.2.1 High level BBVV protocol

Start

1. **Initialise Polling Station**

   1.1 EMB initializes the polling station number.

2. **Authenticate EPoS Identity**

   2.1 EPoS provides identification.

   2.2 If verified, proceed; if not, remove EPoS and notify.

3. **Generate Smart Ballot**

   3.1 EMB generates and assigns a smart ballot to EPoS.

4. **Assign Electoral Proof of Stake (EPoS)**

   4.1 Smart Ballot includes total votes to be cast and votes received by each candidate.

5. **Initialise Voting Parameters**

   5.1 Set initial values for polling station, ballots to be cast, ballots already cast, candidate ballots received, and rejected ballots.

6. **Start Writing to the Block**

   6.1 EPoS writes candidate and party information to the local blockchain.

7. **Reach Consensus**

   7.1 Define and apply the consensus function, consensus(n, N),

   7.2 where $\text{Consensus}(n, N) = 1$

   7.3 if $(n / N) > 67$ otherwise 0.

8. **Consensus Outcomes**

   8.1 **Success:** Validate and commit the vote count transaction.

8.2 **Failure:** Reject the vote count transaction and request a recount.

9. **Write Ratified Vote Count to Cloud Blockchain**

9.1 EMB writes the ratified vote count for national collation.

10. **Validate Smart Ballot Count**

10.1 EPoS checks if their smart ballot was counted.

Stop

This study employed the BGP and BBA protocol as the underpinning theory and the BBVV protocol as the design theory. Ratifying a participating node as a true vote count requires at least two-thirds of validating nodes to reach a consensus. The BBA protocol requires two-thirds of validating nodes to reach consensus, therefore it perfectly suits this study.

2.8.3 Theoretical Framework Relationship with Research Objectives and Questions

The Byzantine Generals Problem and the Binary Byzantine Agreement are essential for the development of a secure blockchain-based vote counting and validation artefact (BBVV). They ensure that all participants in a distributed network agree on a single source of truth even if there are malicious actors, which is essential for trust in election processes.

2.8.3.1 Relation to the research objectives:

- **Review of blockchain solutions:** Examining how existing blockchain voting systems deal with the problem of Byzantine generals serves as a basis for the design of BBVV and demonstrates the need for a system that can achieve consensus despite errors.
- **System Specifications:** BBVV must be designed to be fault tolerant and achieve more two-thirds agreement in vote counting, which is key to maintaining system integrity and user confidence.
- **Blockchain protocol selection:** Choosing a blockchain protocol is about selecting a consensus mechanism that effectively combats byzantine errors for reliable vote validation.

- **Development and evaluation:** Testing the BBVV's resilience to Byzantine errors is fundamental for its reliability and the trust of its users.

2.8.3.2 Answering the research questions:

- **Design approach:** the use of consensus algorithms that address the problem of Byzantine generals and enable binary Byzantine agreement is essential for a trustworthy BBVV design.
- **Existing solutions and challenges:** Reviewing how current systems implement these concepts will guide the development of a more secure and trustworthy BBVV.
- **Trust and performance specifications:** The BBVV must have fault tolerance and data integrity as core features to ensure high performance and user trust.
- **Optimal protocol for validation of votes:** The chosen protocol must provide a balance between security against errors and the practical needs of voters such as speed and simplicity.
- **Performance features and trust:** BBVV's ability to withstand byzantine errors and reach consensus in a transparent manner is fundamental to gaining user trust.

The General Byzantine Problem and the Binary Byzantine Agreement provide a theoretical basis for creating a secure, transparent, and trustworthy BBVV artefact for counting and validating votes.

2.9 Systematic Literature Review (SLR) on Existing Blockchain Vote Counting Solutions: A Comparative Analysis of Methods, Constraints, and Approaches

The systematic review approach, which includes search terms, databases, inclusion, and exclusion criteria (protocols) and search criteria, is explained in this section. The quality and relevance of the assessed research is discussed and the main conclusions from the selected literature are presented. In addition, the systematic review highlights any patterns, tendencies, trends or gaps in the literature.

In this section we present the paper “A systematic literature review on Blockchain Electoral Vote Counting Solutions: A Comparative Analysis of Methods, Constraints, and Approaches

(Patrick Mwansa and Dr Boniface Kabaso). This systematic literature review (SLR) aims to find existing solutions in blockchain electoral vote counting and compare them with each other in terms of methods, constraints, and approaches. The SLR has shared more light on the research gap to start this research.

Abstract— Blockchain technology in electronic voting has emerged as an alternative to other electronic and paper-based voting systems to minimise inconsistencies and redundancies. However, past experiences indicate limited success due to scalability, speed, and privacy issues. This systematic literature review examines the methods, constraints, and approaches in the existing literature on blockchain-based electoral vote-counting solutions. A thorough search of pertinent databases was performed, and selected studies were assessed based on predefined inclusion and exclusion criteria. The review's findings reveal that most existing solutions employ smart contracts and various cryptographic algorithms to create secure and transparent voting systems. However, the study also pinpoints areas that require improvement, such as scalability, privacy, and accessibility. The review recommends exploring different combinations of blockchain platforms, cryptographic algorithms, and programming languages to develop secure and transparent voting systems. Additionally, future research could investigate the potential benefits and challenges of incorporating Internet of Things (IoT) devices, consensus mechanisms, and other technologies into the voting process. The review concludes that more research is needed to enhance the security and transparency of blockchain-based voting systems.

Keywords— *Blockchain, cryptographic algorithms, consensus mechanisms, Internet of Things (IoT), Smart contracts, Systematic Literature Review*

2.9.1 Introduction

Rapid technological development has made it possible for creative solutions to address the most urgent problems in a variety of fields, including election systems. The use of blockchain technology to improve electoral vote-counting procedures is one such ground-breaking breakthrough. Nakamoto (2008) first created blockchain technology for cryptocurrency

transactions, and Noizat (2015) suggests it may increase voting systems' effectiveness, transparency, and security. In order to shed light on the possible benefits and limits of this technology, this research intends to give a thorough comparative examination of different methods, restrictions, and approaches in implementing blockchain-based electoral vote-counting systems.

Recently, an escalating number of nations have been embarking on pilot projects and investigating how to incorporate blockchain technology into their political systems (Swan, 2015; Benabdallah *et al.*, 2022a). Traditional voting systems suffer from problems such as voter theft, vote manipulation, and a lack of accountability, and Blockchain-based voting systems aim to address these issues (Vivek *et al.*, 2020a). This research explores various methods for integrating blockchain technology into political vote tallying systems by assessing technological and administrative aspects and addressing security and accessibility concerns that must be resolved for successful implementation (Al-Maaitah *et al.*, 2021).

Despite blockchain technology's enthusiasm, one must consider various constraints and challenges. These include the digital divide, privacy concerns, and the complexity of adapting existing legal and regulatory frameworks (Vinet & Zhedanov, 2011b). This review aims to find existing solutions in blockchain electoral vote counting and compare them with each other in terms of methods, constraints, and approaches. The goals of this study are to:

- Evaluate the current body of knowledge on blockchain-based solutions for tallying electoral votes.
- Review how existing blockchain electoral vote-counting solutions compare with each other concerning methods, constraints, and approaches.
- Identify the strength of the evidence supporting the different solutions and how best they can be used to create a reliable blockchain artefact that engenders trust in electoral vote counting and validation in developing countries.

By synthesizing the existing literature, this comparative analysis provides valuable insights and recommendations for policymakers, election administrators, and researchers seeking to harness the power of blockchain technology in electoral processes.

In this research article, we present a comparative analysis of blockchain-based electoral vote-counting solutions. Following this introduction, the article is structured as follows: Section II reviews the relevant literature, and Section III details the methodology employed. Section IV presents the findings and discussions, while Section V addresses threats to validity. Section VI concludes the article by summarizing our findings and implications, and Section VII suggests future research directions, focusing on various combinations of platforms, cryptographic algorithms, and programming languages for secure and transparent voting systems.

2.9.2 Related Works

Overall, the research reviewed supports the notion that blockchain technology can significantly improve electronic voting systems and offers a number of benefits, including increased security, transparency, decentralization, and cost-efficiency. Despite this consensus, however, the literature also reveals a complex landscape of challenges and nuances that warrant further exploration.

Some studies underscore the potential of blockchain to revolutionize voting systems by enhancing security and transparency, eliminating the need for third-party trust, and providing a decentralized method for transactions and data storage (Benabdallah *et al.*, 2022; Vivek *et al.*, 2020). Particularly, the extension of the application of this technology may occur beyond voting systems to other sectors such as supply chain management, commerce, and banking (Vivek *et al.*, 2020b).

In contrast, others focused on the importance of incorporating multiple parties into the blockchain-based electronic voting system (Al-Maaitah *et al.*, 2021; Abuidris *et al.*, 2019). This approach was seen to not only enhance security and privacy but also to reduce election costs (Al-Maaitah *et al.*, 2021) . They noted, however, that consensus protocols in such systems still require improvement.

Highlighting another dimension of the discussion, Singh *et al.*, (2022) compared different implementations of blockchain technologies, concluding that private and permissioned blockchains outperformed public ones due to faster transaction verification times. They further

suggested enhancing security by integrating biometric information, illustrating the potential for technological refinement in blockchain-based voting systems.

While the majority of the studies emphasised the potential benefits of blockchain technology, Taş & Tanrıöver (2020b) provided a more critical view, reviewing 63 research articles and concluding that existing blockchain frameworks have limitations, including difficulties with remote participation security and scalability. This demonstrates the ongoing challenges that need to be addressed in order to fully realize the potential of blockchain technology in voting systems.

In summary, the literature reveals a strong belief in the transformative potential of blockchain technology for electronic voting systems, highlighting benefits in areas such as security, privacy, cost-efficiency, and decentralisation. However, this enthusiasm is tempered by a recognition of the need for further development in areas such as consensus protocols, scalability, and remote participation security. Furthermore, there is an interest in the exploration of different blockchain implementations, including the integration of biometric data and the comparison between public and private blockchain systems.

2.9.3 Methodology

To conduct a transparent, reproducible, and scientific literature review of blockchain electoral vote counting, we adopted some features of the PRISMA statement (Moher *et al.*, 2009) and followed a suggested process (Briner & Denyer, 2012). The overall methodological approach included the following steps.

- Identify the need for review, prepare research questions, and develop the review protocol.
- Identify the research questions, select the studies, assess their quality, take notes, extract data, and synthesize it.
- Report the results of the review.

A. Review Protocol

Research Questions

The research questions (RQs) raised for this study are:

RQ1: What are the existing solutions in blockchain electoral vote counting?

RQ2: How do the different solutions found by addressing RQ1 compare concerning methods, constraints, and approaches?

RQ3: What is the strength of the evidence in support of different solutions?

RQ4: What implications will these findings have when creating a new solution?

The researchers followed a PRISMA approach to conduct a Systematic Literature Review to answer the questions raised.

B. Search Query

In this study, a systematic search strategy was developed to identify relevant literature on blockchain vote-counting systems. This search strategy was specifically tailored to the IEEE Digital Library, Association for Computing Machinery (ACM) Digital Library, and Google's Scholarly Article databases, and the following search terms were used.

Blockchain AND (e-voting OR electronic voting) AND ("vote-counting" OR "vote tallying").

All Searches spanned from 2015 to 2022, including journal articles and conference proceedings published in English only. The search limitations were defined as: search conducted between years (2015 and 2022), research article/journal that is published in a peer-reviewed (refereed or scholarly) journal, research article/journal written in English, must be open access and available online, and publications are of type articles or conference proceedings.

C. Study Selection

The selection criteria for the literature included in this systematic search were based on the PRISMA Statement (Moher *et al.*, 2009).

The focus of the investigation was primarily on identifying existing literature on blockchain electoral vote counting within the fields of Social Sciences, Computer Science, Engineering, Mathematics, and Decision Sciences.

1. Inclusion Criteria:

    - Peer-reviewed research articles on blockchain electoral vote-counting,
    - Conference proceedings papers on blockchain electoral vote-counting.

2. Exclusion Criteria:

    - Studies before 2015 or not in English.
    - Review studies.

D. Quality Assessment

The present study was based solely on peer-reviewed research articles and conference papers. This review thoroughly checked for duplicates and meticulously evaluated each research paper to ensure review quality. The abstracts of the articles were critically considered during the analysis and purification processes to guarantee the relevance and quality of the academic literature included in the review. To limit the papers to those published in English only, we applied an additional exclusion criterion and excluded 26 articles from non-English languages. After assessing each article against the inclusion and exclusion criteria, we selected 81 articles for review.

In the review, we used the ten-quality assessment (QA) questions listed in Table 2.2, as recommended in [20]. Scores were assigned as follows: 1 for strongly agree, 0.5 for partially agree, and 0 for disagree. Studies that scored less than 7.0 out of 10 on the quality assessment questions were excluded.

Table 2.2: Adopted Quality Assessment Questions

Quality Assurance Questions
1. Has the research explicitly outlined its objectives?
2. Have the independent variables been precisely identified?
3. Is the size of the data set suitable?
4. Has the process of data collection been explicitly outlined?
5. Has a method for selecting sub-attributes been employed?
6. Are the methods used clearly articulated?
7. Are the results and conclusions presented in a clear manner?
8. Have the limitations pertaining to the study been detailed?
9. Can the research methodology be replicated?
10. Does this study offer new insights or add value to existing literature?

E. Data Extraction Form

Data was gathered from entries by pulling information from studies that met the Quality Assessment (QA) criteria. The structure of the data extraction form that was utilized is displayed in Table 2.3.

Table 2.3: Data Extraction Form Format

Variables
Authors:
Title:
Publication type:
Year:
Field of study:
Total quality assessment score (out of 10):
Electoral vote counting solution provided:
Methodology used:
Constraints or limitations of the study:
Approaches used in the study:
Experiment size:
Strengths:
Weaknesses:

F. Data Synthesis

The collected data did not undergo any statistical analysis, and instead, this paper presents significant facts obtained from the selected studies in textural and tabular formats. This report summarizes specific literature chosen according to the QA criteria.

2.9.4 Findings and Discussions

RQ1 *What are the existing solutions in blockchain electoral vote counting?*

Table 2.4 enumerates the count of research papers at every phase of the evaluation procedure.

Table 2.4: Results of The Review Procedure [The Year 2015 -2022]

Stage	No. of Studies	Remarks
Initial search using search terms	791	Using metadata
Removal of duplicates	721	
Removal of non-English	695	
Filter by title	147	
Filter by abstract	94	
Full text gathered	81	No secondary studies
Included in the extraction form	54	High QA scores

To address the research questions, studies have been concisely summarized. A yearly breakdown of the studies employed in this investigation can be found in Figure 2.8.

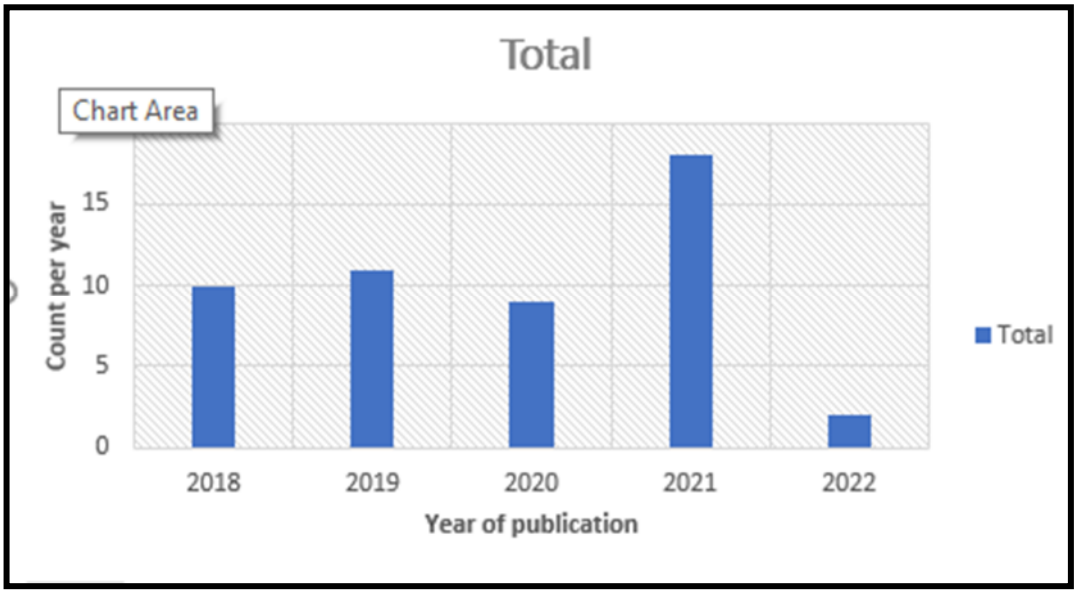


Figure 2-8: Publication on Blockchain Electoral Vote Counting [The Year 2015 -2022]

The literature has examined a number of blockchain vote tallying methods. Studies have looked into the use of machine learning, smart contracts, and private and public blockchains for safe polling systems (Cheema *et al.*, 2020a). Other scholars have considered using permissioned blockchains, like Hyperledger Fabric, as the foundation for voting (Mukherjee *et al.*, 2020). Researchers have also explored the combination of a blockchain-based digital voting system with cryptographic hash functions, such as the SHA 256 Algorithm or non-interactive zero-knowledge proof (Adiputra *et al.*, 2019; Agbesi & Asante, 2019a). Furthermore, they have developed Secure e-voting systems using smart contracts and the Ethereum network (Hjalmarsson *et al.*, 2018b). There have also been proposals for blockchain-based secret contract electronic polling systems (Fernandes *et al.*, 2021). Some studies have examined improving election systems by combining group blockchains or the Ethereum blockchain with IoT (Han *et al.*, 2020). Lastly, the study has looked into how blockchain technology combined with elliptic curve cryptography could provide safe vote tallying methods (Chaieb *et al.*, 2019). Table 2.5 lists the studies and their approach regarding blockchain voting solutions.

Table 2.5: Blockchain Voting Solutions

Studies	Approach
(Cheema *et al.*, 2020a; Parmar *et al.,*2021a; Fezzazi *et al.*,2021).	Private and public blockchains with machine learning and smart contracts.
(Wisessing et al., 2020; Yu *et al.,* 2018a; González *et al.,* 2022; Xu *et al.,* 2021; Vairam *et al.,* 2021; Angsuchotmetee *et al.,* 2019).	Hyperledger Fabric, a permissioned blockchain.
(Jagjivan *et al.,* 2021a; Sharma *et al.,* 2021a; Matile *et al.,* 2019; Pandey *et al.,* 2019; Kumar 2014; Agbesi & Asante 2019a; Srivastava *et al., 2*018; Pawlak & Poniszewska-Marańda 2019; Ingouchi & Jain 2016; Lin & Zhang 2019; Adiputra *et al.,* 2019; Li *et al.,* 2021; H *et al.,* 2020; Luo, 2021; Chaisawat & Vorakulpipat 2020).	A blockchain-based digital voting system and SHA 256 Algorithm or cryptographic Hash function or non-interactive zero-knowledge proof
(Govinda *et al.,* 2021; Matile *et al., 2019*; Thuy *et al.,* 2019; Lyu *et al.,* 2019; Alvi *et al.,* 2020a; Panja *et al.,* 2020; Canessane *et al.,* 2019; Khoury *et al.,* 2019; Sadia *et al.,* 2020b; Shukla *et al.,* 2018; Hjalmarsson *et al.,* 2018b; Abegunde *et al.,* 2021; Rao *et al.,* 2021; Tjahajadi *et al.,* 2018; Zhang *et al.,* 2018; Hardwick *et al.,* 2018b; Al-Madani *et al.,* 2020; Ruparel *et al.,* 2021a; Russo *et al.,* 2021; Jayasooriya *et al.,* 2022).	Ethereum Blockchain and smart contracts
(Fernandes *et al.,* 2021; Othman *et al.,* 2021; Bartolucci *et al.,* 2018).	Secret contract e-voting system based on the blockchain technology
(Han *et al.,* 2020; Zaghloul *et al.,* 2021; Alam *et al.,* 2018).	Consortium blockchain or Ethereum Blockchain and IoT
(Rathore & Ranga 2021a; Luo, 2021).	Blockchain and elliptic curve encryption

RQ2 *How do the different solutions found by addressing* ***RQ1*** *compare concerning methods, constraints, and approaches?*

In this review, we attempted to identify the most commonly used methods and approaches for electronic voting systems while considering the constraints and analysing the details of the preselected papers. Our findings strongly indicate that electronic voting systems can employ blockchain technology. Figure 2.9 depicts how the blockchain e-voting platform leverages network visualization based on the papers reviewed.

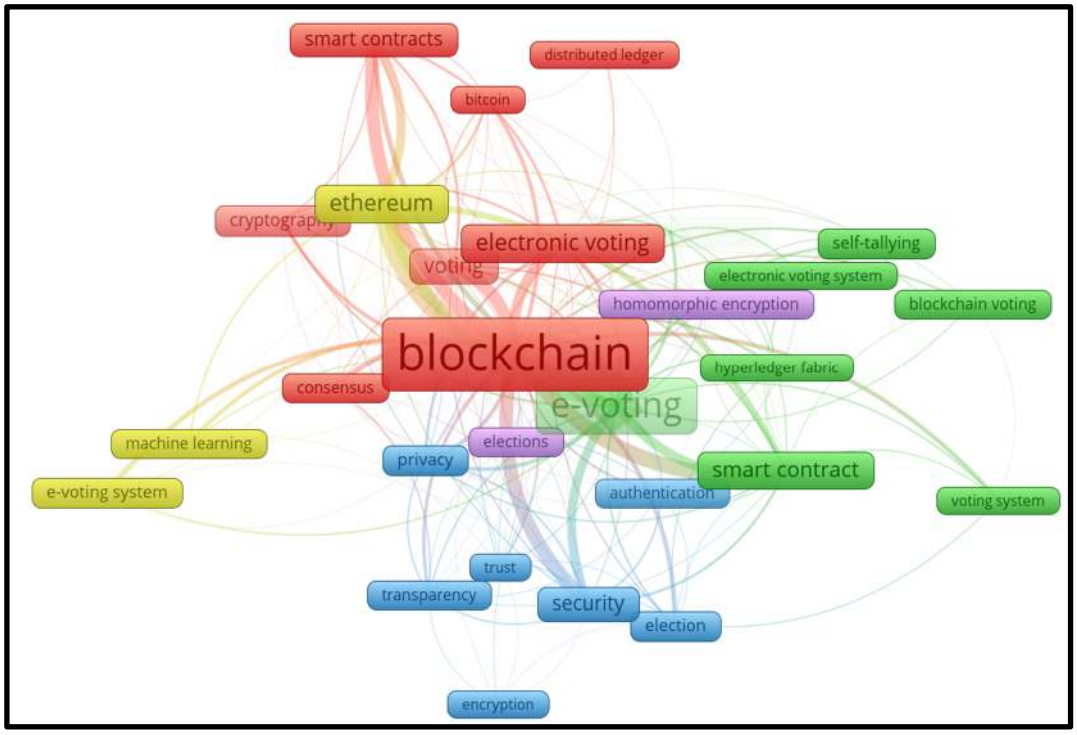


Figure 2-9: Bibliometric Analysis of Keywords

Further investigation of the literature found in **RQ1**, and the network diagram indicated the classifications presented in Table 2.6.

Table 2.6: Studies Classification

Studies	Approach	Methods	Constraints
(Cheema *et al.,* 2020a; Parmar *et al.* 2021a; Fezzazi *et al.,* 2021).	Private and public blockchains with machine learning and smart contracts.	Deep learning algorithms are employed to identify faces and match them to images from IDs/intrusion detection. Voter registration and vote collection are done through smart contracts on a private blockchain, while the public blockchain aggregates and reveals the vote count. Simulation: Web3 libraries, Python, and solidity remix is utilized.	High cost in the Ethers, low transaction throughput. Scalability issues, lack of internet connectivity, Limitations in the Ethers
(Wisessing *et al.,* 2020; Yu *et al.* 2018a; González *et al.,* 2022; Xu *et al.,* 2021; Vairam *et al.,* 2021; Angsuchotmetee *et al.*,2019).	Hyperledger Fabric, a permissioned blockchain.	The system connects the web application to a private Hyperledger Fabric blockchain to limit network security. The system uses the Paillier system for secret vote tallies. The system implements proof of knowledge to validate voters' ballots without exposing their choices. Linkable ring signatures used to ensure untraceable vote verification A Python application generates the system's randomized candidate and voter information, such as name, voter ID, and party	Applied on a smaller network and platform-based or dependent, e.g., Hyperledger. /Experiments were carried out in a pilot capacity as a model. • Scalability: The scalability of the Hyperledger Fabric network can be a limitation for large-scale elections. • Security: Hyperledger Fabric relies on the trust and integrity of the participating nodes. • Cost: Implementing and maintaining a Hyperledger Fabric network can be expensive.

Studies	Approach	Methods	Constraints
(Jagjivan *et al.,* 2021a; Sharma *et al.,* 2021a; Matile *et al.,2019*; Pandey *et al.,* 2019; Kumar 2014; Agbesi & Asante, 2019a; Srivastava *et al.,* 2018; Pawlak & Poniszewska-Marańda 2019; Ingouchi & Jain 2016; Lin & Zhang, 2019; Adiputra *et al.* 2019; Li *et al.,* 2021; H *et al.,*2020; Luo, 2021; Chaisawat & Vorakulpipat, 2020).	a blockchain-based digital voting system and SHA 256 Algorithm or cryptographic Hash function or non-interactive zero-knowledge proof	Blockchain architecture uses SHA-256 to provide security and anonymity. This one-way hash function ensures data validity and non-repudiation. / Every voter can verify that their encrypted vote reflects the choice chosen while retaining ballot privacy using the Zero-Knowledge proof. / Use HashCash variant VoteMaker and Proof of Work employs a nonce's SHA256 hash.	Limitations on steady internet connections and smartphone adaptation for handicapped and older populations, and used for small-scale voting
(Govinda *et al.,* 2021; Matile *et al.,2019*; Thuy *et al.,* 2019; Lyu *et al.*, 2019; Alvi *et al.,* 2020a; Panja *et al.,* 2020; Canessane *et al.,* 2019; Khoury *et al.,* 2019; Sadia *et al.,* 2020b; Shukla *et al.,*2018; Hjalmarsson *et al.,* 2018b; Abegunde *et al.,* 2021; Rao *et al.,* 2021; Tjahajadi *et al.,* 2018; Zhang *et al.,*2018; Hardwick *et al.,* 2018b; Al-Madani *et al.,*2020; Ruparel *et al.,* 2021a; Russo *et al.,* 2021).	Ethereum Blockchain and smart contracts	A smart contract, not the election administrator, does the tallying. The voting mechanism was implemented on Ethereum through Smart Contract. / Ethereum's blockchain technology with smart contracts was written in Solidity	High cost in the Ethers, low transaction throughput • Scalability: Ethereum has limited scalability, which may not be sufficient for large-scale elections. • Security: Smart contracts on Ethereum are vulnerable to various types of attacks. • Cost: Ethereum requires significant computing power and electricity to operate, making it expensive to run and maintain. • Interoperability: Ethereum may not be compatible with other blockchain platforms and applications.

Studies	Approach	Methods	Constraints
(Fernandes *et al.,* 2021; Othman *et al.,* 2021; Bartolucci *et al.,* 2018).	secret contract e-voting system based on the blockchain technology	The protocol SHARVOT is a blockchain-based secret voting mechanism used. The solution employs Shamir's Secret Sharing to allow on-chain votes submission and winner determination. / Blockchain e-voting with hidden contracts. The Enigma (a secure multiparty computation platform)./ secret contracts are used.	Computational costs affect design. Ethereum's computational cost is 'gas.'
(Han *et al.,* 2020; Zaghloul *et al.*, 2021; Alam *et al.,* 2018).	Consortium blockchain or Ethereum Blockchain and IoT	IoT devices like smartphones are used to conduct large-scale elections under the suggested plan. Ethereum and smart contracts are used as formal agreements for voting, so the contract is only fulfilled when the prerequisites are met.	Scalability: Ethereum has limited scalability, which may not be sufficient for large-scale elections. • Security: IoT devices are vulnerable to various types of security threats. • Cost: IoT devices can be expensive to purchase, install, and maintain. • Interoperability: IoT devices may not be compatible with each other or with other applications and systems.

Studies	Approach	Methods	Constraints
(Rathore & Ranga 2021a; Luo, 2021).	Blockchain and elliptic curve encryption	Remote voting does not require voters to prove their attendance at the polls by encrypting their vote with their public key and then again with their RKey before sending it to a permissioned blockchain.	• Scalability: The scalability of the blockchain network can be a limitation for large-scale elections. • Security: Elliptic curve encryption is vulnerable to certain types of attacks. • Cost: Implementing and maintaining a blockchain network and using elliptic curve encryption can be expensive.

Extensive research has demonstrated that integrating smart contracts on blockchain platforms can significantly enhance electronic voting by facilitating cost efficiency and providing new avenues to address scalability constraints (Taş & Tanrıöver, 2020a). However, most rely on the Ethereum blockchain and smart contracts, with other studies implementing Hyperledger Fabric and Ethereum with smart contracts, especially where public and private blockchains need to be used. Studies reviewed in this paper have also indicated using different cryptographies with different security levels. The crypto used ranges from elliptic curve encryption, SHA 256 algorithm, and homophobic to Non-Zero Knowledge Proof. A few studies also looked at using sidechains in blockchain technology to lower the computational cost (Tjahajadi, 2018; Alvi *et al.*, 2020b). The review found that the evaluation of most systems was limited to experimental settings and did not include real-world scenarios (Wisessing *et al.*, 2020; Yu *et al.*, 2018; González *et al.*, 2022; Xu *et al.*, 2021; Vairam *et al.*, 2021). Additionally, Ethereum's use of Ether imposes limitations and can lead to high costs, known as gas fees. The specific functionalities of a smart contract determine the amount of gas required for execution, which varies (Fernandes *et al.*, 2021; Bartolucci *et al.*, 2018). No Proof of Work is necessary since each node is involved in the contract transactions (Chepurnoy & Saxena, 2020). When using Proof of Work as a consensus method, the fastest solver of a computational problem can add a new block to the network (Lasla *et al.*, 2022). These studies only utilized simulations and prototypes.

RQ3 *What is the strength of the evidence in support of the different solutions?*

Many studies claim that utilizing smart contracts on a blockchain platform would have a significant impact on electronic voting by making it more cost-effective and allowing it to solve the scalability issues that currently exist in electronic voting systems (Jafar *et al.*, 2021;Ruparel *et al.*, 2021b; Alvi *et al.*, 2020b; Alvi *et al.*, 2021; Jumaa & Shakir, 2022; Dagher *et al.*, 2018). Therefore, the computational costs, denoted by gas units, are crucial to the completion and execution of transactions in the context of the Ethereum blockchain. They 'lubricate' the network, making it more efficient by reducing the amount of data sent and the computation required to process transactions (Jabbar & Dani, 2020). Reducing computational expenses is seen as a game-changing development in the blockchain community. The two most common types of consensus algorithms, "Proof of Work" and "Proof of Stake," benefit significantly from this (Mondal *et al.*,

2019). Energy consumption at high levels places a heavy burden on limited resources and increases the mining costs of blocks (Ankalkoti & Santhosh, 2017; Stoll *et al.*, 2019). Jabbar and Dani (Jabbar & Dani, 2020) asserts that any transaction that strains Ethereum's resources must cover the cost of processing that transaction. The final price depends on several factors. However, the calculation relies heavily on intensity, frequency, and willingness to pay. The gas price in Ethereum might change depending on the kind of smart contract and its features (Zarir *et al.*, 2021). Additionally, implementing a new solution could be viable if a smart contract's functionality is executed and consumes fewer gas units (a.k.a. gas usage). The amount of gas used is proportional to the processing power required for running functions in a smart contract, which developers can manage.

RQ4 *What implications will these findings have when creating a new solution?*

Several ways exist to improve the blockchain platform for a secure and transparent voting counting system. For example, we could consider using platforms such as Corda or Quorum, which are purposefully designed for this use case, instead of Hyperledger Fabric. Additionally, we could incorporate different cryptographic algorithms and protocols, such as homomorphic encryption or zero-knowledge proofs, to enhance the security and privacy of votes. Furthermore, developers can implement smart contracts in various programming languages, such as Rust and Go, recognized for their security and scalability. Moreover, other IoT devices, such as smart cards or voting machines, can provide added convenience and security to voters. Finally, the consensus mechanism, such as Proof of Stake or Eligibility, could be considered an alternative to Proof of Work or knowledge.

This review further suggests three combinations for a secure and scalable blockchain voting system, as outlined below:

1. Quorum, homomorphic encryption, and Go: In this combination, we would use the Quorum platform for the private blockchain and employ homomorphic encryption to ensure the privacy and security of the votes. Developers write smart contracts in Go, a powerful and efficient language for implementing blockchain applications. This combination provides a secure and transparent voting system, which is scalable and easy to maintain.

2. Corda, secret sharing, and Rust: In combination, we would use the Corda platform for the private blockchain and employ secret sharing to distribute and encrypt the votes securely and privately. Developers write Smart contracts in Rust, a safe and performant language well-suited for implementing complex and secure systems. This combination provides a secure and transparent voting system that is both robust and efficient.
3. Algorand, zero-knowledge proofs, and Scala or Pyteal: In combination, we would use the Algorand platform for the private blockchain and employ zero-knowledge proofs to verify the validity of the votes without revealing their content. Developers write Smart contracts in Scala, a powerful and expressive language well-suited for implementing complex and concurrent systems. This combination provides a secure and transparent voting system that is both fast and scalable.

In the second part of this ongoing research, we will implement the third combination by undertaking the following steps:

1. Install the necessary software and set up the Algorand network, including creating the required accounts and assets.
2. Develop a smart contract for the e-voting system using Algorand SDK and Scala programming language. This contract defines the rules and processes for voting, such as eligible voters, candidates, voting procedures, and the tallying of results.
3. Use zero-knowledge proofs. Pera Wallet / Zero-knowledge proofs are used to verify the validity of the votes without revealing their content. This can be done using a trusted setup, where the smart contract generates a public key and a private key, and the voters use the public key to encrypt their votes and the private key to verify the validity of the encrypted votes.
4. Deploy the smart contract to the Algorand network and test it to ensure it works as intended.
5. The Algorand blockchain explorer and other tools would be used to monitor and verify the transactions on the network and ensure that the votes are being recorded and counted correctly.

6. Use the Algorand API and other tools to integrate the e-voting system with external applications, such as voter registration systems, ID verification systems, and other components of the overall voting infrastructure.

In this case, the edge of a polling place's local network must implement non-relay nodes on the Algorand blockchain. Participating nodes, such as non-relay nodes, reach a consensus on the vote count, and they write the agreed vote count to the archived and indexed relay node that contains the primary blockchain ledger. A "full" node in a blockchain typically stores the entire ledger, which includes all transactions in each block. Archival nodes in Algorand serve the same purpose and store all ledger information (Huré-Maclaurin, 2020). This solution uses Internet resources at the network's edge only by election observers to write the vote count to the blockchain. All polling stations can verify that they have been accounted for by including their final vote count in the latest nationwide compilation of vote count results. Figure 2.10 illustrates this architecture of the proposed blockchain vote-counting artefact on the Algorand platform. The platform guarantees that nobody can modify the vote and enables individuals to verify that their vote has been incorporated into the national tally.

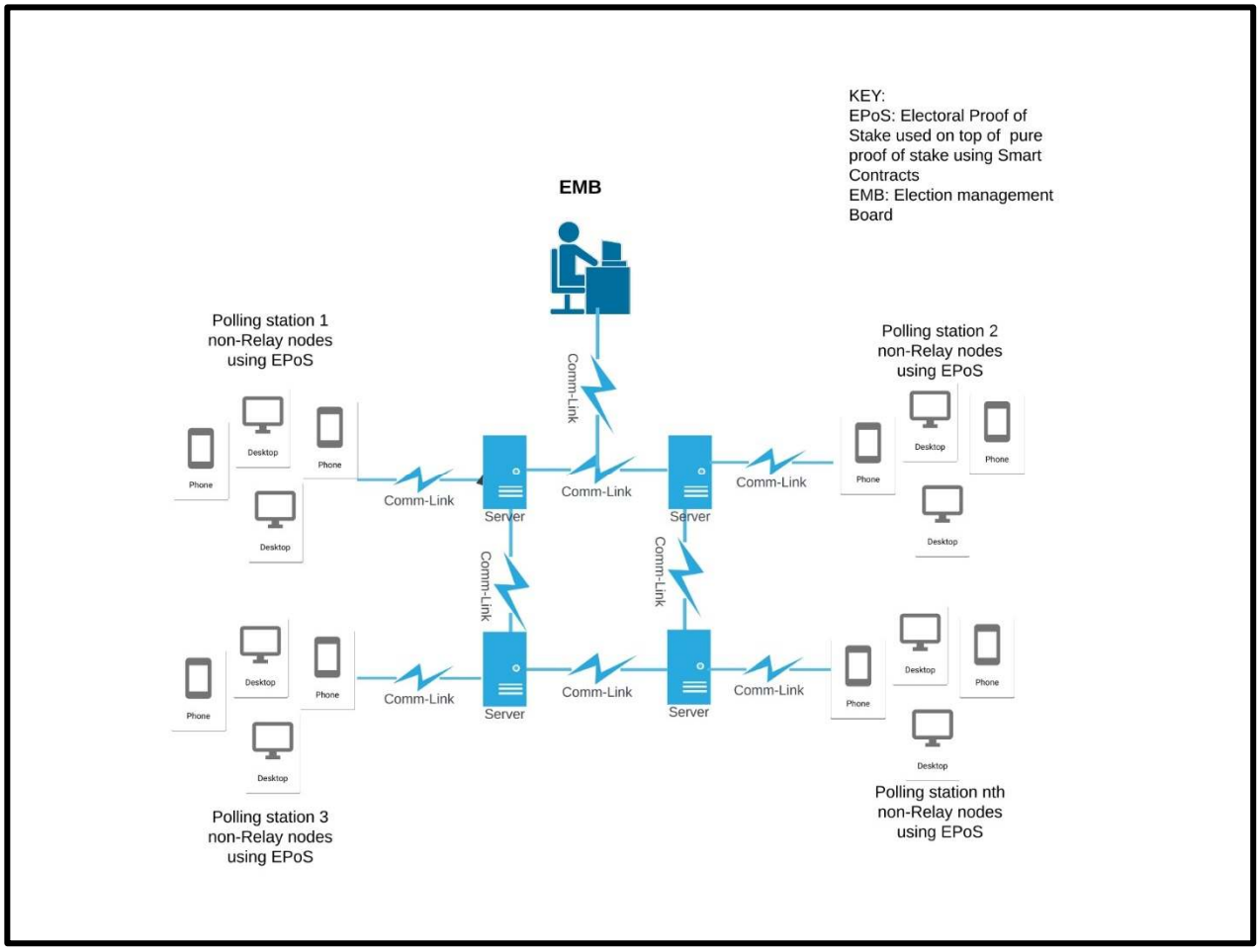


Figure 2-10: Proposed Blockchain-Based Vote Counting and Validation Architecture on The Algorand Platform

2.9.5 Threats to Validity

There are several potential risks associated with performing systematic mapping research. While searching for current blockchain vote-counting solutions, we took precautions to minimise exposure to hazards that would endanger our findings. Kosar *et al.*, (2018), assert that systematic mapping research cannot examine all scientific literature or information sources. This section outlines the problems that the team has identified, addressed, or acknowledged. The team mapped the search criteria and databases to eliminate this risk. The combination of criteria and logical operators helped to expand our scope. Our goal was to locate all pertinent papers using

various keyword combinations. Most studies that followed the exclusion and inclusion criteria were conducted between 2015 and 2022, despite the topic not being new. As a result, we do not expect our study's conclusions to be tainted by one absent article review. Unpublished or linked works not in our chosen scientific database posed a hazard in our setting. Internal validity is unaffected by omitted articles because the databases are well-known. We believe the information we gathered using research questions represents the current findings and recent developments in blockchain e-voting technology. They feature inferences from 2015 to 2022 and studies from various nations; therefore, they are relevant.

2.9.6 Conclusion

This review aimed to find and assess the recent existing literature on blockchain electoral vote counting solutions and how they compare with each other concerning methods, constraints, and approaches. This review presents a systematic mapping of e-voting solution research using blockchain technology. The study provided information on the existing blockchain electronic voting methods. The review identified a classification of blockchain e-voting systems implemented on Ethereum and ML, Ethereum and IoT, Ethereum and Hyperledger Fabric on private and public networks, and Sidechains on Ethereum. Most of these platforms use smart contracts for self-tallying votes. The cryptographic hashing used was elliptic curve encryption, SHA 256 Algorithms, Homophobic, Paillier encryption, proof-of-knowledge, and linkable ring signature, and included non-interactive zero-knowledge proof.

Nonetheless, these solutions are imperfect and provide room for improvement, and the review has suggested several potential combinations of platforms, cryptographic algorithms, and programming languages for implementing a secure and transparent voting system using blockchain. These include using Quorum and homomorphic encryption with Go, and Corda, secret sharing with Rust or Algorand and zero-knowledge proofs with Scala or PyTeal. Each combination provides a unique set of benefits and features, such as security, scalability, efficiency, and expressiveness, which can be tailored to the specific needs and requirements of the voting system.

2.9.7 Future Direction

This review identified several areas of study around blockchain and electronic voting that must be addressed in future studies. In the future direction of study, it would be interesting to investigate different combinations of platforms, cryptographic algorithms, and programming languages to implement a secure and transparent voting system using blockchain. For example, we could use Quorum and homomorphic encryption with Go, Corda, secret sharing with Rust or Algorand and zero-knowledge proofs with Scala. Each combination provides a unique set of benefits and features, such as security, scalability, efficiency, and expressiveness, which can be tailored to the specific needs and requirements of the voting system. Further research could explore the potential advantages and challenges of using different IoT devices, consensus mechanisms, and other technologies in the voting process. However, this ongoing research focuses on Algorand and zero-knowledge proofs using Scala.

2.10 A Reflection on the Systematic Literature Review

2.10.1 Blockchain in E-Voting: Scalability, Privacy and Governance

The accumulated systematic research in section 2.9 provides a comprehensive overview of the current state of blockchain technology in electronic voting systems. A study by Stančíková & Homoliak (2023) on SBvote shows a promising approach to scalable, self-voting blockchain-based voting and points out that scalability is possible but depends on the blockchain platform used. FASTEN, developed by Damle *et al.* (2021b), addresses privacy and fairness in electronic voting and ensures voter anonymity and security on the Ethereum blockchain. While Messias *et al.* (2023) point out governance issues with smart contracts, citing the disproportionate concentration of voting rights and prohibitive costs of participation for small players. In terms of scalability, Capretto *et al.* (2023) propose the setchain, which bypasses the need for full ordering in blockchains and potentially offers a faster sidechain solution for decentralised applications. Sonnino (2021) contributes by focusing on the practicality of blockchain and smart contracts, improving their scalability, latency and privacy through sharding and Byzantine Fault Tolerance.

2.10.2 Gap Analysis: Transition to real-world application

This study focuses on the implementation of the BBVV artefact on the Algorand blockchain platform, which has lower transaction fees at high throughput with PyTeal. This is tested on real election data to bridge the existing gap in moving from simulations to real-world applications, as most systems are evaluated in controlled environments that may not accurately reflect their performance in actual elections. The cost-effectiveness of blockchain solutions is also examined. As Fernandes *et al.*, (2021) and Bartolucci *et al.* (2018) emphasise, Ethereum's gas fees are a significant barrier to cost-effective adoption. Furthermore, discussion concerning the energy-intensive nature of Ethereum's Proof of Work consensus mechanism, suggests the need for more efficient alternatives such as Proof of Stake (Platt *et al.*, 2021).

2.10.3 Strength of evidence and implications for new solutions

The evidence for the use of smart contracts in electronic voting is solid. Several studies confirm their potential to improve cost efficiency and scalability. However, this evidence comes mainly from simulations and prototype testing, suggesting that there is a need for real-world deployment and testing. The implications for new solutions are clear: there is room for improvement in blockchain platforms for voting systems, with potential benefits in exploring platforms such as Corda or Quorum, different cryptographic algorithms, and programming languages for implementing smart contracts to improve security and scalability. The consensus mechanism is also crucial, with Proof of Stake offering a potential advantage over the traditional Proof of Work approach.

2.10.4 Impact of Blockchain Electronic Voting

The impact of blockchain technology on electronic voting systems has been the subject of extensive research, with the most recent studies focussing on its potential to improve the voting process. A study by Faour (2018) provides a comprehensive comparison between existing voting systems and blockchain-based alternatives, highlighting the benefits of blockchain in preserving voter privacy and election security. The study points to the decentralised nature of blockchain as a solution to many electoral challenges and offers a new mechanism for secure and transparent

elections. Despite the promising potential of blockchain for large-scale elections, the study also points to the current limitations of blockchain platforms such as Ethereum, which can only process a limited number of votes per minute, posing a challenge for scalability.

In another study, Gatteschi *et al.* (2018) examine the role of blockchain in reducing the complexity and costs associated with electronic elections. They argue that blockchain can simplify the process by providing a single, standardised method for recording and counting votes, which could potentially increase voter turnout due to the convenience and accessibility of blockchain-based systems. In addition, the authors discuss how the characteristics of blockchain, such as insensitivity to data changes, can help increase stakeholder confidence in electronic voting systems.

2.10.5 This Work and Future research directions

Future research should aim to deploy and test these blockchain-based voting systems in real-world election scenarios to validate their effectiveness. A comparative analysis of cryptographic techniques is necessary to determine the most efficient and secure methods for voting systems. In addition, a detailed cost-benefit analysis of smart contract functions could help to optimise gas consumption and reduce transaction costs. Finally, research into alternative consensus mechanisms could lead to a reduction in energy consumption and an improvement in transaction speed. By closing these gaps, future research can significantly contribute to the development of a robust, scalable, and trustworthy blockchain E-voting voting systems.

2.11 Summary of literature

A comprehensive literature review on existing blockchain-based electoral vote counting solutions, blockchain technology, and edge computing revealed that there is a considerable amount of research and practical applications of electronic voting systems using blockchain with cryptography-embedded trust systems. However, the literature revealed a scarcity of studies on computational offloading through the relocation of resource-intensive computing activities to edge devices. This approach aims to transfer activities such as validating the true vote count to edge devices, enabling faster computation and increasing trust in the results of electoral vote counting

and validation. The literature review also identified several areas of study around blockchain and electronic voting that will need to be addressed in further studies and indicated that, despite the potential of e-voting on certain blockchain platforms, the persistent challenge of achieving optimal balance among speed, security, and scalability remains an ongoing issue. Overall, this chapter served as a foundation for the research and provided a comprehensive understanding of the field of study by giving an insight into the various elements involved in the research of blockchain-based electoral vote.

Chapter 3 deals with the methodology of this study.

CHAPTER THREE: METHODOLOGY

3.1 Organization of the Chapter

This chapter deals with the philosophy and methodology of the research and begins with an 'Introduction' (Section 3.2). It then examines the 'Philosophical Perspective' (Section 3.3) and outlines the 'Aspects of Research Design' (Section 3.4), followed by a discussion of the ‘Research Questions and Objectives' (Section 3.5). The 'Research strategy' (section 3.6) and the 'Validity and reliability measures' (Section 3.7) are then discussed. The remainder of the chapter addresses the 'limitations and potential challenges' (section 3.8) and the reflexivity of the study (section 3.9). It concludes with a comprehensive summary (Section 3.10). This structure provides a clear and systematic overview of the basic approach and operational implementation of the study.

3.2 Introduction

Research questions and Objectives need the thorough formulation of a research plan (Blaikie & Priest, 2019). Data collection, processing, and analysis are all guided by the strategy. This chapter provides an overview and explanation of the research technique and procedures utilised to carry out this study. The research philosophies and paradigms employed in Design Science Research (DSR) are also discussed. The chapter then proceeds on to examine the DSR and how it was employed in this study after establishing and addressing the paradigms. In addition, a description of study ethics, data collection procedures, and sampling (selection of participants) methods is provided. This chapter also discusses and explains issues related to reliability and validity. All necessary and appropriate information about the study's methodology is found in this chapter.

3.3 Methodology

Methodology is the theoretical investigation of the procedures used in a certain area of research. It provides a guide for understanding the "how" and "why" of research, and it is used to help plan and structure research initiatives (Howell, 2013; Mullany & Stockwell, 2021). As an essential part of every academic work, methodology outlines the fundamental ideas and procedures that should

be followed when conducting research. To help determine the methodology for this study, research philosophy assumptions, ontology, epistemology and axiology are identified, described and justified in relation to the needs of this research.

3.3.1 Research Philosophy

The term "research philosophy" refers to a collection of beliefs about the nature of the reality under investigation, and the kind of research philosophy used in a particular field of study is determined by the type of knowledge being researched (Scotland, 2012 as cited in Kirongo & Odoyo, 2020). Research philosophy has been the subject of many papers and dissertations, in which four basic tendencies are identified and described: positivist, interpretivist, pragmatist, and realist (Žukauskas *et al.*, 2018).

Pragmatism's assumptions are a good fit for this investigation. When used as a research paradigm, pragmatism steers clear of arguing philosophical concepts that are contentious, such as truth and reality. Instead, it recognises the possibility that there may be a single or several realities that may be verified by scientific research (Creswell & Clark, 2007). In addition, pragmatism is predicated on the notion that researchers need to choose the philosophical and/or methodological approach that is most appropriate for the research issue that they are attempting to answer at the present time (Tashakkori & Teddlie, 1998 as cited in Kaushik & Walsh, 2019b). It is usually connected to mixed-methods or multiple-methods research, in which reality may exist in both singularity and many, and it is possible to classify it between positivism and constructivism for this reason. In their article Deng and Ji (2018) cited in van der Merwe *et al.*(2020) suggest that pragmatism is the underlying philosophy for DSR, but that it passes through multiple stages in which the researcher is active as an interpretivist, positivist, and constructive observer or intervener as illustrated in Figure 3.1.

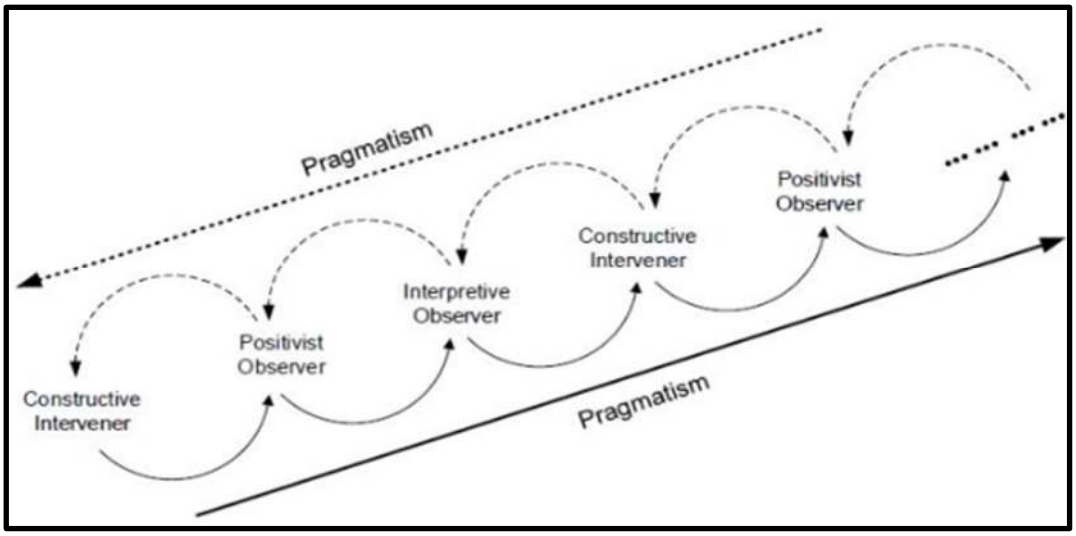


Figure 3-1: Iterative Design Science Process (Deng & Ji, 2018)

Realistic research philosophy is instituted on assumptions that are required to perceive human subjectivity. It is founded on positivist and interpretivist research concepts (Lancaster, 2007). Consequently, Interpretivism makes use of researchers' interpretation of study components, which helps to ground the research in people's real-world concerns. Therefore, interpretative scholars claim that one can only access reality (whether objective or socially created) via such social structures as language, awareness, shared meanings, and tools (Grossoehme, 2014).

Positivism is a philosophical position taken by natural scientists who work with observable reality in society to make generalisations. This is achieved by emphasising the significance of what is given in general, with a greater emphasis on pure data and facts that are not skewed by human interpretation (Scotland, 2012; Saunders *et al.*, 2012 as cited in Alharahsheh & Pius, 2020). Creswell affirms constructivism as based on the study of social discourse, which is documented with data collected through activities such as observations and interviews. It further attempts to discover worldviews, subjective meanings, and viewpoints within social situations and is reliant on the ideas and opinions of people being studied to guide the researcher in identifying patterns and themes (Creswell, 2014, p. 8 as cited in Bogna *et al.*, 2020).

This study used the methods that best suited the needs to design a Blockchain-based Vote-counting and Validation (BBVV) artefact in accordance with the pragmatist philosophy, which places a focus on the practical application of concepts and theories and their utility in solving real-world situations.

3.3.1.1 Ontology

The main objective of this research was to design a Blockchain-based Vote-counting and Validation (BBVV) artefact using symmetric cryptography, blockchain and edge computing to engender trust in the electoral vote counting and validating process. The truth we looked at was the vote count in an election, which always remains the same irrespective of the number of counting/ tallying we make at any given time. To answer the question, "What is reality?" When it comes to reality, ontological philosophy focuses on the differences between reality and our experience of reality, and how this affects everything in our environment (Abidi, 2011). Ontology encompasses the study of the categories, qualities, and interactions between things, as well as the nature of being, existence, or reality (Crotty, 2003). The accuracy of the vote count was established based on one single reality of truth from an ontological perspective.

3.3.1.2 Epistemology

The findings of this research were supported by a wide range of reliable sources of information, including quantitative and qualitative data. The emphasis of epistemology is on how we can recognise, define, and know for sure that the information obtained because of the research study is reliable (Robinson, 2007). Within the scope of this investigation, the pragmatic method was used. Artefacts were constructed and analysed, and the quantitative findings from practical system testing were utilised to arrive at a single truth, which was that the aggregated vote count from an election which is always singular in its nature. In addition, a qualitative method was used to collect input on the system specifications and requirements needs from customers and stakeholders before and throughout the actual development process using an iterative design approach. This was done before the real development began. Because of this, the researcher used a hybrid methodology that included both inductive and deductive reasoning.

Patterns and themes can be identified through Inductive and deductive reasoning. According to Giddings and Grant (2006), inductive reasoning, which is mostly used in qualitative research, has limits in that the research's validity is debatable. Deductive reasoning, on the other hand, which is largely based on the quantitative study, yields numerical proof that is not applicable. As a result, a combination of reasoning techniques is frequently required to enable comprehensive research, and it may be viewed as a creative and adaptable strategy to solve a wide range of research challenges (Giddings & Grants, 2006 as cited in Park *et al.*, 2020)

3.3.1.3 Axiology

Axiologically, this research was two-sided, value-free/biased in that the researcher took the stance of objectivism and subjectivism where necessary as a pragmatic approach. When it comes to conventional research goals such as finding the truth or understanding, design scientists place a higher priority on the ability to creatively manipulate and control their surroundings. In contrast to positivist researchers, designers must be willing to embrace significantly more uncertainty in their work (Vaishnavi & Kuechler, 2004). Accordingly, it is possible that the final product of a design science research project may be poorly understood by the community and yet be deemed a success (Hevner *et al.*, 2004). Successful projects may just need the codification and dissemination of a useful or functional contribution to an existing body of knowledge (Gregor & Hevner, 2013), even if it is only a partial or unfinished theory. Table 3.1 shows the adopted philosophical assumptions for this study. Saunders *et al.*, (2009) research philosophical contrasts between different approaches to inquiry relative to ”Ontology ‘the nature of reality’, Epistemology ‘the acceptable knowledge’, Axiology ‘the role of values in research’, and data collection techniques” and from Vaishnavi & Kuechler, 2004 cited in van der Merwe *et al.*, (2020), philosophical assumptions in DSR, this research has adapted a philosophical perspectives under pragmatism assumption that fits to this study as illustrated in Table 3.1

Table 3.1: Adapted Research Philosophy for The Study (Saunders *et al.*, 2009; Vaishnavi & Kuechler, 2004 cited in van der Merwe *et al.*, 2020)

Concept	Pragmatism
Ontology	External, multiple, view chosen to best enable answering of research question. **(Single reality of truth, the vote count)**
Epistemology	Either or both observable phenomena and subjective meanings can provide acceptable knowledge dependent upon the research question. Focus on practical applied research, integrating different perspectives to help interpret the data. **(Both observable phenomena and subjective meanings)**
Methodology	Developmental, Measure artefactual impact on the composite system
Axiology	Values play a large role in interpreting results, the researcher adopting both objective and subjective points of view. **(two-sided, value-free/biased)**
Data Collection	Mixed or multiple method designs, quantitative and qualitative.

3.4 Research Design

3.4.1 Conceptual Framework of the research

The research's conceptual framework is depicted in Figure 3.2. There are four main stages to this research. The first phase entails collecting Electoral Proof of Stake (EPOS)/ Electoral officials' data and other requirements. This focuses on choosing and involving appropriate stakeholders and methods of data collection and storing for system development usage. Phase 2 involves the use of consensus algorithms/ BBVV protocol based on the Byzantine Theory to agree and authenticate the legitimate vote count on the edge of the network using a permissioned blockchain, the legitimate vote count is then written to the blockchain for national vote aggregation and further, using cryptography keys the validation by EPOS to ascertain if their vote was counted when the national tally is done. This creates trust to produce the true vote count. Phase 3 involves testing correctness of the output and scalability of the system including validating the prototype by testing

on controlled and uncontrolled environments. Phase 4 includes evaluating the system with existing Electoral Voting Systems. Phase 1 and 2 can be viewed under the BUILD stage of DSR, and Phase 3 and 4 fits under the Evaluation phase of DSR. The Byzantine Theory was used in phase 2.

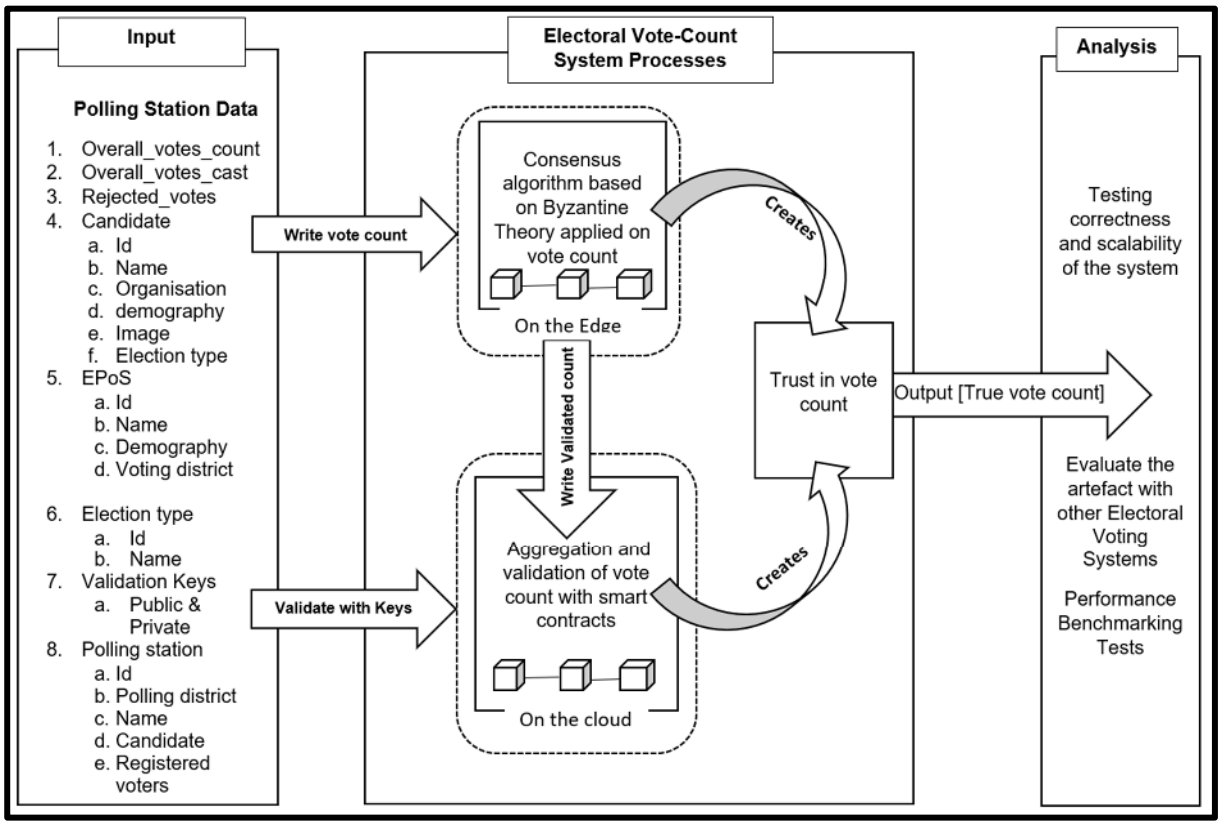


Figure 3-2: Conceptual Framework of The Research

3.4.2 The types of Research from different viewpoints.

Kumar (2014) classifies research into three perspectives, ‘mode of enquiry' viewpoint categorising research kinds based on the many philosophies that underlie them, whereas the 'application' and 'objectives' viewpoints examine research categorisation from the position of uses and purposes. Figure 3.3 illustrates the types of research from a different viewpoint.

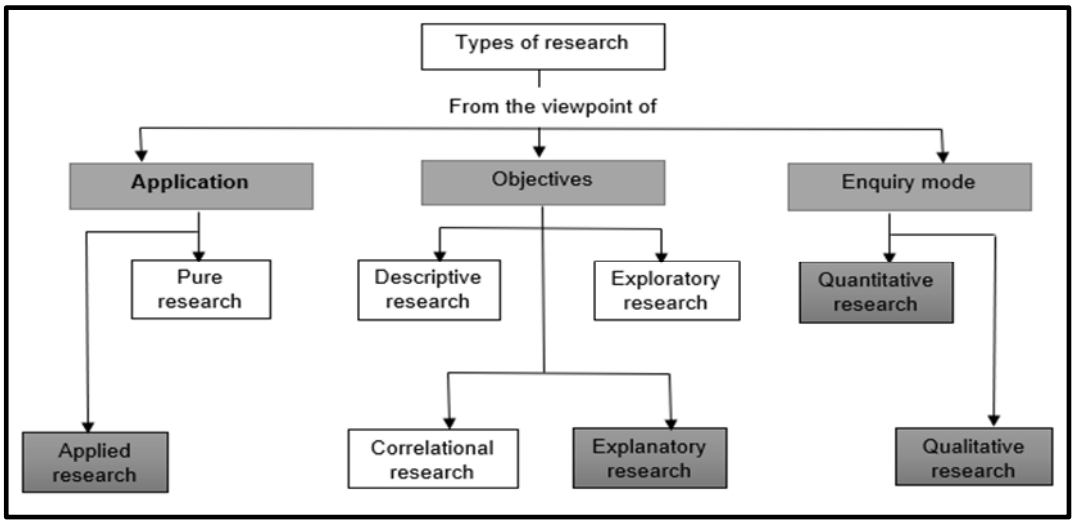


Figure 3-3: Types of Research (Kumar, 2014)

3.4.2.1 Viewpoint of application

This study falls under the category of applied research. Applied research is pragmatic in nature and aims at generating new knowledge that contributes to theory with Its main goal of collecting and generating data to help us better comprehend real-world challenges (Guest *et al.*, 2013:2).

3.4.2.2 Viewpoint of objectives

This study will fit into the explanatory research type. Explanatory research seeks to explain the why and how, parts of an event or phenomena correlate (Kumar, 2014). The projected system's success could assure ‘why’ electoral vote-counting should be validated and ‘how’ the validation should be done to allow contending parties agree on one result.

3.4.2.3 Viewpoint of enquiry

Pragmatic research includes mixed methods approach mode of enquiry. Therefore, a quantitative, or structured approach strategy will be used to collect data to test for correctness, and scalability of the system, while qualitative data will need to be collected at formulating the specification and

requirements of the system during the problem definition in DSR methodology indicated in Figure 3.5.

3.5 Research Questions, Aim and Objectives

3.5.1 Aim of the research:

Main aim: To develop a blockchain-based vote counting and validation (BBVV) artefact using symmetric cryptography, blockchain and edge computing to increase trust in the process of vote counting and validation in elections. This is the overarching goal. It sets the general direction of this research and focuses on increasing trust in electoral processes through technological innovation.

3.5.2 Research Objectives:

Objective 1: To review and identify existing blockchain solutions for voting systems.

Objective 2: To elicit the necessary system specifications for developing a BBVV artefact that exhibits high-performance features and engenders user trust.

Objective 3: To identify an appropriate blockchain protocol that supports trusted vote aggregation and includes a suitable consensus algorithm for vote count validation.

Objective 4: Develop the BBVV artefact for vote counting and validation and evaluate its performance features to handle maximum load, minimise delays, process high transaction volumes, and foster user trust through traffic analysis.

These objectives break down the goal into specific, actionable steps. Each objective is designed to systematically address a component of the overall goal, ensuring a comprehensive approach to achieving the research objective.

3.5.3 Research questions:

Main research question: What approach can be used to design a blockchain-based vote-counting and validation artefact that engender trust in an electoral voting process?

Sub-questions:

1. What are the existing blockchain solutions adopted in electoral vote systems, and how have they addressed their respective challenges?
2. What are the critical specifications and features required for a BBVV artefact to achieve high performance and secure user trust?
3. Which blockchain protocol best supports trusted vote aggregation and offers an optimal consensus algorithm for vote count validation?
4. How effective is the developed BBVV artefact in vote counting and validation, and to what extent do its performance features engender trust among users?

The research questions are directly aligned with the objectives. Each sub-question corresponds to an objective and provides a focused enquiry to guide this research activities. The main question summarises the overall research question and links it to the research main aim.

3.6 Research strategy

This study falls under Design Science Research, studying ways to solve real-world problems by creating new artefacts has been labelled "design research," or "design science research," according to studies on research methodology. Hevner *et al.* (2004 cited in Peffers *et al.*, 2007), claim there are seven principles describing the features of well-executed research which are presented as guidelines for performing DS research in the IS field. The most essential is that the study must generate an “artefact created to address a problem”. In addition, the artefact must be related to the accomplishment of a “heretofore unsolved and important business problem” with “utility, quality, and efficacy” evaluations must be thorough. Both the creation of the artefact and its assessment must be conducted with rigour if the study is to have any credibility. Developing an artefact should be a quest for answers to a specific problem, drawing on existing ideas and

expertise. Finally, findings from the study need to be successfully disseminated to the right audiences. With the help of this study, we were able to create and test a brand-new concept artefact on a more manageable size as a prototype.

3.6.1 Design science research (DSR)

In this research, a design science of build and evaluate through test-driven approach was used. The creation and deployment of the designed artefact achieve knowledge and comprehension of a problem domain and its solution under the design-science paradigm. Design science is concerned with the creation and assessment of artefacts that are intended to suit a specific business requirement (Hevner *et al.*, 2004).

Generally, Identify, Design, Develop, and Test (IDDT) are the four main stages of DSR that are often used in practise. This can also be deduced from Figure 3.4 where Vaishnavi & Kuechler (2004) illustrate how a DSR project progresses via cycles of awareness, suggestion, development, evaluation, and conclusion. As a departure point for development, assessment, and conclusion, the knowledge or theory contribution is depicted on the left as a circumscription. In addition, they believe that the outputs for each step include the proposal during the awareness phase, the preliminary design during the suggestion phase, the artefact during the development phase, performance metrics for the evaluation phase, and finally the outcomes in the conclusion.

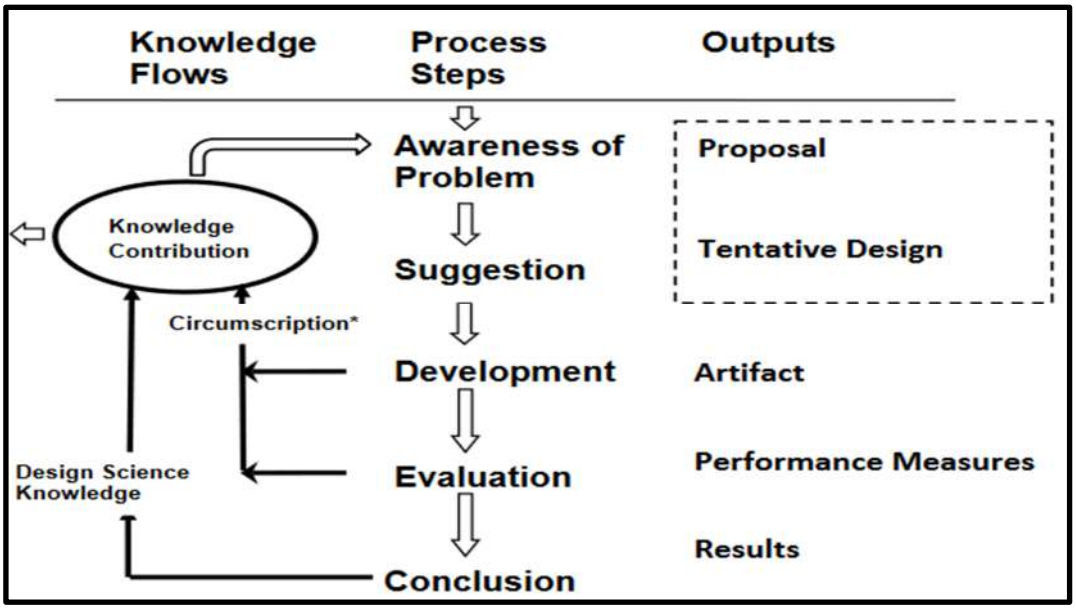


Figure 3-4: DSR Process Model (Vaishnavi & Kuechler, 2004)

According to Gregor & Hevner (2013) “In IS, DSR involves the construction of a wide range of socio-technical artefacts such as decision support systems, modelling tools, governance strategies, methods for IS evaluation, and IS change interventions.” With the design-science paradigm the human and organisational margins are extended by designing new and innovative artefacts this may be done through the build and evaluate activities methodologies as shown in Figure 3.5.

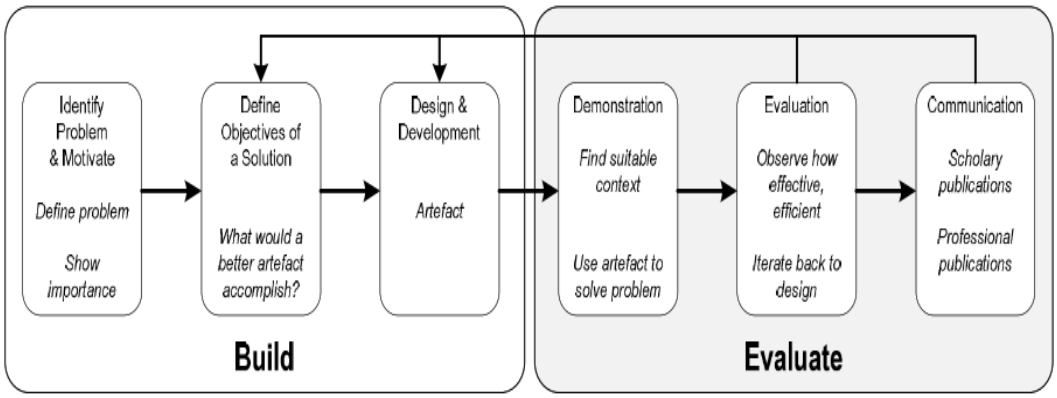


Figure 3-5: Build and Evaluate Methodology (Peffers *et al.*, 2007b)

Figure 3.5 includes the build and evaluate stages in DSR that the BBVV will undergo through its development up until release of the artefacts. The build phase will include information gathering from the customer (customer in this case implies the other party that issues a mandate to develop the system e.g., Electoral commissions) and other stakeholder to properly define the problem and specification requirements. The artefacts will be designed and developed in the build phase. The artefacts demonstration to the customer and stakeholders to test for correctness and scalability will be done in the evaluation stage. Iterative design when off-specifications arise is also part of this stage. The specific steps that were implemented are as follows:

1. Obtain and configure the necessary software to establish the Algorand network, including the creation of accounts and assets.

2. Utilize the Algorand SDK and the PyTeal programming language to design and develop the smart contract for the e-voting system, which will dictate the guidelines and procedures for voting, such as voter eligibility, candidate selection, voting process, and counting of results.

3. Implement authentication proofs to confirm the authenticity of the votes without exposing their contents. This can be accomplished by setting up a trusted system, in which the smart contract generates a public and private key, allowing voters to encrypt their votes using the public key and verify their validity with the private key.

4. Deploy the smart contract on the Algorand network and test it to ensure proper functionality.

5. Use the Algorand blockchain explorer and other tools to oversee and confirm the transactions on the network, ensuring that the votes are being recorded and tallied correctly.

6. Utilise the Algorand API and other tools to integrate the e-voting system with external systems, such as voter registration systems, ID verification systems, and other elements of the overall voting infrastructure.

3.6.2 Sampling and Data Collection

This research adopted the multistage sampling technique. According to Burger & Silima, (2006), in a multistage cluster sampling two or more phases or steps are typically sampled in the majority of cases. It's unlikely that the researcher will be able to gather data from all the instances. Thus, a sample must be chosen. The population is the whole collection of cases from which a researcher's sample is taken. Due to a lack of both time and resources, researchers use sampling techniques to decrease the number of instances studied (Taherdoost, 2018). Multistage sampling technique was appropriate for this study because the population (African continent) was too large to study in its entirety, and therefore, the necessity to select a representative sample of the population to test the BBVV artefact.

The data collection process for this study was conducted on the African continent, with a focus on democratic nations. The continent was divided into five clusters: North, West, Central, East, and Southern Africa. In order to ensure a representative sample, clusters that lacked countries with fully developed democratic systems were removed from the sample selection process. Additionally, countries that do not have a history of mature democracy for at least 27 years were also excluded. Generally, countries with a history of democratic rule for at least 27 years tend to have more developed and institutionalised democratic systems, which are associated with increased stability and reduced risk of democratic breakdown.

In the context of this study, the inclusion of only countries that have a history of mature democracy for at least 27 years in the sample selection process is a sound decision that increases the likelihood of obtaining a sample that represents stable democratic nations on the African continent. From each of the designated clusters, a randomly selected democratic country that met the study's requirements was chosen. Within each of these countries, two constituencies with a minimum of

two polling stations were randomly selected. This process is illustrated in Figure 3.6. The use of a multi-stage sampling technique, starting with the cluster level and then proceeding to the country and constituency level, ensured that the sample was representative of the population of democratic nations on the African continent.

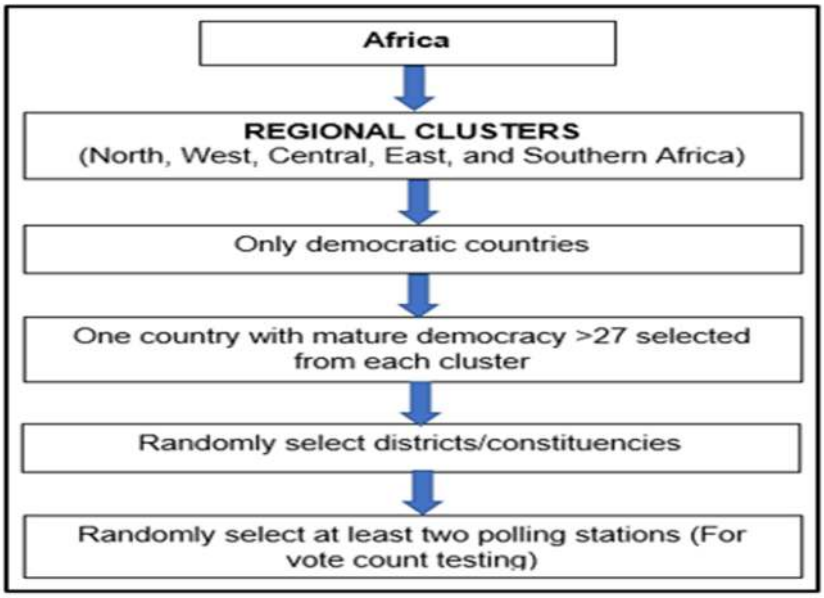


Figure 3-6: Multistage Clustering Sampling

The data for this study was initially obtained through the application of a systematic literature review method. This involved conducting a comprehensive search for relevant literature using a variety of databases, such as IEEE, Google Scholar, and other relevant sources. The search was guided by a pre-established research question, and the literature identified through the search was screened for inclusion criteria. Data was extracted from the studies that were deemed relevant and met the inclusion criteria. Subsequently, a questionnaire was utilised to gather qualitative data. Finally, historical, and past national election results were also analysed as a part of the data collection process. This provided a broader and historical context to the study and helped to test the artefact on transactions for correctness in the vote count.

A questionnaire was used to gather system requirements from randomly selected Electoral Commissions. Requirement's elicitation/gathering is a thorough and exhaustive procedure for

eliciting information from all stakeholders about the artefact to be developed. This involves collecting the needs of a system through meetings, interviews, questionnaires, brainstorming sessions, and prototyping (Ramdhani *et al.*, 2018). The qualitative data was needed to be collected for formulating the specification and requirements, which ranged from functional, non-functional, and domain requirements during the problem definition in the build phase of DSR methodology shown in Figure 3.5. Questionnaires were used in this study. System initialisation data such as aspiring candidates id, name, organisation, election type and eligible voter's details (id, name, demography, voting district etc) was collected from simulated aspiring candidates (simulated aspiring candidates in his context implies randomly selected eligible EPOS) and different cohorts of eligible voters in different locations. Additionally, election type by id, name, and polling station information (id, polling district, name of candidates and registered voters) were captured from existing gazetted electoral forms.

The Electoral Commission supplied historical quantitative data on past election results that were procured from various electoral districts and designated polling stations as a test dataset to assess the validity of the vote counting system. Furthermore, scalability testing was conducted in different contexts, which included laboratory simulations and application of real-world election data for evaluation purposes. The alignment between the research question, objectives, and data collection methods can be discerned in Table 3.3.

Overall, a multi-method approach was adopted in this study to obtain data, including the use of systematic literature review, structured interview schedules, and an analysis of historical and past national election results. This approach allowed for a more comprehensive and holistic view as a pragmatist.

3.6.3 Data Analysis and Artefact Evaluation

In this study, the quantitative approach was utilised to evaluate the system performance through system tests. The data obtained was then utilised as input for the artefact in order to validate the accuracy of the true vote count. Additionally, qualitative information was collected and analysed using Atlas.ti software, which specialises in qualitative data analysis. The purpose of this

qualitative analysis was to assist in specifying and achieving the system specifications necessary for successful system performance.

Creswel (2008) posits that quantitative data analysis involves the process of converting raw numerical data into meaningful information. This can be achieved through various methods, such as calculating the frequency of variables and interpreting the results through logical and critical reasoning. On the other hand, qualitative research primarily focuses on non-numerical data and the interpretation of the researcher's observations in order to identify patterns of behaviour and underlying meanings (Meyer *et al.*, 1983). In the current study, the quantitative data was segmented and organised into categories by province, district, and constituency. Subsequently, the data was transformed into anonymous pseudonyms, as illustrated in Table 3.2.

Table 3.2: Data Classification

PROVINCE_CODE	PROVINCE_NAME	DISTRICT_CODE	DISTRICT_NAME	CONSTITUENCY_CODE	CONSTITUENCY_NAME	FEMALECOUNT	MALECOUNT	TOTAL COUNT
101	xxxxx_01	101001	YYYY_01	1010001	zzzz_01	28746	25040	53786
102	xxxxx_02	101001	YYYY_02	1010002	zzzz_02	25453	23580	49033
103	xxxxx_03	101002	YYYY_03	1010003	zzzz_03	21343	19289	40632
104	xxxxx_04	101003	YYYY_04	1010004	zzzz_04	14879	11720	26599

In order to validate the accuracy of the data validity and performance testing was conducted on the artefact in question. This testing aimed to assess the transaction throughput, saturation, traffic, and performance of the system, as well as its usability and usage. The tests included benchmarking and code usage evaluations. The results of this testing were then used to inform future developments, upgrades, or modifications to the system. Additionally, during the testing phase, the aggregate vote count from various polling stations was compared and validated against the actual individual polling station results.

This research employed the Framework for Evaluation in Design Science (FEDS) suggested by Venable *et al.* (2016). According to Venable *et al.* (2016), FEDS evaluation design process, is utilised to guide design science researchers in developing a strategy for evaluating the artefacts they develop within a DSR project, it comprises of four steps. The first step is to explicate the

goals of the evaluation. The second step involves choosing the evaluation strategy or strategies. The third step is to determine the properties to evaluate, and the final step is to design the individual evaluation episode(s). Furthermore, the author adds that Design Science Research (DSR) utilises two types of evaluation activities, namely formative and summative evaluations. Formative evaluations are employed to assess the progress of a project and provide feedback for further development. They serve the purpose of identifying areas of improvement and ensuring that the project is on track to meet its goals. On the other hand, summative evaluations are used to judge the extent to which the outcomes of a project match expectations. They are employed to certify that the project has met its goals and to provide evidence that the process was effective.

The two-dimensional characterisation of DSR evaluation episodes, as shown on the x and y axis of the FEDS Framework in Figure 3.7, consists of the functional purpose of the evaluation and the paradigm of the evaluation. The functional purpose of the evaluation refers to the type of evaluation, whether formative or summative, while the paradigm of the evaluation refers to the method used to conduct the evaluation, whether artificial or naturalistic.

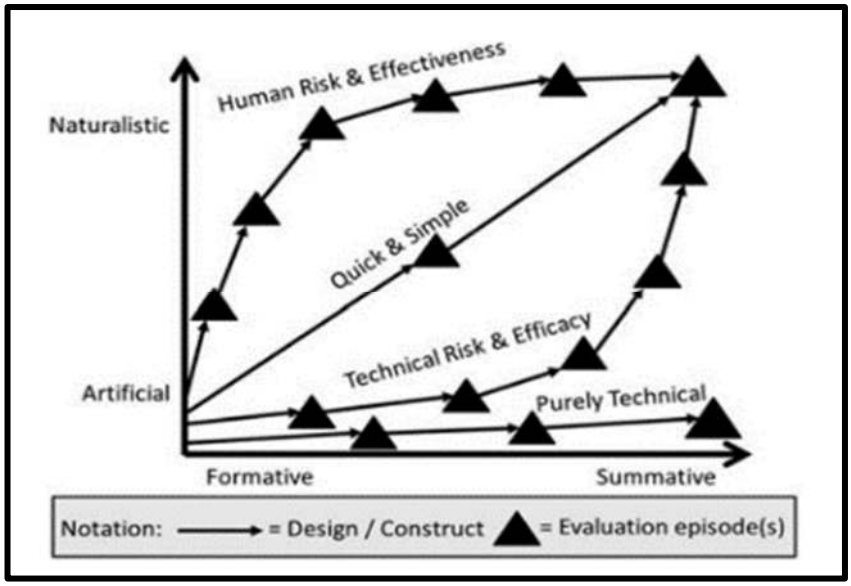


Figure 3-7: FEDS (Framework for Evaluation in Design Science)(Venable *et al.*, 2016)

The FEDS evaluation design process was applied to a Blockchain-based vote counting and validation artefact as follows:

1. Explicate the goals of the evaluation: The goals of the evaluation for this artefact included assessing the accuracy and security of the vote counting and validation process, as well as the feasibility of implementing the artefact in a real-world voting scenario.
2. Choose the evaluation strategy or strategies: In order to evaluate the accuracy and security of the vote counting and validation process, we chose an artificial evaluation strategy such as a simulated voting scenario, where test votes are cast and counted using the artefact. A naturalistic evaluation strategy, such as a pilot study in a real-world voting scenario, was used to assess the feasibility of implementing the artefact.
3. Determine the properties to evaluate: The properties to be evaluated included the accuracy of vote counting, the security of the vote validation process, the transparency of the vote counting process and the feasibility of implementation of the artefact in a real-world scenario.
4. Design the individual evaluation episode(s): The evaluation episodes involved creating a simulated voting scenario to test the accuracy and security of the vote counting and validation process and conducting a pilot study in a real-world voting scenario to assess the feasibility of implementing the artefact. The evaluation included measures such as comparing the test votes counted by the artefact to the expected results, analysing the transparency of the vote counting process, and measuring the ease of use for voters and vote counters.

The above analysis and evaluation approach is important because it allows for a comprehensive evaluation of the system performance. By utilising both quantitative and qualitative methods, a more complete understanding of the system can be obtained. The quantitative approach allows for objective measurements of the system performance through system tests, while the qualitative approach provides a deeper understanding of the user experience and system usability. The use of specialised software such as Atlas.ti for qualitative data analysis ensures that the data is properly analysed and interpreted. Additionally, the use of code usage evaluations and benchmarking in the testing process, along with comparing the aggregate vote count from various

polling stations with the actual individual polling stations results, increases the validity of the data and the confidence in the system. This approach helps to identify any issues with the system and inform any necessary modifications for future developments.

3.6.4 Research ethics

The Cape Peninsula University of Technology Research Ethics Committee had required a completed research ethics form when the study proposal was submitted for review. The dangers to the participants, as well as to everyone else, had to be explicitly emphasised. The university's strict guidelines were met by the study proposal. The research was conducted in accordance with the ethics form's specified protocols. It was apparent to all participants what the research was all about and what they were expected to accomplish. This group was made aware of the possibility of withdrawing from the research at any moment, and that the data obtained would be subject to a mutual decision. Confidentiality was protected by using pseudonyms and not revealing the identities of the participants without their consent.

Bazerman & Gino (2012) describe ethics as a behavioural approach of studying the systematic and predicted behaviour of people who reach ethical conclusions and judgements about others that contradict with the institution and with society as a whole. The data provided by the Electoral Commissions was cleaned (omitted names and identification numbers) in order to protect respondents' private information. Electoral Commissions and Cape Peninsula University of Technology signed an agreement ensuring the privacy and confidentiality of all data.

3.7 Validity and Reliability of the Study

Reliability refers to the consistency with which a measure produces results, while validity refers to the ability of questionnaires to measure exactly what they are intended to measure (Wallace & Sheldon, 2015) . The concept of trustworthiness refers to the level of confidence in the data, analysis and methods used to ensure the quality of the study (Denise F. Polit, 2010). There is a general consensus among researchers about the importance of trustworthiness in research, but there is an ongoing debate in academic circles about the specific criteria that define trustworthiness (Leung, 2015) .

Although the trustworthiness of mixed methods research is not universally recognised, there are strategies to enhance the credibility of this type of research (Shenton, 2004). It is also important to recognise that the validity and reliability of the data obtained depends on the way in which the research questions are formulated and the extent of pilot testing conducted (Saunders *et al.*, 2016). In relation to questionnaires, ensuring validity means checking that the questions are coherent and relevant to the specific nature and objectives of the study.

In this research, we focused on the development of a blockchain-based vote counting and validation artefact (BBVV). Several important steps were taken to ensure the validity and reliability of the data, all underpinned by a pragmatic philosophical approach.

1. Firstly, a mixed methods approach was utilised, integrating both qualitative and quantitative research methods. This involved distributing a questionnaire to gain qualitative insights and systematic power testing for quantitative data. The use of this triangulation method contributed significantly to increasing the validity and reliability of the research findings.
2. The development of the BBVV artefact was approached in an iterative process. Each iteration of the artefact was rigorously tested to assess its performance and trustworthiness. These iterative tests were significant to ensure that the artefact was reliable and valid for practical use in real-life voting scenarios.
3. Stakeholder engagement was another important aspect of the research process. Feedback was actively sought from a wide range of stakeholders, including election officials, IT experts and potential users. This involvement was essential to ensure that the artefact met practical requirements and was perceived as trustworthy, increasing its overall validity and reliability.
4. In terms of technical development, a thorough analysis was conducted to determine the appropriate system specifications and blockchain protocols for the BBVV artefact. This analysis was based on thorough research and adherence to industry standards, which contributed significantly to the technical validity and reliability of the artefact.

5. Experimental testing of the developed artefact was an important part of the research. These tests provided quantitative data on the artefact's performance and proved its reliability and effectiveness in counting and validating votes.
6. A comparative analysis was also conducted in which the BBVV artefact was compared to existing blockchain solutions in voting systems. This comparison, based on experimental data and robust analytical methods, served to confirm the effectiveness and reliability of the BBVV artefact.
7. Detailed documentation and a transparent methodology were maintained throughout the research process. This approach not only facilitated replication and verification but was also critical to the trustworthiness and credibility of the research.
8. Ethical considerations, particularly in relation to data protection and security associated with electoral processes, were strictly adhered to. Compliance with these ethical standards and legal requirements played a crucial role in improving the credibility and reliability of the research findings.
9. Finally, the artefact was designed to be adaptable to different electoral systems and contexts. This adaptability has proven the validity and reliability of the artefact in different scenarios and is consistent with the pragmatic emphasis on context sensitivity.

To summarise, these steps guided by a pragmatic philosophy ensured a comprehensive and robust research approach that emphasised practical outcomes, methodological flexibility and a mix of research methods. This approach was instrumental in ensuring the validity and reliability of the data and overall research findings.

3.8 Limitations and Potential Challenges

This research used both pragmatism and design science as essential elements in the research process. The researcher acknowledges that both the chosen research methodology and philosophical approach possess their own unique limitations and potential challenges. It is necessary for the researcher to be aware of these limitations and challenges in order to effectively address them and ensure the validity and reliability of the research findings. Pragmatism research philosophy is characterised by its focus on solving practical problems and its emphasis on the use

of multiple methods. However, one limitation of pragmatism is that it may not be able to provide a comprehensive understanding of a phenomenon due to its focus on practicality. Additionally, pragmatism may not always be able to generate generalisable knowledge, as the results are often context dependent (Thompson, 1996 as cited in Kaushik & Walsh, 2019). In pragmatism, the integration of quantitative and qualitative research methods in the social sciences presents a significant challenge for researchers. The divergent goals, data collection techniques, and analysis processes of these two methods often make it difficult to effectively combine them. Achieving a harmonious balance between the two requires a high level of skill and experience. Furthermore, the use of methodological pluralism, which involves the utilisation of multiple methodologies, presents additional challenges in terms of effectively managing and synthesising the various elements in order to produce meaningful results (Sobia *et al.*, 2018).

According to Stoeckli *et al.*, (2017) Design Science Research strategy is a field in which the lack of guidance regarding the evaluation of research contributions has resulted in a focus on building rather than evaluation activities. This has led to researchers dedicating insufficient time and effort towards assessing their work prior to presenting it for review by experts in the field. Furthermore, researchers in Design Science often fail to disclose changes made during artefact development, which could provide valuable information for others seeking to replicate similar experiments or build upon existing knowledge.

The paper of Cater-Steel *et al.* (2019) delves into the various challenges that are inherent to Design Science Research (DSR) with the aim of identifying ways to mitigate them. One significant challenge identified is the lack of understanding and appreciation for the underlying philosophy of DSR among scholars, which can lead to inadequate use of relevant guidance when conducting projects. Another challenge that is highlighted is the difficulty in theorising about the work due to issues of scoping or time constraints. Additionally, the paper also addresses the confusion that exists over whether DSR should be considered a paradigm or methodology. Finally, the paper notes the inconsistency in the use of nomenclature within DSR, which can hinder effective communication and understanding of research findings.

Design Science Research (DSR) poses various challenges that need to be mitigated in order to ensure that future scholars can create artefacts that are valued within their environments and

make significant contributions to the knowledge base of computer science. One effective way to address these challenges is through the provision of adequate resources and training for DSR scholars. Furthermore, the IS community should strive for consistency in nomenclature within DSR, as this would aid in the effective communication and understanding of research findings. Additionally, it is crucial for projects to be scoped appropriately and for doctoral candidates to manage their time constraints effectively to ensure that their focus on DSR is successful (Cater-Steel *et al.*, 2019). In addition, Geerts, (2011) suggests the Peffers *et al.* (2007b) DSRM template serves as a valuable resource for addressing prevalent challenges within design science research, including the lack of consistency in recognising results across different studies and the difficulty in incorporating existing literature into operational specifications.

The development of a Blockchain-based vote counting, and validation artefact requires a thorough understanding of both pragmatism and design science as essential elements in the research process. However, it is imperative for the researcher to acknowledge the limitations and challenges associated with each approach in order to produce valid and credible results.

To effectively handle methodological pluralism in pragmatism, the researcher adopted a flexible and adaptable approach. The research question and goals of the study were carefully considered, along with the strengths and limitations of different methods, before selecting the appropriate methods to use. The researcher had a good understanding of the different methodologies and applied them appropriately and had a clear understanding of the ethical and practical considerations that arise when conducting pluralistic research.

The challenges associated with Design Science Research (DSR) were mitigated by the researcher's possession of adequate resources and training in DSR. The project was appropriately scoped, and time constraints were effectively managed. Additionally, consistency in terminology within DSR was employed, which aided in the effective communication and understanding of research findings. The data population being African continent was big enough for data collection and allowed the results to be generalisable as the Blockchain-based vote counting and validation was applied to different contexts.

Finally, the researcher effectively communicated the research findings and the implications encountered when developing the blockchain-based vote counting and validation artefact. This included providing a clear and comprehensive explanation of the research methods and results, as well as highlighting the implications of the findings for the field and providing recommendations for future research. By addressing these limitations and challenges, the researcher ensured the validity and reliability of the research findings and made significant contributions to the knowledge base of computer science.

3.9 Reflexivity

The researcher used the concept of reflexivity (reflection), as proposed by Alvesson & Sköldberg (2018) in the study. Reflexivity involves the researcher thinking about the purpose and objective of the study and ensuring that there is consistency between the research methodology, theoretical framework, and research design (Lowe, 2001). In this study, the researcher considered the relationship between the research focus, data collection methods, interpretation, and research design, and continually reflected on these elements.

The researcher exercised a reflexive approach by remaining cognisant of the dialectical relationships among the various stages and processes of the study, and by considering the impact of the theoretical framework in Chapter 2 Section 2.8 on the interpretation of the data. The following section presents Table 3.3 demonstrating the researcher's efforts to maintain alignment.

Table 3.3: Alignment of Research Questions; Research Objectives; Research Instrument; Variable Type and Analysis

Research Questions	Research Objectives	Data collection tool	Method approach	Variable name (concept/construct)	Analysis method
What are the existing blockchain solutions adopted in electoral vote systems, and how have they addressed their respective challenges?	To review and identify existing blockchain solutions for voting systems.	Systematic search of existing data through Systematic Literature Review	Identify the peer reviewed literature in accredited databases	Accuracy of vote counts, Security and integrity of the vote, User satisfaction, Cost and efficiency of the blockchain	Categorisation or classification analysis and Narrative synthesis
What are the critical specifications and features required for a BBVV artefact to achieve high performance and secure user trust?	To elicit the necessary system specifications for developing a BBVV artefact that exhibits high-performance features and engenders user trust.	Questionnaire	Qualitative methods	Accuracy of vote counts, Security and integrity of the vote, User satisfaction	Categorisation or classification analysis and Narrative synthesis
Which blockchain protocol best supports trusted vote aggregation and offers an optimal consensus algorithm for vote count validation?	To identify an appropriate blockchain protocol that supports trusted vote aggregation and includes a suitable	Systematic search of existing data through Systematic Literature for peer reviewed	Identify the peer reviewed literature or white papers in accredited databases and quantitative methods.	voters, voteCount, voteOptions voteThreshold, winner, isVotingPeriodOver, isVoteCountFinalised.	Narrative synthesis and Analysis of telemetric data/ transaction data on the blockchain

Research Questions	Research Objectives	Data collection tool	Method approach	Variable name (concept/construct)	Analysis method
	consensus algorithm for vote count validation.	articles .whitepapers			
How effective is the developed BBVV artefact in vote counting and validation, and to what extent do its performance features engender trust among users?	Develop the BBVV artefact for vote counting and validation and evaluate the artefact's performance features that foster trust in the users.	Published past election results from Electoral Commissions	Quantitative methods.	uptime, response time, failure rate, concurrency, throughput, and latency.	Analysis of telemetric data/ transaction data on the blockchain and Performance benchmarking test results analysis with throughput and scalability consideration

3.10 Summary

In chapter three, the researcher presented an overview of the philosophical framework that underlay the design and methodology of the research study. This framework was used to define the research questions and guide the investigation. The chapter provided a detailed description of the research methodology and the methods utilised during the study. The researcher demonstrated a thorough understanding of various methodological approaches and critically evaluated their suitability for the research question at hand. Furthermore, the chapter provided a context for interpreting the limitations and reliability of the study's findings. The researcher's approach was characterised by a high degree of intellectual rigour and critical thinking, which was evident throughout the chapter.

Chapter 4 explains the artefact design and development.

CHAPTER FOUR: ARTEFACT DESIGN AND DEVELOPMENT

4.1 Organization of the Chapter

This chapter provides a comprehensive overview of the development and evaluation of the blockchain-based vote validation (BBVV) artefact. It begins with an introduction (Section 4.2) outlining the purpose and scope of the artefact, followed by the theoretical foundations (Section 4.3) on which the BBVV is based. The design process (Section 4.4) and the system architecture (Section 4.5) are then described in detail, leading to a discussion of the specific features of the artefact (Section 4.6). The following sections deal with the integration of Pera Wallet for the validation of votes (section 4.7), the selection of the blockchain protocol (Section 4.8) and the specifics of the BBVV protocol (Section 4.9). The chapter also includes a thorough evaluation of BBVV (Section 4.10), tests of the consensus mechanism (Section 4.11) and practical applications through data interpretation and visualisation (Section 4.12), before concluding with a summary (Section 4.13). This structure ensures a logical and detailed exploration of the BBVV artefact from conception to practical application.

4.2 Introduction

In this chapter, we focus on the development and evaluation of the Blockchain-Based Vote Validation (BBVV) artefact, a novel solution to improve the integrity and trustworthiness of vote counting and validation in modern voting systems. This endeavour is guided by three main objectives: First, to identify the necessary system specifications for the development of a BBVV artefact that has powerful features and inspires user trust; second, to identify a suitable blockchain protocol that supports trustworthy vote aggregation, including a suitable consensus algorithm for vote count validation; and third, to develop and evaluate the performance characteristics of the BBVV artefact that promote user trust.

We begin our investigation with a detailed examination of the essential specifications required for the development of a robust and trustworthy blockchain-based voting artefact. This includes a precise definition of the system requirements, focussing on functional robustness and user trust.

By addressing the design and technological underpinnings of BBVV, we emphasise its potential to ensure transparency, security and user accessibility. Particular attention is paid to the selection of a suitable blockchain protocol and the study of the consensus algorithm, which is essential for the accurate validation of votes. The chapter culminates in a comprehensive evaluation of BBVV's performance, demonstrating its effectiveness in ensuring accurate, secure, and tamper-proof voting. This evaluation not only demonstrates the artefact's capabilities in aggregating and validating votes, but also highlights how it enhances user confidence and promotes the credibility of election results in the digital age.

4.3 Theoretical Foundations

This section recaps the conceptual framework and the theoretical foundations by outlining a four-phase conceptual framework presented in Chapter 3, Section 3.3.1 for the BBVV artefact and the theoretical foundations given in Section 2.8 of Chapter 2. This section also shed light on design principles adopted for the study.

4.3.1 Conceptual framework

The first phase of the conceptual framework involves collecting data from election officials and laying the necessary groundwork for the development of the system, including the selection of stakeholders and data collection methods. The second phase involves the application of consensus algorithms and the BBVV protocol, which is based on Byzantine theory, to authenticate legitimate vote counts on an authorised blockchain. This phase is fundamental to ensure the integrity and trustworthiness of the national vote count. The third phase focuses on testing the correctness and scalability of the system, including the validation of the prototype in different environments. In the final phase, the fourth phase, the newly developed system will be compared with existing voting systems and its effectiveness and improvements will be evaluated.

4.3.2 Theoretical Underpinnings

The theoretical underpinnings of the study, in particular the Byzantine Generals Problem Theory (BGP) introduced by Lamport *et al.* in 1982, is central to understanding how to deal with malfunctioning components within a system, particularly those that might behave maliciously. It uses the metaphor of Byzantine generals having to agree on a battle plan, a concept that has significantly influenced the field of fault-tolerant systems. The research includes the Byzantine Agreement Algorithm (BBA), which is essential for ensuring the honesty and reliability of system participants. The implementation of the BBA is characterised by digital signatures and a simple setup with a common random string that enables secure and efficient communication between participants. This concept reflects the challenges of vote counting, where trust is paramount for a truthful and accurate vote count. Just as the Byzantine generals must reach consensus despite possible deception, the voting system must ensure the integrity of every vote amidst the complexity of digital technologies and human intervention. The BBA is therefore an important tool in creating an electoral system that is not only technologically advanced, but also fundamentally trustworthy and transparent, reflecting the true will of the voters.

4.3.3 Design Principles

In developing the BBVV artefact as a vote counting and validation tool, several important design principles were carefully considered to ensure its effectiveness and reliability. First and foremost is security, which is an important aspect given the sensitivity of election data. The BBVV artefact incorporates advanced cryptographic techniques and robust authentication protocols to protect against unauthorised access and tampering. Another cornerstone of the concept is transparency, which makes it possible to trace and verify every step of the election recording process. This transparency not only facilitates verifiability, but also increases the credibility of the voting process. Furthermore, the concept emphasises user trust, which is fundamental in an electoral context. By integrating mechanisms that allow voters and other stakeholders to verify the authenticity and integrity of their votes, the BBVV artefact promotes trust in the voting process.

It is also fundamental that accuracy is an overriding design principle. The system has been carefully designed to ensure that every vote is accurately recorded and counted to minimise errors and discrepancies. This accuracy is critical to the legitimacy of election results as it guarantees that the final vote count truly reflects the will of the electorate. These design principles — security, transparency, user confidence and accuracy — work together to create a robust and reliable system that maintains the sanctity of the election process and ensures that every vote is accurately counted and reported.

4.4 Design Process

4.4.1 Initial Considerations

The initial design considerations for the blockchain-based vote counting and validation (BBVV) artefact, which integrates symmetric cryptography and edge computing on the Algorand platform, include several critical elements. First, the Algorand network is designed to ensure robust security and transparency. The focus is on creating an infrastructure that can efficiently process high volumes of transactions which is a key factor for scalability in large-scale election scenarios. When developing the BBVV Smart Contract with the Algorand SDK and PyTeal, great emphasis was placed on utilising the immutability of the blockchain to ensure the integrity of the election process. The contract was intentionally designed to be user-friendly and accessible to appeal to a broad user base with varying levels of technical knowledge.

An important aspect of the design is the use of symmetric cryptography, particularly in the verification of votes, to preserve the anonymity and privacy of voters while protecting the validity of individual votes. This approach is central to maintaining the trustworthiness and integrity of the voting system. The testing and implementation phase of the smart contract is carried out with great attention to detail to ensure the functionality, security, and scalability of the system. This phase also includes the implementation of real-time monitoring tools such as the Algorand Blockchain Explorer to increase the transparency of the system and strengthen user trust.

Lastly, the provision for the integration of the BBVV artefact with external applications, especially voter registration and identity verification systems, is essential. This future integration will be strategically managed to maintain the decentralised nature of the system while ensuring its scalability and accessibility to create a comprehensive and inclusive voting infrastructure. Taken together, these initial design considerations ensure that the BBVV artefact is not only secure and transparent, but also accessible and scalable, which is consistent with the fundamental principles of blockchain technology for an efficient and modern electronic voting system.

4.4.2 Requirements Gathering

The BBVV artefact as an election collation system represents a significant step in modernising the collation and monitoring of election results. At the heart of the system is a blockchain-based smart contract that ensures unprecedented integrity and security in the management of election records. This robust backend foundation is complemented by an intuitive client interface that provides users with seamless access to the system's many functionalities. The integration of Pera Wallet further strengthens the security framework, especially at fundamental stages such as authentication and digital signature.

The analysis of system specifications or requirements that was gathered after collecting data from different stakeholders through a questionnaire are presented in this section and are broken down into five themes: technical aspects, accuracy, speed, and efficiency; transparency and security; challenges and improvements; and the role of observers and Election Management Bodies (EMBs).

4.4.2.1 Technical Aspects

The majority of respondents said that they used manually operated vote-counting devices and emphasised the use of digital transmission kits, such as the Integrated Elections Management System (IEMS) and Biometric Voter Authentication System (BVAS), which do not count or verify the results but rather communicate them via scanned pictures of the results sheets. In contrast,

other respondents highlighted using analogue transmission kits while voicing out worries over the possibility of manipulating electronic devices to favour certain parties.

4.4.2.2 Accuracy, Speed, and Efficiency

Several respondents mentioned problems that were caused by the lack of a 3G network, which resulted in delays in the transmission of votes. They added that the manual transmission of votes takes a significant amount of time and that it is possible that the results are not always correct. One respondent underlined that efficiency was not a problem by pointing out that the votes obtained by each candidate were attached to the polling station before they were transferred to the main centre. In contrast, the other respondent stressed that efficiency was an issue. Most respondents attributed accuracy and security as the highly vital performance metric in a vote counting and validation system, with each scoring 75%, with speeds of 62.5% and 50% for ease of use, as indicated in Figure 4.1. On the other hand, they said that there were issues with the speed and efficiency of communicating counted votes and certifying the results. Concerns were also expressed over the possibility of vote rigging.

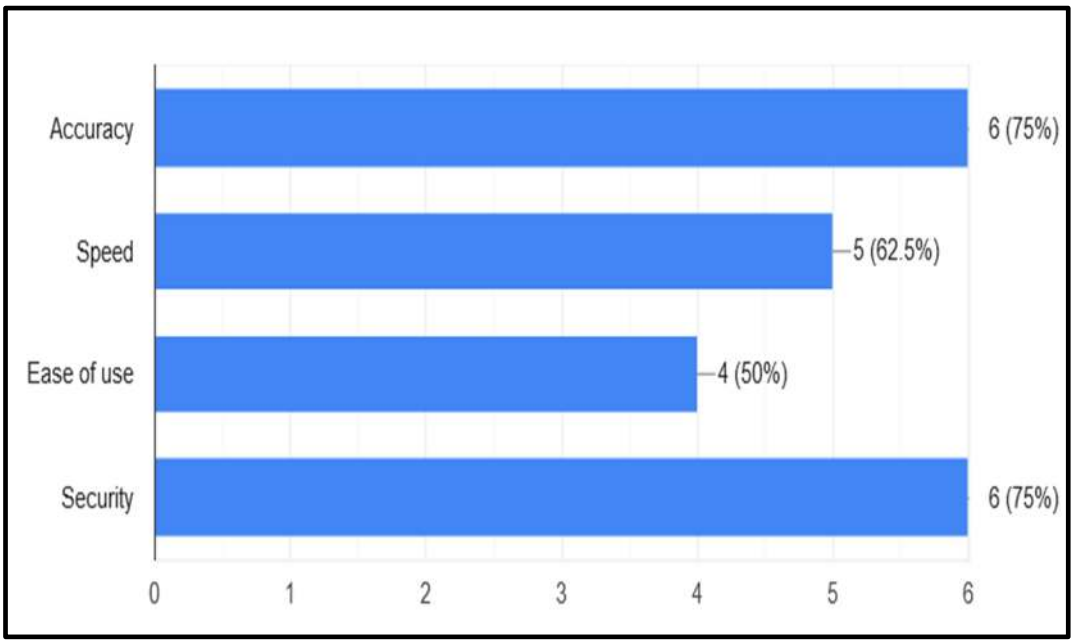


Figure 4-1: Performance Metrics Required

4.4.2.3 Transparency and Security

A common thread that emerged from the responses was the significance of maintaining transparency and accessibility throughout the vote counting and certification processes. Some respondents brought up the need to have a transparent procurement procedure, adequate testing, clear and specific legislation, and an all-encompassing communications plan. Others emphasized the relevance of openness in terms of fostering trust among stakeholders and preserving the will of the people. End-to-end encrypted VPN networks, police monitoring, and cybersecurity characteristics were some of the security measures highlighted by the respondents.

4.4.2.4 Challenges and Improvements

The respondents pointed out many difficulties in the transmission and validation of votes, such as a lack of network coverage, legal concerns, a lack of staff training and vote manipulation. Participation of Stakeholders, improving network coverage, implementing electronic transmission

systems, and changing electoral regulations were suggested by a few respondents as a way to improve the electoral vote counting and validation process.

4.4.2.5 Role of Election Management Bodies (EMBs) and Observers

The significance of the role of observers in guaranteeing the correctness and integrity of vote counting and validation was stressed by respondents. For example, several respondents pointed out the verification of results against physical forms in the presence of agents, but other respondents insisted on the presence of candidates throughout the counting process. Various respondents highlighted that while foreign observers are not accountable for taking steps to assure accuracy, they are able to contribute significant insights and comments on how the system might be improved.

The design of the blockchain-based vote counting, and validation artefact (BBVV) was heavily influenced by the insights of various stakeholders who emphasised the need for a system that ensures accuracy, speed, efficiency, transparency, and security in vote counting and validation. Key feedback centred on the use of digital transmission kits, the need for reliable and secure election verification and the challenges posed by manual processes and insufficient network coverage. Based on this feedback, BBVV focused on integrating robust digital transmission and validation capabilities, prioritising end-to-end security, and increasing transparency to boost stakeholder confidence. In addition, the system was tailored to address legal concerns, prevent voter fraud, and facilitate the involvement of election authorities and observers to ensure the integrity and accuracy of the election process.

4.5 System Architecture Design

The BBVV artefact which is an election collation system is based on a client-server architecture paradigm. The client-side or front-end uses the capabilities of Next.js, an outstanding framework built on top of React. The server-side element consists of a sophisticated smart contract carefully developed using PyTeal by Algorand. To enhance the security of authentication and transaction signatures, the system is seamlessly integrated with Pera Wallet.

4.5.1 Primary Modules:

- Client-side interface: Next.js
- Server-side logic: PyTeal Smart Contract
- Authentication mechanism: Integration with Pera Wallet

4.5.2 Operational Workflow:

- End users access the system interface via standard web browsers.
- Data request and transmission is done through the interaction of the interface with the backend smart contract.
- To enhance security, Pera Wallet provides a mechanism for users to authenticate and digitally sign transactions.

Figure 4.2 and Figure 4.3 shows System Architecture Workflow and integrated components.

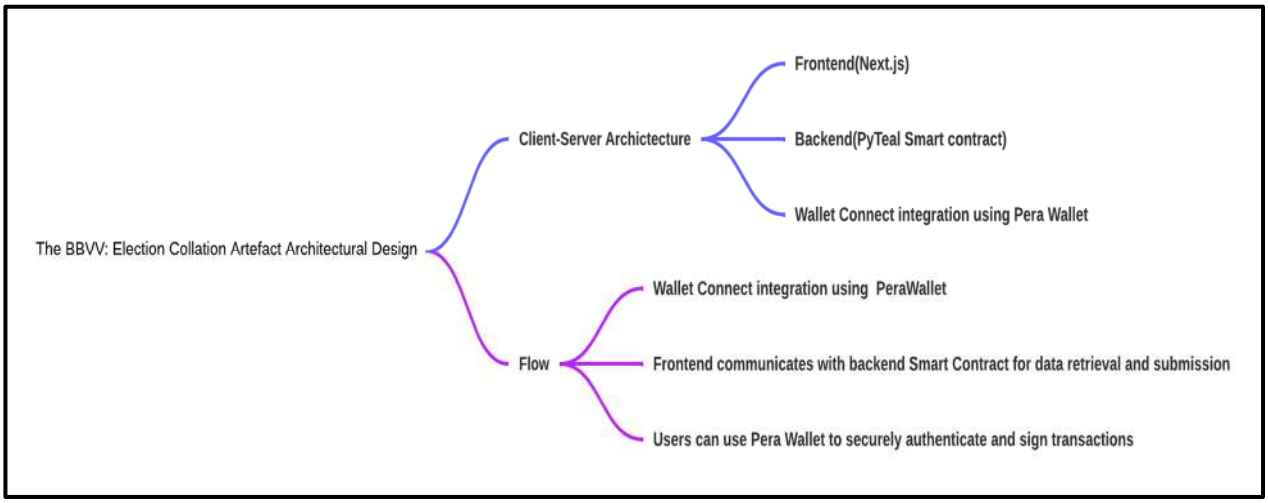


Figure 4-2: System Architecture Workflow

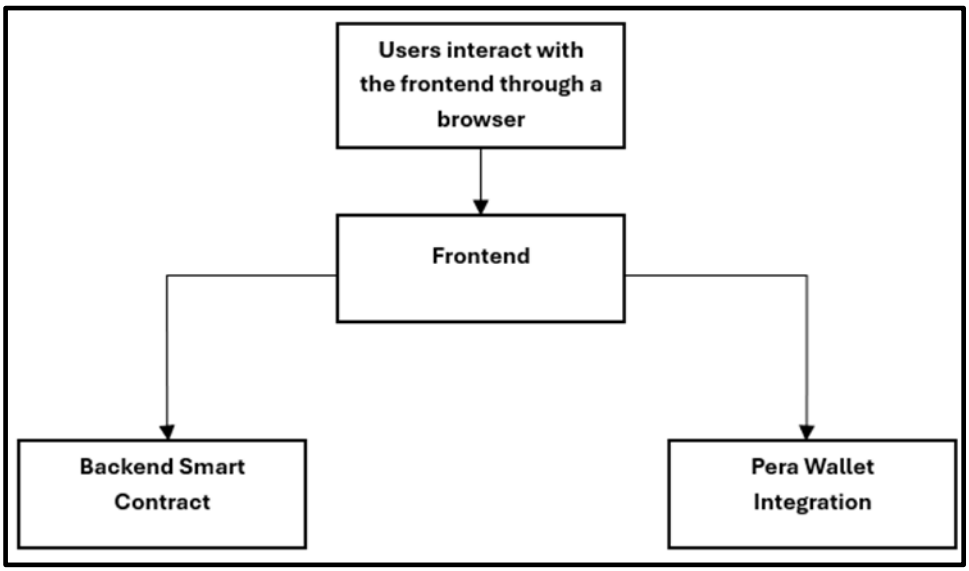


Figure 4-3: Integrated Components

Election data are managed via Algorand's blockchain platform, which is known for its efficiency and speed, especially with its Layer 1 smart contracts. Figure 4-4 shows the structure of the BBVV implementation. Edge blocks, located at the local level of each polling station's blockchain, store the final vote count. Kafka plays a fundamental role as an ingress message broker for these edge blocks and efficiently manages the incoming data. It queues the data from the various polling stations and ensures that the system is not overloaded and that there is an orderly flow of data to the main blockchain.

When the vote count reaches the Algorand blockchain, the layer 1 smart contracts process the data. Algorand's high throughput and low latency are ideal for this purpose. They enable fast and efficient transaction processing, which is essential for election scenarios where timely results are important. The smart contracts aggregate vote counts from different locations to quickly provide a comprehensive nationwide result.

Once processed by Algorand's smart contracts, the aggregated vote count is securely stored on the blockchain. This record is immutable and tamper-proof, providing a reliable and transparent record of all votes cast. The block readers, entities within the blockchain network, are responsible

for verifying the aggregated vote count and determining the appropriate time to publish the results. They ensure that all procedural checks are completed before the data is published.

Once released by the block readers, an egress message broker manages the distribution of the election results to the various subscribers. This step ensures a coordinated release, prevents premature publication, and guarantees that all subscribers receive the information at the same time.

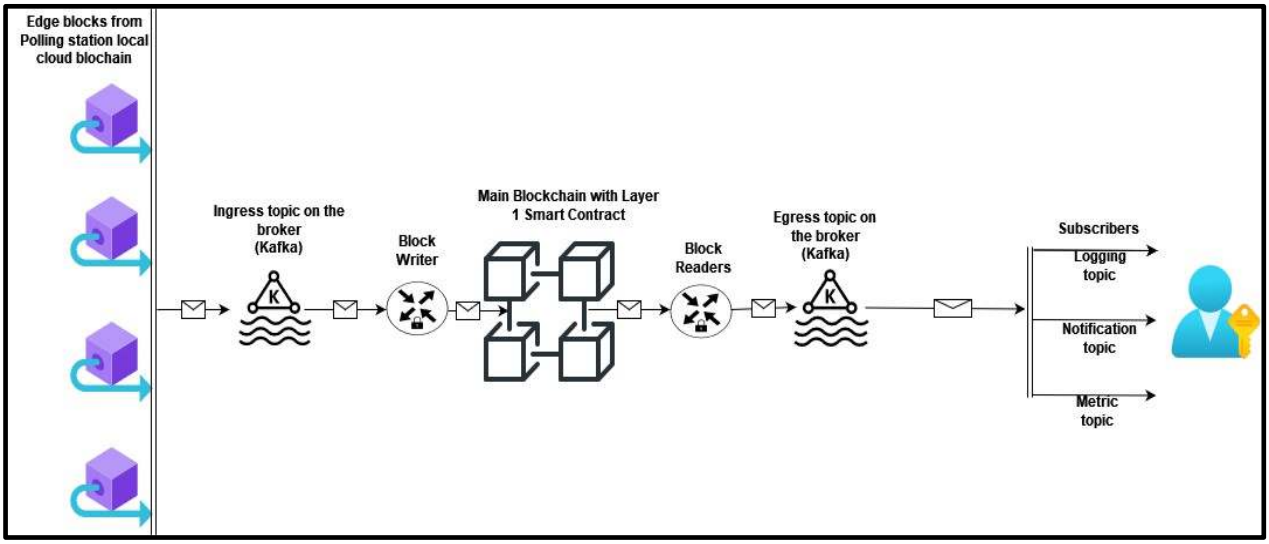


Figure 4-4:The BBVV overall structure.

The implementation of the BBVV outlined in Fig. 4-5, begins with each local polling station maintaining a blockchain in which the votes are recorded as transactions. The last block in this local blockchain, the so-called edge block, contains important data such as the hash key and the total number of votes. This hash key serves as a unique identifier that ensures data integrity between blocks and across the network. Once voting is complete, the data from the edge blocks is transferred to a Kafka system that acts as a message blocker. Kafka, a distributed streaming platform, processes large amounts of data by queuing these blockchain blocks and controlling the flow of data to prevent overloading the system. It forwards the blocks at a certain speed, ensuring a steady and manageable flow of data.

The information released by Kafka are then forwarded to a cloud-based blockchain, which serves as a centralised ledger and consolidates the votes from multiple local blockchains in different polling stations. This centralisation is important for creating a nationwide result and ensuring data consistency and security. As soon as the information arrive on the cloud blockchain, a smart contract is automatically triggered. This smart contract calculates the total number of votes from the incoming data. The smart contracts are designed as self-executing agreements with conditions written directly into the code and automatically calculate the total number of votes as soon as the required information is received.

After the smart contract calculates the total number of votes, the results are distributed to various subscribers, including media, government agencies and other authorized entities interested in the election results. This distribution is handled via the blockchain network, ensuring that all subscribers receive the same tamper-proof data at the same time. To further increase security and trust in the election process, each polling station can independently verify the vote count contained in the national totals using a combination of public and private cryptographic keys. The private key, which is unique to each polling station, is used to confirm the vote total, while the public key allows others on the network to verify that the data comes from a legitimate source and matches the national totals.

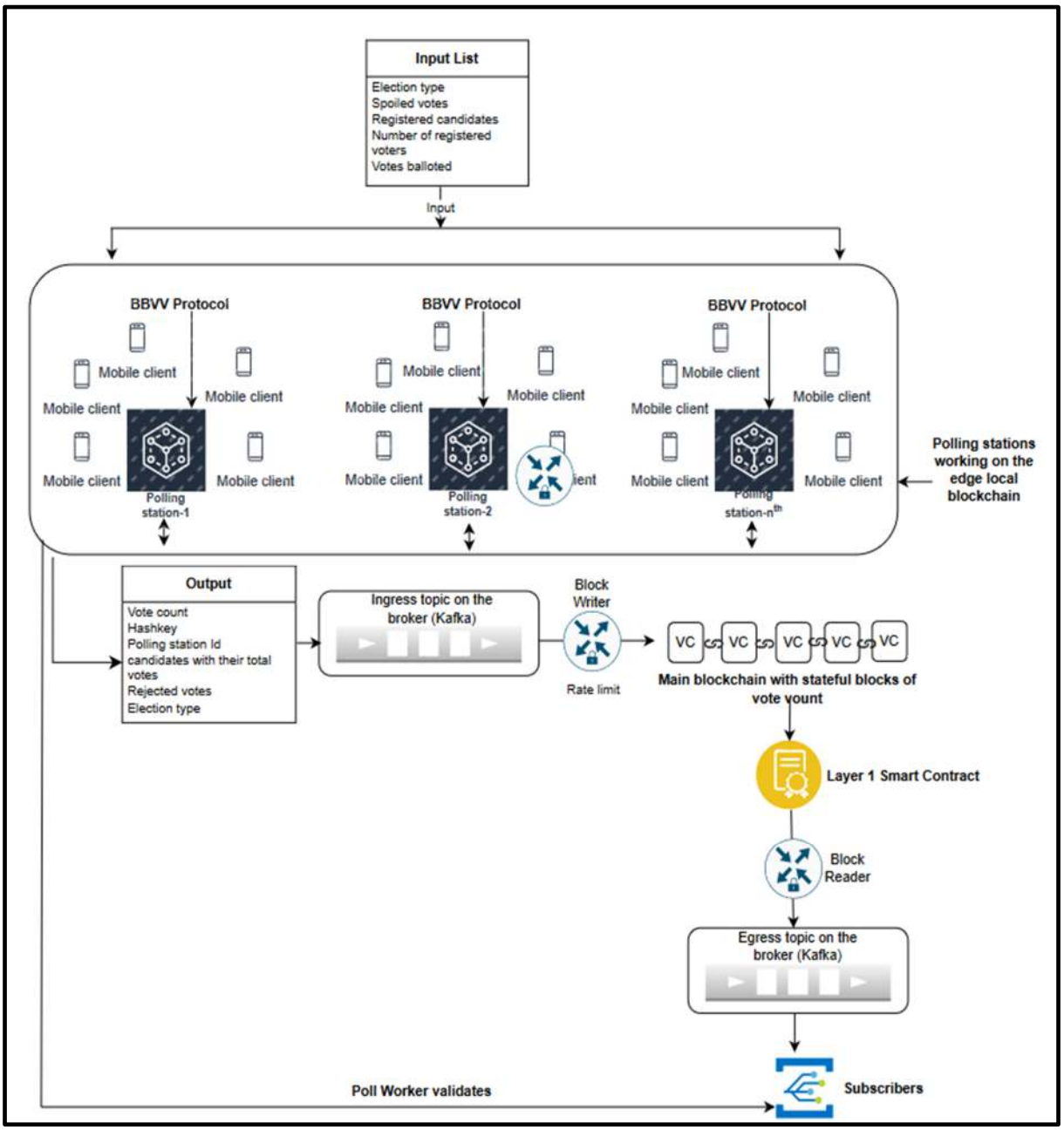


Figure 4-5: The BBVV implementation.

4.5.3 Layer 1 Smart Contract Implementation

Overall, the equations ensure proper recording of votes across time intervals, proper aggregation between polling stations, and a continuous record of the election period without overlaps or gaps. This is critical to maintaining the integrity and verifiability of election results.

4.5.3.1 Definitions

$\boldsymbol{C}(\mathbf{T}, \mathbf{P})$— Vote count for candidate **Y** from polling station **P** received at time **T**.

$\boldsymbol{S}(\mathbf{T_b}, \mathbf{T_c})$—Total votes for candidate **Y** from a set of polling stations received between the beginning of time ($\mathbf{T_b}$) and end of time ($\mathbf{T_c}$)**,** where:

$(\mathbf{T_c} - \mathbf{T_b}) = \mathbf{time}$—Therefore, the time can be changed to suit the time an election vote counting period must run.

$\boldsymbol{ST}$—Total votes for candidate **Y** accumulated over various time intervals ($\mathbf{T_b}, \mathbf{T_c}$) spanning a total period of $\boldsymbol{X_i}$ hour or however long an election runs.

4.5.3.2 Relationship between C and S.

To accumulate the votes for candidate **Y** from multiple polling stations over a time interval from $\mathbf{T_b}$ to $\mathbf{T_c}$, we consider all polling stations $\boldsymbol{P}$ and all relevant timestamps $\boldsymbol{T}$ within the interval $[\mathbf{T_b}, \mathbf{T_c}]$:

This equation in (4.1) sums up all votes $\boldsymbol{C}(\boldsymbol{T}, \boldsymbol{P})$ from each polling station **P** during the specified interval $[\mathbf{T_b}, \mathbf{T_c}]$**.**

$$\boldsymbol{S}(\mathbf{T_b}, \mathbf{T_c}) = \sum \mathbf{p} \sum_{\mathbf{T}=\mathbf{T_b}}^{\mathbf{T_c}} \boldsymbol{C}(\boldsymbol{T}, \boldsymbol{P}) \qquad (4.1)$$

4.5.3.3 Relationship between S and ST.

Given that **ST** in (4.2) is the total number of votes counted over a series of intervals across a total period of $\boldsymbol{X_i}$ hour, where $\boldsymbol{X_i}$ is the number of hours it takes an election to be conducted assuming **n** such intervals:

$$\boldsymbol{ST = \sum_{i=1}^{n} S(T_{bi}, T_{ci})} \qquad (4.2)$$

where $\mathbf{T_{bi}, T_{ci} = 2\ h}$ for each interval **i**, and the series of intervals cumulatively spans $\boldsymbol{X_i}$ hour.

4.5.3.4 Validation of consistency across intervals.

To validate that the intervals properly cover the $\boldsymbol{X_i}$ hour period without overlap or gaps, we can establish the following invariant in (4.3):

$$\mathbf{T_{bi+1} = T_{ci}}$$

$$\mathbf{for\ i = 1\ to\ n - 1} \qquad (4.3)$$

This ensures that each interval begins immediately after the previous one ends, with no overlap or gap between them.

4.5.3.5 Coverage and continuity over X_i Hours.

Ensure the first interval begins at the start of the $\boldsymbol{X_i}$ hour period and the last interval ends precisely at the $\boldsymbol{X_i}$ hour mark: This we can change as in polling closes, or all counting should be carried out, and all coverage carried out, this is shown in (4.4).

$$\mathbf{T_{b1}} = \mathbf{Starttime}$$

$$\mathbf{T_{cn}} = \mathbf{T_{b1}} + \mathbf{X_i} \qquad (4.4)$$

To ensure that the vote counts from individual polling stations are verifiable in the final totals through cryptographic means, such as hashing or digital signatures, we incorporate cryptographic hash functions or signatures into the mathematical model. This addition helps to validate that a specific polling station's data were included in the overall count.

4.5.3.6 Cryptographic Enhancement of the Model

a) Introduction of cryptographic hashes and signatures.

Let **H** represent a cryptographic hash function.

Let Sig **(X, $\mathbf{K_p}$)** represent a digital signature of data **X** with the private key $\mathbf{K_p}$ of polling station **P**. This could be the block hash.

b) Incorporating hash into vote count.

Defined **C(T, P)** in (4.5) not only as the vote count but also include a hash or signature that certifies its authenticity:

$$\mathbf{C(T,P) = (count, Sign(count,KP))} \qquad (4.5)$$

Here, the count is the actual number of votes recorded at polling station **P**, at time **T**, and **Sign(count, KP)** is its digital signature or block chain hash.

c) Aggregation with verification.

When aggregating these counts into the total $\mathbf{S(T_b, T_c)}$ given in (4.6), the process would also involve verifying the signatures to ensure data integrity:

$$\boldsymbol{S}(\mathbf{T_b}, \mathbf{T_c}) = \sum \mathbf{p} \sum_{\mathbf{T=T_b}}^{\mathbf{T_c}} \mathbf{verify}\big(\boldsymbol{C}(\boldsymbol{T}, \boldsymbol{P}), \mathbf{K_p}\big) \qquad (4.6)$$

Here, verify $(\boldsymbol{C}(\boldsymbol{T}, \boldsymbol{P}), \mathbf{K_p})$ checks the signature of the count from polling station **P** to confirm it was indeed issued by **P**.

d) Cumulative verification for total votes **ST**.

The total **ST** is calculated by summing up all verified **S** intervals in (4.7):

$$\mathbf{ST} = \sum_{\mathbf{i=1}}^{\mathbf{n}} \boldsymbol{S}(\mathbf{T_{bi}}, \mathbf{T_{ci}}) \qquad (4.7)$$

The integrity of each interval **S** is ensured by the verification of all included signatures.

e) Providing proof of inclusion.

To prove that the results from a specific polling station **P** have been included in the total, one would need to provide:

The signed vote counts **Sign(count,** $\mathbf{K_p}$**)**, a chain of verified totals from **S** to **ST** showing the inclusion of **P's** counts.

This is facilitated by using the Merkle trees of blockchain or similar cryptographic structures, where each node is a hash of its children, providing a verifiable path from each individual entry to the root (in aggregate).

4.5.4 Entity-Relationship Diagram

The Entity-Relationship (ER) diagram you see in Figure 4.6 represents the system architecture of the election code provided in Appendix A. Here we will find an explanation for each part of the diagram:

ElectionState entity: This is the central entity that manages various aspects of the election system. It contains several counters and a submission period that are critical to tracking the election process. The attributes include:

candidate_counter: A counter for the candidates.

election_counter: A counter for the polling stations.

polling_station_counter: A counter for the polling stations.

submission_counter: A counter for the submissions.

submission_period: Represents the period in which submissions of vote counts are accepted.

CandidateRecord entity: This entity represents the records of the candidates participating in the election. Its attributes are:

candidate_id (primary key): A unique identifier for each candidate.

name: The name of the candidate.

party_name: The name of the candidate's party.

timestamp: A timestamp that marks the creation or update of the record.

AgentRecord entity: This entity stores information about the election agents. Its attributes include:

agent_id (primary key): A unique identifier for each agent.

account: The agent's account information.

polling_station_id (foreign key): Refers to the PollingStationRecord entity that specifies the polling station to which the agent is assigned.

timestamp: A timestamp for the record.

PollingStationRecord entity: This entity contains details of the polling stations. The attributes are:

polling_station_id (primary key): A unique identifier for each polling station.

agent_id (foreign key): Refers to the AgentRecord entity that specifies the agent assigned to the polling station.

timestamp: The timestamp for the record.

SubmitVoteCount Entity: This entity is used to record the vote counts submitted by agents. Its attributes are:

submission_id (primary key): A unique identifier for each submission.

agent_id, polling_station_id, candidate_id (foreign keys): These refer to the corresponding **AgentRecord, PollingStationRecord** and **CandidateRecord** entities and specify the respective agent, polling station and candidate for the vote count.

candidate_vote_count: The number of votes for the candidate.

timestamp: The timestamp for the transmission.

Relationships:

ElectionState manages CandidateRecord, AgentRecord, PollingStationRecord and SubmitVoteCount.

CandidateRecord is linked to SubmitVoteCount (one candidate in one transmission).

AgentRecord is linked to SubmitVoteCount (an agent in a transmission) and is located at a PollingStationRecord.

PollingStationRecord is linked to SubmitVoteCount (a polling station in a template) and has an AgentRecord located there.

Each entity and relationship in this diagram correspond to a piece of code and shows how the different components of the voting system interact and are structured.

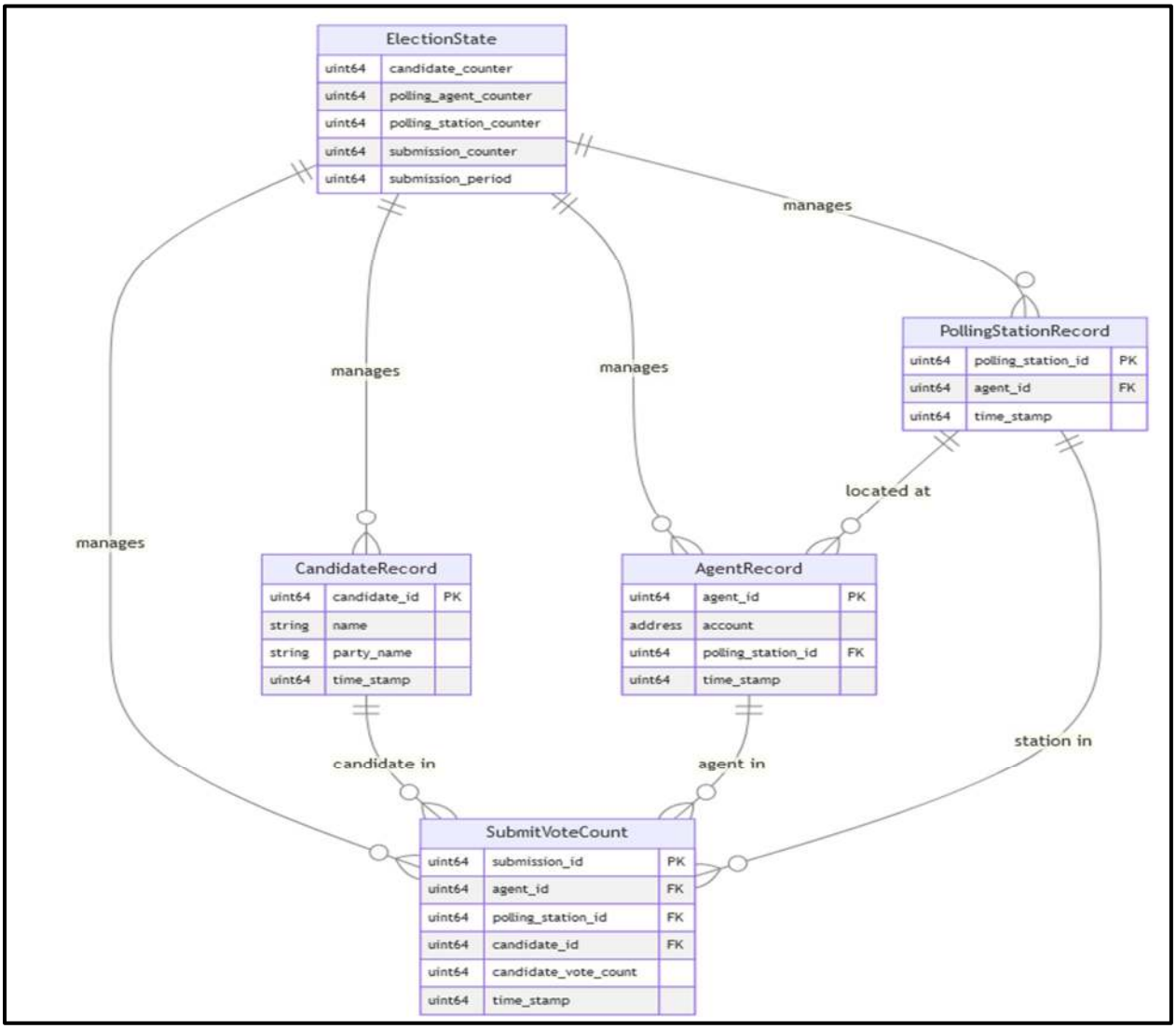


Figure 4-6:The BBVV Entity Relationship

4.5.5 Sequence Diagram

The sequence diagram in Figure 4.7 illustrates the development phases of a blockchain-based application for validating elections. It starts with the client-side development, where Next.js is used to create a responsive and interactive user interface. This interface interacts with the server-side logic implemented with Algorand PyTeal's smart contract, which ensures the secure and efficient

processing of blockchain transactions. The authentication mechanism is integrated via Pera Wallet, providing a robust and secure method for user authentication and digital signing. Version control is managed with Git, which ensures efficient tracking and management of the different versions of the application throughout the development cycle. Finally, the application is deployed using Vercel for the client-side components, with the smart contract going live on the Algorand Testnet. This streamlined process ensures a secure, efficient, and user-friendly system for election monitoring and control.

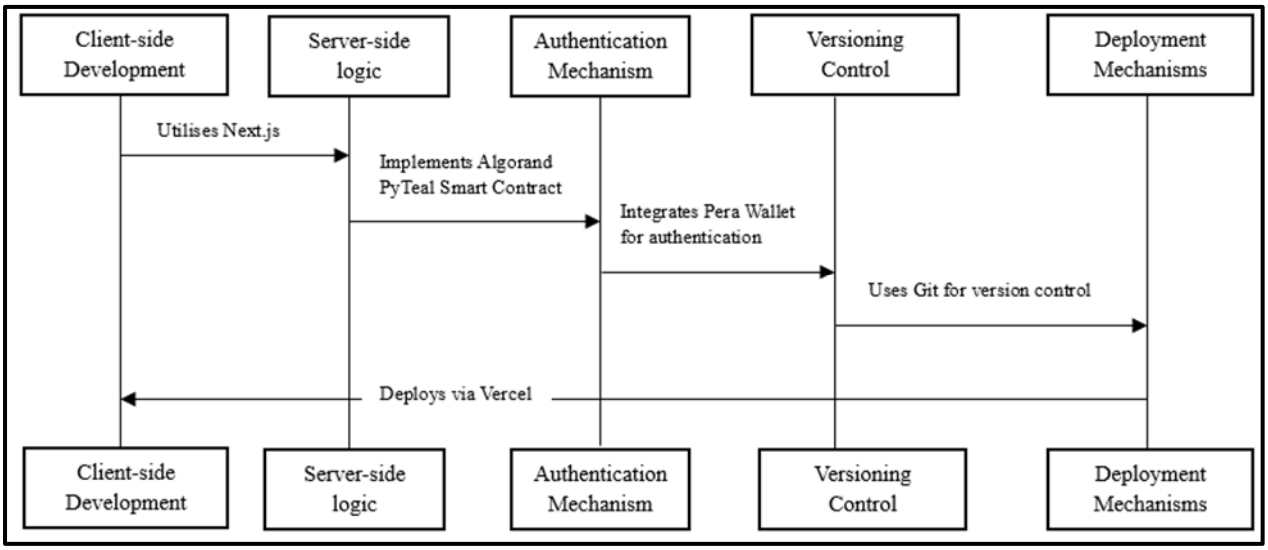


Figure 4-7: Sequence Diagram

4.5.6 Technological Stack Employed

- Client-side development: Next.js (Based on React)
- Server-side logic: Algorand PyTeal Smart Contract
- Authentication mechanism: Pera Wallet
- Versioning control: Git
- Deployment mechanisms: Vercel (for the client side), with the smart contract commissioned on the testnet iteration of the Algorand.

4.5.7 Functional Overview of the System

The BBVV is designed to streamline the collation and monitoring of election results. At its core, it uses a blockchain-anchored smart contract to ensure the integrity and secure management of election records. The client-side interface is not only intuitive, but also provides users with a comprehensive portal to interact with the backend. The integration of Pera Wallet underlines the security framework, especially during the authentication and digital signing processes.

4.6 Distinctive Features of the Artefact

- Immutable data retention: election records, including results, find a secure repository on the blockchain thanks to the PyTeal Smart Contract, which ensures inviolability and enhanced security.
- Synchronous data reflection: The client-side interface can provide synchronous updates that reflect the collection and validation of election results in real time.
- Enhanced user identity verification: Pera Wallet integration increases security and provides users with a strengthened authentication process.
- Secure data transfer: Pera Wallet integration gives users the ability to add digital signatures to transactions, increasing data integrity during transmission.
- Comprehensive audit functions: The design of the blockchain ensures a comprehensive, tamper-proof log of all transaction activities and enables transparent and traceable audit trails.

4.7 Vote Validation with Pera Wallet

The integration of Pera Wallet into a blockchain-based vote counting and validation (BBVV) artefact using symmetric cryptography and edge computing represents a significant step forward in ensuring transparent, secure and trustworthy election processes.

Below you will learn how these components have been integrated and connected:

1. Leveraging Edge Computing:
    - Decentralised processing: edge computing enables the decentralised processing of votes. This reduces latency and dependency on centralised servers and makes the system more resilient and scalable.
    - Local storage and management of keys: Edge nodes have been used for local storage and management of keys, increasing security and reducing the risk of key compromise.
2. Pera Wallet integration for validation:
    - Wallet integration: voters and poll workers can use Pera Wallet to interact with the BBVV system. This includes voting or performing administrative tasks.
    - Transaction Signing: Pera Wallet allows users to securely sign blockchain transactions, ensuring that votes are cast by legitimate voters.
    - Verification of transactions: Election officials can use Pera Wallet to verify transactions on the Algorand blockchain to ensure the integrity of the vote count.
3. This ensures security, transparency and trust:
    - End-to-end verification: from voting to counting, every step is verifiable. Voters can verify their votes on the blockchain, and election officials can check the entire process.
    - Immutable record: The blockchain provides an immutable record of all votes, preventing tampering and ensuring the integrity of the voting process.
    - Real-time verification: The use of edge computing enables real-time verification of the voting process, increasing transparency and trust.
4. User interface and accessibility:
    - Accessible interface for voting: a user-friendly interface is critical. Voters should be able to cast their vote easily, and Pera Wallet integration should be intuitive and straightforward.

- Feedback and confirmations: Voters receive instant feedback and confirmation once their vote has been recorded on the blockchain, enhancing user experience and trust.

The integration of Pera Wallet with a BBVV artefact that uses symmetric cryptography and edge computing represents a ground-breaking approach to voting processes. This system not only ensures the security and confidentiality of votes, but also strengthens transparency and trust between voters and election authorities. By utilising the strengths of blockchain technology, symmetric cryptography and edge computing, this innovative solution can significantly improve the reliability and integrity of vote counting and validation.

4.8 Blockchain Protocol Selection

This section provides an analysis of various consensus algorithms used in blockchain technology, focusing on their security, performance, scalability, energy efficiency, decentralization, and fairness. Table 4.1 indicates a comparative analysis of blockchain consensus algorithms across key performance indicators.

Proof of Work (PoW) is a consensus algorithm that has demonstrated robust security against attacks such as double spending due to the computational power required to create new blocks. However, it is susceptible to 51% attacks, where an attacker with majority control of the network's hash rate could manipulate the blockchain (Eyal & Sirer, 2018). PoW networks tend to have lower transaction throughput and higher latency compared to other consensus algorithms due to the resource-intensive nature of mining (Bonneau *et al.*, 2015). Scalability is a significant challenge for PoW networks, as an increasing number of transactions and nodes put more pressure on the mining process (Croman *et al.*, 2016). PoW has been criticized for its high energy consumption, as mining requires substantial computational resources and electricity (Mora *et al.*, 2018). While theoretically decentralized, mining power in PoW is often concentrated in large mining pools, leading to centralization concerns (Gervais *et al.*, 2014). Additionally, PoW mining rewards are more likely to be concentrated among miners with more computational resources, leading to potential inequality in reward distribution (Houy, 2014).

Practical Byzantine Fault Tolerance (PBFT) is designed to be secure and resistant to Byzantine faults, even in the presence of malicious actors (Yang, 2018). However, it may not be suitable for large-scale networks or open, permissionless systems (Miller *et al.*, 2016;Feng *et al.*, 2018). PBFT networks can achieve high transaction throughput and low latency, as they rely on a deterministic, round-based message exchange process (Xiao *et al.*, 2020). However, PBFT has some scalability limitations, as the communication overhead increases with the number of nodes in the network (Miller *et al.*, 2016) . PBFT is more energy-efficient than PoW, as it does not require resource-intensive mining (Vukolić, 2016). PBFT is generally used in permissioned blockchains, resulting in a more centralized structure compared to permissionless systems (Vukolić, 2016). Its fairness depends on the specific implementation and the governance model used (Vukolić, 2016).

Proof of Stake (PoS) is considered to be secure and resistant to common attacks, but it may be more vulnerable to long-range and grinding attacks, which can be mitigated through additional mechanisms (Buterin & Griffith, 2017; David *et al.*, 2018). PoS networks generally provide higher transaction throughput and lower latency compared to PoW networks, as the selection of validators is more efficient (Kiayias *et al.*, 2017). PoS networks are generally more scalable than PoW networks, as they can handle an increasing number of transactions and nodes more efficiently (Zheng *et al.*, 2017). PoS is significantly more energy-efficient than PoW, as it doesn't rely on resource-intensive mining (Anupama & Sunitha, 2022). PoS is designed to maintain decentralization, but there are concerns about the concentration of power among large token holders (Borse *et al.*, 2022). PoS aims to achieve a more equitable distribution of rewards and influence, but this can be skewed if large token holders dominate the validator selection process (Saleh, 2021).

Delegated Proof of Stake (DPoS) is considered secure, as it can withstand Byzantine faults and Sybil attacks (Larimer, 2019). However, it may be susceptible to collusion or malicious delegate behaviour, which can be addressed with proper incentivization and governance mechanisms (Haque *et al.*, 2022). DPoS networks typically have higher transaction throughput and lower latency compared to PoW and PoS, as they rely on a smaller number of trusted validators (Larimer, 2019). DPoS is designed to be more scalable than PoW and PoS, as it can handle increased nodes and transactions more efficiently due to its delegated validation process (Hu *et*

al., 2021). DPoS is more energy-efficient than PoW, as it does not require resource-intensive mining (Ekparinya *et al.*, 2020). While DPoS aims to maintain decentralization, it may result in some degree of centralization due to the limited number of delegates (Haque *et al.*, 2022). DPoS intends to provide a fair reward distribution and influence, but there can be concerns about the potential concentration of power among the top delegates (Hu *et al.*, 2021).

Proof of Authority (PoA) is considered secure for permissioned networks, as validators are trusted and identifiable, which helps deter malicious behaviour. However, it may not be as suitable for open, permissionless systems, where validators cannot be easily vetted (Ekparinya *et al.*, 2020). PoA networks typically have high transaction throughput and low latency, as the limited number of trusted validators streamlines the consensus process (Ullah *et al.*, 2022). PoA is more scalable than PoW and PoS, as it can efficiently handle increased nodes and transactions due to its reliance on trusted validators (Ullah *et al.*, 2022). PoA is energy-efficient, as it does not require resource-intensive mining or staking processes (Ullah *et al.*, 2022). PoA is more centralized than PoW or PoS, as it relies on a limited number of trusted validators, often known by their real-world identity (Ullah *et al.*, 2022). PoA's focus is primarily on network security and efficiency, and its fairness depends on the specific implementation and governance model used (Ullah *et al.*, 2022).

Pure Proof of Stake (PPoS) is designed to be secure and resistant to common attacks, including Sybil attacks and long-range attacks, by employing a cryptographically secure random selection process for validators (Gilad *et al.*, 2017) . PPoS networks achieve high transaction throughput and low latency by using a fast and efficient consensus mechanism known as the Algorand Byzantine Agreement (ABA) protocol (Chen & Micali, 2019). PPoS is more scalable than PoW and traditional PoS, as it can efficiently handle an increased number of nodes and transactions due to its random validator selection process (Gilad *et al.*, 2017) . PPoS is energy-efficient, as it does not require resource-intensive mining processes like PoW (Gilad *et al.*, 2017). PPoS aims to provide a more decentralized consensus mechanism by employing a random selection process for validators, which reduces the concentration of power among large token holders (Chen & Micali, 2019). PPoS intends to achieve a more equitable distribution of rewards and influence by selecting validators randomly and proportionally to their token holdings (Gilad *et al.*, 2017) .

Federated Consensus is considered secure for permissioned networks, as it relies on a predefined set of trusted nodes. However, it may not be suitable for open, permissionless systems where nodes cannot be easily vetted (Mazières, 2015). Federated consensus networks typically have high transaction throughput and low latency, as they rely on a limited number of trusted nodes for validation (Sankar *et al.*, 2017). Federated consensus is more scalable than PoW and PoS, as it can efficiently handle increased nodes and transactions due to its reliance on trusted nodes (Mazières, 2015). Federated consensus is energy-efficient, as it does not require resource-intensive mining or staking processes (Sankar *et al.*, 2017). Federated consensus is more centralized than PoW or PoS, as it relies on a predefined set of trusted nodes for validation (Sankar *et al.*, 2017). Federated consensus focuses on network security and efficiency. Its fairness depends on the specific implementation and governance model used (Sankar *et al.*, 2017).

Hedera Hashgraph is designed to be secure and resistant to common attacks, as it uses a virtual voting algorithm based on the gossip-about-gossip protocol to achieve consensus (Baird, 2016; Leemon *et al.*, 2020). Hedera Hashgraph achieves high transaction throughput and low latency due to its fast and efficient consensus algorithm that does not require traditional block confirmation (Leemon *et al.*, 2020), (Baird, 2016). Hedera Hashgraph is highly scalable, as it can efficiently handle an increased number of nodes and transactions due to its gossip-based consensus mechanism [30]. Hedera Hashgraph is energy-efficient, as it does not require resource-intensive mining or staking processes like PoW or PoS (Leemon *et al.*, 2020). Hedera Hashgraph aims to provide a more decentralized consensus mechanism by employing a distributed network of nodes that participate in the consensus process (Leemon *et al.*, 2020). Hedera Hashgraph is designed to achieve a fair and equitable distribution of rewards and influence by using a fair timestamping and transaction ordering mechanism (Leemon *et al.*, 2020). Table 4.1 illustrates a comparative analysis of consensus algorithms.

Table 4.1: Comparative Analysis of Blockchain Consensus Algorithms Across Key Performance Indicators

Consensus Algorithm ⬇	Security	Performance	Scalability	Energy Efficiency	Decentralization	Fairness
Proof of Work (PoW)	Robust security but susceptible to 51% attacks (Eyal & Sirer, 2018).	Lower transaction throughput and higher latency (Bonneau *et al.*, 2015).	Significant scalability challenges (Croman *et al.*, 2016).	High energy consumption (Mora *et al.*, 2018) .	Potential centralization in large mining pools (Gervais *et al.*, 2014).	Potential inequality in reward distribution (Houy, 2014) .
Practical Byzantine Fault Tolerance (PBFT)	Resistant to Byzantine faults (Yang, 2018).	High transaction throughput and low latency (Yang, 2018).	Scalability limitations due to communication overhead (Miller *et al.*, 2016)..	More energy efficient than PoW (Vukolić, 2016).	More centralized structure (Vukolić, 2016).	Depends on specific implementation and governance model (Vukolić, 2016).
Proof of Stake (PoS)	Resistant to common attacks but vulnerable to long-range and grinding attacks (Buterin & Griffith, 2017; David *et al.*, 2018).	Higher transaction throughput and lower latency than PoW efficient (Kiayias *et al.*, 2017).	More scalable than PoW (Zheng *et al.*, 2017).	More energy efficient than PoW (Anupama & Sunitha, 2022).	Concerns about power concentration among large token holders (Borse *et al.*, 2022).	Potential skew if large token holders dominate validator selection (Saleh, 2021).
Delegated Proof of Stake (DPoS)	Resistant to Byzantine faults and Sybil attacks but susceptible to collusion (Ekparinya *et al.*, 2020; Haque *et al.*, 2022).	Higher transaction throughput and lower latency than PoW and PoS (Larimer, 2019).	More scalable than PoW and PoS (Hu *et al.*, 2021),	More energy efficient than PoW (Ekparinya *et al.*, 2020),	Potential centralization due to the limited number of delegates (Haque *et al.*, 2022),	Concerns about power concentration among top delegates (Hu *et al.*, 2021),

Consensus Algorithm ⬇	Security	Performance	Scalability	Energy Efficiency	Decentralization	Fairness
Proof of Authority (PoA)	Secure for permissioned networks (Ekparinya *et al.*, 2020).	High transaction throughput and low latency (Ullah *et al.*, 2022).	More scalable than PoW and PoS (Ullah *et al.*, 2022).	Energy-efficient (Ullah *et al.*, 2022).	More centralized than PoW or PoS (Ullah *et al.*, 2022).	Depends on specific implementation and governance model (Ullah *et al.*, 2022).
Pure Proof of Stake (PPoS)	Resistant to common attacks (Gilad *et al.*, 2017).	High transaction throughput and low latency (Chen & Micali, 2019).	More scalable than PoW and traditional PoS (Gilad *et al.*, 2017).	Energy-efficient (Gilad *et al.*, 2017).	More decentralized due to random validator selection (Chen & Micali, 2019).	Equitable distribution of rewards and influence (Gilad *et al.*, 2017).
Federated Consensus	Secure for permissioned networks (Mazières, 2015).	High transaction throughput and low latency (Sankar *et al.*, 2017).	More scalable than PoW and PoS (Mazières, 2015).	Energy-efficient (Sankar *et al.*, 2017).	More centralized than PoW or PoS (Sankar *et al.*, 2017).	Depends on specific implementation and governance model (Sankar *et al.*, 2017).
Hedera Hashgraph	Resistant to common attacks (Leemon *et al.*, 2020; Baird, 2016).	High transaction throughput and low latency (Leemon *et al.*, 2020; Baird, 2016).	Highly scalable (Baird, 2016) .	Energy-efficient (Leemon *et al.*, 2020) .	More decentralized due to distributed network of nodes (Leemon *et al.*, 2020).	Fair and equitable distribution of rewards and influence (Leemon *et al.*, 2020) .

In summary, each consensus algorithm provides unique solutions to the Byzantine General problem in the context of blockchain networks. Proof of Work provides robust security but has scalability and energy efficiency issues. Practical Byzantine Fault Tolerance provides resistance to Byzantine faults but may not scale well in larger networks. Proof of Stake and Delegated Proof of Stake both offer higher efficiency and scalability than PoW but have concerns about power concentration among large token holders. Proof of Authority and Federated Consensus are secure for permissioned networks and offer high efficiency but are more centralized. Pure Proof of Stake and Hedera Hashgraph both aim to provide a more decentralized consensus mechanism with high efficiency and scalability. However, the effectiveness of each algorithm can vary depending on specific network conditions and requirements. In terms of contributions, this research introduces a novel vote aggregation and validation algorithm. Nonetheless, it should be highlighted that this contribution is primarily theoretical, as no empirical experiments have been executed to validate the algorithm's practical efficacy.

4.9 Proposed BBVV protocol

In this study, we propose a protocol designed to streamline the voting process via the implementation of blockchain technology. This is achieved with the application of the Byzantine General's Problem Theory as an underpinning theoretical framework. The steps involved in executing the protocol are as follows:

- **Initialization:**

P: This is the number of the polling station. Each polling station is assigned a unique identifier called **P**. This is important in order to be able to distinguish between different polling stations.

- **Authentication:**

Auth(E): This function represents the authentication process of the Electoral Proof of Stake **(EPoS),** which is labeled **EE**. The function returns **1** if the **EPoS** has been successfully authenticated and **0** if authentication has failed. This step is important to ensure that only authorized persons can participate in the vote.

- **Creation and allocation of Cryptotally:**

CryptoTally(E): This function allows an authenticated **EPoS** to write to the blockchain. An **EPoS** right to write to the blockchain is only created if **Auth(E)** returns the value **1**, indicating successful authentication. The function contains important tallied votes data, such as the total number of all counted votes and the current number of votes for each candidate.

- **Initialization of the counted votes writing process:**

X: This variable represents the total number of counted votes in the election.

Vi: These variables represent the counted votes each candidate has received. This is part of the setup process where the initial counted vote writing to blockchain parameters are set.

- **Write blockchain:**

WriteBlockchain (E, V1, V2,…, Vn): This function symbolizes the process by which the **poll worker/ EPoS** writes the voting data to the blockchain. This includes entering information about candidates, their party names, and party IDs.

- **Consensus and validation:**

Consensus (n, N): This function checks whether a consensus has been reached on the vote count. It returns **1** if at least 67% (the majority) of the **poll workers / EPoS** are of the opinion that the vote count is correct, where **n** stands for the number of officials or agents who agree and **N** for the total number of officials or agents present.

- **Termination:**

Close (C, E): This function represents the conclusion of the vote count writing process, which depends on the consensus result **CC**. If a consensus is reached, the vote count is confirmed and transferred to the blockchain.

Validation and completion:

Validate(E): This function allows a polling station to verify that its vote count has been added or counted correctly in the total national vote aggregation. This step is crucial to ensure the integrity and transparency of the election process.

4.9.1 The BBVV protocol

The BBVV protocol is presented here as a structure illustrated in section 4.9.1.1.

4.9.1.1 The Structure of the BBVV protocol

Start:

1. Initialization

    1.1 Let P be the polling station number, uniquely identifying each station.

2. Authentication

    21 Define a function $\mathbf{Auth}(E)$ where E represents Electoral Proof of Stake (EPoS).

    2.2 if authentication is successful, 0 otherwise as shown in (4.7).

$$\mathbf{f(x)} = \begin{cases} \mathbf{1}, & \textbf{if EPoS is authenticated} \\ \mathbf{0}, & \textbf{otherwise} \end{cases} \tag{4.7}$$

3. CryptoTally assignment:

    3.1 Define a function $\mathbf{CryptoTally}\ (E)$ that generates the right to write for authenticated EPoS given in (4.8).

$$3.2\ \mathbf{CryptoTally}(E) = \mathbf{Auth}(E) \times \textbf{right to write} \tag{4.8}$$

CryptoTally contains information such as: Total counted votes to be **written (y)**, Counted votes for each **candidate (a,b,c,...)**

4. Counted Vote Writing Process Initialization

4.1 Let $\boldsymbol{X}$ be the total number of counted votes to be written.

4.2 Let $\boldsymbol{Vi}$ be the counted votes received by candidate $\boldsymbol{i}$.

5. Consensus and Validation

5.1 Define a consensus function, **consensus(n,N)**, where n is the total number of agreeing officials and $\boldsymbol{N}$ is the total number of officials at the polling station given in (4.9).

$$\textbf{Consensus}(\mathbf{n},\mathbf{N}) = \begin{cases} \mathbf{1} & \begin{cases} \textbf{if} = \dfrac{\mathbf{100n}}{\mathbf{N}} > \mathbf{67} \\ \textbf{otherwise} \end{cases} \\ \mathbf{0} & \end{cases} \qquad (4.9)$$

6. Finalization

6.1 Define a function

6.2 **Finalize(C,E)**, where $\boldsymbol{C}$ is the consensus result and $\boldsymbol{E}$ is the EPoS , this is shown in (4.10).

6.3 **Finalize(C,E)=C×WriteBlockchain(E,$V1$,$V2$,...,Vn)** (4.10)

7. Validation

7.1 Define a function **Validate(E)** for each polling station to verify their counted votes as part of the national totals.

Stop.

Figure 4.8 Illustrates the structured algorithm flow diagram.

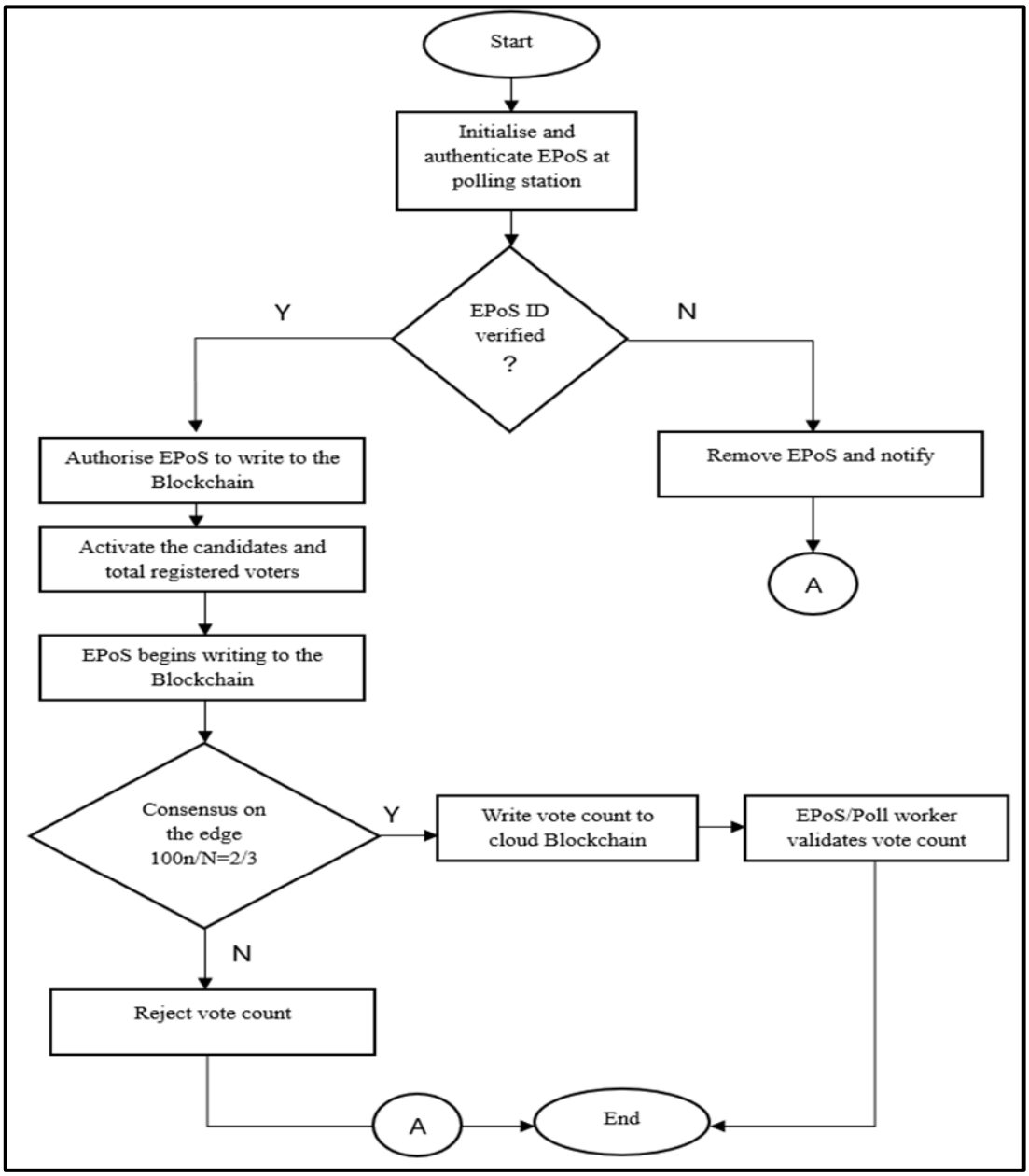


Figure 4-8: Algorithm Flow Diagram: The BBVV Protocol

The proposed algorithm is designed to function at the periphery of the network, enabling a consensus-based vote count that is recorded on the blockchain. Only votes that reach the required consensus are validated and approved.

4.10 Evaluating the BBVV Artefact

This section is dedicated to a careful evaluation of the performance characteristics of the system, emphasising their important role in building trust with the user. This aspect is particularly important for digital systems tasked with monitoring critical processes, such as elections. Furthermore, the evaluations are discussed in detail in this section. The collaborative integration of blockchain technology, complemented by an accessible interface and enhanced by the inclusion of Pera Wallet, offers a dual benefit: operational efficiency and increased user trust. This study not only presents an innovative algorithm for aggregating and validating votes, but also experimentally tests its effectiveness using specific test scenarios. This underlines our intention to fully understand and underline the trustworthiness and reliability of the system.

4.11 Testing the consensus

4.11.1 Assumptions.

Presuming that votes are manually cast and tallied, with only the results from each polling station being recorded on the blockchain, each official involved in the manual counting process should input the results into the smart contract. This allows the smart contract to determine a consensus, provided that each official inputs the same count. If the smart contract achieves a consensus from 67% of all officials who input the same count, then that count is recorded on the blockchain. Subsequently, officials from each polling station should verify whether their total count is included in the national vote aggregate.

4.11.2 Purpose of the test

The purpose of these tests is to verify that vote counts entered by the voting agents, from each polling station and for each candidate satisfy a consensus of 67% of the entered vote counts from the polling agents in that polling station.

a) If a consensus of 67% by the polling agents at that polling station and for a given candidate is reached then the vote count from that polling station for that candidate is written to the blockchain.

b) If a consensus of 67% by the polling agents at that polling station and for a given candidate is NOT (i.e., < 67%) reached then the vote count from that polling station and for that candidate is NOT written to the blockchain.

c) If there is a consensus (i.e., > 67%) from the different polling stations for some candidates then the entered vote counts to the blockchain are aggregated into a national aggregate for those candidates.

4.11.3 Initial verifications on the system

Table 4.2 show the function and the result of the Test Case (TC) executed.

Table 4.2: Test Cases Executed

Function	Description	TC executed	TC passed
Access voting system url -->https://algo-election.vercel.app/	Verifying that the link works	100,00%	100,00%
New Admin	Create a new admin user following provided steps	100,00%	100,00%
Pera Wallet admin user	Create a new Pera Wallet Admin user following provided steps	100,00%	100,00%
Pera Wallet user	Create a Pera Wallet user (polling station agent) and assign Algos.	100,00%	100,00%
New polling station	As Admin create a new polling station	100,00%	100,00%
New candidate	As Admin create a new candidate	100,00%	100,00%
New Polling agent	As Admin create a new Polling agent.	100,00%	100,00%
Submission time extension	Verify that Admin user can extend the vote counts submission time	100,00%	100,00%

Scenario 1

Scenario 1 aims to verify the working of the consensus on some polling stations involving 10 polling agents, i.e., 5 on each polling station, 2 candidates and polling stations based on the 67% consensus formula.

Polling station (PS) 3

In this scenario the 5 agents in the polling station all enter the same number of vote counts as shown in Table 4.3.

Table 4.3: PS3 Votes Entered

Polling agent ID	Candidate no.3 vote count
9	10
10	10
11	10
12	10
13	10

In Table 4.3, on this polling station candidate 3 has a consensus (5/5 =100% consensus) from the five polling agents ---> 10 this will be written to the blockchain for aggregation.

Polling station (PS4) 4

On this scenario from the 5 agents in the polling station, two polling agents enter the same number of vote counts and the other two agents also enter the same number of vote counts while the 5th agent enters a different number of vote counts. This is shown in Table 4.4.

Table 4.4: PS4 Votes Entered

Polling agent	Candidate no.4 vote count
14	11
15	11
16	12
17	12
18	13

In Table 4.4, on this polling station there is NO consensus thus no vote count is written to the blockchain therefore national aggregate will be from the consensus from polling station 3 ----> 10.

Consensus reached on one polling station for one candidate only (candidate no. 3). Consensus was reached only for candidate 3 from PS3. Candidate 4 from polling station 4 had no consensus. Therefore, the National aggregate is only from candidate 3 which is 10 votes.

Scenario 2

In this scenario from the 5 agents in the polling station, two polling agents enter the same number of vote counts, and the other two agents also enter the same number of vote counts while the 5th agent enters a different number of vote counts, as shown in Table 4.5.

Table 4.5: Polling Station 3

Polling agent	Candidate no.4 vote count
9	10
10	10
11	11
12	11
13	12

On this polling station candidate 3 has NO consensus from the five polling agents ---> 0

Polling station 4

In this scenario from the 5 agents in the polling station, two pooling agents enter the same number of vote counts, and the other two agents also enter the same number of vote counts while the 5th agent enters a different number of vote counts. Shown in Table 4.6.

Table 4.6: Polling Station 4

Polling agent	Candidate no.3 vote count
14	11
15	11
16	12
17	12
18	13

On this polling station there is NO consensus either therefore national aggregate will be from the consensus from polling station 3 ----> 10. No consensus reached for any candidates for both polling stations.

No consensus reached on both polling stations, National aggregate for candidate 3 remains 10.

Scenario 3

Polling station (PS) 5

In this scenario from the 5 agents in the polling station, 3 polling agents enter the same number of vote counts and the other 2 agents also enter the same number of vote counts. Shown in Table 4.7.

Table 4.7: Polling Station 5

Polling agent	Candidate no.5 vote count
15	20
16	20
17	20
18	21
19	21

On this polling station candidate 5 has NO consensus from the five polling agents ---> 0. No consensus reached (3/5 = 0.6) on polling station 5.

National aggregate still remains 10 for candidate 3.

Scenario 4

Polling station 6

On this polling station of the 5 polling agents 4 enter the same number of vote counts while the 5th polling agent enters a different vote count. Shown in Table 4.8.

Table 4.8: Polling Station 6

Polling agent	Candidate no.6 vote count
20	5
21	5
22	5
23	5
24	6

On this polling station candidate 6 has consensus from the five polling agents ---> 5.

4 polling agents submit same count for candidate 6 against 1.

After National aggregate candidate 6 votes are added

Scenario 5

Polling station (PS) 5

In this polling station of the 4 polling agents, 2 enter the same vote counts and the other 2 polling agents do NOT turn people. Shown in Table 4.9.

Table 4.9: Polling Station 7

Polling agent	Candidate no.5 vote count
30	21
31	21
32	
1	

On this polling station 2 polling agents did not submit and 2 submitted identical for the same candidate.

Candidate 5 vote counts not included in National aggregate.

Scenario 6 --- National aggregates

The following abbreviations are used for polling stations.

Polling agents: ZH2NA ---> polling agent Id = 9

QO47N ---> polling agent Id = 10

EH4MT ---> polling agent Id = 11

5W4HY ---> polling agent Id = 12

O3F5H ---> polling agent Id = 13

RPCDE ---> polling agent Id = 14

UTH6O ---> polling agent Id = 15

7CFEW ---> polling agent Id = 16

WLUNH ---> polling agent Id = 17

3X2NX ---> polling agent Id = 18

Polling stations: Polling station Id 1, Polling station Id 2

Candidates: Candidate name = Shaka, Candidate Id = 1

Candidate name = TEST, Candidate Id = 2

Candidate name = ECOFORUM, Candidate Id = 3

Candidate name = EFF, Candidate Id = 4

Candidate name = GOOD, Candidate Id = 5

Candidate name = VF PLUS, Candidate Id = 6

Table 4.10 shows the entered vote counts by the 5 agents for the 6 candidates for polling station 1.

Polling station 1

Table 4.10: Six Candidates Vote Counts Ps 1

	Submitted vote counts for candidates					
Polling Agents Id	Id = 1	Id = 2	Id = 3	Id = 4	Id = 5	Id = 6
ZH2NA Id 9	5	6	8	10	14	20
QO47N Id 10	5	6	8	10	15	21
EH4MT Id 11	5	6	8	11	16	22
5W4HY Id 12	5	6	9	12	17	0
O3F5H Id 13	5	7	9	13	18	0
Consensus (Yes/ No)	Yes	Yes	No	No	No	No

Table 4.11 shows entered vote counts by the 5 agents for the 6 candidates for polling station 2.

Polling station 2

Table 4.11: Six Candidates Vote Counts Ps 2

	Submitted vote counts for candidates					
Polling Agents Id	Id = 1	Id = 2	Id = 3	Id = 4	Id = 5	Id = 6
RPCDE Id 14	2	3	4	6	15	9
UTH6O Id 15	2	3	4	6	15	10
7CFEW Id 16	2	3	4	7	0	11
WLUNH Id 17	2	3	5	7	0	12
3X2NX Id 18	2	4	5	8	0	13
Consensus (Yes/ No)	Yes	Yes	No	No	No	No

4.11.4 Test Report Summary

The system works well and fulfils the requirements in the user stories for a voting system. Verifying accessibility and operability of the system the following functions were verified.

A)

Creation of Admin users

Creation of Pera Wallet users

Allocation of Algos to Pera Wallet users to enable them to submit vote counts.

Creation of polling stations

Creation of polling agents

Creation of voting candidates

B)

In a series of experiments, the effectiveness of a consensus algorithm requiring 67% agreement for consensus was evaluated in five different scenarios. These tests used five polling agents, four candidates and two polling stations. The scenarios provided demonstrate the performance of the algorithm. In particular, they show the successful recording on the blockchain of vote counts that meet the consensus criteria, while at the same time excluding and not recording those counts that do not reach the required consensus.

C)

In Scenario 6, we build on the foundations laid in Scenarios 1 to 5 by increasing the number of agents and candidates involved. Our experiments involved 6 candidates and 10 polling agents, with 5 polling agents per polling station evenly distributed across 2 polling stations. We carefully examined different permutations of the vote counts recorded by all 10 polling agents in both polling stations for each candidate. Corresponding tables are attached to this report for further illustration. Before consolidating the national aggregate for each candidate, we ensured that the consensus was validated. The national aggregate result calculated by the system matched seamlessly with the expected result based on the vote counts entered.

4.12 Interpretation and Visualisation on Actual Data

The data analysis and visualisation presented provides valuable insights into various aspects of a blockchain-based voting system and offers a comprehensive understanding of data trends and results. The data includes information on consensus reached, transaction performance, traffic patterns and election-related statistics. These insights can help decision-makers, network operators and stakeholders make informed decisions, optimise system performance, and evaluate the efficiency of the election process.

In the evaluation carried out, a random number of polling agents were introduced to input the same vote count, symbolising the small ‘n’ in the formula 100n/N=2/3 majority (67% and above), keeping ‘N’ constant.

4.12.1 Consensus reached and not reached

The graph in Figure 4.9 shows a bar chart. The red bar represents No (consensus not reached), and the blue bar represents Yes (consensus reached). The above analysis shows that a larger percentage of the vote count did not reach consensus.

Labelling of the X-axis ("consensus"): This label indicates the categories plotted on the X-axis, i.e., the different types of consensuses.

Y-axis label ("Number"): The label on the y-axis indicates that the number of occurrences is measured.

Interpretation:

- This plot is a bar chart that shows the distribution of different consensus outcomes.
- It helps visualise how many times each type of consensus outcome (e.g., "Yes" or "No") has been reached in the data.
- By observing the height of the bars, you can quickly determine the frequency or count of each consensus outcome.
- The colours differentiate between different types of consensus outcomes. In this case, red and blue bars represent different consensus results, such as "Consensus Reached - Yes" and "Consensus Reached - No."

Given the above interpretation and the bar chart. It shows that only about 5% of the of the officials arrived at a consensus level the remaining 95% did not reach consensus.

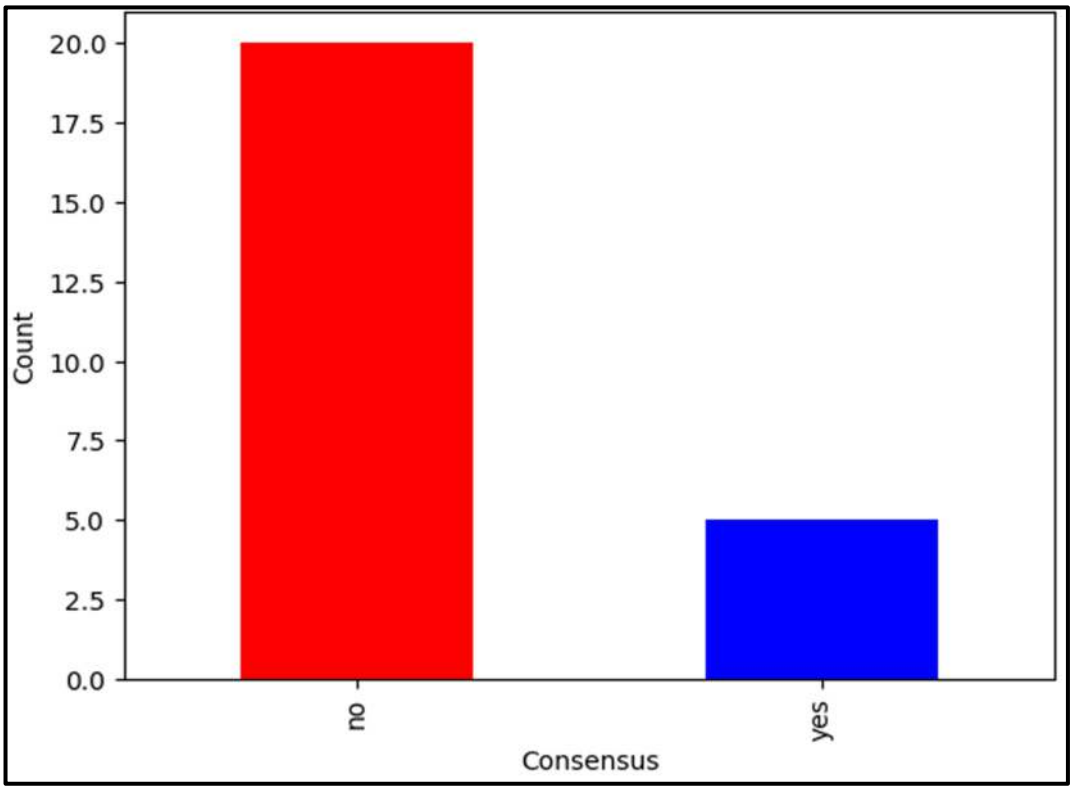


Figure 4-9: Consensus Reached

4.12.2 Actual data compared to the aggregation of consensus reached

In Figure 4.10, the bar on the left, labelled 'Total Vote Count,' represents the total vote count for all data, irrespective of whether 'Consensus Reached' is 'Yes' or ‘Not’.

The bar on the right, labelled 'Total Vote Count (Consensus Reached Yes), represents the total vote count, considering only the rows where 'Consensus Reached' is 'Yes.'

The plot allows you to visually compare these two categories of vote counts. It's a straightforward way to see how the total vote count changes when 'Consensus Reached' is 'Yes' and when it is not. The colour-coding (blue and green) helps distinguish between the two categories.

This information is useful for understanding the impact of 'Consensus Reached' on the total vote count. The above plot shows that the total number of vote count is greater than the

aggregate consensus vote count. Only about 10% of the vote count submitted will be taken into consideration as those were the vote count that reached consensus.

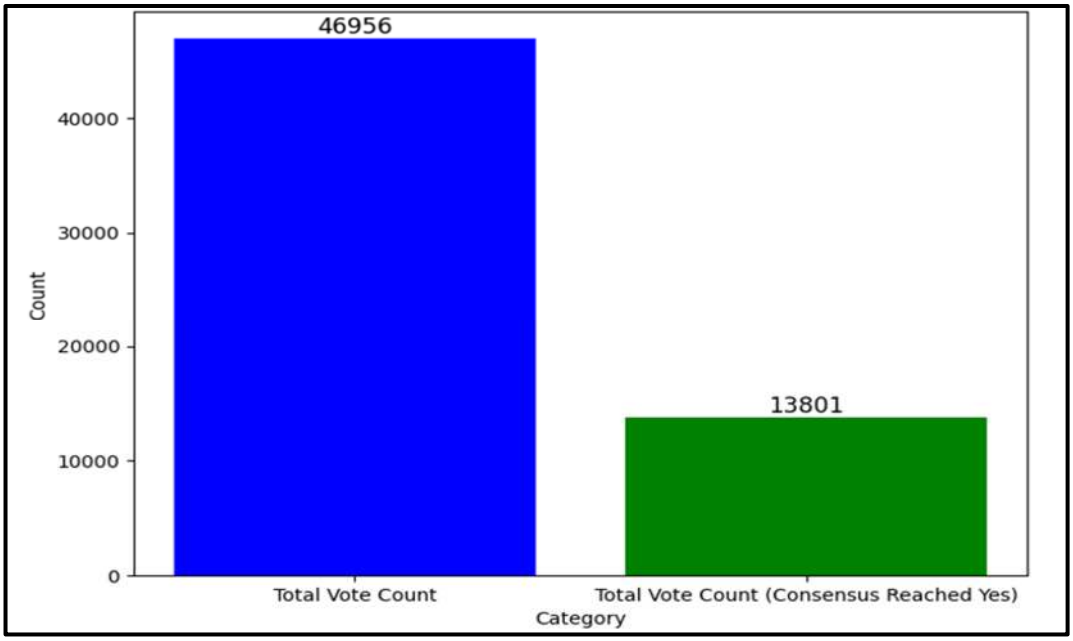


Figure 4-10: Comparative Analysis of Actual Vote Count and Consensus Vote Count

4.12.3 Officials in agreement compared with total officials

The Officials in Agreement (n) vs Total Number of Officials (N) were also visualised as indicated in Figure 4.11, where:

Y-Axis (Count): The y-axis represents the count, which measures the number of officials in agreement (n) and the total number of officials (N).

X-Axis Label (S/N): The label on the y-axis specifies that the count is being measured.

Legend: The legend on the plot explains the colour code for the bars. The green bars represent "Officials in Agreement," while the blue bars represent "Total Number of Officials (N)."

Interpretation:

- This plot provides a visual comparison between the count of officials who agree and the total number of officials.
- By observing the height of the bars, it can be determined whether most officials agree or if there is a significant disagreement on the vote count captured at the polling station.
- The plot is useful for decision-makers or officials to quickly grasp the level of consensus or disagreement among a group of officials.
- If the green bars (Officials in Agreement) are close in height to the blue bars (Total Number of Officials), it indicates a high level of agreement. Conversely, if the green bars are significantly shorter, it suggests a lower level of agreement.

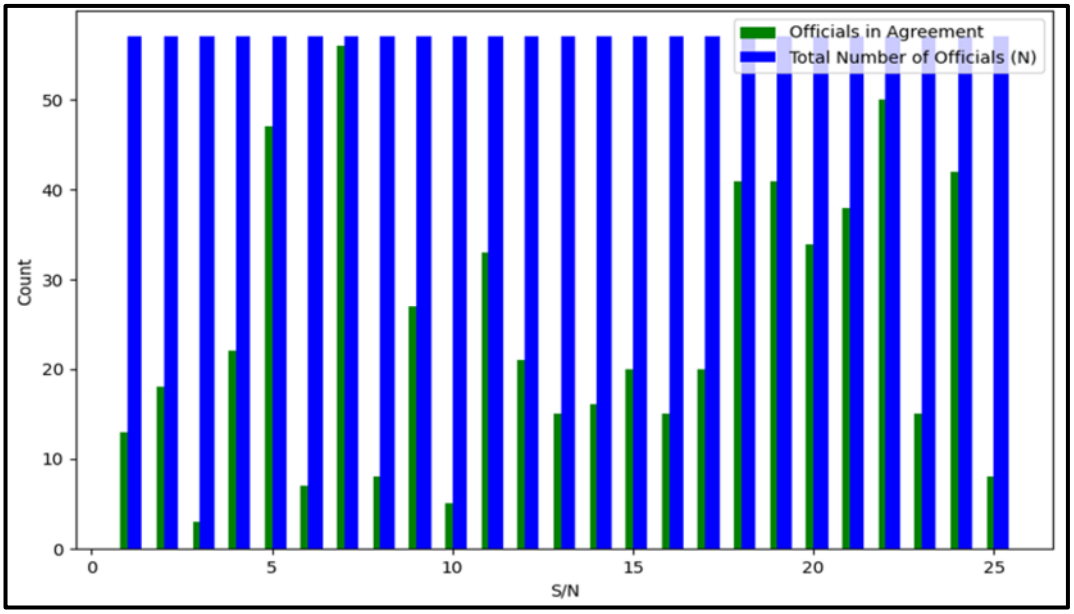


Figure 4-11: Officials in Agreement vs Total Number of Officials

In summary, this plot is a visual tool for officials to assess and understand the degree of consensus or agreement among a group of officials in a clear and concise manner. And the above plot shows a significant level of disagreement between the officials. Which means little level of consensus was reached however, this was caused by the randomised data which was introduced in the actual data.

4.12.4 Transaction Performance Metric Analysis

The graph in Figure 4.12, visualises the transaction confirmation time over different confirmed rounds.

Interpretation:

The plot allows you to observe how the confirmation time for transactions varies over different rounds. You can look for patterns, spikes, or fluctuations in confirmation times. Sudden peaks may indicate delays in transaction processing, while valleys represent quicker confirmations. There was a delay in the transaction at point 35000 seconds which was confirmed in 3.20 confirmed rounds.

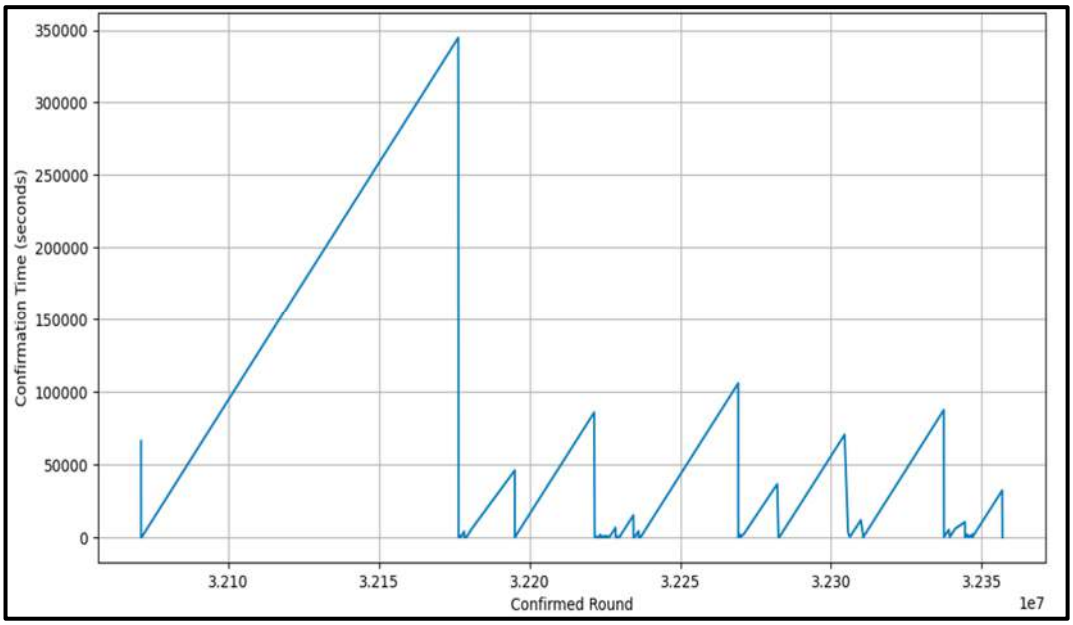


Figure 4-12: Transaction Metrics

4.12.5 Transaction Throughput Over Rounds Analysis

The illustrated plot in Figure 4.11, visualises transaction throughput over different confirmed rounds.

Interpretation:

The graph in Figure 4.13 helps to understand the capacity of the system to process transactions. It shows how many transactions were confirmed per second during different rounds. Higher peak values indicate better throughput, while lower values may suggest congestion or reduced processing capacity. The confirmed rounds at 3.20, 3.222 and 3.23 respectively had a higher peak value, indicating better throughput.

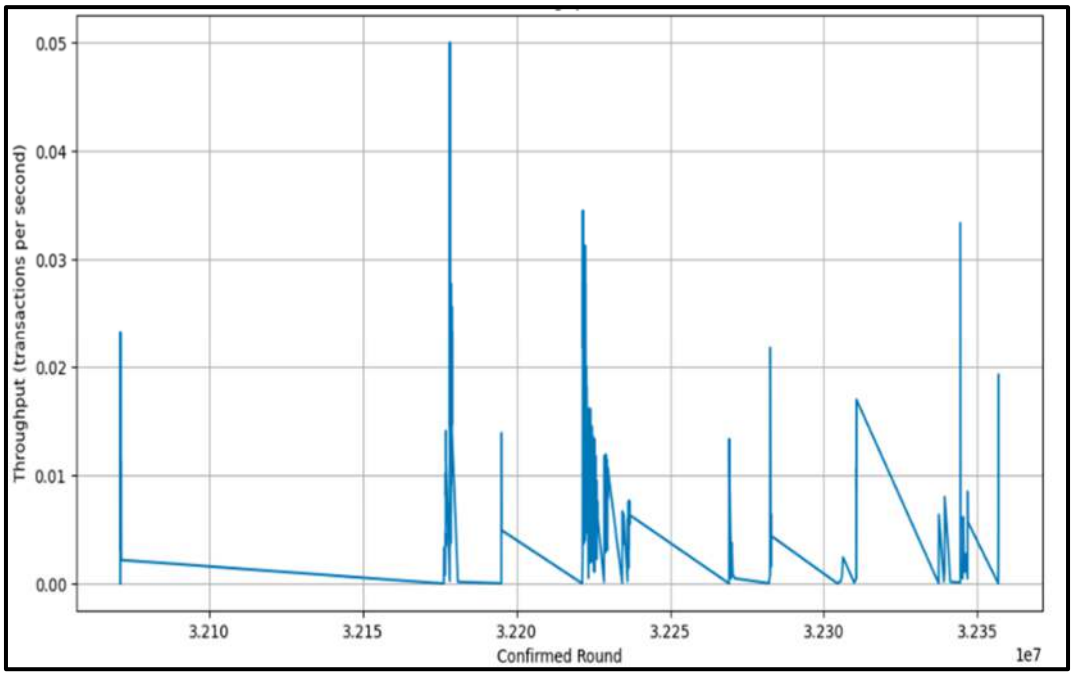


Figure 4-13: Transaction Throughput

4.12.6 Saturation Analysis

The graph in Figure 4.14 shows a line graph, where each point on the line corresponds to a specific timestamp (time) and its associated transaction fee. The points are marked with circular markers ("o") connected by lines ("-"). This visualization method allows you to track changes in transaction fees over time.

X-Axis (Timestamp): The x-axis represents time in the form of timestamps. It shows when the transactions were confirmed. This axis allows you to track the progression of time.

Y-Axis (Transaction Fee in Algos): The y-axis represents the transaction fee in Algos. It quantifies the cost associated with each transaction. Transaction fees are typically used to incentivise network nodes to process and confirm transactions.

Interpretation:

- The plot provides an overview of how transaction fees change over time. It can help you identify trends and patterns in transaction fees on the blockchain network.
- Rising transaction fees might indicate increased demand for network resources, potentially suggesting network congestion.
- Falling transaction fees may indicate reduced demand or improved network efficiency.
- Sudden spikes in transaction fees could be linked to particular events, such as a surge in network usage or the introduction of new applications or assets on the blockchain.
- A consistent flat line could suggest stability in the network with relatively constant transaction fees.

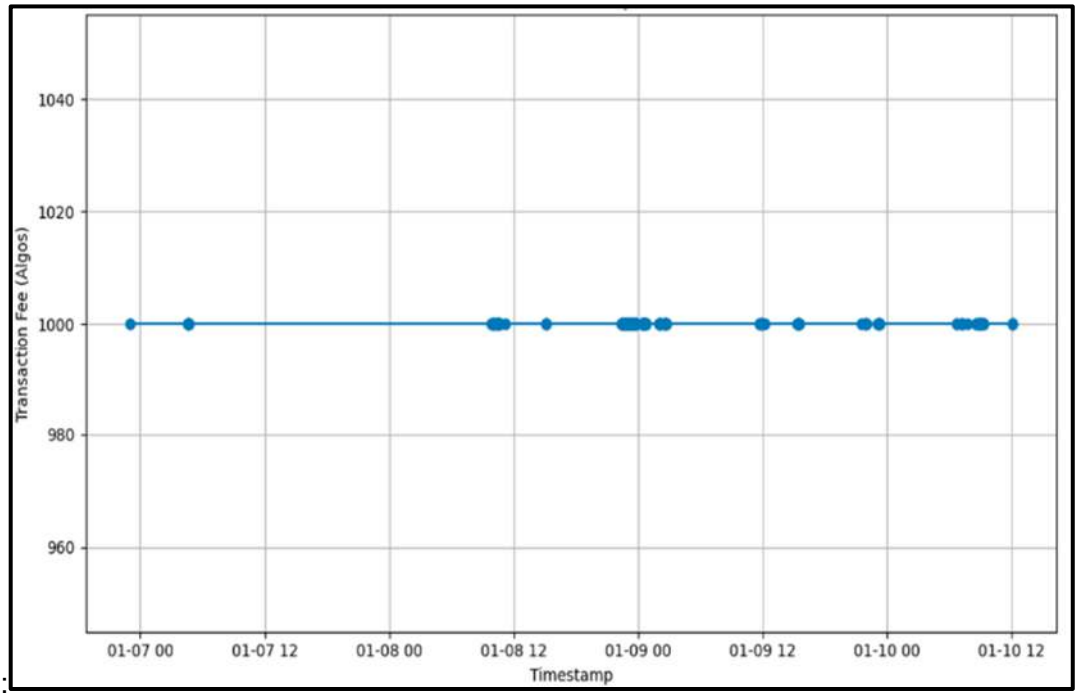


Figure 4-14: Saturation Analysis

The Saturation Analysis plot in Figure 4.12, shows a consistent flat transaction fee across different timestamp and transactions. This suggests stability of the BBVV artefact on the Algorand network. Understanding how transaction fees change over time is essential for blockchain users, developers, and network operators to make informed decisions and adapt to changing conditions on the network. The visualization can also be useful for forecasting and optimising transaction costs.

4.12.7 Latency Analysis

The graph provided in Figure 4.15, helps in understanding the latency in the confirmation of transactions over a period. The plot is a line graph, with each data point represented as a circular marker ("o") connected by lines ("-"). This visualization method allows you to track changes in latency over time.

Interpretation:

- The plot provides insights into the latency experienced by transactions on the blockchain network.
- An upward trend in latency suggests that transaction confirmation times are increasing, which might indicate network congestion or increased demand.
- A downward trend in latency indicates decreasing confirmation times, potentially due to network optimisation or reduced demand.
- Spikes in latency might be linked to specific events or congestion periods when transactions are taking longer to confirm.
- Consistent, stable latency indicates that the network is maintaining a relatively constant confirmation time.
- Fluctuations in latency can reveal patterns and help users and developers understand the performance of the blockchain network at different times.

This plot is valuable for assessing the efficiency and responsiveness our artefact (BBVV) on the Algorand blockchain network in processing transactions. Monitoring and analysing latency trends can assist in making informed decisions about when to submit transactions to achieve desired confirmation times and to identify periods of network stress or congestion. The plot

indicates an upward trend in latency which suggest that confirmation times are increasing, which might indicate network congestion or increased demand.

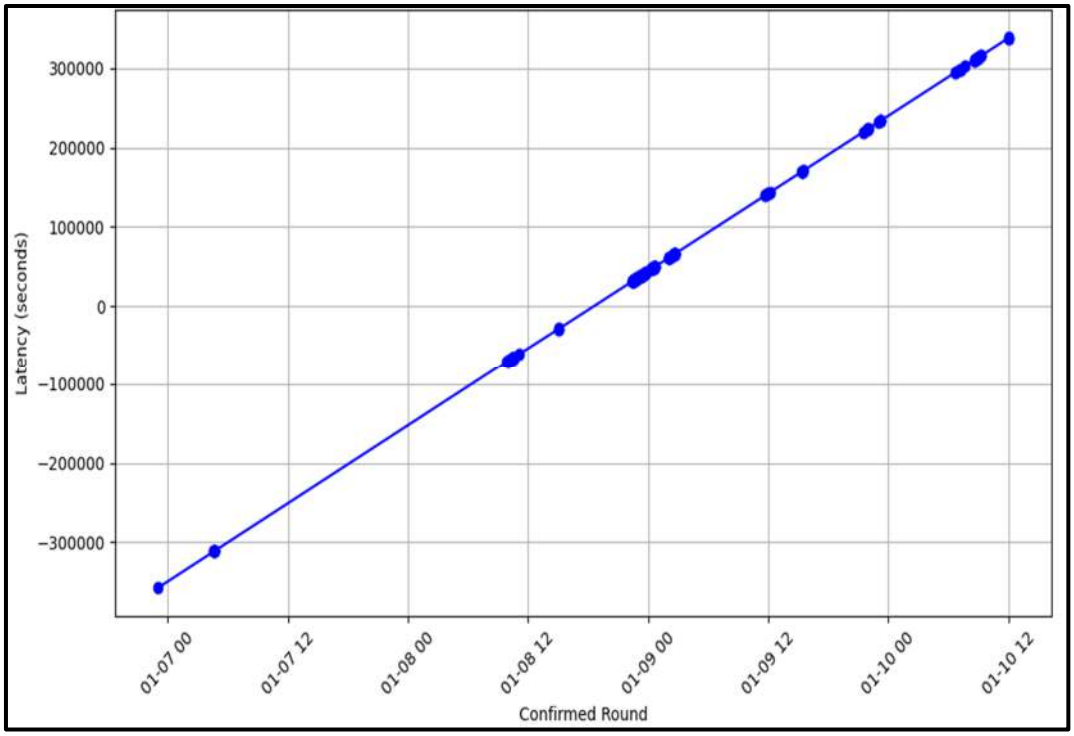


Figure 4-15: Latency Analysis

4.12.8 Traffic Analysis

This type of analysis is useful for understanding transaction behaviour and identifying trends or anomalies in the dataset over time. It can be helpful for monitoring network activity, identifying peak usage times, or analysing the impact of specific events on transaction traffic. Figure 4.16 counts the number of transactions in each round and plots the results as a line chart.

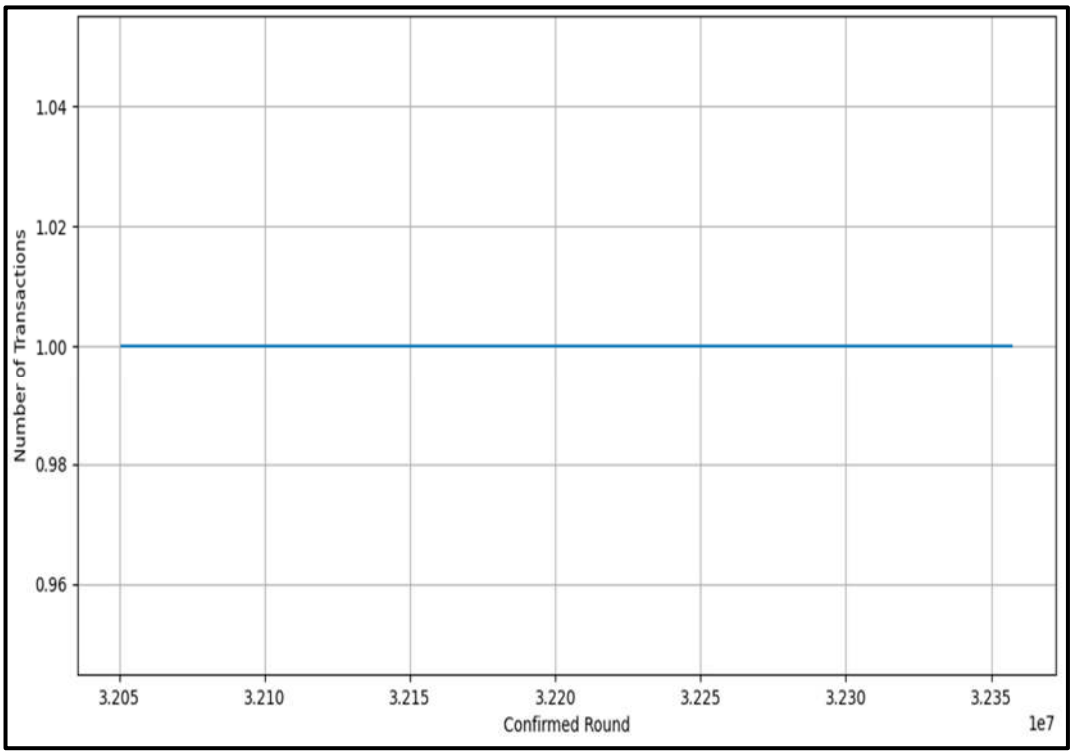


Figure 4-16: Traffic Analysis

Here's an interpretation of the plot:

X-Axis (Confirmed Round): This represents the "confirmed round" of the transactions, which appears to be a measure of time or sequence of events. As the confirmed round increases, it indicates the progression of time or the order in which transactions were confirmed.

Y-Axis (Number of Transactions): This axis represents the number of transactions that were confirmed in each round. It measures the intensity of transaction activity during each round.

Interpretation:

The plot in Figure 4.12 shows how the number of transactions varies over time (confirmed rounds). You can see patterns, spikes, or fluctuations in transaction activity. For example, if there are sudden peaks in the graph, it suggests moments of high transaction activity, while flat regions indicate periods with lower transaction volumes. The above graph shows flat regions which indicate a prolong moments of low transactions.

Grid Lines: The grid lines help in reading the values more accurately and are present in both the X and Y axes.

4.13 Conclusion

In order to achieve the second objective of identifying the necessary system specifications for the BBVV artefact, this study explored the perceptions and expectations of electoral stakeholders in relation to vote counting and validation processes in different African countries. The data collected was subjected to thematic analysis. Challenges such as poor network connections, lack of staff training and corruption were identified. However, through this analysis, key specifications for a vote counting and validation system were established to improve the accuracy and overall integrity of the elections. To ensure a smooth electoral process, the system should primarily ensure accuracy, speed, efficiency, transparency and security during the counting, validation and transmission phases.

For the third objective of this research, the study looked at the world of blockchain protocols and consensus algorithms. It is noticeable that each consensus algorithm offers different solutions to the general Byzantine problem in the Blockchain context. While some, like Proof of Work, offer robust security, they struggle with scalability and power issues. In contrast, options such as Pure Proof of Stake and Hedera Hashgraph aim to provide a decentralised consensus mechanism that comes with efficiency and scalability. However, their effectiveness may depend on the specific network conditions and requirements. In this study, an innovative vote aggregation and validation algorithm was proposed, but its effectiveness was experimentally tested in the next chapter.

Regarding the fourth objective of this study, the development and evaluation of the BBVV artefact represented by the vote collection artefact has been carefully conducted, including a thorough evaluation in terms of performance, saturation, traffic analysis and transaction throughput. The front-end of this system is based on a client-server architecture model that integrates Next.js with a smart contract developed by Algorand with PyTeal on the back-end. As security is critical, the system includes Pera Wallet for robust authentication and advanced transaction signatures. This configuration allows users to interact with the front-end via browsers, exchange data with the smart contract and utilise Pera Wallet for superior security for both authentication and transactions. The comprehensive evaluation of the system, which

focuses on performance, ability to handle high traffic and peak loads (saturation), traffic analysis to optimise data flow and transaction throughput efficiency, ensures that the BBVV artefact not only meets its design and functional criteria, but also adheres to the highest standards of reliability and trustworthiness that are essential for modern voting systems.

Chapter 5 looks at research findings by discussions of this study.

CHAPTER FIVE: FINDINGS AND DISCUSSIONS

5.1 Organisation of the Chapter

Chapter 5 offers a comprehensive examination of the study. It begins with an 'Introduction' (Section 5.2), which sets the outline for the chapter. This is followed by a 'Review and identification of existing blockchain solutions in voting systems' (Section 5.3), before moving on to the 'System specifications for the BBVV artefact' (Section 5.4). The chapter continues with the 'Selection of the blockchain protocol and consensus algorithm' (section 5.5), followed by the 'Development and evaluation of the BBVV artefact' (Section 5.6). The implications of these results are analysed in the 'Discussions' (Section 5.7). The section 'Design Science Research in Action' (Section 5.8) demonstrates the application of these principles. Theoretical concepts are applied in 'The Byzantine Generals Problem in Action' (Section 5.9) and 'The Binary Byzantine Agreement Protocol (BBA)' (Section 5.10). A 'Comparative analysis of the results with the literature' (Section 5.11) contextualises the research findings. The chapter concludes with a 'Conclusion' (Section 5.12), which summarises the most important results and findings.

5.2 Introduction

In this important chapter, we summarise and analyse the results of our extensive research into the development of a blockchain-based voting validation artefact (BBVV) to improve the integrity and reliability of vote systems. This research journey was guided by four distinct but interrelated objectives, all contributing to the overarching goal of creating a more secure, transparent, and trustworthy electoral process through innovative blockchain technology.

Our first objective was a thorough review and identification of existing blockchain solutions for vote systems. This research was crucial to understand the current landscape, identify best practises and recognise gaps in existing technologies. The insights gained here formed the basis for our subsequent goals and the development of the BBVV artefact.

The second objective was to identify the necessary system specifications to develop a BBVV artefact with powerful features that would inspire user confidence. Here we looked in depth at the technical and functional requirements that are essential for a robust voting system. We

analysed aspects such as the system architecture, security protocols, user interface and scalability.

Our third objective was to find a suitable blockchain protocol that not only supports the trustworthy aggregation of votes, but also integrates a suitable consensus algorithm to validate the vote count. Choosing the right blockchain protocol was crucial as it forms the backbone of the BBVV artefact and ensures the accuracy, transparency, and security of the voting process.

Finally, the fourth objective led us to the actual development and rigorous evaluation of the BBVV artefact. This phase was important to bring our research into a tangible form. We evaluated the artefact's performance characteristics, including its ability to handle real-life voting scenarios, its tamper resistance, and its overall effectiveness in promoting trust between users.

This chapter provides a detailed analysis of the results in relation to each of these goals. We discuss the implications of our research, the challenges we encountered, and the innovative solutions we developed to overcome them. Through this discussion, we aim to contribute valuable insights in the field of voting systems and pave the way for more secure, efficient, and trustworthy voting processes in the digital age.

5.3 Review and Identification of Existing Blockchain Solutions in Electoral Systems

5.3.1 Findings

A systematic literature review was conducted to answer four primary research questions related to the application of blockchain technology in vote counting. For research question 1 (RQ1), which focuses on existing blockchain solutions for vote counting, the review process was initiated with 791 studies and narrowed down to 54 high-quality papers. These studies examined a variety of methods, including the use of private and public blockchains with machine learning and smart contracts, permissioned blockchains such as Hyperledger Fabric, and cryptographic functions such as the SHA-256 algorithm, as well as integration with IoT and elliptic curve cryptography.

In answering Research Question 2 (RQ2), the comparative analysis of these solutions highlighted common methods and approaches, with Ethereum and Hyperledger Fabric emerging as common choices. However, challenges such as high computational costs (especially Ethereum's gas fees), scalability issues and security vulnerabilities were identified as major limitations.

For research question 3 (RQ3), the strength of evidence for different solutions was assessed. It was found that the use of smart contracts on blockchain platforms could significantly improve the cost efficiency and scalability of electronic voting systems. The importance of consensus algorithms, particularly Proof of Work and Proof of Stake, was also emphasised due to their potential to reduce computational costs and improve system efficiency.

Research Question 4 (RQ4) explored the implications of these findings for the development of new solutions. The review suggested possible improvements, including the introduction of alternative platforms such as Corda or Quorum, other cryptographic algorithms and other programming languages. Suggested combinations included Quorum with homomorphic encryption and Go, Corda with secret sharing and Rust, and Algorand with zero-knowledge proofs and Scala or PyTeal, each offering a unique blend of security, scalability and efficiency.

The implementation of these proposed solutions included setting up the Algorand network, developing smart contracts using the Algorand SDK and PyTeal, and using Pera Wallet to validate votes without revealing their contents (Mwansa & Kabaso, 2023a). The proposed architecture on the Algorand platform includes non-relay nodes to achieve consensus in vote counting and ensure the accurate inclusion of each polling station's votes in the national count. This systematic literature review thus provides a comprehensive understanding of the current landscape of blockchain technologies in election systems and provides a roadmap for future advances in secure and transparent voting processes.

5.3.2 Discussions

In our discussion of the results of the systematic literature review, it becomes clear that blockchain technology offers significant potential for improving the integrity and transparency of vote counting systems in elections. The variety of approaches identified in the review indicates a growing interest and experimentation in this area.

The use of private and public blockchains in conjunction with machine learning and smart contracts, as in the studies by Cheema *et al.* (2020b), Parmar *et al.* (2021b) and Fezzazi *et al.* (2021), demonstrates an innovative approach to secure and efficient voting systems. These methods leverage the strengths of blockchain technology, including decentralisation and immutability, to ensure the security and accuracy of vote counting. However, the high computational costs and scalability issues, particularly with Ethereum gas fees, as noted by Wisessing *et al.* (2020) and Yu *et al.* (2018a), pose significant challenges that need to be addressed.

The use of permissioned blockchains such as Hyperledger Fabric, explored in studies by Jagjivan *et al.* (2021b) and Sharma *et al.* (2021b), provides a controlled environment that may be more suitable for voting systems. However, the scalability and security concerns raised by these authors also emphasise the need for further research and development in this area.

The integration of cryptographic functions, in particular the SHA 256 algorithm and non-interactive zero-knowledge proof, as discussed by Agbesi & Asante (2019b) and (Adiputra *et al.* (2019), adds an additional layer of security to the voting process. This approach ensures the anonymity of voters and vote integrity, which are fundamental for maintaining the trustworthiness of the electoral process.

As the studies by Hjalmarsson *et al.* (2018a) and Fernandes *et al.* (2021) show, the implementation of smart contracts, especially on the Ethereum platform, is promising for automating and securing the voting process. However, the associated high costs and limited scalability emphasise the need for more efficient and cost-effective solutions.

Exploring alternative platforms and cryptographic methods, as proposed by Rathore & Ranga, (2021b) and Luo (2021), is one way to overcome these limitations. The proposed combinations, such as the use of quorum with homomorphic encryption and Go and Algorand with zero-knowledge proofs and Scala or PyTeal, offer innovative solutions that could address the current challenges in blockchain-based voting systems.

To summarise, while blockchain technology offers promising solutions for secure and transparent vote counting, the challenges of high computational costs, scalability and security vulnerabilities still need to be thoroughly addressed. The exploration of alternative platforms,

cryptographic methods and programming languages, as highlighted in this review, provides a direction for future research and development in this area. The implementation of these innovative solutions could significantly improve the efficiency, security, and trustworthiness of electronic voting systems.

5.4 System Specifications for BBVV Artefact

5.4.1 Findings

The research results for the requirements specifications received from the stakeholders of the study on the development of a blockchain-based artefact for vote counting and validation are summarised in five key themes:

1. **Technical aspects:** The majority of respondents used manually operated equipment to count votes and pointed to the use of digital transmission devices such as IEMS and BVAS, which transmit results via scanned images but do not count or verify them. Concerns were raised that the electronic devices could potentially be manipulated in favour of certain parties.
2. **Accuracy, speed, and efficiency:** Respondents reported problems with delays in vote transmission due to poor 3G network coverage and inaccuracies in manual vote transmission. While opinions on efficiency varied, there was a consensus on the importance of accuracy and security as critical performance metrics, with concerns about speed and efficiency in voice transmission and certification.
3. **Transparency and security:** Respondents emphasised the need for transparent procurement, adequate testing, clear legislation and comprehensive communication plans to maintain transparency and build trust. Security measures such as encrypted VPN networks and policing were emphasised as significant.
4. **Challenges and improvements:** Challenges cited included limited network coverage, legal issues, lack of staff training and potential election manipulation. Suggestions for improvement included stakeholder participation, better network coverage, electronic transmission systems and electoral regulation reforms.
5. **The role of electoral management bodies (EMBs) and observers:** The importance of observers in ensuring the accuracy and integrity of vote counting and validation was emphasised. Respondents suggested verification through forms and the presence of

agents and candidates during the counting process. While foreign observers are not responsible for the accuracy of the count, they provide valuable insights.

The application of activity theory provided insights into the interplay of various factors in the voting process, such as the impact of aids, community engagement and the division of labour between stakeholders. The challenges identified, such as poor network coverage, inadequate staff training and corruption, were understood as results of these interactions.

From this analysis, system requirements for a vote counting and validation artefact were derived, focusing on accuracy, speed, efficiency, ease of use, security, transparency, scalability, reliability, compliance with rules and regulations, stakeholder engagement and monitoring capabilities.

The Unified Modelling Language (UML) was used to specify these requirements and describe the interactions between election officials, central election collection points and stakeholders for different use cases. This approach provided a comprehensive overview of the necessary functions and interactions for a successful election system and highlighted the need for accurate, efficient, transparent, and secure processes in modern election systems. In Figure 5.1 shows the following processes:

1. Counting the votes (UCb): In this step, the poll worker totals all the votes cast.
2. Recording of votes (UCa): Here the poll worker logs every vote cast by a voter.
3. Validation of results (UCc): At this stage, the poll worker checks the accuracy of the votes counted.
4. Transmission of results (UCd): Finally, the poll worker sends the confirmed and validated results to the central election collection centre.

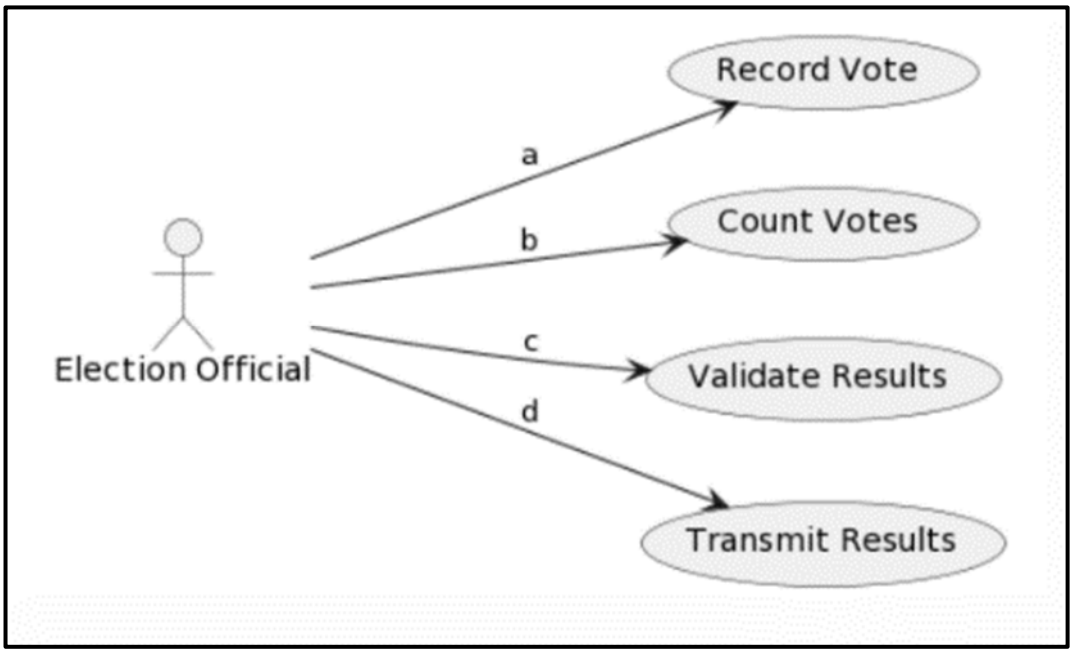


Figure 5-1: Interactions (Mwansa & Kabaso, 2023b)

Figure 5.2 shows the activity diagram in which three main actors are involved: the election official, the central election collection centre, and the stakeholder. In this diagram, the use cases are represented as rectangular nodes, while the actions of the actors are indicated by directional arrows.

The process begins with the poll worker recording each vote. These votes are then counted. Once counted, the election officer validates the results to ensure their accuracy. After validation, the results are forwarded to the Central Election Collation Centre. At this stage, the centre is responsible for monitoring the transmission of the results and producing reports based on the data received. In the final step, the stakeholder takes on the task of checking these results (Mwansa & Kabaso, 2023b).

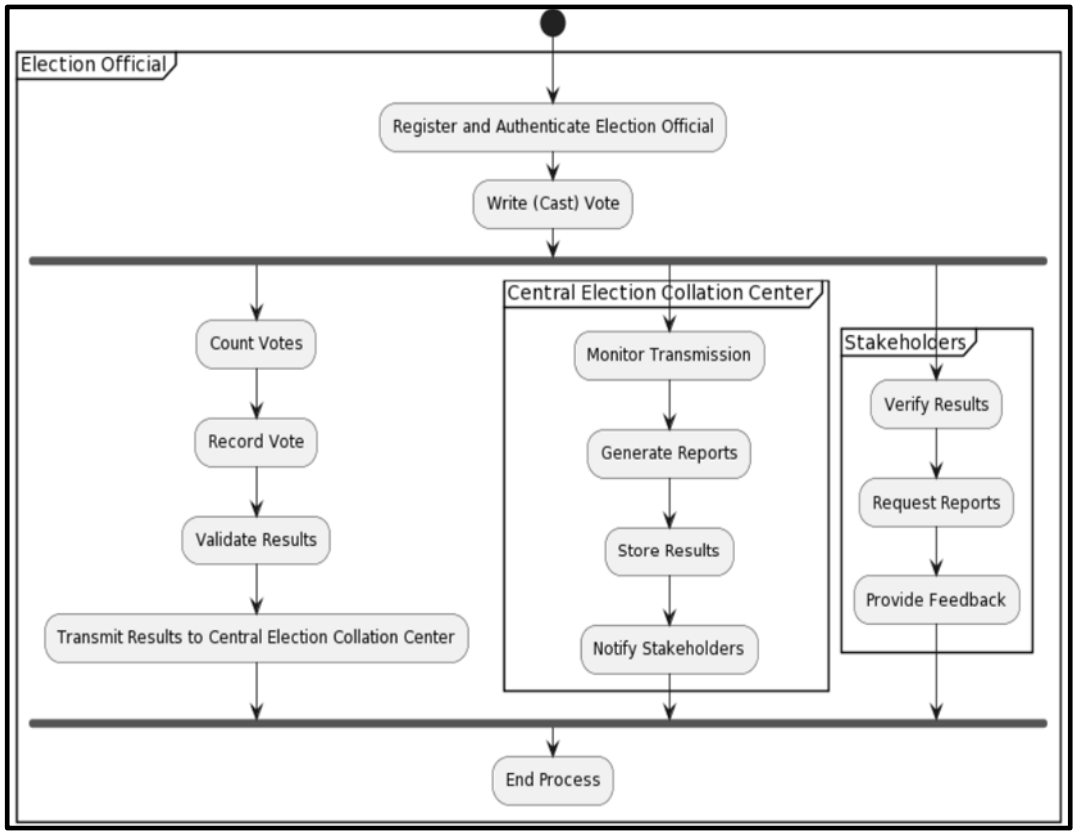


Figure 5-2: Activities in the election process

5.4.2 Discussions

The discussion of how the identified specifications for a blockchain-based vote counting and validation artefact align with user needs and existing challenges, as well as their implications for system development, can be structured as follows:

5.4.2.1 Alignment with User needs and Challenges.

Technical aspects: The preference for manually operated vote counting devices and the use of digital transmission kits such as IEMS and BVAS reflects the need for systems that combine reliability and technological advancement. Even though these systems primarily transmit the results and do not count or verify them, their integration with blockchain-based voting removes concerns about possible manipulation and strengthens confidence in the impartiality of the system.

Accuracy, speed and efficiency: The problems associated with network connectivity and the accuracy of manual vote transmission underline the need for a blockchain-based system that ensures fast data transmission and minimises human error. The importance placed on accuracy and security in the research emphasises the need for a blockchain system that is both reliable and efficient, addressing the existing inefficiencies and delays in traditional voting systems.

Transparency and security: The emphasis on transparent processes and robust security measures such as end-to-end encryption and monitoring is in line with the inherent characteristics of blockchain technology, which provides transparency in vote counting and increased security against unauthorised access and tampering.

Challenges and improvements: Challenges such as network coverage, legal concerns and staff training reflect the complexity of deploying blockchain technology in different electoral environments. Overcoming these challenges requires a system that is adaptable, user-friendly and compliant with legal standards. These are the key considerations when developing blockchain-based voting systems.

The role of EMBs and observers: The importance of EMBs and observers in ensuring the integrity of elections demonstrates the need for systems that enable real-time monitoring and verification. Blockchain technology, with its ability to create an immutable audit trail, fulfils this need and provides transparency and verifiability for various stakeholders.

5.4.2.2 Implications for System Development

Accuracy and reliability: Developing a system that prioritises accuracy and reliability is essential. The immutability of blockchain can ensure that once a vote has been recorded, it cannot be altered, which directly addresses concerns about accuracy and potential vote tampering.

Network and technical requirements: Different network conditions need to be considered during development, especially in regions with poor connectivity. This means that lightweight blockchain solutions need to be developed that can work effectively in low bandwidth environments.

User-friendly interface: Considering the challenges of training employees, the system must have an intuitive, user-friendly interface that requires minimal training. This is in line with the principles of universal design and makes the system accessible to a wide range of users.

Compliance with legal and regulatory requirements: The system must be developed in line with existing legal frameworks and electoral regulations. This means that the technology can be adapted to different legal frameworks and updated as regulations evolve.

Security protocols: The implementation of robust security measures, including encryption and secure communication channels, is essential. This ensures protection against cyber threats, which are a major concern with digital voting systems.

Stakeholder engagement and transparency: The system should facilitate stakeholder engagement and ensure transparency throughout the voting process. Features such as real-time monitoring and open audit trails can increase stakeholder trust and participation.

Scalability and flexibility: The system must be scalable to handle different numbers of voters and flexible enough to adapt to different types of elections. This requires a modular structure that can be customised to the specific needs of voters.

To summarise, the specifications derived from the research closely match the needs and challenges of blockchain-based voting systems. They emphasise the importance of accuracy, transparency, security, and user-friendliness in system development. The development process must take these factors into account in order to create a blockchain-based voting artefact that is not only technologically advanced, but also compliant with the practical realities and legal framework of electoral processes.

5.5 Selection of Blockchain Protocol and Consensus Algorithm

5.5.1 Findings

The analysis of consensus algorithms in blockchain technology shows clear trade-offs and strengths in terms of security, performance, scalability, energy efficiency, decentralisation, and fairness.

Proof of Work (PoW) offers robust security but faces challenges such as vulnerability to 51% attacks, lower transaction throughput, scalability issues, high energy consumption, potential centralisation in mining pools and unequal distribution of rewards.

Practical Byzantine Fault Tolerance (PBFT) is resistant to Byzantine faults but may not be suitable for large or open systems. It offers high transaction throughput with scalability limitations, more energy efficiency than PoW, a more centralised structure and fairness that depends on implementation.

Proof of Stake (PoS) resists common attacks but is vulnerable to certain types of attacks, such as long-range attacks. It improves transaction throughput and scalability compared to PoW and is more energy efficient, but there are still concerns about concentration of power with large token holders.

Delegated Proof of Stake (DPoS) resists Byzantine bugs and Sybil attacks but is vulnerable to collusion. It outperforms PoW and PoS in terms of transaction throughput and scalability and is more energy efficient, although it can lead to some centralisation and concerns about concentration of power with top delegates.

Proof of Authority (PoA) is safe for permissioned networks with high transaction throughput and scalability, energy efficiency, but more centralisation and fairness depending on implementation.

Pure Proof of Stake (PPoS) and Federated Consensus both have high security for their respective networks, high transaction throughput, scalability, and energy efficiency, but differ in terms of decentralisation and fairness depending on the implementation.

Hedera Hashgraph is characterised by security, transaction throughput, scalability and energy efficiency and offers a more decentralised approach with fair distribution of rewards and influence.

The algorithm proposed in this study focuses on streamlining the voting process over the blockchain and utilises the theory of the Byzantine General Problem. It includes several steps, from the initialisation of polling station numbers, the authentication of the Electoral Proof of Stake (EPoS), the creation of smart ballots to the consensus-based validation and recording

of votes in the blockchain. The structured algorithm ensures an efficient, transparent, and reliable vote counting, with votes only being validated once the required consensus has been reached.

5.5.1.1 Selected Algorithms

The study chooses the Pure Proof of Stake (PPoS) blockchain protocol and a customised algorithm based on the Byzantine General Problem Theory to streamline the voting process. Here you can find a detailed explanation of the decisions:

Rationale:

Security and decentralisation: the security features and decentralised nature of PPoS make it suitable for a voting system where trust and impartiality are paramount.

Performance and scalability: High transaction throughput and scalability are essential for the efficient processing of large amounts of voting data.

Energy efficiency: The energy efficiency of the system is in line with sustainable technology trends, an important aspect of modern digital solutions.

Fairness: The equitable distribution of rewards and influence is key to maintaining the integrity of an electoral system.

5.5.1.2 Customised Algorithm based on the Theory of the Byzantine General Problem

Process: Initialisation of polling station numbers, authentication of EPoS (Electoral Proof of Stake), generation of smart ballots and consensus-based validation of votes.

Consensus: Only votes that reach the required consensus (67% or more approval among officials or representatives) are validated and recorded in the blockchain.

Security and transparency: Integrates identification verification and consensus building for a transparent and secure vote counting.

Justification:

Increased security and integrity: by applying the Byzantine General's theory, the algorithm solves potential security issues in the voting process and ensures that only verified and agreed votes are recorded.

Transparency and trust: The consensus mechanism increases transparency and creates trust between participants in the voting process.

Efficiency: Streamlining the voting process with this algorithm enables an efficient and accurate vote count, which is crucial in elections.

The combination of PPoS and the custom algorithm provides a robust framework for a blockchain-based voting system that combines security, transparency, efficiency and fairness, all essential elements for a reliable and trustworthy voting process.

5.5.2 Discussion

The results of the analysis of different consensus algorithms in blockchain technology highlight the complexity of balancing factors such as security, performance, scalability, energy efficiency, decentralisation, and fairness. These factors are critical in the context of blockchain-based voting systems, where the integrity, reliability and public trust in the voting process are of paramount importance.

5.5.2.1 Trade-off considerations for consensus algorithms

While Proof of Work (PoW) offers robust security, it struggles with challenges such as vulnerability to 51% attacks, lower transaction throughput and high energy consumption. These issues raise concerns for its application in voting systems, where efficiency and environmental sustainability are increasingly prioritised.

Practical Byzantine Fault Tolerance (PBFT) and Proof of Authority (PoA) have scalability limitations and centralisation concerns, despite their high transaction throughput and resilience to certain errors. In the context of elections, this centralisation could be problematic and undermine the perception of a fair and open electoral process.

Proof of Stake (PoS) and Delegated Proof of Stake (DPoS) show improvements in performance and energy efficiency over PoW. However, their vulnerability to certain attacks and the potential concentration of power with certain actors could affect the perceived fairness and security of the election process.

The Hedera Hashgraph, with its emphasis on decentralisation and fair distribution of rewards, represents a more balanced approach, making it an interesting consideration for future election systems.

5.5.2.2 Rationale for the Selection of PPoS and the Byzantine General Problem-Based Algorithm

The choice of Pure Proof of Stake (PPoS) is based on its strengths in terms of security, decentralisation, performance, scalability, and energy efficiency. For a voting system, these properties are essential to ensure a secure, efficient, and environmentally friendly process. The decentralisation aspect of PPoS is particularly important to ensure the integrity and impartiality of the voting process.

The custom algorithm, which is based on Byzantine general problem theory, was chosen for its increased security and integrity to ensure that only verified votes are recorded. This addresses one of the biggest challenges in electronic voting - the risk of manipulation and fraud. The consensus requirement of 67% approval for the validation of votes further strengthens the reliability and democratic nature of the voting process. Emphasising the transparency and efficiency of the algorithm meets the need for an electoral process that is both understandable and accessible to the public, thus promoting trust and participation.

5.5.2.3 Implications for Blockchain Voting Systems.

The combination of PPoS and the customised algorithm underlines a comprehensive approach to overcoming the multiple challenges of blockchain-based voting systems. This approach ensures a balance between technical efficiency and democratic principles. It shows a way in which voting systems can utilise the benefits of blockchain technology while mitigating its inherent risks and challenges.

To summarise, the results and subsequent selection of the PPoS and the algorithm based on the Byzantine General Problem show a nuanced understanding of the requirements for a blockchain-based voting system. This system must not only be technologically sound, but also comply with the general principles of democratic fairness, transparency, and public trust.

5.6 Development and Evaluation of BBVV Artefact

5.6.1 Findings

5.6.1.1 Development Process

The development process of the Blockchain-Based Vote Validation (BBVV) artefact, a voting system, is characterised by its advanced and secure architecture. The system is based on a client-server model, with the client-side interface utilising Next.js for a responsive user experience and the server-side logic powered by a PyTeal smart contract developed with Algorand. This architecture is made even more secure by the integration of Pera Wallet, which improves the authentication and signing of transactions.

Key Components of the System include:

Client-side interface: utilising Next.js for dynamic and interactive user experiences.

Server-side logic: A smart contract developed with PyTeal by Algorand that ensures secure and efficient processing of blockchain transactions.

Authentication mechanism: Utilisation of Pera Wallet for robust user authentication and digital signing.

The workflow is simple. End users access the system via a web browser and interact with the backend smart contract for data requests and transfers. Pera Wallet is integrated to increase security during the authentication and transaction processes.

The architecture of the system also includes an Entity-Relationship (ER) diagram that represents various entities such as ElectionState, CandidateRecord, AgentRecord and

PollingStationRecord and their interactions that correspond to the various components of the voting system refer to Chapter 4, Section 4.5.3, Figure 4.4.

In addition, the sequence diagram (Chapter 4, Section 4.5.4, Figure 4.5) illustrates the development phases, including the client-side development with Next.js, the server-side implementation of the logic via Algorand's PyTeal Smart Contract and the integration of Pera Wallet for authentication. Version control is managed via Git, with the application deployed to the Algorand testnet using Vercel for the client-side components and the smart contract.

5.6.2 The Technology Stack used is as follows:

- Client-side development using Next.js.
- Server-side logic via Algorand PyTeal Smart Contract.
- Pera Wallet for authentication.
- Git for version control.
- Deployment via Vercel, with the smart contract in Algorand's test network.

The BBVV system is designed to streamline the collation and monitoring of election results. Its special features include immutable data storage, synchronised data mirroring, enhanced user identity verification, secure data transfer and comprehensive audit capabilities.

Election validation with Pera Wallet uses edge computing for decentralised processing and local storage of keys, increasing security and scalability. The integration enables secure transaction signing and verification, ensuring the integrity of the vote count. This system provides end-to-end verification, real-time verification and a user-friendly interface that significantly improves reliability, security and trust in the voting process.

5.6.2.1 Evaluation

The results of the data analysis and visualisation provide valuable insights into various aspects of a blockchain-based voting system, in particular the BBVV artefact. The most important findings include:

Consensus analysis: the data shows that a significant majority, approximately 95%, of vote counts did not reach consensus. This was illustrated in a bar chart showing the frequency of

'yes" and 'no" consensus results. A comparative analysis of the actual total number of votes with the number of votes where consensus was reached showed that only about 10% of the total number of votes were eligible for consensus.

Analysis of agreement among officials: The visualisation shows a high level of disagreement among officials and only a low level of agreement. This indicates that only a low level of agreement was achieved due to random data in the current data set as shown in Figure 5.3.

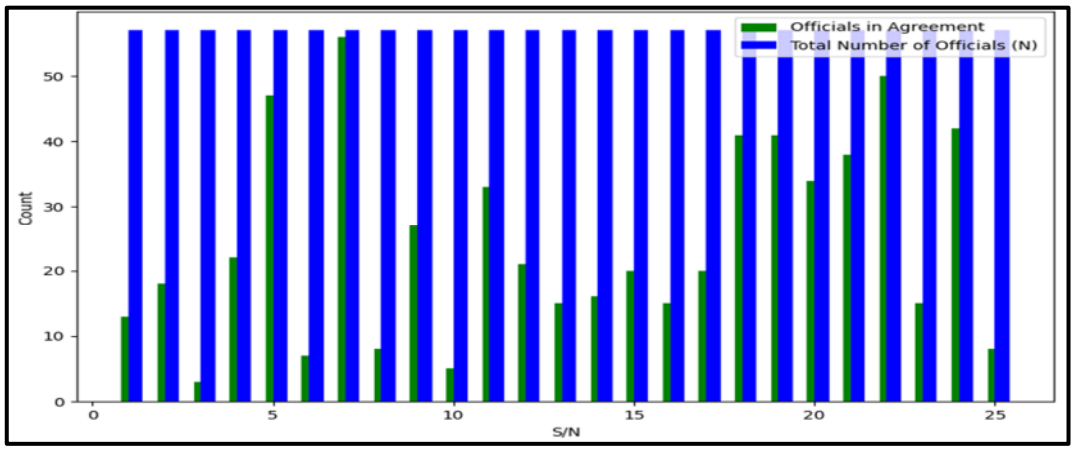


Figure 5-3: Agreement VS Disagreement

Transaction performance metrics: Analysing the transaction confirmation time across different rounds revealed occasional delays in transaction processing, such as a delay at 35000 seconds, which was confirmed in 3.20 rounds, this is illustrated in Figure 5.4.

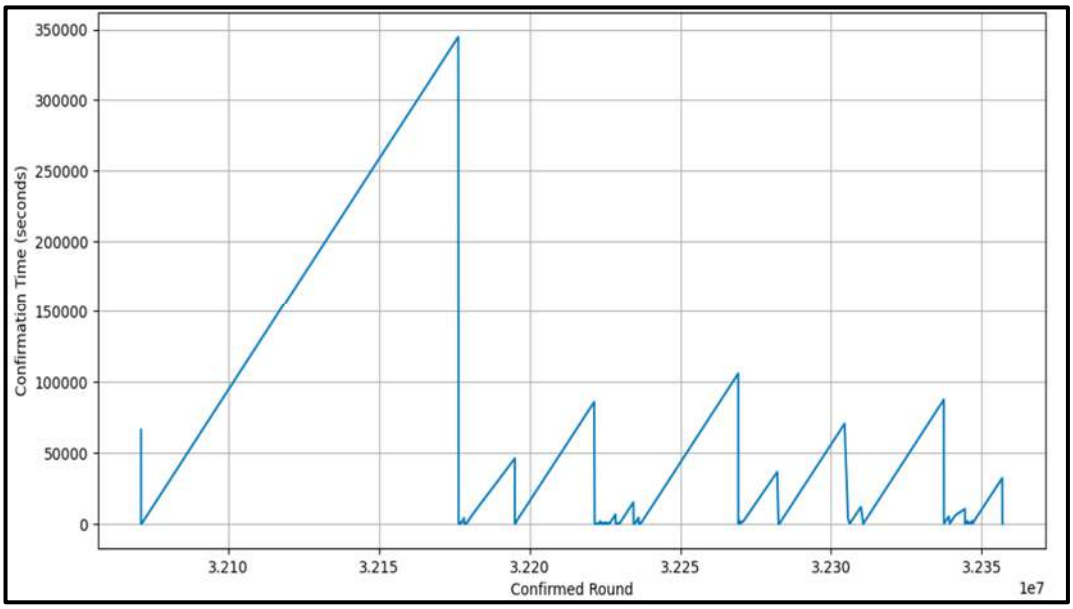


Figure 5-4: Transaction Metrics

Transaction throughput analysis: The system exhibited different throughput rates in different rounds, with certain rounds showing higher peaks, indicating better processing capacity.

Saturation analysis: This analysis showed a consistent transaction fee across different timestamps, indicating the stability of the BBVV artefact in the Algorand network.

Latency analysis: An upward trend in latency times was observed, indicating increasing confirmation times which could indicate network congestion or higher demand.

Traffic analysis: The number of transactions per round fluctuated, with the data showing longer periods of low transaction activity, indicated by flat areas in the graph.

These results are critical to understanding the performance and efficiency of the BBVV artefact and provide insight into its reliability, scalability and effectiveness in a real-world electoral context.

5.7 Findings from the Application of the Methodology

The results of the application of the methodology can be summarised as follows:

5.7.1 Achieving Consensus:

- The blockchain-based vote counting and validation (BBVV) system using the Byzantine Generals Problem (BGP) was tested with randomised historical election data on the Algorand blockchain TestNet.
- The BBVV protocol aimed to reach local consensus on the vote count at polling stations before aggregating them on the blockchain at the national level.
- Consensus was only reached in around 5% of election scenarios, with significant discrepancies found between officials. This low consensus rate was due to the strict requirements of the protocol and the erroneous values generated by the randomised dataset.

5.7.2 Validation of the election:

- Due to the strict consensus requirements, only 10% of the total votes were considered valid.
- Significant discrepancies were found between officials, resulting in a non-consensus rate of 95, largely due to the randomised data.

5.7.3 Performance metrics:

- The BBVV system was evaluated using transaction metrics, saturation, throughput, traffic, and latency.
- The system demonstrated that blockchain technology can improve the integrity of elections by ensuring a transparent, secure and accurate vote counting process.

5.7.4 System architecture and implementation:

- The BBVV system utilised the Algorand blockchain platform, which is known for its efficiency and speed, especially with its Layer 1 smart contracts.
- The architecture included edge computing for decentralised processing of votes, reducing latency and reliance on central servers and increasing system resilience and scalability.

- Pera Wallet was integrated for authentication and digital signing of transactions to increase security and traceability.

5.7.5 Visual and data analysis:

- The study included various visualisations and data analysis to understand the performance of the system and the impact of consensus on the overall vote count.
- The graphical representations showed significant inconsistencies between officials due to random data entry and transaction processing delays at certain points.

The study has shown that blockchain technology, in conjunction with BGP theory, has the potential to improve the integrity of elections by enabling a secure and transparent vote counting process. However, achieving consensus among officials at polling stations remains a major challenge that needs to be addressed for wider implementation.

5.8 Discussions

5.8.1 Practical Implications of Findings

5.8.2 Trust and Governance:

The observed divergence in the counting of votes and the inability of a significant proportion to reach consensus raises concerns about the governance of the network. There is a potential risk of dishonest activities, such as vote rigging. This points to the need for tighter monitoring and possibly improved security measures to ensure the integrity of the voting process.

5.8.3 Network efficiency:

Insights into transaction performance, particularly observed delays and spikes, suggest that the network may face challenges in handling large transaction volumes, especially at peak times. This requires technology upgrades or optimisations to improve the network's processing capacity and reduce bottlenecks.

5.8.4 Stability and predictability:

While the constant trend in transaction fees indicates stability, it also serves as a reminder for network administrators to remain proactive. Ensuring predictable transaction costs is critical to user satisfaction, and any change, no matter how small, could disrupt this stability. This means that continuous monitoring and a willingness to implement adaptive measures are required.

5.8.5 Latency and scalability:

Increasing network latency is a clear sign of potential congestion problems. This could lead to lower user confidence and transaction efficiency. To counter this, it may be necessary to explore advanced technological solutions, such as sharding or layer 2 solutions, to ensure that the network remains scalable and responsive.

5.8.6 Strategic planning:

Insights from traffic analysis, such as understanding periods of low activity and peak periods, can support strategic decisions. For example, network maintenance or upgrades can be scheduled during periods of low activity to minimise inconvenience to users. In addition, resource allocation at times of high traffic can ensure network resilience and efficiency.

5.8.7 Transparency and credibility:

Detailed analysis of election-related data underscores the importance of transparency in the electoral process. The availability of such comprehensive data can enhance the confidence of network participants and observers. This suggests that maintaining transparency and providing detailed data should be a priority for any blockchain-based election system.

5.8.8 Holistic approach:

The multi-layered nature of blockchain operations, as highlighted by the findings, suggests that effectively addressing the challenges and impacts requires a comprehensive approach. This includes a combination of technological innovation, strategic planning, continuous monitoring, and proactive action.

In essence, the findings highlight the need for continuous improvement, proactive monitoring, and strategic planning to ensure the robustness, reliability, and efficiency of the Algorand network. Addressing these practical implications will not only increase user confidence but also facilitate wider adoption of the network.

In summary, this data analysis and visualisation provides a comprehensive overview of blockchain-based election data. It sheds light on consensus results, transaction performance, traffic patterns and election statistics. Overall, the Algorand blockchain is well suited for this research as the transaction fee is only 0.001 algo and remains the same regardless of network congestion. Furthermore, a more accurate consensus has been achieved as the election results submitted by the different polling stations are publicly available. These insights are invaluable for optimising system performance, understanding transaction dynamics and improving the integrity of the electoral process. Stakeholders, officials, and network operators can use these insights to make data-driven decisions and continuously improve the blockchain-based election system. It highlights the importance of data analytics in ensuring transparency, efficiency, and trust in the electoral process within a Blockchain network.

5.9 Design Science Research (DSR) in Action

As described, the development of the BBVV artefact follows the Design Science Research (DSR) approach, a problem-solving process that involves the creation and evaluation of innovative artefacts. The DSR approach typically involves identifying a problem, developing an artefact as a solution and evaluating the effectiveness of the artefact. Here you can see how the development of the BBVV artefact is in line with the DSR approach:

5.9.1 Problem Identification and Motivation (Relevance Cycle)

The first phase of the DSR approach is about understanding the problem area. For the BBVV artefact, this was achieved by examining the perceptions and expectations of election stakeholders in African countries. The thematic analysis revealed challenges such as poor network connections, inadequate staff training and corruption, which justified the need for a new system.

5.9.2 Objectives of a Solution (Rigor Cycle)

The study then defined the objectives for a solution, which included ensuring accuracy, speed, efficiency, transparency and security in the voting process. The system also needed to be resilient to network issues, litigation and corruption, while encouraging active stakeholder participation and compliance with electoral rules.

5.9.3 Design and Development (Design Cycle)

In the design and development phase, the BBVV artefact was conceived with a clear system architecture. The BBVV artefact was designed using a client-server model, using Next.js for the client-side interface, PyTeal for the server-side smart contract logic on Algorand and Pera Wallet for secure authentication and transaction signatures. In this phase, primary modules and an operational workflow were created detailing user interactions with the system via web browsers, data requests and transfers.

5.9.4 Artefact Description

The technological stack used, and the functional overview of the system were described in detail, emphasising special features such as immutable data storage, synchronous data reflection, improved user identity verification, secure data transmission and comprehensive audit functions. This description meets the DSR's requirement for a clear and detailed presentation of artefacts.

5.9.5 Demonstration and Evaluation (Design Cycle)

While the demonstration and experimental evaluation of the novel vote aggregation and validation algorithm were set to be conducted in this chapter, the design and development phase laid the groundwork for these future steps. The system's architecture and operational workflow were established to demonstrate the artefact's capabilities in a controlled environment.

5.9.6 Communication (Relevance, Rigor, and Design Cycles)

The final phase of the Design Science Research (DSR) approach is the communication of the problem, the artefact and its utility to an academic and practitioner audience. This is done by disseminating the knowledge gained, the methods used and the implications of the artefact's design. The conclusion of the study and subsequent publications tie back to the original objectives and challenges and summarise how the design and development of the BBVV artefact addresses the identified problems and contributes to the field of blockchain-based voting systems.

The research underlying the BBVV artefact has been successfully communicated through academic publications and conference presentations, demonstrating the relevance and rigour of the work undertaken. These efforts ensure that the solution is not only theoretically sound, but also practically relevant, with a clear path to empirical testing and validation in the real world. The publications serve as a bridge to industry practitioners, providing a comprehensive overview of the state of the art in blockchain-based voting systems and emphasising the practical implications of the research. They highlight the potential impact on future electoral processes and the improvement of democratic practises through technology, demonstrating the contribution of the BBVV artefact to both academic discourse and practical application.

5.10 The Byzantine Generals Problem in Action

The application of the theory of the Byzantine Generals Problem (BGP) in the context of blockchain-based voting systems is a direct analogy to the challenges of reaching consensus in distributed systems. Here you can see how the application of the theory relates to the Byzantine Generals Problem:

5.10.1 Purpose of the Test

The tests described aim to verify the ability of the blockchain system to reach consensus on the vote count, which is a practical application of BGP theory. The scenarios tested demonstrate the resilience of the system to dishonest reporting, as consensus requires a supermajority to ensure that the final vote count is accurate and accepted by the majority of election officials, thus reflecting the true will of the voters. To recap, applying the theory of the

Byzantine Generals Problem to blockchain-based voting systems provides a framework for understanding how distributed consensus can be achieved in an environment where participants do not necessarily trust each other. The practical implementation of this theory through blockchain technology ensures that the integrity of the voting process is maintained and that the final vote count accurately and verifiably reflects the collective decision of the voters.

5.10.2 Application of the Theory

In the context of blockchain-based voting, the "generals" are analogous to the poll workers or officials at each polling station, and the "city" is the correct vote count that must be agreed upon. The blockchain serves as a communication channel through which the generals send their plans (vote count) to each other. The smart contract on the blockchain is designed to record the vote count only when a consensus of 67% is reached, similar to how the generals must agree on a common plan of action.

5.10.3 The Byzantine Generals Problem Theory Applied

5.10.3.1 Trust and Consensus

The BGP theory emphasises the problem of trust between parties who must agree on a single value (in this case, the vote count). The role of the blockchain is to create a trust less environment in which consensus can be reached without the parties having to trust each other, as the integrity of the vote count is guaranteed by the immutable ledger of the blockchain.

5.10.3.2 Tolerance to Malicious Actors

The theory's requirement that consensus can be reached even if some participants are malicious (up to a third) is reflected in the voting system's requirement of 67% consensus. This ensures that, even if some electoral officials are dishonest, they cannot influence the total number of votes as long as the majority (more than two thirds) are honest.

5.10.3.3 Cryptography and Digital Signatures

The use of digital signatures in BGP theory is reflected in the blockchain voting system through the use of cryptographic hashing and smart contracts. These digital signatures ensure that once a vote count has been entered, it cannot be altered and the identity of the poll worker entering the data can be verified.

5.11 The Binary Byzantine Agreement Protocol (BBA)

5.11.1 Honest Majority

The BBA's trust in the honesty of more than two-thirds of the participants is directly reflected in the voting system's requirement for a consensus of 67%. This ensures that the system is immune to a minority of dishonest participants.

5.11.2 Randomness and Unpredictability

The use of a common random string in the BBA to prevent predictability and ensure fairness is analogous to randomness in blockchain networks, where the order of transactions (and thus the recording of votes) cannot be easily predicted or manipulated.

5.11.3 Iterative Consensus

The three-stage loop of the BBA, in which the participants exchange Boolean values until a consensus is reached, is similar to the iterative process of reaching consensus on the blockchain. The voting agents enter the number of votes, and the smart contract iteratively checks whether the 67% threshold has been reached before recording the number.

5.12 Comparative Analysis of the Findings to Literature

The results of the study on the BBVV artefact on the Algorand network, particularly in relation to voting inconsistency and transaction performance, can be critically analysed in light of the existing literature on blockchain technology and voting systems. The concerns about possible dishonest manipulation of vote counting identified in the research are directly addressed in the literature by Onur & Yurdakul (2023) and Bartolucci *et al.* (2018). These studies emphasise

the importance of voter anonymity and security through zero-knowledge proofs, decentralisation and Shamir's secret sharing and suggest potential mitigation strategies for the risks highlighted in the Algorand network.

Furthermore, the observed transaction delays and bottlenecks in the Algorand network coincide with the scalability challenges highlighted by Spanos & Kantzavelou (2023) and Stančíková & Homoliak (2023). They emphasise scalable solutions such as EtherVote and SBvote that could identify strategies to improve the processing capacity issues identified in the study. The analysis of transaction fees and network latency aligns with concerns raised about the efficiency and integrity of blockchain-based systems, as noted by Faour (2018) and Bulut *et al.*, (2019b). These studies suggest that maintaining a stable and efficient network is essential for user trust, which is also emphasised by research on the Algorand network.

Regarding the integrity and transparency of elections, the need to analyse election data in detail is supported by the emphasis on transparent and tamper-proof systems in the literature. The SHARVOT protocol by Bartolucci *et al.* (2018) and the Ethereum-based prototype by Mukherjee *et al.* (2023) emphasise the importance of such systems that can increase trust and credibility in blockchain-based elections and address some of the concerns raised in the study.

The study does not explicitly mention quantum security, but this emerging threat is addressed by Mishra *et al.* (2022), suggesting that the integration of quantum-resistant functions into the Algorand network may be an important future consideration. Furthermore, the delicate balance between transparency in vote counting and the protection of voter privacy addressed in the study is a much-discussed challenge in the literature. This challenge is to maintain transparency and fairness while ensuring security, as Bartolucci *et al.* (2018) emphasise.

To summarise, the results of the study on the BBVV artefact in the Algorand network are consistent with the broader challenges and solutions discussed in the literature. Emphasising voter anonymity, scalability, transparency, and security in blockchain-based voting systems is critical to addressing these challenges. Ongoing research and technological advances in this area provide valuable insights into potential strategies for improving the performance and reliability of blockchain networks such as Algorand in electoral contexts.

5.13 Conclusion

To recap, the integration of blockchain technology into the electoral process, as demonstrated in this study, provides a robust solution to the challenges of consensus building and maintaining the integrity of the vote count. Applying the theory of the Byzantine Generals Problem to blockchain-based voting systems ensures a trustworthy environment in which consensus can be reached even in the presence of potentially dishonest participants. The data analysis and visualisation performed on the Algorand blockchain illustrates the effectiveness of this approach, showing clear consensus results, consistent transaction performance and recognisable traffic patterns and voting statistics. The low and stable transaction fee on the Algorand platform emphasises its suitability for processing election data, even under changing network conditions. The transparency created by making election results from different polling stations publicly available on the blockchain has led to a more accurate consensus, which is crucial for the legitimacy of the electoral process. These findings are not only theoretical in nature, but also provide practical insights that can be used by stakeholders, election authorities and network operators to improve the performance of the system and increase user trust. Ultimately, this study highlights the central role of data analytics in enhancing transparency, efficiency and trust in blockchain-based voting systems and marks a significant step forward in the modernisation of democratic processes.

Chapter 6 concludes the research findings by discussing each of the objectives of this study.

CHAPTER SIX: CONCLUSION

6.1 Organisation of the Chapter

Chapter 6 concludes the study by methodically addressing the individual objectives of the study. It begins with an 'Introduction' (Section 6.2), followed by detailed analysis of 'Objective 1' to 'Objective 4' (Sections 6.3 to 6.6). The chapter then looks at the practical implications of the findings (Section 6.7), followed by the assumptions and limitations of the study (Section 6.8), highlights the limitations and challenges (Section 6.9) and the 'research contributions' (Section 6.10), and presents the policy recommendation (Section 6.11) and a summarising 'conclusion' (Section 6.12). Finally, a possible 'future path' for related research is outlined (Section 6.13).

6.2 Introduction

This chapter summarises the main findings of our research and addresses each of the objectives set at the beginning. First, a comprehensive survey was conducted to identify existing blockchain solutions in the field of electoral systems. This investigation revealed a spectrum of applications, each with its own strengths and limitations. Then, through a careful elicitation process, we established the essential system specifications for a Blockchain-based Voting and Validation System (BBVV). These specifications were aimed not only at high performance, but also at instilling deep trust in users. In our search for an optimal blockchain protocol, we proposed one that not only supported trustworthy vote aggregation, but also included a consensus algorithm tailored to validate the vote count. Finally, the BBVV artefact was developed, and its performance characteristics were critically evaluated. The results underlined its potential to revolutionise the electoral landscape by providing a trustworthy and efficient solution.

6.3 To review and identify existing blockchain solutions that have been used in the electoral vote systems.

The goal of this review was to find and assess the current literature on blockchain solutions for vote counting and how they compare in terms of methods, limitations, and approaches. The methodology included a systematic review of research on e-voting solutions using blockchain technology. The study looked at existing Blockchain methods for e-voting to

provide a comprehensive understanding. The main findings of the study are a classification of Blockchain systems for e-voting implemented on Ethereum and ML, Ethereum and IoT, Ethereum and Hyperledger Fabric in private and public networks, and sidechains on Ethereum. Most of these platforms use smart contracts for self-tallying. The cryptographic hashing techniques observed were elliptic curve encryption, SHA 256 algorithms, homophobia, Paillier encryption, proof-of-knowledge, and linkable ring signature, which includes a non-interactive zero-knowledge proof. In addition, the study suggested several potential combinations of platforms, cryptographic algorithms, and programming languages to develop a secure and transparent voting system using blockchain.

In summary, several areas of study emerged around blockchain and e-voting that should receive attention in future research. An interesting direction for future studies would be to investigate different combinations of platforms, cryptographic algorithms, and programming languages to develop a secure and transparent voting system using Blockchain. There is an opportunity to explore the benefits and challenges of incorporating different IoT devices, consensus mechanisms and other technologies into the voting process. Ongoing research is currently focused on creating Algorand smart contracts, Pera Wallet integration and with PyTeal.

6.4 To elicit the necessary system specifications for developing a BBVV artefact that exhibits high-performance features and engenders user trust.

The objective meant to understand the perceptions and expectations of electoral stakeholders in relation to vote counting and validation in different African countries. A thematic analysis was conducted to analyse the data, using activity theory as a starting point. This approach helped to understand the various themes that emerged, such as technical aspects, accuracy, speed, efficiency, transparency, security, challenges and improvements, and the role of observers and Election Management Bodies (EMBs).

The study identified several issues related to vote counting and validation. These issues included technical aspects, accuracy, speed, efficiency, transparency, security, challenges and improvements, and the role of observers and EMBs. Challenges such as poor network

coverage, inadequate staff training and corruption were particularly highlighted. From the analysis, several key requirements for the vote counting and validation artefact were identified. These specifications, if followed, could significantly improve the accuracy, efficiency, transparency, and security of the electoral process.

The findings underscore the importance of an electoral system that guarantees accuracy, speed, efficiency, transparency and security. Such a system should be resilient to various challenges, including network connectivity issues, litigation and corruption risks. It should also encourage active stakeholder participation and ensure compliance with rules and regulations governing the electoral process. The findings of the study contribute to a broader understanding of electoral processes in African countries and provide a basis for future research. This research can address areas such as the impact of the legal framework, voter education, the technical challenges of electronic voting systems and the potential of technologies such as blockchain in the electoral process.

6.5 To identify an appropriate blockchain protocol that supports trusted vote aggregation and includes a suitable consensus algorithm for vote count validation.

This objective aimed to analyse and understand the unique solutions offered by different consensus algorithms to the general Byzantine problem in the context of blockchain networks.

The study undertook a comprehensive review and analysis of various consensus algorithms, including Proof of Work, Practical Byzantine Fault Tolerance, Proof of Stake, Delegated Proof of Stake, Proof of Authority, Federated Consensus, Pure Proof of Stake and Hedera Hashgraph. In addition, a novel algorithm for aggregating and validating votes was presented, and its practical effectiveness in was carried out. Each consensus algorithm offers different solutions to the general Byzantine problem. Proof of Work is safe but has problems with scalability and energy efficiency. Practical Byzantine Fault Tolerance resists Byzantine faults but may have scalability issues in larger networks. Proof of Stake and Delegated Proof of Stake are more efficient and scalable than PoW but raise concerns about concentration of power. Proof of Authority and Federated Consensus are efficient and secure for authorised networks but tend towards centralisation. Finally, Pure Proof of Stake and Hedera Hashgraph

aim for decentralised consensus with high efficiency and scalability. The effectiveness of each algorithm can vary depending on the specific network conditions and requirements.

The results of this study contribute to a broader understanding of consensus algorithms in blockchain networks. The introduction of a new vote aggregation and validation algorithm (BBVV protocol) adds to the existing body of knowledge. Future research directions include improving the scalability and energy efficiency of consensus algorithms, ensuring equitable power distribution and enhancing security in permission-based networks. In addition, newer algorithms such as Pure Proof of Stake and Hedera Hashgraph should be further investigated. Comparative studies can also shed light on the performance trade-offs of the individual algorithms and thus help in the selection of suitable consensus mechanisms for different blockchain applications.

6.6 Develop the BBVV artefact for vote counting and validation and evaluate its performance features to handle maximum load, minimise delays, process high transaction volumes, and foster user trust through traffic analysis.

The goal of this objective was to provide a comprehensive analysis and visualisation of blockchain-based election data, focusing on consensus results, transaction performance, traffic patterns and election statistics. The study used the Algorand blockchain for its analysis, as it charges a constant transaction fee of 0.001 algo regardless of network congestion. The study involved the collection and analysis of election results submitted by different polling stations and made publicly available on the blockchain. This data was then visualised and interpreted to provide insights into the performance of the system and the integrity of the electoral process.

The Algorand Blockchain proved to be an effective platform for this research, as the election results from the different polling stations were transparently available, allowing for a more accurate consensus. The insights gained from the data analysis are invaluable for optimising system performance, understanding transaction dynamics and improving the integrity of the electoral process. The research highlights the importance of data analytics in ensuring transparency, efficiency, and trust within a blockchain-based election system.

The findings highlight the potential of blockchain technology to revolutionise the electoral process by ensuring transparency, efficiency, and trust. Stakeholders, officials, and network operators can use these findings to make informed decisions and continuously refine the Blockchain-based election system. Future research directions include refining the consensus algorithm, scaling the system, improving the BBVV artefact user interface, and integrating advanced authentication measures. The overall goal is to strengthen the legitimacy and transparency of the system while optimising its operational efficiency.

6.7 Practical implications of the Findings

The results of the blockchain-based election data analysis reveal several important practical implications for the BBVV artefact on the Algorand network. Issues with vote counting and consensus signal the need for improved monitoring and security to prevent risks such as vote tampering and to ensure trust and control. Network efficiency is being challenged by transaction performance issues, so technology upgrades are needed to manage peak loads and avoid bottlenecks. Stability and predictability are critical, as evidenced by consistent transaction fees that require network administrators to ensure predictable costs through continuous monitoring and adaptability. Increasing network latency indicates potential congestion issues, highlighting the need for advanced technology solutions for scalability and responsiveness.

Strategic planning is essential, with insights from traffic analysis guiding decisions on maintenance planning and resource allocation to improve network efficiency. Transparency and credibility in the electoral process are critical, emphasising the need for detailed data to gain user trust. To overcome these challenges, a holistic approach combining technological innovation, strategic planning, continuous monitoring and proactive action is recommended. Overall, these implications emphasise the need for continuous improvement and strategic foresight to improve the robustness, reliability and efficiency of the network and ultimately increase user confidence and encourage wider adoption. The role of data analytics is central to ensuring transparency, efficiency, and trust in the voting process within the blockchain network.

6.8 Assumptions and Limitations

6.8.1 Assumptions:

- The literature reviewed and platforms such as Ethereum and Algorand provide a comprehensive account of the current state of blockchain solutions for vote counting and voting systems.
- The perceptions and expectations of election stakeholders in African countries are representative of the wider population.
- The issues identified through the thematic analysis and the consensus algorithms analysed are comprehensive and capture the totality of the data.
- The performance and characteristics of the consensus algorithms are consistent across different implementations and use cases.

6.8.2 Limitations:

- The reviews may not include all existing blockchain solutions, especially those that are proprietary, emerging, or not well documented.
- The challenges identified, such as poor network coverage in African countries, may not be generally applicable in all contexts.
- The practical effectiveness of newly introduced algorithms, such as the vote aggregation and validation algorithm, remains tested only on publicly available historic election results data.
- The results could be influenced by cultural, political, or social biases in the regions studied and may not be generalisable to blockchain networks with other characteristics or requirements.
- The studies rely on self-reported or publicly available data, which may have biases or inaccuracies or may not capture all aspects of the voting process.

6.9 Limitations and Challenges

During the development of the Blockchain-Based Vote Validation (BBVV) artefact on Algorand's TestNet, several challenges were encountered that had a significant impact on the

research results. To overcome these, a number of mitigation strategies were employed. The behaviour of the BBVV artefact on TestNet did not fully reflect real-world voting conditions, which was mitigated by conducting controlled pilot tests in actual voting scenarios. The lack of real-world challenges, such as high voter turnout in the TestNet, was compensated for by simulating high traffic and various user interactions. The problem of data and configuration loss due to TestNet resets was solved by creating backup copies and restoring them when necessary. The performance discrepancies observed between the TestNet and the MainNet were addressed by analysing the performance under different loads and preparing the artefact for scalability and optimisation in the MainNet.

The challenge of obtaining real election data, especially from countries with restricted data release, was overcome by using a larger population of countries with mature democracies of at least 27 years and above. Finally, limited feedback from the TestNet community was supplemented by actively soliciting insights from various stakeholders, including election officials. Taken together, these strategies improved the reliability and practicality of the BBVV artefact for real-world election scenarios.

6.10 Research Contributions

6.10.1 Practical Contributions

This thesis makes practical contribution to the field of electoral systems by addressing critical challenges in the practise of vote counting and validation. This study implements a Blockchain-Based Vote Counting and Validation (BBVV) artefact that consists of a Layer 1 smart contract on Algorand's blockchain to process data from polling stations, ensuring fast and efficient transaction processing. This smart contract aggregates vote counts from different locations to provide a comprehensive nationwide result. The research includes detailed equations to ensure the proper recording of votes across time intervals, proper aggregation between polling stations, and maintaining the integrity and verifiability of election results. The smart contract is designed as a self-executing agreement that calculate the total number of votes from the incoming data automatically. This ensures that all subscribers receive tamper-proof data simultaneously, enhancing security and trust in the election process. Despite significant progress in this area, practical hurdles such as network instability, corruption and lack of transparency remain. The research conducted here offers tangible solutions and insights,

bridging the gap between theoretical knowledge and practical application in the field of blockchain-based voting systems.

This research lies in the application of Design Science Research (DSR) methodology to the development of the BBVV artefact. This approach differs significantly from existing practises, which often involve centralised systems that are vulnerable to manipulation and lack transparency. By applying DSR to the development of BBVV, significant improvements have been achieved in terms of accuracy, speed, efficiency, transparency and security of the voting process. Utilising the Algorand blockchain with its low and consistent transaction fees further increases the practicality and reliability of this innovative system.

The practical applications of this research have been implemented through a series of pilot experimental testing and collaborations with electoral authorities. One notable implementation involved a simulated voting process under controlled conditions using the BBVV artefact. The results of these implementations showed improved reliability and integrity of the vote counting process and confirmed the effectiveness of the approach in real election scenarios.

The impact of these practical contributions attempts to go beyond the immediate applications. They have the potential to revolutionise practises in electoral systems and set new standards for the security and transparency of voting processes. In addition, they offer valuable insights for policymaking on governance and electoral reform that could lead to better-informed and more effective decisions. The long-term benefits of these applications could be significant, particularly in terms of strengthening democratic integrity and public confidence in electoral systems.

Although the practical applications developed in this thesis represent significant progress, there is still room for further development. Future work could investigate the integration of this technology into different electoral systems worldwide and assess its scalability and adaptability. Although the approach has proven effective in current applications, it would be useful to consider its applicability and adaptability to other contexts or challenges, e.g., decentralised government models or other public sector applications. Addressing potential scalability issues and exploring ways to further improve the system's resilience to cyber threats will be critical in these future endeavours.

6.10.2 Theoretical Contributions

This work contributes to the theoretical understanding of blockchain technology in voting systems. Despite advances in this field, there are still theoretical challenges, such as how to effectively deal with trust and consensus in decentralised environments. This research aimed to address these gaps by proposing an innovative application of the Byzantine General Problem (BGP) and the Binary Byzantine Agreement Protocol (BBA) within blockchain technology. It offers new insights and perspectives that challenge the conventional understanding of blockchain-based voting systems.

The theoretical innovations in this work revolve around the application of BGP and BBA theories to blockchain-based vote counting and validation (BBVV). These contributions offer a new perspective on consensus mechanisms traditionally understood via simpler majority voting systems. By introducing a 67% consensus requirement and integrating cryptographic hashing (Pera Wallet) and smart contracts, this research extends the theoretical boundaries of blockchain applications in voting systems and provides a more comprehensive and detailed understanding of trust and consensus in trust less environments.

The development of these theoretical contributions was based on a methodology that included a comprehensive review of the literature on blockchain technology, BGP and BBA, as well as the practical application of these theories in blockchain-based voting systems. This process allowed for a thorough examination of existing theories while demonstrating their limitations in explaining trust issues in decentralised systems. Through comparative analysis and theoretical modelling, an integrative framework was created that better addresses trust, consensus, and security in blockchain-based electoral processes.

The implications of these theoretical contributions are far-reaching. They not only advance the academic discourse on blockchain technology and voting systems, but also have potential overlaps with cybersecurity and digital governance. These contributions offer new viewpoints for the study of decentralised trust mechanisms that challenge and enrich current academic debates. In practical terms, they could influence the design of secure and transparent election systems and offer new approaches to address the challenges of digital election processes.

While the theoretical contributions of this work represent a significant advance in the understanding of blockchain applications in electoral systems, they are not without limitations. In particular, the reliance on 67% consensus may not be universally applicable in all electoral contexts, and the complexity of BGP and BBA theories could pose a challenge in practical implementation. Future theoretical research could build on these foundations by exploring other consensus thresholds or simplifying the theoretical models for broader application. Such work would further enrich the theoretical landscape of blockchain technology in voting systems and potentially lead to even more groundbreaking insights.

6.10.3 Methodological Contributions

The methodological contribution of this work represents a contribution in the field of computer science, particularly in the application of blockchain technology to electoral processes. The research combines the practical focus of pragmatism with the development of artefacts and the evaluation of DSR. This methodology involved iterative testing and refinement with input from experts in blockchain technology and voting systems. Given the challenge of integrating different research approaches and meeting the specific requirements of secure and transparent vote counting, previous methods have consistently failed. This research aimed to address these critical gaps by developing a new methodology that combines pragmatism and Design Science Research (DSR) to provide more effective, accurate and efficient solutions in the context of blockchain-based voting systems.

The originality of this research lies in the unique integration of pragmatism and design science research principles. Traditional methods in this field have often been limited by their singular approach, focussing either too much on practical problem solving or on theoretical aspects without adequate practical application. In contrast, this new approach combines the practical focus of pragmatism with artefact development and evaluation of DSR. This method was developed through a comprehensive process that involved iterative testing and refinement, with significant input from experts in blockchain technology and voting systems.

The implementation of this method involved a detailed process, including extensive data collection from various voting systems and the development of blockchain-based artefact. Critical to this process was the integration of quantitative and qualitative research methods to ensure a comprehensive understanding of the complexity of blockchain applications for

elections. The methodology underwent validation that included real-world data experimental testing and simulations to ensure its reliability and effectiveness. Challenges encountered, such as matching theoretical models with practical election scenarios, were addressed through iterative refinement.

The practical applications of this methodology attempt to go beyond academic research. It is particularly well suited to real-world electoral systems where efficiency, security and transparency can be critical. In addition, it has far-reaching implications for broader areas such as digital governance and cybersecurity and could influence policy and practise in these areas. This approach tries to set a new precedent in the field of computer science and paves the way for more innovative and secure digital election processes worldwide.

Although the methodological contributions of this work represent an advance in the field of computer science and blockchain applications, they are not without limitations. These include potential scalability challenges and the need to adapt to different political or regulatory contexts. Future research should aim to refine the scalability of blockchain models and explore their application in different electoral environments. Such efforts could improve the applicability and robustness of the methodology and potentially extend its utility to other areas of digital governance and cybersecurity.

6.11 Policy Recommendation

Recent studies question the view that African countries have a sufficiently developed infrastructure for mobile and blockchain systems. Ayim *et al.* (2020) identify limitations in the agricultural sector due to poor technological infrastructure and low user capacity. Olusanya *et al.* (2022) refer to the vulnerability of healthcare systems in Africa due to limitations in digital technologies, Martinez-Cesena *et al.* (2015) refer to the lack of data and the challenges in planning energy infrastructure, which is essential for advanced technologies, Aly Bouke *et al.* (2023) point to issues such as different legal systems and cybersecurity threats that affect the development of such infrastructure, Salat *et al.* (2019) argue that mobile phone data, which is essential for infrastructure planning, does not correlate effectively with population density. These findings point to significant gaps in African countries' readiness for advanced digital systems. The challenges span various sectors, including agriculture, healthcare, and

regulatory frameworks. Addressing these issues is critical to the successful adoption of mobile and blockchain technologies.

Despite the above challenges, the policy recommendation recognises that African countries have now developed sufficient infrastructure to support mobile and blockchain-based systems (Awoleye, 2021; Tian *et al.*, 2022). Given this milestone, it is opportune to integrate blockchain technology into their electoral systems. The recommendation favours investment in further infrastructure development and staff training, as well as the creation of a supportive legal framework. It also emphasises the importance of stakeholder engagement, particularly in voter education, to ensure broad acceptance and understanding of the new technology. The policy emphasises the need for continuous research, empirical testing, and iterative improvements of blockchain-based voting systems. It also emphasises the importance of using data analytics for transparency, international cooperation to share best practises and regular monitoring to ensure the security and efficiency of these systems.

6.12 Conclusion

In summary, the Design Science Research (DSR) methodology in the systematic development of the Blockchain-Based Vote Verification (BBVV) artefact has been instrumental in overcoming the complex challenges of vote counting and validation identified by the thematic analysis. The BBVV artefact, with its strategic design and technological integration, directly addresses issues such as network instability and rigging in elections and embodies the principles of accuracy, speed, efficiency, transparency, and security. This focus not only improves the electoral process, but also demonstrates the artefact's utility in promoting a trustworthy electoral environment.

The application of the theory of the Byzantine Generals Problem in the blockchain-based voting system is a testament to the robustness of the artefact, which ensures a consensus mechanism that is resilient even in the face of potential dishonesty among participants. The Algorand blockchain, with its low and consistent transaction fees, proves to be an optimal platform for this endeavour as it enables clear consensus results, reliable transaction performance and recognisable traffic patterns and voting statistics. The transparency achieved by recording election results from the various polling stations on the blockchain has

been instrumental in achieving a more accurate consensus, which is essential for the legitimacy of the electoral process.

These theoretical advances and practical applications provide a comprehensive overview of the potential of blockchain technology in revolutionising e-voting systems. The exploration of different blockchain protocols and building of a proposed BBVV protocol opens ways to create secure and transparent voting mechanisms. The development of the BBVV protocol for aggregating and validating votes, which has been experimentally tested with real data, represents a significant contribution to this area and points the way for future research to improve the scalability, energy efficiency and security of consensus algorithms.

Ultimately, the results of this study will be invaluable to stakeholders, election officials and network operators as they support the continuous improvement of blockchain-based voting systems. The overarching goal is to improve the legitimacy, transparency, and operational efficiency of these systems, thereby strengthening the democratic process. This study not only highlights the central role of data analytics in improving transparency, efficiency, and trust in elections, but also represents a significant step in the modernisation of democratic processes through blockchain technology.

6.13 Future Directions

Future research on blockchain-based voting systems should focus on improving scalability and energy efficiency, integrating sophisticated security measures such as advanced cryptographic techniques, and exploring the potential of IoT integration for improved accessibility. Empirical studies and real-world trials are fundamental for evaluating performance and user feedback, while also considering the legal and ethical implications of such technologies. Comparative studies across different policy contexts will provide insights into adaptability and effectiveness. In addition, the use of data analytics and AI to analyse voting patterns can increase transparency and efficiency. Educating the public and stakeholders about these technologies is essential for their successful implementation and wider acceptance in order to strengthen the democratic process through technological innovation.

REFERENCES

Abegunde, J., Spring, J. & Xiao, H. 2021. SEVA: A Smart Electronic Voting Application Using Blockchain Technology. *Proceedings - 2021 IEEE International Conference on Blockchain, Blockchain 2021*: 353–360. https://ieeexplore.ieee.org/abstract/document/9680588/ 9 April 2022.

Abidi, S.R. 2011. Ontology-based knowledge modeling to provide decision support for comorbid diseases. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 6512 LNAI: 27–39. https://link.springer.com/chapter/10.1007/978-3-642-18050-7_3 10 September 2021.

Abraham, I., Devadas, S., Dolev, D., Nayak, K. & Ren, L. 2017. Efficient Synchronous Byzantine Consensus. http://arxiv.org/abs/1704.02397 6 October 2023.

Abuelhija, A., Abudouleh, A., Abumuhsen, B. & Awad, F. 2020. Secure Voting System Using Distributed Ledger Technology. In *2020 11th International Conference on Information and Communication Systems, ICICS 2020*. Institute of Electrical and Electronics Engineers Inc.: 48–52.

Abuidris, Y., Kumar, R. & Wenyong, W. 2019. A survey of blockchain based on e-voting systems. *ACM International Conference Proceeding Series*: 99–104.

Adiputra, C.K., Hjort, R. & Sato, H. 2019. A Proposal of Blockchain-Based Electronic Voting System. *Proceedings of the 2nd World Conference on Smart Trends in Systems, Security and Sustainability, WorldS4 2018*: 185–192.

Agbesi, S. & Asante, G. 2019a. Electronic Voting Recording System Based on Blockchain Technology. In *2019 12th CMI Conference on Cybersecurity and Privacy, CMI 2019*. IEEE. https://ieeexplore-ieee-org.libproxy.cput.ac.za/document/8962142/ 9 April 2022.

Agbesi, S. & Asante, G. 2019b. Electronic Voting Recording System Based on Blockchain Technology. *2019 12th CMI Conference on Cybersecurity and Privacy, CMI 2019*.

Al-Maaitah, S., Qatawneh, M. & Quzmar, A. 2021. E-Voting System Based on Blockchain Technology: A Survey. *2021 International Conference on Information Technology, ICIT 2021 - Proceedings*: 200–205.

Al-Madani, A.M., Gaikwad, A.T., Mahale, V. & Ahmed, Z.A.T. 2020. Decentralized E-voting system based on Smart Contract by using Blockchain Technology. *Proceedings of the 2020 International Conference on Smart Innovations in Design, Environment, Management, Planning and Computing, ICSIDEMPC 2020*: 176–180.

Alam, A., Rashid, S.M.Z.U., Salam, M.A. & Islam, A. 2018. Towards Blockchain-Based E-voting System. In *2018 International Conference on Innovations in Science, Engineering and Technology (ICISET)*. IEEE. https://ieeexplore-ieee-org.libproxy.cput.ac.za/document/8745613/ 1 April 2022.

Alharahsheh, H.H. & Pius, A. 2020. A Review of key paradigms: positivism VS interpretivism. *Global Academic Journal of Humanities and Social Science*, 2(3): 39–43. https://www.researchgate.net/publication/338244145 15 July 2021.

Allen, N.W. 2015. Clientelism and the personal vote in Indonesia. *Electoral Studies*, 37: 73–85. http://dx.doi.org/10.1016/j.electstud.2014.10.005.

Alpos, O. & Cachin, C. 2020. Consensus beyond Thresholds: Generalized Byzantine Quorums Made Live. *Proceedings of the IEEE Symposium on Reliable Distributed Systems*, 2020-Septe: 21–30. https://arxiv.org/abs/2006.04616v2 12 November 2023.

Alvi, S.T., Islam, L., Rashme, T.Y. & Uddin, M.N. 2021. BSEVOTING: A Conceptual Framework to Develop Electronic Voting System using Sidechain. *International Conference on Electrical Engineering, Computer Science and Informatics (EECSI)*, 2021-Octob: 10–15.

Alvi, S.T., Uddin, M.N., Islam, L. & Ahamed, S. 2020a. A blockchain based cost effective digital voting system using SideChain and smart contracts. *Proceedings of 2020 11th International Conference on Electrical and Computer Engineering, ICECE 2020*: 467–470.

Alvi, S.T., Uddin, M.N., Islam, L. & Ahamed, S. 2020b. A blockchain based cost effective digital voting system using SideChain and smart contracts. In *Proceedings of 2020 11th International Conference on Electrical and Computer Engineering, ICECE 2020*. IEEE: 467–470. https://ieeexplore-ieee-org.libproxy.cput.ac.za/document/9393081/ 25 March 2022.

Aly Bouke, M., Alshatebi, S.H., Abdullah, A., Cengiz, K. & Atigh, H. El. 2023. African Union Convention on Cyber Security and Personal Data Protection: Challenges and Future Directions. https://arxiv.org/abs/2307.01966v1 25 November 2023.

Androulaki, E., Barger, A., Bortnikov, V., Muralidharan, S., Cachin, C., Christidis, K., De Caro, A., Enyeart, D., Murthy, C., Ferris, C., Laventman, G., Manevich, Y., Nguyen, B., Sethi, M., Singh, G., Smith, K., Sorniotti, A., Stathakopoulou, C., Vukolić, M., Cocco, S.W. & Yellick, J. 2018. Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains. *Proceedings of the 13th EuroSys Conference, EuroSys 2018*, 2018-Janua. https://dl.acm.org/doi/10.1145/3190508.3190538 11 November 2023.

Angsuchotmetee, C., Setthawong, P. & Udomviriyalanon, S. 2019. BlockVOTE : An Architecture of a Blockchain-based Electronic Voting System. In *ICSEC 2019 - 23rd International Computer Science and Engineering Conference*. Institute of Electrical and Electronics Engineers Inc.: 110–116.

Ankalkoti, P. & Santhosh, S.G. 2017. A Relative Study on Bitcoin Mining. *Imperial Journal of Interdisciplinary Research (IJIR)*, 3(5): 1757–1761. http://www.imperialjournals.com/index.php/IJIR/article/view/5024/4834 13 September 2022.

Anupama, B.S. & Sunitha, N.R. 2022. Analysis of the Consensus Protocols used in Blockchain Networks - An overview. *IEEE International Conference on Data Science and Information System, ICDSIS 2022*: 1–6.

Aranha, D.F., Barbosa, P.Y.S., Cardoso, T.N.C., Araújo, C.L. & Matias, P. 2019. The return of software vulnerabilities in the Brazilian voting machine. *Computers and Security*, 86: 335–349.

Awoleye, O.M. 2021. Reconfiguring Data Infrastructure Ecosystem in Africa: A Primer Toward Digital Sovereignty. *arXiv preprint arXiv:2109.14186*. https://arxiv.org/abs/2109.14186%0Ahttps://arxiv.org/pdf/2109.14186 15 November 2023.

Ayim, C., Kassahun, A., Tekinerdogan, B. & Addison, C. 2020. Adoption of ICT innovations in the agriculture sector in Africa: A Systematic Literature Review. https://arxiv.org/abs/2006.13831v1 25 November 2023.

Baird, L. 2016. Hashgraph consensus: fair, fast, byzantine fault tolerance. : 1–24.

Al Barghuthi, N.B., Hamdan, I., Al Suwaidi, S., Lootah, A., Al Amoudi, B., Al Shamsi, O. & Al Aryani, S. 2019. An Analytical View on Political Voting System using Blockchain Technology-UAE Case Study. In *ITT 2019 - Information Technology Trends: Emerging Technologies Blockchain and IoT*. Ras Al Khaimah, United Arab Emirates: IEEE: 132–137.

Bartolucci, S., Bernat, P. & Joseph, D. 2018. SHARVOT: Secret SHARe-based VOTing on the blockchain. *Proceedings - International Conference on Software Engineering*: 30–34.

Bazerman, M.H. & Gino, F. 2012. Behavioral ethics: Toward a deeper understanding of moral judgment and dishonesty. *Annual Review of Law and Social Science*, 8: 85–104.

Benabdallah, A., Audras, A., Coudert, L., El Madhoun, N. & Badra, M. 2022a. Analysis of Blockchain Solutions for E-Voting: A Systematic Literature Review. *IEEE Access*, 10(July): 70746–70759.

Benabdallah, A., Audras, A., Coudert, L., El Madhoun, N. & Badra, M. 2022b. Analysis of Blockchain Solutions for E-Voting: A Systematic Literature Review. *IEEE Access*, 10(June): 70746–70759.

Bennett Moses, L., Goré, R., Levy, R., Pattinson, D. & Tiwari, M. 2017. No more excuses: Automated synthesis of practical and verifiable vote-counting programs for complex voting schemes. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 10615 LNCS: 66–83.

Berenschot, W. 2018. The Political Economy of Clientelism: A Comparative Study of Indonesia's Patronage Democracy. *Comparative Political Studies*, 51(12): 1563–1593.

Bhattacharya, P., Tanwar, S., Shah, R. & Ladha, A. 2020. Mobile edge computing-enabled blockchain framework—A survey. In *Lecture Notes in Electrical Engineering*. Springer: 797–809. https://link.springer.com/chapter/10.1007/978-3-030-29407-6_57 27 April 2021.

Blaikie, N. & Priest, J. 2019. Designing Social Research: The Logic of Anticipation - Norman Blaikie, Jan Priest - Google Books. https://books.google.co.uk/books?hl=en&lr=&id=CwOEDwAAQBAJ&oi=fnd&pg=PT8&dq=blaikie+priest+designing+&ots=BoSJaDGXO4&sig=DjZfVBud6LVt65OImUEqwZ8ELpQ#v=onepage&q=blaikie priest designing&f=false 21 November 2023.

Bogna, F., Raineri, A. & Dell, G. 2020. Critical realism and constructivism: merging research paradigms for a deeper qualitative study. *Qualitative Research in Organizations and Management: An International Journal*, 15(4): 461–484. https://www.emerald.com/insight/1746-5648.htm 15 July 2021.

Bonneau, J., Miller, A., Clark, J., Narayanan, A., Kroll, J.A. & Felten, E.W. 2015. SoK: Research perspectives and challenges for bitcoin and cryptocurrencies. *Proceedings - IEEE Symposium on Security and Privacy*, 2015-July: 104–121.

Borse, M., Shendkar, P., Undre, Y., Mahadik, A. & Patil, R.Y. 2022. A Review of Blockchain Consensus Algorithm. *Lecture Notes in Networks and Systems*, 444: 415–426.

Briner, R.B. & Denyer, D. 2012. Systematic Review and Evidence Synthesis as a Practice and Scholarship Tool. *The Oxford Handbook of Evidence-Based Management*, (November 2015).

Bulut, R., Kantarci, A., Keskin, S. & Bahtiyar, S. 2019a. Blockchain-Based Electronic Voting System for Elections in Turkey. *UBMK 2019 - Proceedings, 4th International Conference on Computer Science and Engineering*: 183–188.

Bulut, R., Kantarci, A., Keskin, S. & Bahtiyar, S. 2019b. Blockchain-Based Electronic Voting System for Elections in Turkey. *UBMK 2019 - Proceedings, 4th International Conference on Computer Science and Engineering*: 183–188. https://ieeexplore.ieee.org/abstract/document/8907102/ 9 April 2022.

Burger, A. & Silima, T. 2006. Sampling and sampling design | Journal of Public Administration. *Journal of Public Administration*, Vol. 41(No. 3). https://journals.co.za/doi/abs/10.10520/EJC51475 20 June 2022.

Buril, F. 2020. The credibility challenge: how democracy aid influences election violence. *Democratization*, 27(5): 901–903. https://books.google.co.za/books?hl=en&lr=&id=EsCIDwAAQBAJ&oi=fnd&pg=PR7&dq=Elections+in+developing+nations+frequently+neglect+to+satisfy+worthy+guidelines+of+fairness,+and+this+in+turn+can+result+in+protest,+violence,+and+fragility&ots=VRbkOzIovJ&sig=ORT 19 June 2021.

Buterin, V. & Griffith, V. 2017. Casper the Friendly Finality Gadget. http://arxiv.org/abs/1710.09437 14 July 2023.

Çabuk, U.C., Adıgüzel, E. & Karaarslan, E. 2018. A Survey on Feasibility and Suitability of Blockchain Techniques for the E-Voting Systems. *Ijarcce*, 7(3): 124–134. http://arxiv.org/abs/2002.07175 11 November 2023.

Canessane, R.A., Srinivasan, N., Beuria, A., Singh, A. & Kumar, B.M. 2019. Decentralised Applications Using Ethereum Blockchain. In *5th International Conference on Science Technology Engineering and Mathematics, ICONSTEM 2019*. IEEE: 75–79. https://ieeexplore-ieee-org.libproxy.cput.ac.za/document/8918887/ 1 April 2022.

Capretto, M., Ceresa, M., Anta, A.F., Russo, A. & Sánchez, C. 2023. Improving Blockchain Scalability with the Setchain Data-type. https://arxiv.org/abs/2302.04744v1 12 November 2023.

Cater-Steel, A., Toleman, M. & Rajaeian, M.M. 2019. Design science research in doctoral projects: An analysis of Australian theses. *Journal of the Association for Information Systems*, 20(12): 1844–1869. https://aisel.aisnet.org/jais/vol20/iss12/3 15 January 2023.

Chaieb, M., Yousfi, S., Lafourcade, P. & Robbana, R. 2019. Verify-your-vote: A verifiable blockchain-based online voting protocol. *Lecture Notes in Business Information Processing*, 341: 16–30. https://link.springer.com/chapter/10.1007/978-3-030-11395-7_2 17 January 2023.

Chaisawat, S. & Vorakulpipat, C. 2020. Fault-tolerant architecture design for blockchain-based electronics voting system. In *JCSSE 2020 - 17th International Joint Conference on Computer Science and Software Engineering*. IEEE: 116–121. https://ieeexplore-ieee-org.libproxy.cput.ac.za/document/9268264/ 9 April 2022.

Chang, Y.-X., Li, Q.-L., Wang, Q. & Song, X.-S. 2022. Dynamic Practical Byzantine Fault Tolerance and Its Blockchain System: A Large-Scale Markov Modeling. http://arxiv.org/abs/2210.14003 12 November 2023.

Chang, Y.-X., Wang, Q., Li, Q.-L. & Ma, Y. 2023. Performance and Reliability Analysis for Practical Byzantine Fault Tolerance with Repairable Voting Nodes. http://arxiv.org/abs/2306.10960.

Cheema, M.A., Ashraf, N., Aftab, A., Qureshi, H.K., Kazim, M. & Azar, A.T. 2020a. Machine Learning with Blockchain for Secure E-voting System. *Proceedings - 2020 1st International Conference of Smart Systems and Emerging Technologies, SMART-TECH 2020*: 177–182.

Cheema, M.A., Ashraf, N., Aftab, A., Qureshi, H.K., Kazim, M. & Azar, A.T. 2020b. Machine Learning with Blockchain for Secure E-voting System. *Proceedings - 2020 1st International Conference of Smart Systems and Emerging Technologies, SMART-*

TECH 2020: 177–182. https://ieeexplore.ieee.org/abstract/document/9283806/ 9 April 2022.

Chege, K. & Otieno, O. 2020. Research Philosophy Design and Methodologies: A Systematic Review of Research Paradigms in Information Technology. *Global Scientific Journals*, 8(5): 33–38. www.globalscientificjournal.com.

Chen, J. and Micali, S., 2016. ALGORAND. arXiv preprint arXiv:1607.01341.

Chen, J. & Micali, S. 2019. Algorand: A secure and efficient distributed ledger. *Theoretical Computer Science*, 777: 155–183. https://doi.org/10.1016/j.tcs.2019.02.001.

Chen, P. & Kim, T. 2014. *European Design Science Symposium, EDSS 2013*.

Chepurnoy, A. & Saxena, A. 2020. Bypassing non-outsourceable proof-of-work schemes using collateralized smart contracts. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 12063 LNCS: 423–435. https://link.springer.com/chapter/10.1007/978-3-030-54455-3_30 8 September 2022.

COG. 2016. *Zambia General Elections and Referendum, 11 August 2016*.

COG. 2018. *Zimbabwe Harmonised Elections 2018 Final Commonwealth Observer Group Report: 30 July 2018*. Commonwealth Secretariat Marlborough House, Pall Mall London SW1Y 5HXUnited Kingdom: Commonwealth.

Conway, A., Blom, M., Naish, L. & Teague, V. 2017. An analysis of New South Wales electronic vote counting. In *ACM International Conference Proceeding Series*. Association for Computing Machinery.

Creswell, J.W. 2008. Re[1] J. W. Creswel, Research Design: Qualitative, Quantitative, and Mixed Methods Approaches. SAGE Publications, 2008.search Design: Qualitative, Quantitative, and Mixed Methods Approaches. *sage publications*: 3–22.

Creswell, J.W. & Clark, V.L.P. 2007. Designing & Conducting Mixed Methods Research + The Mixed Methods Reader (bundle). *Designing & conducting mixed methods research + the mixed methods reader*, 1(2): 24–27.

Creswell, J.W. & Plano-Clark, V.L. 2011. *Choosing a mixed methods design*. 2nd ed. A. Tashakkori & C. Teddlie, eds. Los Angeles: SAGE Publications. http://scholar.google.com/scholar?hl=en&btnG=Search&q=intitle:Choosing+a+mixed+methods+design#0 14 July 2021.

Croman, K., Decker, C., Eyal, I., Gencer, A.E., Juels, A., Kosba, A., Miller, A., Saxena, P., Shi, E., Sirer, E.G., Song, D. & Wattenhofer, R. 2016. On scaling decentralized blockchains (A position paper). *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*,

9604 LNCS: 106–125. https://link.springer.com/chapter/10.1007/978-3-662-53357-4_8 13 July 2023.

Crotty, M. 2003. Crotty, M. (2003). The Foundations of Social Research:... - Google Scholar. https://scholar.google.com/scholar?hl=en&as_sdt=0%2C5&q=Crotty%2C+M.+%282003%29.+The+Foundations+of+Social+Research%3A+Meaning+and+Perspective+in+the+Research+Process.+London%3A+Sage+Publications.&btnG= 18 December 2022.

Dagher, G.G., Marella, P.B., Milojkovic, M. & Mohler, J. 2018. Bron covote: Secure voting system using ethereum's blockchain. *ICISSP 2018 - Proceedings of the 4th International Conference on Information Systems Security and Privacy*, 2018-Janua: 96–107. https://scholarworks.boisestate.edu/cs_facpubs/170 12 September 2022.

Damle, S., Gujar, S. & Moti, M.H. 2021a. FASTEN: Fair and secure distributed voting using smart contracts. *IEEE International Conference on Blockchain and Cryptocurrency, ICBC 2021*: 1–3.

Damle, S., Gujar, S. & Moti, M.H. 2021b. FASTEN: Fair and secure distributed voting using smart contracts. *IEEE International Conference on Blockchain and Cryptocurrency, ICBC 2021*: 2021–2023.

David, B., Gaži, P., Kiayias, A. & Russell, A. 2018. Ouroboros praos: An adaptively-secure, semi-synchronous proof-of-stake blockchain. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 10821 LNCS: 66–98. https://link.springer.com/chapter/10.1007/978-3-319-78375-8_3 14 July 2023.

Deng, Q. & Ji, S. 2018. A Review of Design Science Research in Information Systems: Concept, Process, Outcome, and Evaluation. *Pacific Asia Journal of the Association for Information Systems*, 10(1): 1–36. https://aisel.aisnet.org/pajais/vol10/iss1/2/ 22 June 2022.

Denise F. Polit, C.T.B. 2010. Essentials of Nursing Research: Appraising Evidence for Nursing Practice - Denise F. Polit, Cheryl Tatano Beck - Google Books. : 610. https://books.google.co.za/books?hl=en&lr=&id=7GtP8VCw4BYC&oi=fnd&pg=PA574&dq=Polit,+D.+F.+%26+Beck,+C.+T.+2014.+Essentials+of+nursing+research:+Appraising+evidence+for+nursing+practice+(8th+ed.).+Philadelphia,+PA:+Wolters+Kluwer/Lippincott+Williams+%26+W 14 November 2023.

Desai, Z. & Lee, A. 2021. Technology and protest: The political effects of electronic voting in India. *Political Science Research and Methods*, 9(2): 398–413. https://doi.org/10.1017/psrm.2019.51.

Ekparinya, P., Gramoli, V. & Jourjon, G. 2020. *The Attack of the Clones Against Proof-of-Authority*. https://github.com/poanetwork/.

Ellervee, A., Matulevicius, R. & Mayer, N. 2017. A comprehensive reference model for blockchain-based distributed ledger technology. *CEUR Workshop Proceedings*, 1979: 320–333. http://nmayer.eu/publis/ER2017-forum-paper.pdf 7 September 2022.

Eyal, I. & Sirer, E.G. 2018. Majority Is Not Enough: Bitcoin mining is vulnerable. *Communications of the ACM*, 61(7): 95–102. https://link.springer.com/ 13 July 2023.

Faour, N. 2018. Transparent Voting Platform Based on Permissioned Blockchain. http://arxiv.org/abs/1802.10134 11 November 2023.

Febriyanto, E., Triyono, Rahayu, N., Pangaribuan, K. & Sunarya, P.A. 2020. Using Blockchain Data Security Management for E-Voting Systems. In *2020 8th International Conference on Cyber and IT Service Management, CITSM 2020*. Institute of Electrical and Electronics Engineers Inc.

Feng, L., Zhang, H., Chen, Y. & Lou, L. 2018. Scalable dynamic multi-agent practical byzantine fault-tolerant consensus in permissioned blockchain. *Applied Sciences (Switzerland)*, 8(10): 1919. https://www.mdpi.com/2076-3417/8/10/1919/htm 13 July 2023.

Fernandes, A., Garg, K., Agrawal, A. & Bhatia, A. 2021. Decentralized Online Voting using Blockchain and Secret Contracts. *International Conference on Information Networking*, 2021-Janua: 582–587.

Fezzazi, A. El, Adadi, A. & Berrada, M. 2021. Towards a Blockchain based Intelligent and Secure Voting. *5th International Conference on Intelligent Computing in Data Sciences, ICDS 2021*.

Gandhi, S.S., Kiwelekar, A.W., Netak, L.D. & Wankhede, H.S. 2023. Security Requirement Analysis of Blockchain-Based E-Voting Systems. *Lecture Notes on Data Engineering and Communications Technologies*, 131: 73–85. http://arxiv.org/abs/2208.01277 11 November 2023.

Gatteschi, V., Lamberti, F., Demartini, C., Pranteda, C. & Santamaria, V. 2018. To Blockchain or Not to Blockchain: That Is the Question. *IT Professional*, 20(2): 62–74.

Geerts, G.L. 2011. A design science research methodology and its application to accounting information systems research. *International Journal of Accounting Information Systems*, 12(2): 142–151.

Gervais, A., Karame, G.O., Capkun, V. & Capkun, S. 2014. Is Bitcoin a Decentralized Currency? *IEEE Security and Privacy*, 12(3): 54–60.

Giddings, L.S. & Grant, B.M. 2006. Mixed methods research for the novice researcher. *Contemporary nurse : a journal for the Australian nursing profession*, 23(1): 3–11. https://www.tandfonline.com/doi/abs/10.5172/conu.2006.23.1.3 15 November 2023.

Gilad, Y., Hemo, R., Micali, S., Vlachos, G. & Zeldovich, N. 2017. Algorand: Scaling Byzantine Agreements for Cryptocurrencies. *SOSP 2017 - Proceedings of the 26th ACM Symposium on Operating Systems Principles*: 51–68.

González, C.D., Mena, D.F., Muñoz, A.M., Rojas, O. & Sosa-Gómez, G. 2022. Electronic Voting System Using an Enterprise Blockchain. *Applied Sciences (Switzerland)*, 12(2). https://doi.org/10.3390/app12020531.

Govinda, H.S., Chandrakant, Y., Girish, D.S., Lokesh, S., Ravikiran & Jayasri, B.S. 2021. Implementation of Election System Using Blockchain Technology. In *Proceedings of the 2021 IEEE International Conference on Innovative Computing, Intelligent Communication and Smart Electrical Systems, ICSES 2021*. IEEE. https://ieeexplore-ieee-org.libproxy.cput.ac.za/document/9633828/ 1 April 2022.

Gregor, S. & Hevner, A.R. 2013. Positioning and presenting design science research for maximum impact. *MIS Quarterly: Management Information Systems*, 37(2): 337–355. http://www.misq.org 15 April 2021.

Grossoehme, D.H. 2014. Overview of Qualitative Research. *Journal of Health Care Chaplaincy*, 20(3): 109–122.

Guest, G., Namey, E.E. & Mitchell, M.L. 2017. *Collecting Qualitative Data: A Field Manual for Applied Research*. SAGE Publications, Inc. https://dx.doi.org/10.4135/9781506374680.

H, P., M. V., M.K., H A, S., B S, P., Thomas, L. & Murthy Y V, S. 2020. End-to-End Verifiable Electronic Voting System Using Delegated Proof of Stake On Blockchain. *SSRN Electronic Journal*: 2019. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3511409 1 April 2022.

Hackfeld, J. 2019. A lightweight BFT consensus protocol for blockchains. http://arxiv.org/abs/1903.11434 12 November 2023.

Haines, T. & Roenne, P. 2021. New Standards for E-Voting Systems: Reflections on Source Code Examinations. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 12676 LNCS: 279–289.

Halderman, J.A. & Teague, V. 2015. The New South Wales iVote system: Security failures and verification flaws in a live online election. In *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*. Springer: 35–53.

Han, G., Li, Y., Yu, Y., Choo, K.K.R. & Guizani, N. 2020. Blockchain-based self-tallying voting system with software updates in decentralized IoT. *IEEE Network*, 34(4): 166–172.

Hao, F. & Ryan, P.Y.A. 2016a. Real-world electronic voting: Design, analysis and deployment. *Real-World Electronic Voting: Design, Analysis and Deployment*: 1–461.

Hao, F. & Ryan, P.Y.A. 2016b. Real-world electronic voting: Design, analysis and deployment. *Real-World Electronic Voting: Design, Analysis and Deployment*, 1(1): 1–461.

Haque, S., Eberhart, Z., Bansal, A. & McMillan, C. 2022. Semantic Similarity Metrics for Evaluating Source Code Summarization. *IEEE International Conference on Program Comprehension*, 2022-March: 36–47. https://doi.org/10.1145/nnnnnnn.nnnnnnn 18 July 2023.

Hardwick, F.S., Gioulis, A., Akram, R.N. & Markantonakis, K. 2018a. E-Voting with Blockchain: An E-Voting Protocol with Decentralisation and Voter Privacy. *Proceedings - IEEE 2018 International Congress on Cybermatics: 2018 IEEE Conferences on Internet of Things, Green Computing and Communications, Cyber, Physical and Social Computing, Smart Data, Blockchain, Computer and Information Technology, iThings/Gree*: 1561–1567.

Hardwick, F.S., Gioulis, A., Akram, R.N. & Markantonakis, K. 2018b. E-Voting with Blockchain: An E-Voting Protocol with Decentralisation and Voter Privacy. *Proceedings - IEEE 2018 International Congress on Cybermatics: 2018 IEEE Conferences on Internet of Things, Green Computing and Communications, Cyber, Physical and Social Computing, Smart Data, Blockchain, Computer and Information Technology, iThings/Gree*: 1561–1567. https://ieeexplore.ieee.org/abstract/document/8726645/ 9 April 2022.

Helliar, C. V., Crawford, L., Rocca, L., Teodori, C. & Veneziani, M. 2020. Permissionless and permissioned blockchain diffusion. *International Journal of Information Management*, 54(October 2019): 102136. https://doi.org/10.1016/j.ijinfomgt.2020.102136.

Hevner, A.R., March, S.T., Park, J. & Ram, S. 2004. Essay in Information Design Science systems. *Management Information Systems*, 28(1): 75–105.

Hjalmarsson, F.P., Hreioarsson, G.K., Hamdaqa, M. & Hjalmtysson, G. 2018a. Blockchain-Based E-Voting System. *IEEE International Conference on Cloud Computing, CLOUD*, 2018-July: 983–986.

Hjalmarsson, F.P., Hreioarsson, G.K., Hamdaqa, M. & Hjalmtysson, G. 2018b. Blockchain-Based E-Voting System. *IEEE International Conference on Cloud Computing, CLOUD*, 2018-July: 983–986.

Holotescu, V. & Vasiu, R. 2020. Challenges and Emerging Solutions for Public Blockchains. *Brain. Broad Research in Artificial Intelligence and Neuroscience*, 11(1): 58–83. https://www.academia.edu/download/73697546/download.pdf 11 November 2023.

Houngnikpo, M.C. 2016. *Guarding the guardians: Civil-military relations and democratic governance in Africa*. Routledge.

Houy, N. 2014. GROUPE D'ANALYSE ET DE THÉORIE ÉCONOMIQUE LYON---ST ÉTIENNE It will cost you nothing to 'kill' a Proof---of---Stake crypto---currency It will cost you nothing to 'kill' a Proof-of-Stake crypto-currency [v.0.1]. http://www.gate.cnrs.fr 13 July 2023.

Howell KE. 2013. an Introduction To the Philosophy of Methodolo. : 32–54.

Hu, Q., Yan, B., Han, Y. & Yu, J. 2021. An Improved Delegated Proof of Stake Consensus Algorithm. *Procedia Computer Science*, 187: 341–346. www.sciencedirect.comwww.sciencedirect.com 18 July 2023.

Huang, J., He, D., Obaidat, M.S., Vijayakumar, P., Luo, M. & Choo, K.K.R. 2021. The Application of the Blockchain Technology in Voting Systems. *ACM Computing Surveys*, 54(3). https://doi.org/10.1145/3439725.

Huré-Maclaurin, L. 2020. *Scalable System for Indexing and Providing Access to Verifiable Blockchain Transaction Data*. Harvard University. https://search.proquest.com/openview/00a49c40c83cada42ec1a0d8db0a91e5/1?pq-origsite=gscholar&cbl=18750&diss=y 24 September 2022.

Ingouchi, T. & Jain, P. 2016. Japanese politics today: From karaoke to kabuki democracy. *Japanese Politics Today: From Karaoke to Kabuki Democracy*: 1–222. https://link.springer.com/chapter/10.1057/9780230370838_7 15 April 2021.

Jabbar, A. & Dani, S. 2020. Investigating the link between transaction and computational costs in a blockchain environment. *International Journal of Production Research*, 58(11): 3423–3436. https://www.tandfonline.com/doi/abs/10.1080/00207543.2020.1754487 13 September 2022.

Jafar, U., Aziz, M.J.A. & Shukur, Z. 2021. Blockchain for electronic voting system—review and open research challenges. *Sensors*, 21(17): 5874. https://doi.org/10.3390/s21175874.

Jagjivan, M.P., Shrikant, J.P., Vijay, J.N., Pradeep, K.R. & Suhas, P.A. 2021a. Secure Digital Voting system based on Aadhaar Authentication by using Blockchain Technology. In *2021 IEEE Mysore Sub Section International Conference, MysuruCon 2021*. IEEE: 862–870. https://ieeexplore-ieee-org.libproxy.cput.ac.za/document/9641577/ 2 April 2022.

Jagjivan, M.P., Shrikant, J.P., Vijay, J.N., Pradeep, K.R. & Suhas, P.A. 2021b. Secure Digital Voting system based on Aadhaar Authentication by using Blockchain Technology. In *2021 IEEE Mysore Sub Section International Conference, MysuruCon 2021*. IEEE: 862–870. https://ieeexplore-ieee-org.libproxy.cput.ac.za/document/9641577/ 25 March 2022.

Jalalzai, M.M. & Busch, C. 2018. Window Based BFT Blockchain Consensus. *Proceedings - IEEE 2018 International Congress on Cybermatics: 2018 IEEE Conferences on*

Internet of Things, Green Computing and Communications, Cyber, Physical and Social Computing, Smart Data, Blockchain, Computer and Information Technology, iThings/Gree: 971–979.

Jayasinghe, U., Lee, G.M., MacDermott, Á., Rhee, W.S. & Elgazzar, K. 2019. TrustChain: A Privacy Preserving Blockchain with Edge Computing. *Wireless Communications and Mobile Computing*, 2019: 1–17.

Jayasooriya, H., Bandara, D., Hemachandra, N., Kuruwitaarachchi, N. & Kahandawala, S. 2022. Integrity Assured Digital Voting System by using Blockchain as the Technology. *Proceedings - 2022 IEEE International Conference on e-Business Engineering, ICEBE 2022*: 276–281.

Jingzhong, W., Yue, Z. & Haibin, L. 2020. Electronic voting protocol based on ring signature and secure multi-party computing. *Proceedings - 2020 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery, CyberC 2020*: 50–55.

Judmayer, A., Stifter, N., Krombholz, K. & Weippl, E. 2017. *Blocks and Chains: Introduction to Bitcoin, Cryptocurrencies, and Their Consensus Mechanisms*. R. S. Elisa Bertino, ed. Morgan & Claypool Publishers LLC. https://booksc.org/book/65416363/1c7292 26 April 2021.

Jumaa, M.H. & Shakir, A.C. 2022. Iraqi E-Voting System Based on Smart Contract Using Private Blockchain Technology. *Informatica (Slovenia)*, 46(6): 87–94. https://www.informatica.si/index.php/informatica/article/view/4241 12 September 2022.

Kalu, T.O. & Gberevbie, D.E. 2018. Election violence and Democracy in Nigeria: A study of the 2011 and 2015 General Elections in Lagos State. *Kaduna Journal of Humanities*, 2(1): 60–70.

Kaushik, V. & Walsh, C.A. 2019a. Pragmatism as a research paradigm and its implications for Social Work research. *Social Sciences*, 8(9). www.mdpi.com/journal/socsci.

Kaushik, V. & Walsh, C.A. 2019b. Pragmatism as a research paradigm and its implications for Social Work research. *Social Sciences*, 8(9): 1–17.

Kazi, S., Md, M., Kumar, P. & Anik, I. 2019. *Blockchain Based Secured E-voting by Using the Assistance of Smart Contract*.

Keefer, P. & Vlaicu, R. 2017. Vote buying and campaign promises. *Journal of Comparative Economics*, 45(4): 773–792. https://doi.org/10.1016/j.jce.2017.07.001.

Kemmoe, V.Y., Stone, W., Kim, J., Kim, D. & Son, J. 2020. Recent Advances in Smart Contracts: A Technical Overview and State of the Art. *IEEE Access*, 8: 117782–117801.

Khoury, D., Kfoury, E.F., Kassem, A. & Harb, H. 2019. Decentralized Voting Platform Based on Ethereum Blockchain. *2018 IEEE International Multidisciplinary Conference on Engineering Technology, IMCET 2018*.

Kiayias, A., Russell, A., David, B. & Oliynykov, R. 2017. Ouroboros: A provably secure proof-of-stake blockchain protocol. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 10401 LNCS: 357–388. https://bitcointalk.org/index.php?topic=27787.0. 14 July 2023.

Kim, H., Kim, K.E., Park, S. & Sohn, J. 2021. E-voting System Using Homomorphic Encryption and Blockchain Technology to Encrypt Voter Data. http://arxiv.org/abs/2111.05096 11 November 2023.

Kosar, T., Bohra, S. & Mernik, M. 2018. A Systematic Mapping Study driven by the margin of error. *Journal of Systems and Software*, 144: 439–449. https://www.researchgate.net/publication/326558571 9 June 2022.

Kumar, R. 2014. *Research methodology: a step-by-step guide for beginners*. Fourth. Los Angeles: SAGE Publications Inc.

Kuo, P.C., Chung, H., Chao, T.W. & Cheng, C.M. 2020a. Fair byzantine agreements for blockchains. *IEEE Access*, 8: 70746–70761. https://arxiv.org/abs/1907.03437v1 11 November 2023.

Kuo, P.C., Chung, H., Chao, T.W. & Cheng, C.M. 2020b. Fair byzantine agreements for blockchains. *IEEE Access*, 8: 70746–70761. http://arxiv.org/abs/1907.03437 11 November 2023.

Lai, W.J., Hsieh, Y.C., Hsueh, C.W. & Wu, J.L. 2019. DATE: A Decentralized, Anonymous, and Transparent E-voting System. In *Proceedings of 2018 1st IEEE International Conference on Hot Information-Centric Networking, HotICN 2018*. Institute of Electrical and Electronics Engineers Inc.: 24–29.

Lamport, L., Shostak, R. & Pease, M. 1982. The Byzantine Generals Problem. *ACM Transactions on Programming Languages and Systems (TOPLAS)*, 4(3): 382–401.

Lancaster, G. 2007. *Research Methods in Management*. https://books.google.co.za/books?hl=en&lr=&id=0f8rBgAAQBAJ&oi=fnd&pg=PP1&dq=Lancaster+G.+Research+Methods+in+Management:+A+Concise+Introduction+to+Research+in+Management+and+Business+Consultancy.+Oxford:+Butterworth-Heinemann%3B+2005&ots=O5w_zmGLHN&sig=YV 10 September 2021.

Larimer, D. 2019. “Delegated proof-of-stake (dpos). *Bitshare Whitepaper, 3*.

Lasla, N., Al-Sahan, L., Abdallah, M. & Younis, M. 2022. Green-PoW: An energy-efficient blockchain Proof-of-Work consensus algorithm. *Computer Networks*, 214: 109118.

Leemon, B., Mance, H. & Paul, M. 2020. Hedera: A Public Hashgraph Network & Governing.

Leung, L. 2015. Validity, reliability, and generalizability in qualitative research. *Journal of Family Medicine and Primary Care*, 4(3): 324. https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4535087/ 14 November 2023.

Lewis, S.J., Pereira, O. & Teague, V. 2019. How not to prove your election outcome The use of non-adaptive zero knowledge proofs in the Scytl-SwissPost Internet voting system, and its implications for decryption proof soundness. : 1–11.

Li, H., Li, Y., Yu, Y., Wang, B. & Chen, K. 2021. A Blockchain-Based Traceable Self-Tallying E-Voting Protocol in AI Era. *IEEE Transactions on Network Science and Engineering*, 8(2): 1019–1032. https://ieeexplore-ieee-org.libproxy.cput.ac.za/document/9149825/ 9 April 2022.

Lin, L., Liao, X., Jin, H. & Li, P. 2019. Computation Offloading Toward Edge Computing. *Proceedings of the IEEE*, 107(8): 1584–1607.

Lin, Y. & Zhang, P. 2019. Blockchain-based Complete Self-tallying E-voting Protocol. , (November): 47–52.

Liu, Y. & Wang, Q. 2017. An E-voting protocol based on Blockchain. *IACR Cryptology ePrint Archive*: 1–13. https://eprint.iacr.org/2017/1043.pdf.

Lowe, A. 2001. *Reflexive Methodology: New Vistas for Qualitative Research*. Third. SAGE Publications Ltd.

Luo, T. 2021. An Efficient Blockchain Based Electronic Voting System Using Proxy Multi-signature. In *2021 3rd International Academic Exchange Conference on Science and Technology Innovation, IAECST 2021*. IEEE: 513–516. https://ieeexplore-ieee-org.libproxy.cput.ac.za/document/9695917/ 25 March 2022.

Lyu, J., Jiang, Z.L., Wang, X., Nong, Z., Au, M.H. & Fang, J. 2019. A secure decentralized trustless E-voting system based on smart contract. In *Proceedings - 2019 18th IEEE International Conference on Trust, Security and Privacy in Computing and Communications/13th IEEE International Conference on Big Data Science and Engineering, TrustCom/BigDataSE 2019*. IEEE: 570–577. https://ieeexplore-ieee-org.libproxy.cput.ac.za/document/8887296/ 25 March 2022.

Ma, X., Zhou, J., Yang, X. & Liu, G. 2020. A blockchain voting system based on the feedback mechanism and wilson score. *Information (Switzerland)*, 11(12): 1–13. https://www.mdpi.com/2078-2489/11/12/552/htm 26 September 2022.

Mao, Y., You, C., Zhang, J., Huang, K. & Letaief, K.B. 2017. A Survey on Mobile Edge Computing: The Communication Perspective. *IEEE Communications Surveys and Tutorials*, 19(4): 2322–2358.

Martin Fernandez, C., Diaz Rodriguez, M. & Rubio Munoz, B. 2018. An edge computing architecture in the internet of things. *Proceedings - 2018 IEEE 21st International Symposium on Real-Time Computing, ISORC 2018*: 99–102.

Martinez-Cesena, E.A., Mancarella, P., Ndiaye, M. & Schläpfer, M. 2015. Using Mobile Phone Data for Electricity Infrastructure Planning. https://arxiv.org/abs/1504.03899v1 25 November 2023.

Matile, R., Rodrigues, B., Scheid, E. & Stiller, B. CaIV : Cast-as-Intended Verifiability in Blockchain-based Voting. : 24–28.

Mazières, D. 2015. The Stellar Consensus Protocol: A Federated Model for Internet-level Consensus. *Stellar Development Foundation*, 120(42): 1–45.

van der Merwe, A., Gerber, A. & Smuts, H. 2020. *Guidelines for conducting design science research in information systems*.

Messias, J., Pahari, V., Chandrasekaran, B., Nl, C., Gummadi, K.P. & Loiseau, P. 2023. Understanding Blockchain Governance: Analyzing Decentralized Voting to Amend DeFi Smart Contracts. *Proceedings of ACM Conference (Conference'17)*, 1. https://arxiv.org/abs/2305.17655v1 12 November 2023.

Meyer, S.M., Blalock, A. & Blalock, H. 1983. *Introduction to Social Research*.

Miller, A., Xia, Y., Croman, K., Shi, E. & Song, D. 2016. The Honey Badger of BFT protocols. *Proceedings of the ACM Conference on Computer and Communications Security*, 24-28-Octo: 31–42.

Mishra, S., Thapliyal, K., Rewanth, S.K., Parakh, A. & Pathak, A. 2022. Anonymous voting scheme using quantum assisted blockchain. *arxiv.orgS Mishra, K Thapliyal, SK Rewanth, A Parakh, A PathakarXiv preprint arXiv:2206.03182, 2022•arxiv.org*. http://arxiv.org/abs/2206.03182 6 October 2023.

Moher, D., Liberati, A., Tetzlaff, J. & Altman, D.G. 2009. Preferred reporting items for systematic reviews and meta-analyses: the PRISMA statement. *Journal of clinical epidemiology*, 62(10): 1006–1012.

Mondal, S., Wijewardena, K.P., Karuppuswami, S., Kriti, N., Kumar, D. & Chahal, P. 2019. Blockchain inspired RFID-based information architecture for food supply chain. *IEEE Internet of Things Journal*, 6(3): 5803–5813. https://ieeexplore.ieee.org/abstract/document/8674550/ 13 September 2022.

Mora, C., Rollins, R.L., Taladay, K., Kantar, M.B., Chock, M.K., Shimada, M. & Franklin, E.C. 2018. Bitcoin emissions alone could push global warming above 2°C. *Nature Climate Change*, 8(11): 931–933. http://dx.doi.org/10.1038/s41558-018-0321-8.

Mouton, J. 2001. *How to Succeed in Your Master's and Doctoral Studies: A South African Guide and Resource Book*. Pretoria: Van Schaik. https://books.google.co.za/books/about/How_to_Succeed_in_Your_Master_s_and_Doct.html?id=uX4IAQAAIAAJ&pgis=1.

Mukherjee, A., Majumdar, S., Kolya, A.K. & Nandi, S. 2023a. A Privacy-Preserving Blockchain-based E-voting System. http://arxiv.org/abs/2307.08412 6 October 2023.

Mukherjee, A., Majumdar, S., Kolya, A.K. & Nandi, S. 2023b. A Privacy-Preserving Blockchain-based E-voting System. http://arxiv.org/abs/2307.08412 11 November 2023.

Mukherjee, P.P., Boshra, A.A., Ashraf, M.M. & Biswas, M. 2020. A Hyper-ledger Fabric Framework as a Service for Improved Quality E-voting System. *2020 IEEE Region 10 Symposium, TENSYMP 2020*: 394–397. https://ieeexplore.ieee.org/abstract/document/9230820/ 31 March 2023.

Mullany, L. & Stockwell, P. 2021. *Qualitative, quantitative and mixed methods research (Dörnyei)*. file:///C:/Users/Harrison/Downloads/John W. Creswell & J. David Creswell - Research Design_ Qualitative, Quantitative, and Mixed Methods Approaches (2018).pdf%0Afile:///C:/Users/Harrison/AppData/Local/Mendeley Ltd./Mendeley Desktop/Downloaded/Creswell, Cr.

Mwansa, P. & Kabaso, B. 2023a. Blockchain Electoral Vote Counting Solutions: A Comparative Analysis of Methods, Constraints, and Approaches. *6th International Conference on Artificial Intelligence, Big Data, Computing and Data Communication Systems, icABCD 2023 - Proceedings*: (pp. 1-10). IEEE.

Mwansa, P. & Kabaso, B. 2023b. Perception and Expectations of Vote Counting and Validation Systems: A Survey of Electoral Stakeholders. *6th International Conference on Artificial Intelligence, Big Data, Computing and Data Communication Systems, icABCD 2023 - Proceedings*: 1-10). IEEE.

Nakamoto, S. 2008. Bitcoin: A Peer-to-Peer Electronic Cash System | Satoshi Nakamoto Institute. *Bitcoin.Org*: 1–9. https://bitcoin.org/files/bitcoin-paper/bitcoin_pt_br.pdf 12 November 2023.

Noizat, P. 2015. *Blockchain Electronic Vote*. Elsevier Inc. http://dx.doi.org/10.1016/B978-0-12-802117-0.00022-9.

Olusadum, N.J. & Anulika, N.J. 2018. Electronic Voting and Credible Election in Nigeria: A Study of Owerri Senatorial Zone. *Journal of Management and Strategy*, 9(3): 30.

Olusanya, O.A., White, B., Melton, C.A. & Shaban-Nejad, A. 2022. Examining the Implementation of Digital Health to Strengthen the COVID-19 Pandemic Response and Recovery and Scale up Equitable Vaccine Access in African Countries. *JMIR Form Res*, 6(5): 34363. http://arxiv.org/abs/2206.03286 25 November 2023.

Onur, C. & Yurdakul, A. 2023. ElectAnon: A Blockchain-based, Anonymous, Robust, and Scalable Ranked-choice Voting Protocol. *Distributed Ledger Technologies: Research and Practice*, 2(3): 1–25. https://dl.acm.org/doi/10.1145/3598302 11 November 2023.

Othman, A.A.H., Muhammed, E.A.A., Mujahid, H.K.M., Muhammed, H.A.A. & Mosleh, M.A.A. 2021. Online Voting System Based on IoT and Ethereum Blockchain. *2021 International Conference of Technology, Science and Administration, ICTSA 2021*.

Pandey, A., Bhasi, M. & Chandrasekaran, K. 2019. VoteChain: A Blockchain Based E-Voting System. In *2019 Global Conference for Advancement in Technology (GCAT)*. IEEE. https://ieeexplore-ieee-org.libproxy.cput.ac.za/document/8978295/ 9 April 2022.

Panja, S., Bag, S., Hao, F. & Roy, B. 2020. A Smart Contract System for Decentralized Borda Count Voting. *IEEE Transactions on Engineering Management*, 67(4): 1323–1339.

Park, D., Irwan Bahrudin, F. & Han, J. 2020. Circular Reasoning for the Evolution of Research Through a Strategic Construction of Research Methodologies. *International Journal of Quantitative and Qualitative Research Methods*, 8(3): 1–23.

Parmar, A., Gada, S., Loke, T., Jain, Y., Pathak, S. & Patil, S. 2021a. Secure E-Voting System using Blockchain technology and authentication via Face recognition and Mobile OTP. In *2021 12th International Conference on Computing Communication and Networking Technologies, ICCCNT 2021*. IEEE. https://ieeexplore-ieee-org.libproxy.cput.ac.za/document/9580147/ 9 April 2022.

Parmar, A., Gada, S., Loke, T., Jain, Y., Pathak, S. & Patil, S. 2021b. Secure E-Voting System using Blockchain technology and authentication via Face recognition and Mobile OTP. *2021 12th International Conference on Computing Communication and Networking Technologies, ICCCNT 2021*: 6–10.

Pawlak, M. & Poniszewska-Marańda, A. 2019. Blockchain e-voting system with the use of intelligent agent approach. *ACM International Conference Proceeding Series*: 145–154.

Peffers, K., Tuunanen, T., Rothenberger, M.A. & Chatterjee, S. 2007a. A design science research methodology for information systems research. *Journal of Management Information Systems*, 24(3): 45–77.

Peffers, K., Tuunanen, T., Rothenberger, M.A. & Chatterjee, S. 2007b. A design science research methodology for information systems research. *Journal of Management Information Systems*, 24(3): 45–77. https://www-tandfonline-com.ezproxy.cput.ac.za/doi/abs/10.2753/MIS0742-1222240302 15 January 2023.

Platt, M., Sedlmeir, J., Platt, D., Tasca, P., Xu, J., Vadgama, N. & Ibañez, J.I. 2021. The Energy Footprint of Blockchain Consensus Mechanisms Beyond Proof-of-Work. *Proceedings - 2021 21st International Conference on Software Quality, Reliability and Security Companion, QRS-C 2021*: 1135–1144. http://arxiv.org/abs/2109.03667 12 November 2023.

Potrafke, N. & Roesel, F. 2019. *A banana republic? The effects of inconsistencies in the counting of votes on voting behavior*. Springer US. https://doi.org/10.1007/s11127-018-00626-8.

Purkayastha, R. & Roy, A. 2021. An Integrated Environment for Cloud Voting System using Edge Computing. *SSRN Electronic Journal*, (Icicnis): 293–306.

Ramalingam, M., Saranya, D. & Shankarram, R. 2021. An Efficient and Effective Blockchain-based Data Aggregation for Voting System. *2021 International Conference on System, Computation, Automation and Networking, ICSCAN 2021*.

Ramdhani, M.A., Maylawati, D.S. adillah, Amin, A.S. & Aulawi, H. 2018. Requirements elicitation in Software Engineering. *International Journal of Engineering and Technology(UAE)*, 7(2.29 Special Issue 29): 772–775.

Rao, V., Singh, A. & Rudra, B. 2021. Ethereum Blockchain Enabled Secure and Transparent E-Voting. *Advances in Intelligent Systems and Computing*, 1290: 683–702.

Rathore, D. & Ranga, V. 2021a. Secure remote E-voting using blockchain. In *Proceedings - 5th International Conference on Intelligent Computing and Control Systems, ICICCS 2021*. IEEE: 282–287. https://ieeexplore-ieee-org.libproxy.cput.ac.za/document/9432249/ 25 March 2022.

Rathore, D. & Ranga, V. 2021b. Secure remote E-voting using blockchain. *Proceedings - 5th International Conference on Intelligent Computing and Control Systems, ICICCS 2021*, (Iciccs): 282–287.

Reznik, O., Slinko, T., Kravchuk, M., Serohin, V. & Strelianyi, V. 2021. Use of Information and Communication Technologies in the Election Process: Ukrainian Realities and Foreign Experience. *Journal of Legal, Ethical and Regulatory Issues*, 24(1): 1–7.

Risnanto, S., Rahim, Y.B.A., Herman, N.S. & Abdurrohman, A. 2020. E-Voting readiness mapping for general election implementation. *Journal of Theoretical and Applied Information Technology*, 98(20): 3280–3290.

Robinson, P. 2007. *Designing and Conducting Mixed Methods Research*. 3rd editio. SAGE Publications Inc.

Ruparel, H., Hosatti, S., Shirole, M. & Bhirud, S. 2021a. Secure Voting for Democratic Elections: A Blockchain-Based Approach. *Lecture Notes in Electrical Engineering*, 733 LNEE: 615–628.

Ruparel, H., Hosatti, S., Shirole, M. & Bhirud, S. 2021b. Secure Voting for Democratic Elections: A Blockchain-Based Approach. *Lecture Notes in Electrical Engineering*, 733 LNEE: 615–628. https://link.springer.com/chapter/10.1007/978-981-33-4909-4_47 12 September 2022.

Russo, A., Anta, A.F., Vasco, M.I.G. & Romano, S. Pietro. 2021. Chirotonia: A Scalable and Secure e-Voting Framework based on Blockchains and Linkable Ring Signatures. *Proceedings - 2021 IEEE International Conference on Blockchain, Blockchain 2021*: 417–424.

Sadia, K., Masuduzzaman, M., Paul, R.K. & Islam, A. 2020a. Blockchain-Based Secure E-Voting with the Assistance of Smart Contract. : 161–176. https://arxiv.org/abs/1910.13635v1 11 November 2023.

Sadia, K., Masuduzzaman, M., Paul, R.K. & Islam, A. 2020b. Blockchain-Based Secure E-Voting with the Assistance of Smart Contract. , (June): 161–176.

Salat, H., Smoreda, Z. & Schläpfer, M. 2019. Mobile phone data's potential for informing infrastructure planning in developing countries. https://arxiv.org/abs/1907.04812v2 25 November 2023.

Saleh, F. 2021. Blockchain without Waste: Proof-of-Stake. *Review of Financial Studies*, 34(3): 1156–1190.

Sankar, L.S., Sindhu, M. & Sethumadhavan, M. 2017. Survey of consensus protocols on blockchain applications. *2017 4th International Conference on Advanced Computing and Communication Systems, ICACCS 2017*.

Saunders, M.A., Lewis, P. & Thornhill, A. 2016. *Research Methods for Business Students Sixth Edition Research Methods for Business Students*. Sixth edit. Pearson Education. www.pearson.com/uk%0Ahttps://www.amazon.com/Research-Methods-for-Business-Students/dp/1292208783/ref=sr_1_2?dchild=1&qid=1614706531&refinements=p_27%3AAdrian+Thornhill+%2F+Philip+Lewis+%2F+Mark+N.+K.+Saunders&s=books&sr=1-2&text=Adrian+Thornhill+%2F+Phili.

Scotland, J. 2012. Exploring the philosophical underpinnings of research: Relating ontology and epistemology to the methodology and methods of the scientific, interpretive, and critical research paradigms. *English Language Teaching*, 5(9): 9–16. https://eric.ed.gov/?id=EJ1080001 10 September 2021.

Seftyanto, D., Amiruddin, A. & Hakim, A.R. 2019. Design of blockchain-based electronic election system using hyperledger: Case of indonesia. In *2019 4th International Conference on Information Technology, Information Systems and Electrical Engineering, ICITISEE 2019*. Institute of Electrical and Electronics Engineers Inc.: 228–233.

Shahzad, B. & Crowcroft, J. 2019. Trustworthy Electronic Voting Using Adjusted Blockchain Technology. *IEEE Access*, 7: 24477–24488.

Sharma, B., Maheshwari, K., Kumar, D. & Jaiswal, A. 2021a. Mobile Friendly Fully Decentralized Voting System using Blockchain Technology and IPFS. In *Proceedings of the 5th International Conference on Trends in Electronics and Informatics, ICOEI*

2021. IEEE: 588–595. https://ieeexplore-ieee-org.libproxy.cput.ac.za/document/9453092/ 9 April 2022.

Sharma, B., Maheshwari, K., Kumar, D. & Jaiswal, A. 2021b. Mobile Friendly Fully Decentralized Voting System using Blockchain Technology and IPFS. *Proceedings of the 5th International Conference on Trends in Electronics and Informatics, ICOEI 2021*: 588–595.

Shenton, A.K. 2004. Strategies for ensuring trustworthiness in qualitative research projects. *Education for Information*, 22(2): 63–75.

Sheranova, A. 2020. Cheating the Machine: E-voting Practices in Kyrgyzstan's Local Elections. *European Review*, 28(5): 793–809.

Shi, W., Cao, J., Zhang, Q., Li, Y. & Xu, L. 2016. Edge Computing: Vision and Challenges. *IEEE Internet of Things Journal*, 3(5): 637–646.

Shukla, S., Thasmiya, A.N., Shashank, D.O. & Mamatha, H.R. 2018. Online Voting Application Using Ethereum Blockchain. In *2018 International Conference on Advances in Computing, Communications and Informatics, ICACCI 2018*. IEEE: 873–880. https://ieeexplore-ieee-org.libproxy.cput.ac.za/document/8554652/ 1 April 2022.

Singh, S., Wable, S. & Kharose, P. 2022. A Review Of E-Voting System Based on Blockchain Technology. *International Journal of New Practices in Management and Engineering*, 10(04): 09–13.

Sobia, D., Shah, S., Asif, D., Shah, A. & Khaskhelly, N. 2018. Pragmatism Research Paradigm: a Philosophical Framework of Advocating Methodological Pluralism in Social Science Research. *Grassroots* , 52(1): 90–102.

Solanki, J. & Meva, Di. 2019. Comparative Study Indian Electoral Reforms in Indian Context. In *IEEE International Conference on Issues and Challenges in Intelligent Computing Techniques, ICICT 2019*. GHAZIABAD, India: IEEE: 1–6.

Sonnenberg, C. & Vom Brocke, J. 2012. Evaluation patterns for design science research artefacts. *Communications in Computer and Information Science*, 286 CCIS: 71–83. https://doi-org.libproxy.cput.ac.za/10.1007/978-3-642-33681-2_7.

Sonnino, A. 2021. Scaling Distributed Ledgers and Privacy-Preserving Applications. https://arxiv.org/abs/2102.12273v1 12 November 2023.

Spanos, A. & Kantzavelou, I. 2023. A Blockchain-based Electronic Voting System: EtherVote. http://arxiv.org/abs/2307.10726.

Springall, D., Finkenauer, T., Durumeric, Z., Kitcat, J., Hursti, H., MacAlpine, M. & Halderman, J.A. 2014. Security analysis of the estonian internet voting system. In *Proceedings of the ACM Conference on Computer and Communications Security*. CCS '14. New York, NY, USA: ACM: 703–715.

Srivastava, G., Dwivedi, A.D. & Singh, R. 2018. Crypto-democracy: A decentralized voting scheme using blockchain technology. *ICETE 2018 - Proceedings of the 15th International Joint Conference on e-Business and Telecommunications*, 2(Icete): 508–513.

Stančíková, I. & Homoliak, I. 2023. SBvote: Scalable Self-Tallying Blockchain-Based Voting. *Proceedings of the ACM Symposium on Applied Computing*: 203–211. https://dl.acm.org/doi/10.1145/3555776.3578603 11 November 2023.

Stoeckli, E., Neiditsch, G., Stoeckli, E. & Neiditsch, G. 2017. Association for Information Systems AIS Electronic Library (AISeL) Towards an understanding of how and why Design Science Research scholars evaluate Towards an understanding of how and why Design Science Research scholars evaluate. In *ACIS 2017 Proceedings*. 16.

Stoll, C., Klaaßen, L. & Gallersdörfer, U. 2019. The Carbon Footprint of Bitcoin. *Joule*, 3(7): 1647–1661. https://www.sciencedirect.com/science/article/pii/S2542435119302557 13 September 2022.

Swan, M. 2015. *Blockchain: Blueprint for a new economy*. O'Reilly Media, Inc. https://books.google.com/books?hl=en&lr=&id=RHJmBgAAQBAJ&oi=fnd&pg=PR3&dq=M.+Swan,+Blockchain:+Blueprint+for+a+new+economy.+O'Reilly+Media,+2015.+Accessed:+Mar.+31,+2023.+%255BOnline%255D.+Available:+https://books.google.com/books/about/Blockchain.html%253Fid%253 12 November 2023.

Taherdoost, H. 2018. Sampling Methods in Research Methodology; How to Choose a Sampling Technique for Research. *SSRN Electronic Journal*. https://papers.ssrn.com/abstract=3205035 20 June 2022.

Tan, C. & Xiong, L. 2020. *DPoSB: Delegated Proof of Stake with node's behavior and Borda Count*.

Taş, R. & Tanrıöver, Ö.Ö. 2020a. A systematic review of challenges and opportunities of blockchain for e-voting. *Symmetry*, 12(8): 1–24. www.mdpi.com/journal/symmetry.

Taş, R. & Tanrıöver, Ö.Ö. 2020b. A systematic review of challenges and opportunities of blockchain for e-voting. *Symmetry*, 12(8): 1–24. https://www.mdpi.com/2073-8994/12/8/1328/htm 8 September 2022.

Teague, V. 2020. Submission to the inquiry into the future conduct of elections operating in times of emergency Early voting. : 1–4.

The Carter Center. 2018. *Kenya 2017 General and Presidential Elections Report*. One Copenhill453 Freedom Parkway Atlanta, GA 30307 (404) 420-5100: The Carter Center.

The Commonwealth Observer Group. 2015. *Tanzania General Elections*. Commonwealth Secretariat Marlborough House, Pall Mall London SW1Y 5HXUnited Kingdom:

Commonwealth. http://thecommonwealth.org/sites/default/files/inline/2015 Tanzania COG FINAL REPORT_PRINT.PDF.

Thompson, A. 1996. Political Pragmatism and Educational Inquiry. *Philosophy of Education*: 425–434.

Thuy, L.V.-C.-, Cao-Minh, K., Dang-Le-Bao, C. & Nguyen, T.A. 2019. Votereum: An Ethereum-Based E-Voting System. In *2019 IEEE-RIVF International Conference on Computing and Communication Technologies (RIVF)*. IEEE. https://ieeexplore-ieee-org.libproxy.cput.ac.za/document/8713661/ 9 April 2022.

Tian, Y., Wang, C., Asutosh, A., Woo, J. & Adriaens, P. 2022. Blockchain-enabled tokenization for sustainable and inclusive infrastructure investment. *AMCIS 2020 Proceedings*: 40. https://aisel.aisnet.org/amcis2020/adv_info_systems_research/adv_info_systems_research/19 15 November 2023.

Tjahajadi, A., of, T.R.-I.J. & 2018, undefined. 2018. Ethereum Blockchain and Smart Contract Modelling For Presidential E-Voting System in Indonesia. *International Journal of Technology and Engineering Studies*, 4(2): 50–56. https://kkgpublications.com/wp-content/uploads/2018/10/ijtes.4.10002-2.pdf 25 March 2022.

Tjahajadi, A.J. 2018. Ethereum Blockchain and Smart Contract Modelling For Presidential E-Voting System in Indonesia. *International Journal of Technology and Engineering Studies*, 4(2): 50–56.

Ullah, Z., Raza, B., Shah, H., Khan, S. & Waheed, A. 2022. Towards Blockchain-Based Secure Storage and Trusted Data Sharing Scheme for IoT Environment. *IEEE Access*, 10: 36978–36994.

Vairam, T., Sarathambekai, S. & Balaji, R. 2021. Blockchain based Voting system in Local Network. *2021 7th International Conference on Advanced Computing and Communication Systems, ICACCS 2021*: 363–366.

Vaishnavi, V. & Kuechler, B. 2004. Genres of Inquiry in D Esign -S Cience R Esearch : J Ustification and E Valuation. , 39(3): 541–564.

Valenta, M. & Sandner, P. 2017. Comparison of Ethereum, Hyperledger Fabric and Corda. *Frankfurt School Blockchain Center*, (June): 8. www.fs-blockchain.decontact@fs-blockchain.dewww.twitter.com/fsblockchainwww.facebook.de/fsblockchain%0Ahttps://medium.com/@philippsandner/comparison-of-ethereum-hyperledger-fabric-and-corda-21c1bb9442f6 7 September 2022.

Venable, J., Pries-Heje, J. & Baskerville, R. 2016. FEDS: A Framework for Evaluation in Design Science Research. *European Journal of Information Systems*, 25(1): 77–89. https://link.springer.com/article/10.1057/ejis.2014.36 15 January 2023.

Vinet, L. & Zhedanov, A. 2011a. *A 'missing' family of classical orthogonal polynomials*. https://books.google.com/books/about/Blockchain.html?id=RHJmBgAAQBAJ&pgis=1 11 November 2023.

Vinet, L. & Zhedanov, A. 2011b. *A 'missing' family of classical orthogonal polynomials*. O'Reilly Media. https://books.google.com/books/about/Blockchain.html?id=RHJmBgAAQBAJ&pgis=1 31 March 2023.

Vinkel, P. & Krimmer, R. 2017. The how and why to internet voting an attempt to explain e-stonia. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 10141 LNCS: 178–191. https://link-springer-com.libproxy.cput.ac.za/chapter/10.1007/978-3-319-52240-1_11 13 September 2021.

Vivek, S.K., Yashank, R.S., Prashanth, Y., Yashas, N. & Namratha, M. 2020a. E-Voting Systems using Blockchain: An Exploratory Literature Survey. In *Proceedings of the 2nd International Conference on Inventive Research in Computing Applications, ICIRCA 2020*. Institute of Electrical and Electronics Engineers Inc.: 890–895.

Vivek, S.K., Yashank, R.S., Prashanth, Y., Yashas, N. & Namratha, M. 2020b. *E-Voting Systems using Blockchain: An Exploratory Literature Survey*.

Vukolić, M. 2016. The quest for scalable blockchain fabric: Proof-of-work vs. BFT replication. *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 9591: 112–125. https://inria.hal.science/hal-01445797 13 July 2023.

Wallace, M. & Sheldon, N. 2015. Business Research Ethics: Participant Observer Perspectives. *Journal of Business Ethics*, 128(2): 267–277.

Wang, B., Sun, J., He, Y., Pang, D. & Lu, N. 2018. Large-scale Election Based on Blockchain. In *Procedia Computer Science*. Elsevier B.V.: 234–237.

Wisessing, K., Ekthammabordee, P., Surasak, T., Huang, S.C.H. & Preuksakarn, C. 2020. The prototype of thai blockchain-based voting system. *International Journal of Advanced Computer Science and Applications*, 11(5): 63–68. https://pdfs.semanticscholar.org/f3a2/df5e7dfeff9971ca30670f69e1c8dbd5c1c1.pdf 25 March 2022.

Wust, K. & Gervais, A. 2018. Do you need a blockchain? *Proceedings - 2018 Crypto Valley Conference on Blockchain Technology, CVCBT 2018*, (i): 45–54.

Www, S. 2020. *S ato shi N a k a m oto A Peer-to-Peer Electronic Cash System*.

Xiao, Y., Zhang, N., Lou, W. & Hou, Y.T. 2020. A Survey of Distributed Consensus Protocols for Blockchain Networks. *IEEE Communications Surveys and Tutorials*, 22(2): 1432–1465.

Xiong, Z., Zhang, Y., Niyato, D., Wang, P. & Han, Z. 2018. When mobile blockchain meets edge computing. *IEEE Communications Magazine*, 56(8): 33–39.

Xu, D., Shi, W., Zhai, W. & Tian, Z. 2021. Multi-Candidate Voting Model Based on Blockchain. *IEEE/CAA Journal of Automatica Sinica*, 8(12): 1891–1900.

Yang, Y. 2018. LinBFT: Linear-Communication Byzantine Fault Tolerance for Public Blockchains. http://arxiv.org/abs/1807.01829 13 July 2023.

Yi, H. 2019. Securing e-voting based on blockchain in P2P network. *Eurasip Journal on Wireless Communications and Networking*, 2019(1): 137. https://doi.org/10.1186/s13638-019-1473-6.

Yu, B., Liu, J., Sakzad, A., Nepal, S., Steinfeld, R., Rimba, P. & Au, M.H. 2018a. Platform-independent secure blockchain-based voting system. In *Springer*. 369–386. https://link.springer.com/chapter/10.1007/978-3-319-99136-8_20 10 May 2022.

Yu, B., Liu, J., Sakzad, A., Nepal, S., Steinfeld, R., Rimba, P. & Au, M.H. 2018b. Platform-independent Secure Blockchain-Based Voting System. In *In International Conference on Information Security*. Springer: 369–386.

Zaghloul, E., Li, T. & Ren, J. 2021. D-BAME: Distributed Blockchain-Based Anonymous Mobile Electronic Voting. *IEEE Internet of Things Journal*, 8(22): 16585–16597.

Zarir, A.A., Oliva, G.A., Jiang, Z.M.J. & Hassan, A.E. 2021. Developing Cost-Effective Blockchain-Powered Applications: A Case Study of the Gas Usage of Smart Contract Transactions in the Ethereum Blockchain Platform. *ACM Transactions on Software Engineering and Methodology*, 30(3). https://dl.acm.org/doi/10.1145/3431726 13 September 2022.

Zhang, J., Chen, B., Zhao, Y., Cheng, X. & Hu, F. 2018. Data Security and Privacy-Preserving in Edge Computing Paradigm: Survey and Open Issues. *IEEE Access*, 6(March): 18209–18237.

Zheng, Z., Xie, S., Dai, H., Chen, X. & Wang, H. 2017. An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends. *Proceedings - 2017 IEEE 6th International Congress on Big Data, BigData Congress 2017*: 557–564.

Zheng, Z., Xie, S., Dai, H.N., Chen, W., Chen, X., Weng, J. & Imran, M. 2020. An overview on smart contracts: Challenges, advances and platforms. *Future Generation Computer Systems*, 105: 475–491.

Zheng, Z., Xie, S., Dai, H.N., Chen, X. & Wang, H. 2018. Blockchain challenges and opportunities: A survey. *International Journal of Web and Grid Services*, 14(4): 352–375.

Žukauskas, P., Vveinhardt, J. & Andriukaitienė, R. 2018. Philosophy and Paradigm of Scientific Research. *Management Culture and Corporate Social Responsibility*. https://www.intechopen.com/chapters/58890 10 September 2021.