ISAAC KAPAMBWE

A Blockchain and Zero Knowledge Proof Model for decentralised drug distribution and stock transfer

A Final Year Research Project submitted in partial fulfilment of the requirements for the degree of

Master of Science in Computer Science

ZCAS University

2023

DECLARATION

Name: Isaac Kapambwe

Student Number: G00197

I hereby declare that this final year research project is the result of my own work, except for quotations and summaries which have been duly acknowledged.

Plagiarism check: %

Signature: Date:

Supervisor Name:

Supervisor Signature:

Date:

ABSTRACT

This research project proposes a blockchain and zero knowledge proof model for decentralised drug distribution and stock transfer in public health care facilities in Zambia. The model aims to improve the efficiency, security, privacy and transparency of the drug supply chain and enable peer-to-peer drug stock transfer among health facilities. The model is supported by several theories from computer science, cryptography, supply chain management and health informatics. A proof-of-concept application is developed and evaluated using relevant performance metrics. The research contributes to the advancement of patient data confidentiality, smart contract functionality and network reliability in the pharmaceutical supply chain sector.

Keywords: Blockchain, Zero knowledge proof, Decentralised drug distribution, Smart contract, Proof of Stake, Proof of Work

ACKNOWLEDGEMENT

I would like to take this opportunity to express my gratitude and appreciation to my supervisor, Dr. Aaron Zimba for his insightful guidance, patience during correction and invaluable advice throughout this project.

I also would like to express my appreciation to the Ministry of Health Rufunsa District Health office for the assistance given to me throughout the research period

THANK YOU.

DEDICATION

This research project is dedicated to the healthcare workers in Zambia who tirelessly strive to provide quality healthcare services to their communities. Their unwavering commitment and dedication, especially during challenging times and medicine shortages, inspire us to seek innovative solutions to improve healthcare delivery. This work is also dedicated to the patients who are the ultimate beneficiaries of our efforts. May this contribution bring us one step closer to ensuring that everyone, regardless of their location or circumstances, has access to the essential medicines they need. Finally, this work is dedicated to the future researchers in this field, with the hope that it will inspire them to continue exploring and innovating for the betterment of global healthcare.

Table of Contents

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

ZAMMSA: Zambia Medicines and Medical Supplies Agency

MSL: Medical Stores Limited

PoW: Proof of Work

PoS: Proof of Stake

EVM: Ethereum Virtual Machine

IDE: Integrated Development Environment

ZKPs: Zero Knowledge Proofs

DApps: Decentralized Applications

8NDP: 8th National Development Plan

SDG: Sustainable Development Goal

WHO: World Health Organization

NGOs: Non-Governmental Organisations

GDP: Gross Domestic Product

WMS: Warehouse Management System

EHR: Electronic Health Records

PoC: Proof of Concept

USAID: United States Agency for International Development

CHAPTER 1
INTRODUCTION

1.1 Background to the study

Efficient access to medicine by patients is a fundamental human right and a pivotal component of healthcare delivery (Shukar et al., 2021). The United Nations (UN) Sustainable Develop Goal (SDG) target 3.8 aims to achieve Universal Health Coverage (UHC) by 2030, included in the target is access to quality, safe, affordable and effective medicines and vaccines for everyone in the world (World Health Organisation, 2023). Government Hospitals and clinics continue to experience essential drug shortages (Ministry of Finance and National Planning, 2022) as the country's population continues to grow exponentially with an annual growth rate of 2.8% (2022) (Zambia Statistics Agency, 2022), privately owned pharmacies have been established across the country to take advantage of the shortage in public health facilities to enable patients with the required resources to pay out of their own pocket (OOP), but even the privately owned pharmacies cannot meet the demand of critical drugs, particularly for non-communicable diseases (Kaiser et al., 2019). The existing centralised pharmaceutical distribution systems have several limitations, including inefficiencies, delays and vulnerability to fraudulent activities (Siyal et al., 2019). Decentralised Blockchain based technology of drug distribution, emerges as a viable solution to improve the efficiency of drug distribution and enable direct secure intra-facility drug stock transfer in public health centres through the use of smart contracts (Khan et al., 2021). Under this model, healthcare centres facing rapid medication depletion can directly request and acquire medical supplies from other centres which may not be facing the same shortage, this would maximise drug usage and reduce the chance of wasting medicine due to expiry all while reducing the over-reliance on a centralised system (Khatoon, 2020).

Leveraging blockchain technology in conjunction with zero-knowledge proof is one way to facilitate efficient, confidential and secure decentralised drug distribution and stock transfer in public hospitals and clinics (Sharma et al., 2020). Blockchain technology offers a secure, transparent and decentralised ledger system that would record all drug-related transactions and leverage smart contract technologies without the need for a trustworthy central authority, while zero-knowledge proof safeguards the confidentiality of sensitive patient information and provides additional security from various cyber-attacks (Gaba et al., 2022). By utilising this innovative approach, the efficiency of the drug distribution

processes, protect against fraud and theft, lessen the burden on the healthcare system, increase donor confidence, improve patient confidentiality and most importantly save the lives of patients.

The words “drug” and “medicine” are used interchangeably in this report.

1.2 Problem Statement

The scarcity of essential medicines in public clinics and hospitals in Zambia is a critical and recurrent challenge being faced by the Government of Zambia and despite increased funding and investments the procurement of medicines, a poorly functioning supply chain continues to impede sufficient availability of essential drugs to Zambian Citizens (Vledder et al., 2015), this stands as a major hurdle the nation's goal to supply essential healthcare to all Zambian citizens particularly those who cannot afford to access essential medicine from privately owned pharmaceutical companies, most of which also cannot meet the demand of the population (Kaiser et al., 2019). In the 8th National Development Plan (8NDP), The Zambian Government has outlined their goal of increasing availability of essential drugs and medical supplies to at least 90% by 2026 from 40% in 2020) (Ministry of Finance and National Planning, 2022). This goal is directly aligned with their pursuit to achieve the United Nations Strategic Development Goals (SDG) 10 (“reduce inequality within and across countries”) (Gallien et al., 2021) and SDG 3 (“ensure healthy lives and promote well-being for all at all ages”) (World Health Organisation, 2023). The ongoing drug shortages are made worse by population growth (Zambia Statistics Agency, 2022), theft, fraud and inefficiencies in the drug supply chain (Chileshe, 2021) which is increasing the demand on an already resource-constrained healthcare system. Urgent multi sectoral intervention and a robust secure distribution model are required to mitigate this deficiency and provide a solid foundation for secure, fraud free healthcare accessibility and delivery in Zambia (Gallien et al., 2021), increased funding alone will not resolve the problem of drug shortage as corruption and financial mis-management are also threats to healthcare around the world (Mackey & Liang, 2012). An Estimation has shown that in any given country, up to 70% of resources are wasted due to poor drug management systems and the World Bank has indicated that in many developing countries, a high percentage of essential medicine losses occur in the procurement, storage, distribution and utilisation systems that governments use (Iqbal et al., 2017). This research endeavours to study the drug shortage challenges by reviewing the current drug distribution models used by the Zambian Government and explore a decentralised Blockchain and Zero Knowledge Proofs (ZKPs) concept for drug distribution and stock transfer.

1.3 Aim

The aim of this research is to develop A blockchain and Zero Knowledge Proof model for decentralised drug distribution and stock transfer. This has the potential to prevent fraud, increase the efficiency, transparency, trust and security of the drug distribution chain and increase funding towards essential drug procurement by improving donor confidence.

1.4 Objectives

The objectives of this research are:

I. To review the challenges and limitations of the current drug distribution model in public health care facilities in Zambia.

II. To develop a decentralised Blockchain and Zero Knowledge Proof model for drug distribution in public health care facilities in Zambia.

III. To develop a scalable decentralised proof of concept application using Blockchain and Zero Knowledge Proofs technologies for drug distribution and stock transfer in public health care facilities in Zambia.

IV. To evaluate the model that has been developed using relevant performance metrics for Blockchain, Zero Knowledge Proof, distribution and stock transfer.

1.5 Research Questions

I. What are the primary challenges being faced in the current drug distribution model in public health care facilities in Zambia?

II. How can Blockchain technology and Zero Knowledge Proofs be used to decentralise drug distribution and enhance the security and confidentiality of drug distribution processes in public health care facilities?

III. What tools and platforms are available for use in the development of decentralised applications.

IV. What are the key performance metrics that should be considered when evaluating the decentralised Blockchain and Zero Knowledge Proof model for drug distribution and stock transfer?

1.6 Significance of the Project

UNICEF states that a child under the age of 5 dies nearly every minute from Malaria due of a lack of timely access to medicine (*UNICEF - Malaria*, 2023). The intrinsic value of human life highlights the significance of this research as millions of people around the world die every year due to communicable, treatable diseases. The lives that could be saved are the fundamental motivation of this study. Zambia is experiencing exponential growth in her population (Zambia Statistics Agency, 2022) which is resulting in an ever increasing demand for essential drugs and vaccines and while funding from the Zambian Government for essential drugs is improving, drug shortages in public healthcare facilities remains a pertinent challenge in the delivery of quality healthcare by the government through the ministry of Health (Ministry of Finance and National Planning, 2022). The impact of an efficient, reliable and fraud-free medicine distribution system cannot be overstated as even marginal improvements in the essential medications supply chain can be the difference between life and death of patients (Ko et al., 2020). Furthermore, this study can contribute to the confronting of medical funding challenges using Blockchain technology, a transparent, decentralised, secure, fraud-free and timely delivery of medicine to patients who need it the most has the potential to attract even more funding from donor agencies and countries (Ko et al., 2020) because they are guaranteed that their donations will reach their intended target, this has the potential to cover the financial constraints currently being faced the government.

Zero Knowledge Proofs (ZKPs) technology can insure the safe, traceable but private delivery of medications to patients, ZKPs can achieve this by allowing patients to prove their eligibility for a given medication to a healthcare provider without revealing any additional information ensuring that their sensitive patient information remains confidential. This has the potential to prevent medical fraud as verification of prescription and validity add an extra layer of security (Al-Aswad et al., 2021).

Additionally, a decentralised blockchain and Zero Knowledge proof distribution framework will alleviate the limitations of using a centralised drug distribution system and enable direct peer to peer stock transfer between health centres via the use of Smart Contracts, a process which reduces the reliance of a centralised model which is time consuming when it comes to approval of medicine transfer (Dick-Sagoe et al., 2021).

1.7 Scope and Limitation

This research embarks on an innovative exploration of a Blockchain and Zero Knowledge Proof model for decentralised drug distribution and stock transfer, with a primary focus medicines required for the treatment of both communicable and non-communicable diseases in major public healthcare facilities (clinics and hospitals) in Zambia at both country and district level. The research will cover a range of diseases that are responsible for the highest number of recorded deaths in the Country, like Malaria, Tuberculosis, Hypertension, Diabetes and HIV/AIDS. Major health facilities are central to this inquiry since they account for very large numbers of patients attended to. Improving efficiency of drug supply systems by leveraging Blockchain technology will also be covered in this research, this will include improving protection of sensitive systems against unauthorised access, counterfeit prescriptions, and other fraudulent activities within the pharmaceutical supply chain using smart contracts. Additionally, a pivotal aspect of this research is the advancement of patient data confidentiality through ZKPs, establishing a framework to safeguard sensitive patient information when they need access to drugs. This ensures that only the minimum essential information is disclosed to relevant individuals for the purpose of validating the eligibility of a prescription. Efficiency optimisation over centralised systems is a core objective, with the integration of Blockchain technology streamlining processes, reducing administrative overheads and enhancing timely access to medications. Medications and systems required to treat conditions outside of communicable and noncommunicable diseases (like those required for plastic surgery and non-life-threatening cosmetic condition) are deliberately excluded from the scope, while the research will highlight response to breakouts, global pandemics like COVID 19 will not be covered in depth due to their vast coverage and the need to maintain a focused and achievable research undertaking within the limited time frame. While a proof-of-concept application will be developed for the purpose of evaluation and demonstration, the system will not be a fully-fledged logistics management system or pharmaceutical management system, the decentralised application will be developed with the sole purpose of demonstrating the deployment the proposed model and how the model provides a security framework for medicine distribution. This research seeks to pioneer a transformative model tailored to the needs of improved efficiency and security of drug distribution and stock transfer in the Zambian governments pharmaceutical supply chains.

1.8 Outline of the research

The rest of the research is outlined in the figure below.

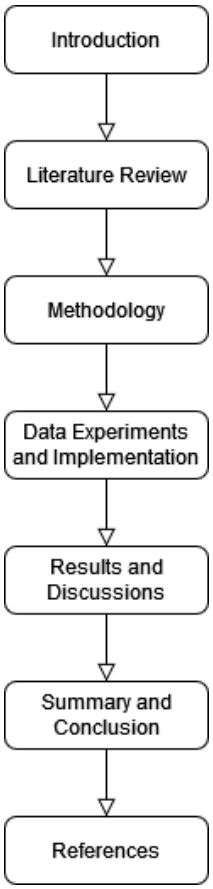


Figure 1 - Research outline

CHAPTER 2

LITERATURE REVIEW

2.1 General Background

The World Health Organization (WHO) recognises two models of distribution of medicines, the push and pull models (Peltoniemi, 2021). The pull method, which is the more common method in developed countries, involves local health facilities requisitioning for medicines from distribution centres or hubs. In this model, the health centre has to figure out how much medicines they'll need prior to making the requisition (HEART, 2016). The push model involves a centralised authority dispatching medicines to all health facilities without the facilities having to requisition for them. This can be helpful in situations like emergencies or when there's not enough data on how much medicine has been used before but does often result in overstocking for certain drugs that aren't in high demand in a given region or health facility (WHO, 2014).

According to (IDC, 2017) the Zambia Medicines and Medical Supplies Agency (ZAMMSA) previously named Medical Stores limited (MSL) is a limited company owned by the Ministry of Finance (98%) and Ministry of Health (2%). ZAMMSA is tasked with the responsibility of storing and distributing essential medicines to all public health institutions in Zambia. (Tembo Mwanaumo et al., 2023) states that drugs are distributed from a main central warehouse in Lusaka to all public health facilities in the province and to smaller distribution hubs around the country. ZAMMSA and Ministry of Health use Warehouse Expert, which is a 3rd party Warehouse Management System (WMS) in 2019 and the system was successfully rolled out to all regional hubs by September 2021. The Warehouse Expert system is integrated with NetLog, a centralised reporting tool that enables the real time monitoring of transactions and stock across all hubs this has improved stock tracking and is a step towards the Ministry of Health's decentralisation policy in which each regional hub can become an inventory managing entity and not only a cross-docking facility as it currently operating (USAID, 2021). However, limitations exist because the tools that monitor medicine in hubs are not integrated with the SMART Care system which is used by patients when getting medicine from public healthcare facilities. Furthermore, poor and in some cases none consistent electronic reporting has resulting in incomplete datasets and reports (Walter, 2018).

According to (Bvuchete et al., 2020), South Africa utilises a pure "push" approach similar to Zambia. Developed countries such as the United States of America (USA) and most countries

in the European Union have adopted the use of the "pull" system, using Stock Management Systems that are integrated with Electronic Health Records (EHR) systems (Toscano et al., 2018).

(Mackey & Cuomo, 2020) states that up to 30% of spending in public procurement is lost due to corruption and mismanagement. Fraud detection technologies are required in e-procurement and stock management systems to combat corruption, improve transparency in the medicine supply chain system.

2.2 Broad literature review of the topic

(Rawat, 2022) proposes the integration of Blockchain Technology in Internet of Medical Things (IOMT) as a means of enhancing security in IOMT systems. According to (Mackey & Cuomo, 2020), machine learning and artificial intelligence integration into e-procurement could be used to combat public healthcare fraud in the medical supply chain. (Kumar, 2023) Recommends the use of digital drug serialisation to tackle the medical fraud.

2.3 Critical review of related works

(Uthayakumar & Priyan, 2013) developed a mathematical model that takes into account various pharmaceutical products, varying lead times (time taken from manufacturing to delivery), allowable payment delays, space limitations and the desired customer service level (CSL). The model can identify the best solutions for inventory lot size, varying lead times and the quantity of deliveries needed to meet CSL targets for hospitals while minimising the total cost of the entire supply chain. (Priyan & Uthayakumar, 2014) also developed a model that operates within a fuzzy stochastic environment. In this model, the total cost of inventory management is used as a fuzzy variable in a multi-tier, multi-product, and multi-constraint inventory system, utilising the distance method as a basis for calculation.

(Kim, 2005) Developed an online procurement system based on a model that incorporates a supply chain network with pharmaceutical companies, wholesalers and hospitals. The model enables real-time access to information by relevant stake holders in order to increase the efficiency of pharmaceutical inventory control.

(Stecca et al., 2016) developed a linear programming model for a drug distribution network in the healthcare industry. The model is made up of a multi-level distribution system where the primary objective is to minimise the total costs involved in drug delivery.

(Tezel et al., 2021) discusses 3 Blockchain models for supply chain management developed on Ethereum. The models present various benefits and challenges.

(Baboli et al., 2011) proposes two models, a centralised and decentralised model, The basic model consists of a single warehouse and a single retailer. The model assumes that the products have a predictable demand, which means they are items that are consistently in high demand and have a high turnover rate. In the centralised model, the warehouse and retailer are treated as one organisation, while in the decentralised model, the two entities treated as separate units.

2.4 Comparison with related works

Multiple related works were reviewed, and the criteria used to compare them is listed below.

Table 2.1

No.	Models	Focus	Data Privacy and Security	Main objectives	Weaknesses
1.	Mathematical Model (Uthayakumar & Priyan, 2013)	Lead times, payment delays, space limitations, and CSL.	Not Addressed	Identify optimal inventory lot size and delivery quantity	Limited applicability to dynamic and uncertain environments
2.	Fuzzy Stochastic Model (Priyan & Uthayakumar, 2014)	Total cost of inventory management used as a fuzzy variable.	Not Addressed	Optimise inventory decisions in a fuzzy stochastic environment	Complexity in parameter tuning for fuzzy variables
3.	Online Procurement System (Kim, 2005)	Real-time access to information for efficient inventory control.	Not considered	Improve efficiency in pharmaceutical inventory management	Dependency on robust and reliable online connectivity resulting in a single point of failure.
4.	Linear Programming Model (Stecca et al., 2016)	Multi-level distribution system, minimize total costs	Not covered	Optimise costs in a multi-level drug distribution network	Assumes linear relationships, may not capture nonlinearities.

5.	Blockchain Models for SCM (Tezel et al., 2021)	Discuss benefits and challenges of 3 Blockchain models	Security through Decentralised and transparent transactions protected by cryptography, no focus on specific privacy requirements.	Explore blockchain in project Bank Accounts (PBAs), reverse auction–based tendering for bidding and asset tokenization for project financing.	Scalability and integration of the blockchain technology with current technologies.
6.	Centralized & Decentralized Models (Baboli et al., 2011)	Assumes predictable demand, central vs. decentralized approach	Not covered	Compare centralized and decentralized supply chain models.	Limited adaptability to sudden changes in demand or supply
7.	Blockchain and Zero Knowledge proof Model	Blockchain and Zero Knowledge proofs in medicine distribution.	Patient data confidentiality is handled with Zero Knowledge Proof techniques while data security is handled by cryptography in blockchain tools and platforms.	Developing a Blockchain and Zero Knowledge proof model for secure and verified anonymous access to medicines in healthcare facilities.	Power consumption at scale is likely to be high as it is reliant on deployment methods and mining configurations.

2.5 Theoretical and Conceptual framework

This section presents the theoretical and conceptual framework that supports the proposed model of using blockchain and zero knowledge proofs for decentralised drug distribution and stock transfer. Blockchain and Zero Knowledge proofs integration into the current drug distribution system (in public healthcare facilities) is also covered, lastly the theories that support the proposed model and the theoretical frameworks used to guide the research are explained.

2.5.1. Integration of Blockchain and Zero Knowledge Proofs

Blockchain is a distributed ledger technology that enables secure, transparent, and immutable transactions among peers without the need for a central authority or intermediary (Hamilton, 2020). Blockchain can be used to record and verify the provenance, ownership, and movement of drugs along the supply chain, as well as to

enforce smart contracts that automate the execution of predefined rules and agreements among the stakeholders (Khan et al., 2021). Blockchain can also enable peer-to-peer drug stock transfer among health facilities, removing or reducing the reliance on a centralised distribution system and improving the efficiency and availability of drugs (Khatoon, 2020).

Zero knowledge proofs (ZKPs) are cryptographic techniques that allow one party (prover) to prove to another party (verifier) that a statement is true without revealing any additional information (Sun et al., 2021). ZKPs can be used to protect the privacy and confidentiality of patient data and prescriptions as well as to provide additional security against fraud and cyberattacks (Sharma et al., 2020). ZKPs can also enable anonymous and verified access to drugs by patients, allowing them to prove their eligibility for a given prescription without disclosing their identity or medical history (Al-Aswad et al., 2021).

The integration of blockchain and zero knowledge proofs can therefore provide a solution to some of the challenges being faced in the Zambian health sector particularly regarding drug distribution and stock transfer,

2.5.2. Theories Supporting the Proposed Model

The proposed model is supported by several theories from different disciplines, these include computer science, cryptography (Mathematics), supply chain management, and health informatics. The following relevant theories are covered:

a) **Distributed Systems Theory:** This theory studies the design, performance, and properties of systems that consist of multiple autonomous components that communicate and work together to achieve a common goal (Ghosh & Ghosh, 2023). Blockchain technology is an example of a distributed system, this it because it's operation is reliant on a network of nodes (compute nodes) that maintain a shared and consistent state of the ledger through a consensus mechanism (Zhang et al., 2020). Distributed systems theory can help to analyse and evaluate the scalability, reliability, performance and security of blockchain-based medicine distribution systems.

b) **Game Theory:** First conceived in the field of economics, Game theory studies the strategic interactions and decision making of rational agents in situations of conflict or cooperation (De Giovanni, 2020). Game theory can help to model and understand the incentives, behaviours, and outcomes of the various stakeholders involved in the public sector medicine distribution, such as district pharmacists (in charge of medicine supply to all health facilities in a district), patients (including those with chronic illnesses), suppliers, donors, doctors, health facility pharmacists and regulators. Game theory can also help in the design and implementation of smart contracts that align the interests and objectives of the stakeholders while ensuring fair, transparent and efficient transactions throughout the distribution model (Khan et al., 2021).

c) Complex Systems Theory: This theory studies the emergence, adaptation, resilience and evolution of complex systems that consist of many interacting components which exhibit self-organising, nonlinear, resilient and unpredictable behaviour (Dawkins & Barker, 2020). Complexity theory can aid in the capture and explanation of the existing challenges and opportunities in the medicine distribution sector (system/model), this is because it is a complex system that involves multiple stakeholders (as mentioned in Game Theory above), environmental factors (such as seasonal outbreaks of disease) and multiple uncertainties (sudden epidemics and pandemics) (Dawkins & Barker, 2020). Furthermore, Complexity theory can aid in the identification and leveraging of the potential of Blockchain and zero knowledge proofs technologies to enable self-organisation, innovation and system resilience (Dos Santos, 2017).

2.6 Proposed model

The proposed model is the use of Blockchain and Zero Knowledge proofs technologies for decentralised drug distribution and stock transfer. The model is illustrated in the figure below.

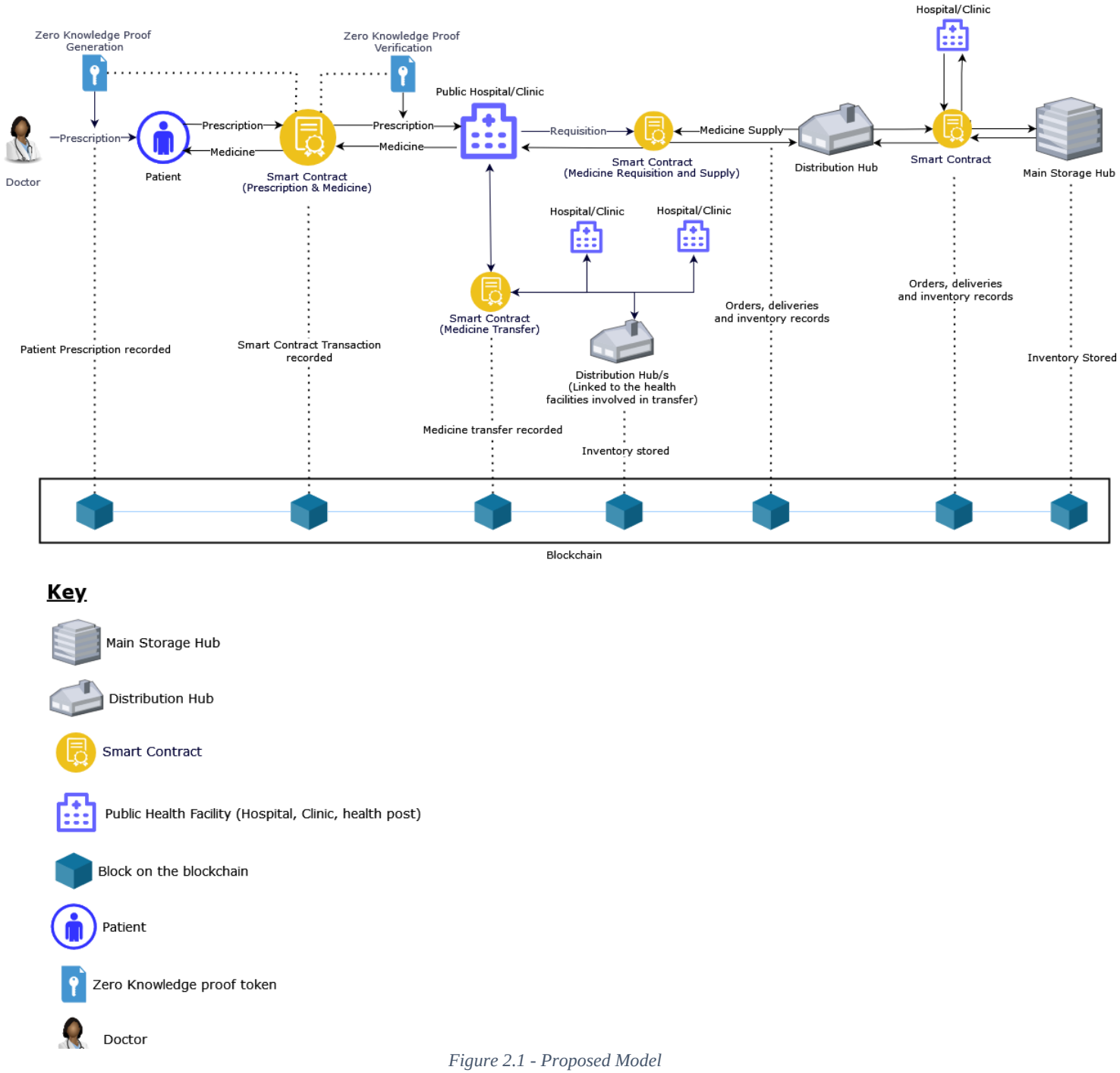


Figure 2.1 - Proposed Model

2.7 Chapter Summary

This chapter reviews the existing literature on the challenges and limitations of the current drug distribution model in public health care facilities in Zambia, and the potential of decentralised applications to improve the efficiency, security, privacy and transparency of the drug distribution and stock transfer processes. The chapter also proposes a blockchain and Zero Knowledge model as a solution to the challenges and limitation of the current distribution model. The proposed model is also compared with related works from different academic publications. The chapter also presents the theoretical and conceptual framework that supports the proposed model and explains how blockchain and zero knowledge proofs technologies can be used to develop decentralised applications for secure medicine distribution without the reliance on a central authority (Ministry of Health).

CHAPTER 3

METHODOLOGY

This chapter explains Zero Knowledge Proofs (ZKPs) technology and how it can safe-guard confidential patient information, it also provides an explanation of how smart contracts interact with blockchains. Additionally, this chapter covers the concepts of proof of work and proof of stake in blockchain technology. Finally, it lays out the steps taken to complete the investigation, design of research, chosen approach and justification.

1.1 Understanding Zero Knowledge Proofs

Zero Knowledge Proofs is cryptographic technique which enables one party (a prover) to prove to another party (the verifier) that a given statement is true without revealing any information about the statement itself. The statement is kept secret because "zero" (no) knowledge of the statement itself is required in order to prove it's validity. In the context of this research, Zero Knowledge Proofs can enable a patient to prove to a pharmacy officer/operator that the prescription they received from the Doctor/Physician is valid and belongs to them without revealing any information of their identity or who the medication belongs to (in case of claiming for a minor). The Sudo code below (next page) provides an illustration of how ZKPs function:

3.1.1 ZKPs Sudo code

1. *Begin ZKP Patient Info Safeguarding Algorithm*

2. *Input:*

   - Patient Information (PI) to be safeguarded
   - ZKPs Cryptography Protocols

3. *Initialize:*

   - ConfidentialPatientInfo (CPI) //for confidential patient information
   - Prover (P) // Prover of the validity of statement without revealing details
   - Verifier (V) // Entity verifying the proof

4. *Procedure:*

   i. CPI = EncryptPatientInfo (PI) // Encrypt patient information
   ii. P generates a ZKP for CPI:
   - Proof = GenerateZKP(CPI)
   iii. P sends Proof to V without disclosing CPI:
   - Transmit (Proof)
   iv. V receives Proof and verifies it without gaining knowledge of the actual data:
   - VerificationStatus = VerifyZKP(Proof)
   v. If VerificationStatus is True:
   - AccessGranted = GrantAccessToMedication()
   - PatientInfoConfidentialityMaintained()

5. End ZKP Safeguarding Algorithm

1.2 Smart Contracts

Smart contracts are self-executing contracts with the terms to me meet written directly into code. Smart Contracts have been included in the proposed model as a means of inventory management and secure transfer of medicine. These contracts enable the secure and reliable decentralised distribution of medicine enabling peer to peer requisition and supply of essential medicines (even directly from a health facility to another). Smart contracts ensure transparent and secure transactions on blockchain networks. The integration of smart contracts in the proposed model streamlines the processes of medicine transfer amongst health facilities and distribution hubs, without the need of central authority (Provincial Health Office in Zambia). In the current distribution model, if a health facility in Zambia needs to request for the urgent supply of essential medicine directly from another health facility which may have the required medicine in abundance then a request needs to be sent to the district office, which through the district pharmacist manually processes the transfer request and sends it to the provincial office for approval, if approval is granted, the reverse order is followed, the approval is sent to the respective district office, then processed by the district pharmacist who can the facilitate and monitor the transfer of medicines between two respective health facilities (the one requesting and the one supplying). A process which is so time consuming that it's barely utilised, health officials at public health facilities would rather give the patient a referral letter to the health facility that is likely to have the medication in abundance (Seyed-Nezhad et al., 2021).

1.3 Consensus Mechanisms - Proof of Work (PoW) and Proof of Stake (PoS)

3.3.1 Proof of Work (PoW)

Proof of Work (PoW): is a consensus mechanism in blockchain technology that confirms transactions, produces new blocks and adds them to the blockchain network. PoW involves solving complex mathematical problems through the process known as mining. And while the solution is challenging to find, it's easy to verify. The purpose of PoW is to prevent fraudulent activities and ensure all transactions are recorded in a decentralised manner, creating trust and agreement among network members. However, is characterised by high energy (electricity) consumption due to the scale of computational resources required to mine on the blockchain.

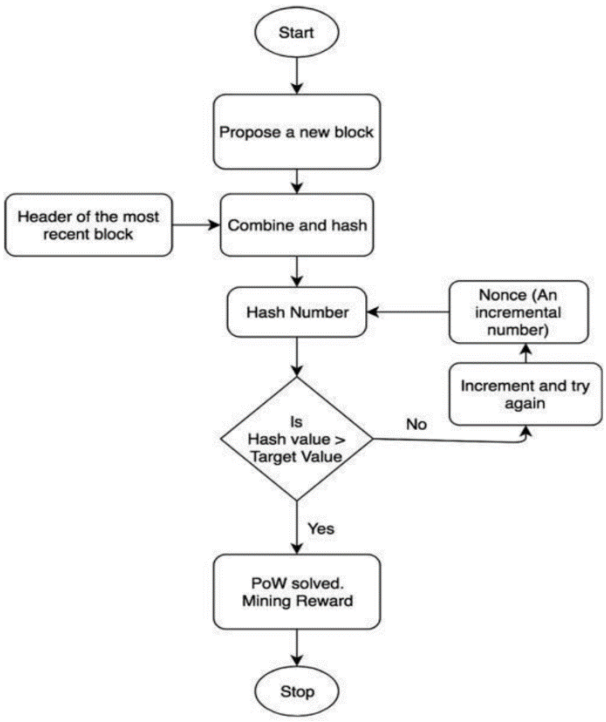


Figure 3.1 Proof of Work Algorithm

Proof of Stake (PoS)

PoS is a consensus algorithm used in blockchain networks to validate and confirm transactions and create new blocks. Instead of miners solving complex mathematical problems (PoW), validators are chosen to create new blocks based on the amount of cryptocurrency they hold and are willing to "stake" as collateral. Figure 3.2 below illustrates how it works.

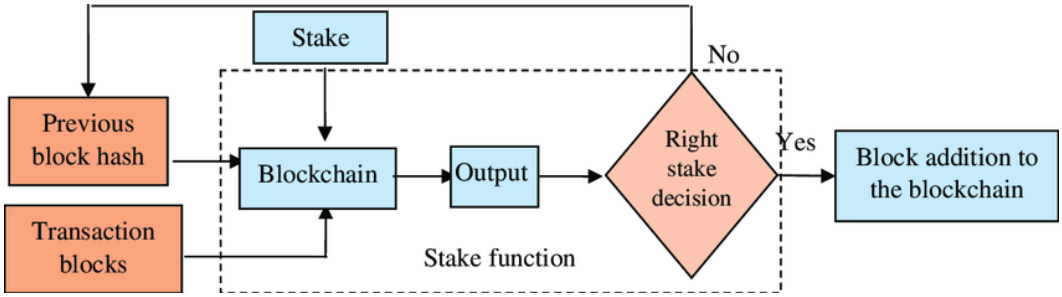


Figure 3.2 Proof of Stake Algorithm

3.1 Research design

This research adopts a quasi-experimental design (Maciejewski, 2020), this design is suitable because of to the inherent difficulties in obtaining sensitive medical data for experimental purposes, particularly that involving patient and patient records. This also makes random assignment impractical when dealing with confidential information as some assumptions may not directly reflect real world variables. A quasi-experimental approach will enable the navigation of these considerations and still collect valuable insights from a real-world context without compromising data integrity.

1.1 Adopted method and Justification

The chosen methodology leverages Zero Knowledge Proofs (ZKPs), Smart Contracts, and Proof of Stake (PoS) in blockchain technology. ZKPs serve as a cryptographic technique ensuring the confidentiality of patient information, while Smart Contracts enable secure and decentralized medicine distribution. The adoption of PoS as a consensus mechanism ensures transaction verification and network reliability.

This methodological framework aligns seamlessly with the project goals of enhancing pharmaceutical supply chain practices. The integration of ZKPs ensures patient information privacy, Smart Contracts streamline decentralized medicine distribution, and PoS secures the blockchain network. Together, these methodologies contribute to a robust and efficient solution for the challenges faced in the healthcare distribution landscape.

By adopting a quasi-experimental design and integrating these advanced technologies, the research methodology not only navigates the complexities of the pharmaceutical supply chain but also ensures that the proposed model is well-equipped to address real-world challenges effectively.

1.2 Association of research method to project

The research method is intricately tied to the project's overarching goal of revolutionizing pharmaceutical supply chains. ZKPs safeguard patient information, Smart Contracts streamline medicine transfer, and PoS for network security. This alignment signifies a strategic integration of novel technologies to address the specific challenges within the healthcare distribution sector in Zambia.

The association of the research method to the project is reinforced by its real-world applicability. The chosen methodologies - ZKPs, Smart Contracts, and PoS - collectively address the specific challenges faced by stakeholders in the pharmaceutical supply chain. By aligning the research method with the project's goals, the study positions itself to provide tangible solutions that go beyond theoretical frameworks, contributing to the practical improvement of healthcare distribution practices.

1.3 Research data and datasets

Due to the privacy policies placed on accessing medical records data this research focuses on the use of secondary data obtained from declassified government records and reports and publications provided by Non-Governmental Organisations (NGOs).

3.4.1. Population and population growth.

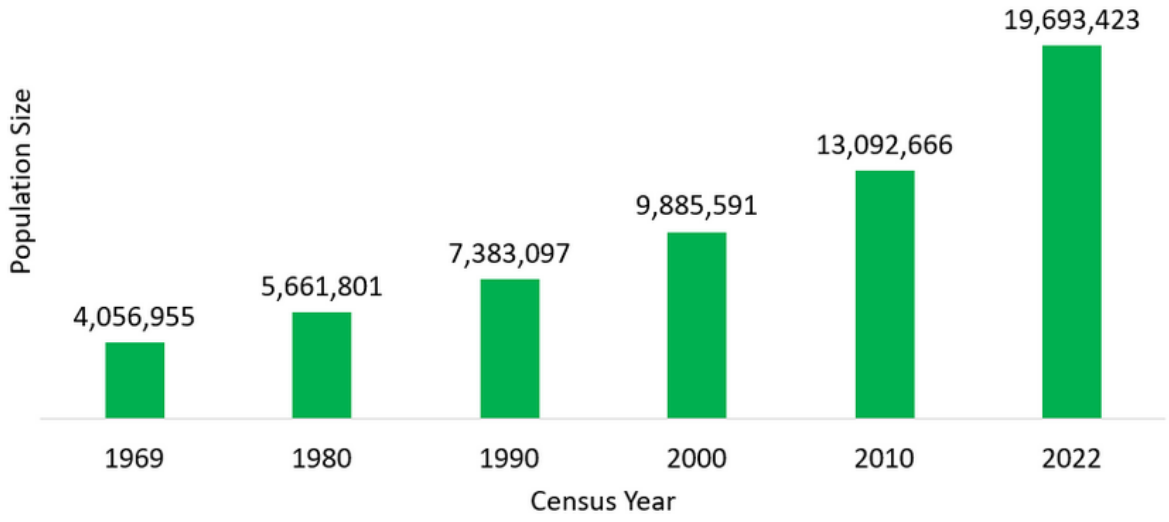


Figure 3.2 - Population of Zambia (Zambia Statistics Agency)

Zambia is experiencing an exponential growth in population as illustrated in figure 3.1 above, this growth has resulted in higher demand for essential medicines.

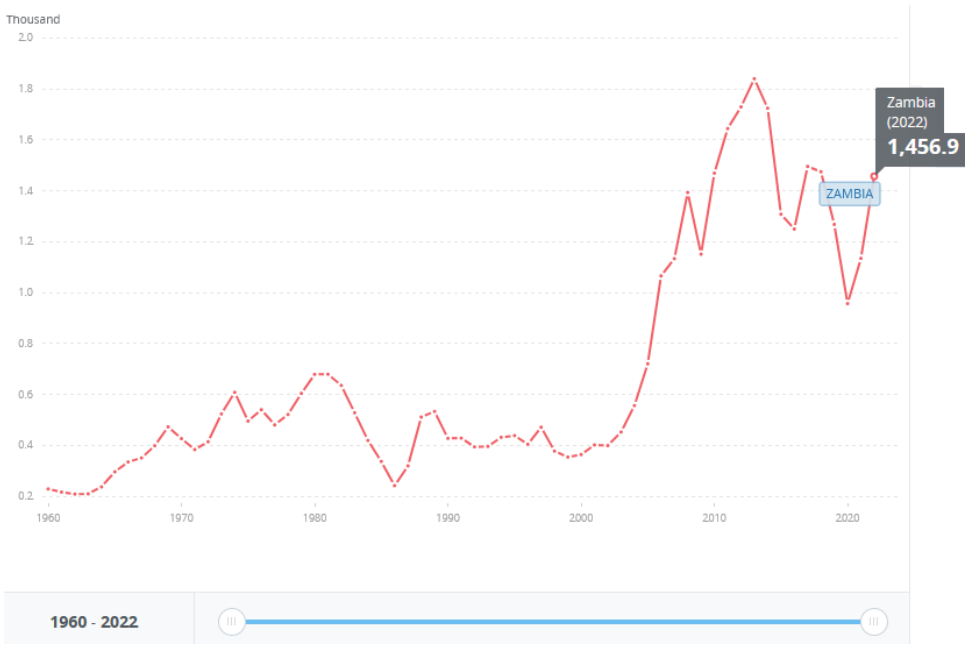


Figure 3.3: Zambia's GDP Per Capita (Thousand US $ - World Bank)

Similar to the population growth in Figure 3.1 Zambia has been experiencing exponential growth in Gross Domestic Product (GDP) Per Capita since the year 2000. However, despite this growth in population and GDP Per capita, government healthcare expenditure per capita has stagnated as illustrated in figure 3.3 below.

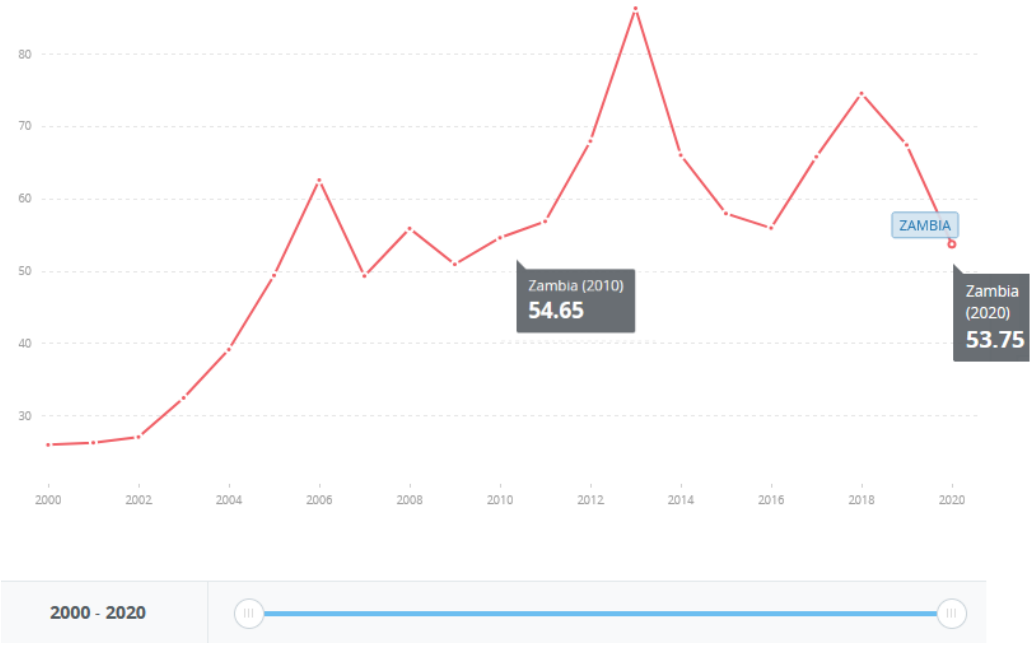


Figure 3.4 - Government expenditure Per Capita in US Dollars (World Bank)

As at 2020 (most recent update during the writing of this research paper) government healthcare expenditure stood at $53.75US which is lower than it was 10 years prior ($54.65 US in 2010). This factor further compounds the current problem of essential medicine shortages in healthcare facilities. More emphasis is placed on the importance of minimising fraud, theft and inefficiency distribution systems of medicine to ensure that the limited resources that are available reach patients in need. Otherwise the problem is compounded even further.

Table 3.1 - Projected fill rate requirement of essential medicine (8th National Development plan)

Year	Fill Rate (%)	Progression Required (Percentage Points)	Expected Population	Population Growth
2020	40	-	19,693,423	+552,483
2021	50	+10	20,236,742	+543,319
2022	60	+10	20,786,468	+549,726
2023	70	+10	21,342,849	+556,381
2024	80	+10	21,905,151	+562,302
2025	85	+5	22,473,649	+568,498
2026	90	+5	23,048,641	+574,992

According to the Zambian 8th National Development Plan (8NDP), Government has the aim of achieving a fill rate of 90% for essential medicines in public health facilities by 2026, however, real time tracking of progression (or lack of it) is not possible with the current distribution model. This is because of gaps in the reporting system, an example of this is a lack of confirmation of medicine delivery by the provincial health office after they approve the direct transfer of medicines from one health facility to another (In different districts). It is therefore important that the proposed model provides a solution to track fill rates across health facilities and the country as a whole, this will ensure reliable reports which will result in better access to essential medicine by patients (Ministry of Finance and National Planning, 2022).

3.6 Ethical concerns related to the research

The main ethical concern is sensitivity of any data relating to patients, regardless of whether the data relates to them directly or indirectly. The limited information made available will be with the consent of relevant stakeholders. Ensuring that the confidentiality of patient

information is maintained. The research design ensures compliance with ethical guidelines, safeguarding the confidentiality and integrity of the data involved.

3.7 Chapter Summary

Chapter 3 outlines the methodologies employed, integrating advanced technologies to address healthcare challenges. It highlights the relevance of ZKPs, smart contracts, and PoW in achieving project goals, while considering ethical implications and real-world applicability. The chapter also covers secondary dataset findings from World Bank and Zambia Statistics Agency that provide more insight into the ever growing problem of medicine shortages in Zambia.

CHAPTER 4

DATA, EXPERIMENTS, AND IMPLEMENTATION

This section outlines the implementation of a Proof of Concept (PoC) for the proposed decentralised ZKPs application on the Ethereum blockchain. The PoC is designed to validate the feasibility of specific technical elements rather than developing a comprehensive logistics or pharmacy management system.

4.1 Appropriate modelling in relation to project

Proof of Stake (PoS), a consensus mechanism was selected for the PoC for its energy efficiency and faster speed of processing transactions in comparison to PoW where mining is involved. Mining would not offer benefits in a private blockchain network.

Rationale for using Ethereum:

Cost-effectiveness: Ethereum uses PoS which eliminates the need for energy-intensive mining, reducing operational costs and making it a cost-effective choice for private blockchain implementations.

Better Scalability: Ethereum is highly scalable this is essential for building private DApps that may require scalability to handle a growing number of users, transactions and additional functionality.

Smart Contract Functionality: Ethereum supports the use of smart contracts with the ability to connect to them using multiple supported languages including JavaScript, making it a robust platform for implementing complex decentralised applications with self-executing code.

Interoperability: Ethereum's popularity and widespread use allowing for seamless integration with other blockchain tools such as Ganache and MetaMask, which provide reliable testing platforms for decentralised systems. Ethereum also allows developers to test on several of their test networks that mimic real world performance of sending transactions to multiple nodes around the world.

Security: Ethereum's mature ecosystem and PoS consensus provide a secure environment for deploying private blockchain DApps, ensuring data integrity and confidentiality even in testing environments.

4.2 Techniques, algorithms, mechanisms

KECCAK-256: KECCAK-256 is the cryptographic hashing algorithm that Ethereum for the following techniques:

Transaction Verification: When a transaction is created, the transaction data is hashed using KECCAK-256. This hash is then signed with the sender's private key to create a digital signature. Anyone with access to the sender's public key can validate this signature, confirming that the transaction is authentic and has not been altered.

Block Verification: Each block in the Ethereum blockchain includes a hash of the previous block, created using KECCAK-256. This guarantees the integrity of the blockchain network because changing any block in any way would require changing all subsequent blocks in the blockchain, a process which is not computationally feasible.

Smart Contract Verification: KECCAK-256 is also used to hash the code of smart contracts. Anyone may use this to confirm that the code they are working with matches the hash stored on the blockchain, hence the trust in the smart contract.

Consensus Mechanism: Ethereum's PoS consensus mechanism uses KECCAK-256. New block creators are selected by validators using a random selection procedure that involves the use of KECCAK-256.

Solidity: Solidity is an object-oriented, high-level programming language for Ethereum smart contract development. Solidity is geared at the Ethereum Virtual Machine (EVM), the Ethereum smart contract runtime environment, and is influenced by C++, Python, and JavaScript. Solidity is a powerful and expressive language for implementing complicated logic and functionality in smart contracts because it supports a wide range of features, including inheritance, libraries, user-defined types, and sophisticated data structures.

Remix: This is an online integrated development environment (IDE) for creating, assembling, troubleshooting, and implementing Solidity smart contracts. Remix is a handy and potent tool for creating smart contracts because of its user-friendly interface, syntax highlighting, code analysis, auto-completion, and testing facilities. Remix also enables developers to connect to other Ethereum networks, including test networks, local networks, and the main network, and to engage with their smart contracts via a web browser.

Ganache: Ganache is an Ethereum based personal blockchain that enables devlopers create apps, test them, and publish contracts. Because Ganache mimics a whole Ethereum client, it can process transactions, create blocks, and respond to queries in a realistic manner. In addition, Ganache offers a command line interface (CLI) that enables developers to alter network parameters like block time, gas limit, and network ID. The GUI shows accounts, balances, transactions, contracts, and events on the blockchain. Additionally, Ganache may be used with other programs like Remix and MetaMask to offer a complete environment for testing and development.

MetaMask: MetaMask enables users may communicate with Ethereum DApps without having to launch a complete Ethereum node (separate from existing nodes). By serving as a conduit between the Ethereum network and the browser, MetaMask offers a graphical user interface for account management, transaction transmission, and message signing. Additionally, users may connect to and switch between other Ethereum networks with ease using MetaMask, including the main network, test networks, and local networks. MetaMask supports the majority of Ethereum DApps and standards, including ERC-20 and ERC-721 coins, and is compatible with the majority of web browsers, including Chrome, Firefox, and Brave.

4.3 Implementation

This section outlines the architecture of the PoC system and a flowchart illustration of how the different components connect.

Architecture

The architecture of the system consists of a private (test) Ethereum blockchain network running on Ganache, a Bootstrap 5 User Interface (UI) and web3 connection of the smart contracts running on the blockchain with the UI, Web3 is used to enable users to interact with the blockchain using a user-friendly interface and not the command line terminal.

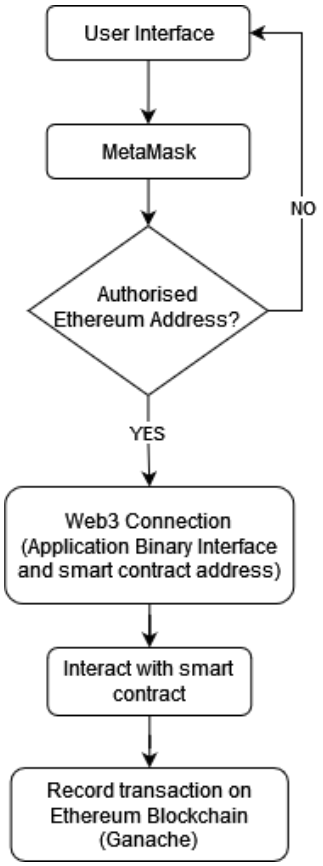


Figure 4.1 PoC Architecture

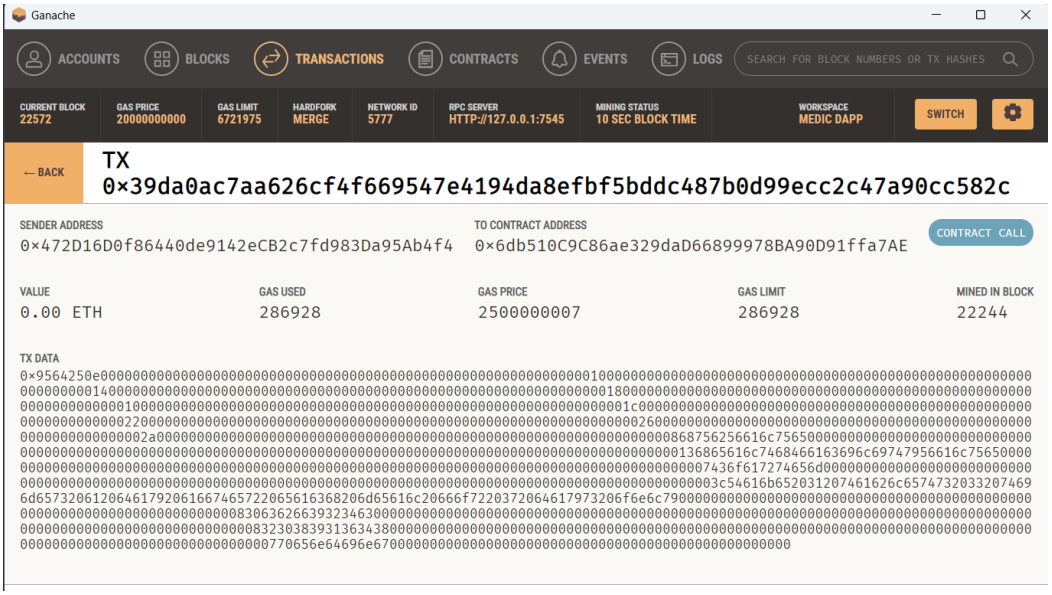
Code snippets

Initiating connection to smart contract using Web3

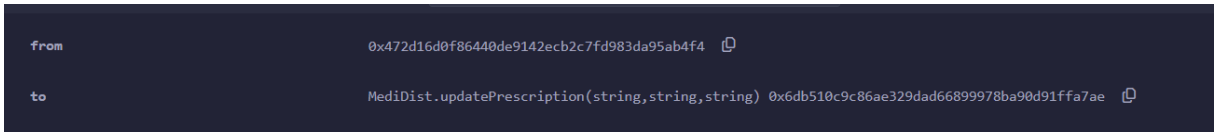
```
var medicineContract;
    document.addEventListener('DOMContentLoaded', async () => {
    const web3 = new Web3(window.ethereum);
    var address = "0x6db510C9C86ae329daD66899978BA90D91ffa7AE";
    var abi =[
{…
},
{…
},
{…
```

Address (“var address”) above is passed through MetaMask to the blockchain, the log below shows the transaction with the blockchain (address under “to” is equal to “var address above”) enabling the interaction with the blockchain via the solidity smart contracts.

Ganache Block and transaction Hash values



Values in Remix IDE Logs



Handling of Prescriptions

This flowchart below illustrates the process of handling prescriptions, a Doctor/Clinical officer prescribes medicine to a patient, an email is sent to the patient with 2 tokens (passphrase to check availability and OTP to get medication once availability is confirmed) No personal information is stored in the prescription and none is required to be provided when a patient is getting their prescribed medication, furthermore because the prescription is stored on the blockchain the patient can use their prescription at any public health facility if the one they got the prescription from has a medicine shortage. The fill rate of each health facility is automatically calculated based on the percentage of medicine that's available in comparison to all the prescriptions generated at that given health facility.

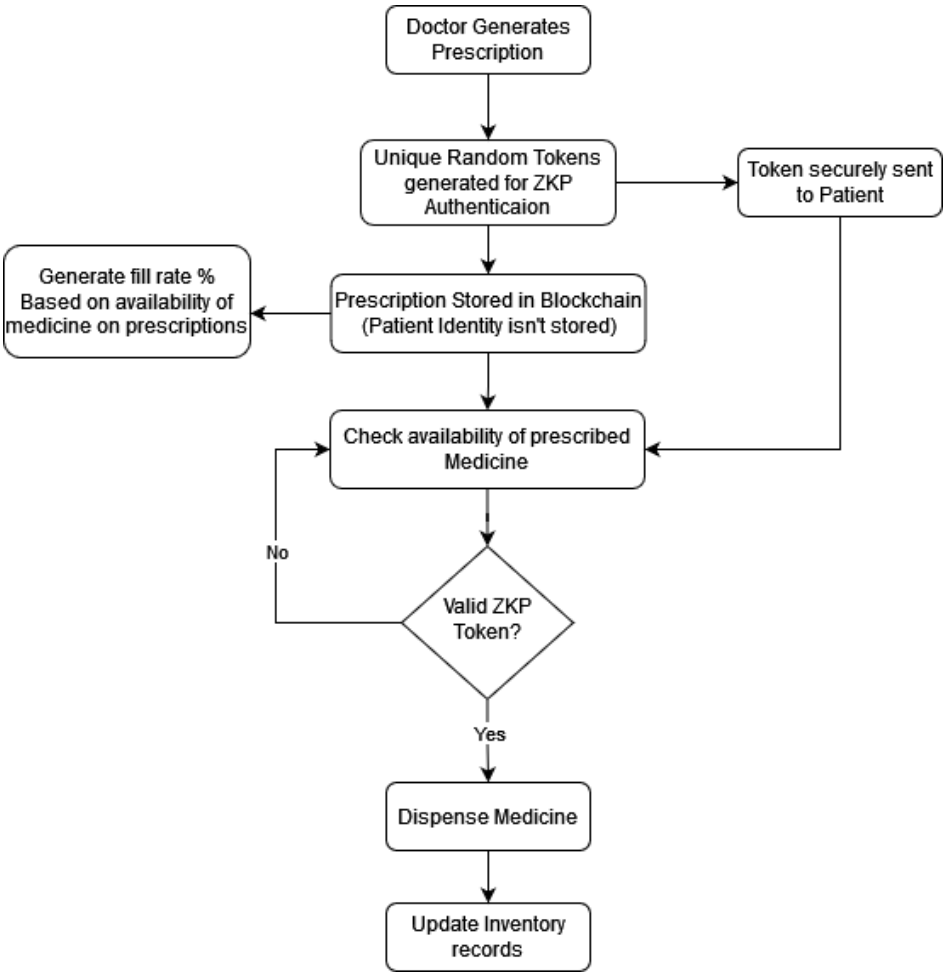


Figure 4.2 - Prescription flowchart

Code snippets

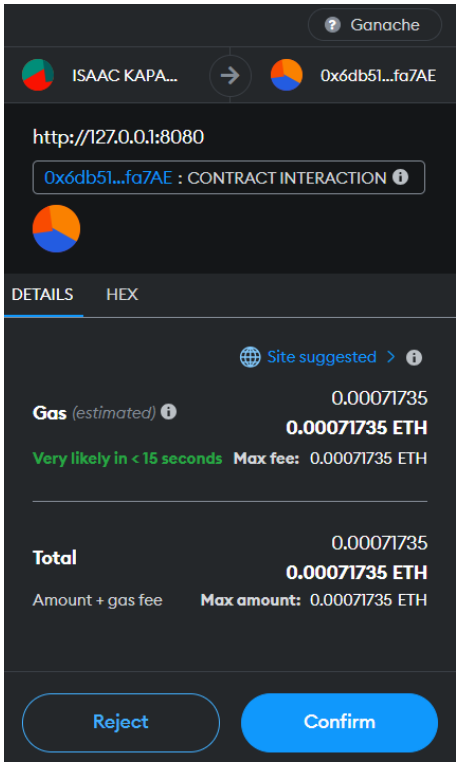
Smart contract to create prescription

```
    struct prescription {

    uint id;
    string hub;
    string healthFacility;
    string medicineName;
    int doses;
    string DrNotes;
    string passphrase;
    string otpCode;
    string status;
}

//Array of prescription struct
prescription[] public prescriptions;

//increment id for each prescription
uint public nextPrescriptionId = 1;

function createPrescription(string memory hub, string memory healthFacility, string memory medicineName, int doses, string memory DrNotes,
    prescriptions.push(prescription(nextPrescriptionId, hub, healthFacility, medicineName,doses,DrNotes,passphrase,otpCode,status));
    nextPrescriptionId++;
}
```

MetaMask account selection (“[0]” for current account)

```
let account = (await web3.eth.getAccounts())[0];

// Call the createPrescription function
contractInstance.methods.createPrescription(
    hub,
    healthFacility,
    medicineName,
    doses,
    DrNotes,
    passphrase,
    otpCode,
    status
).send({ from: account })
.on('receipt', function(receipt){
    // Prescription created successfully
    alert('Transaction successful!');
```

MetaMask transaction confirmation



Token Generation

The generation of the 2 tokens takes place once confirmation is made in MetaMask, the patient's phone number, their email address and the current time are used as a seed for the creation of 2 unique tokens, the first one is a passphrase used to check medicine availability and the second one is an OTP used to initiate medicine collection once availability is confirmed, they can't be revered engineered to obtain their patient information.

```
// Generate a unique passphrase
let seed = medicineName + doses + new Date().getTime() + phone;
//let passphrase = web3.utils.sha3(seed).substring(0, 7);
let passphrase = web3.utils.keccak256(seed).substring(2, 10);
let otpCode = String(Math.floor(10000000 + web3.utils.keccak256(seed + Math.random()) % 90000000));
```

Output

Generated Tokens and a blockchain record of the prescription is created.

```
0cbf924c                                    prescribe-medicine:1183
20891648                                    prescribe-medicine:1184
```

Check availability of medicine (Solidity Smart contract)

```
//Read an instance of a prescription using the passphrase
function readPrescription(string memory passphrase) view public returns(uint, string memory, string memory, string memory, int, string mem
uint i = findPrescription(passphrase);
return (
    prescriptions[i].id,
    prescriptions[i].hub,
    prescriptions[i].healthFacility,
    prescriptions[i].medicineName,
    prescriptions[i].doses,
    prescriptions[i].DrNotes,
    prescriptions[i].passphrase,
    prescriptions[i].otpCode,
    prescriptions[i].status
    );
}
```

JavaScript interaction with smart contract

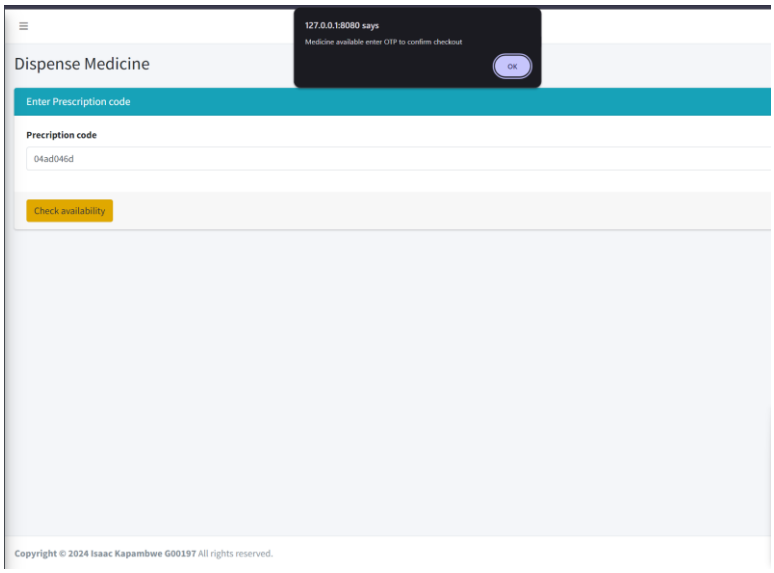
```
const contractAddress = '0x6db510C9C86ae329daD66899978BA90D91ffa7AE';
// Create a new contract instance
const contract = new web3.eth.Contract(abi, contractAddress);

document.getElementById('btnCheckAvailability').addEventListener('click', async () => {
// Get the user's account
const accounts = await ethereum.request({ method: 'eth_requestAccounts' });
const account = accounts[0];

// Get the prescription code from the form
const prescriptionCode = document.getElementById('txtPassphrase').value;

try {
    // Call the readPrescription function
    const result = await contract.methods.readPrescription(prescriptionCode).call({ from: account });

    if (result) {
        const pOtpCode = result[7];
        if(pOtpCode.length > 8){
            alert('Invalid or expired Prescription code');
            return;
        } else {
        const pDoses = result[4];
        const pMedName = result[3];
        const pHubName = result[1];
        const pDocNotes = result[5];
        console.log(result);
        console.log(pDoses);
        console.log(pMedName);
        console.log(pHubName);

            ////////////          Reading medicine from same hub         //////////
            const resultReadMedicine = await contract.methods.readMedicine(pMedName).call({ from: account });
            if (resultReadMedicine) {
                        const readMedId = resultReadMedicine[0];
                        const readMedDoses = resultReadMedicine[6];
                        console.log(readMedDoses);
                        console.log(readMedId);

                        //checking if doses are available
                        if(readMedDoses > pDoses){
                            //Updating dose value
                            updateMedDoses = readMedDoses - pDoses;
                            console.log(updateMedDoses);
                            //Displaying the checkout form
                            var form = document.getElementById('frmCheck');
```

```
var form = document.getElementById('frmCheck');
form.classList.remove('d-none');
alert('Medicine available enter OTP to confirm checkout');

//grey out button after successful check
document.getElementById('btnCheckAvailability').classList.add('disabled');
document.getElementById('btnCheckAvailability').disabled = true;

//Processing checkout with OTP code
//getting otp code when button is clicked

document.getElementById('btnMedCheckout').addEventListener('click', async () => {
    //getting otp from form
    const formOTPCodeCheckout = document.getElementById('numOTP').value;

    // Call the readPrescription function
    const resultPrescptionOTPCheck = await contract.methods.readPrescription(prescriptionCode).call({ from: account });
    // If a record is found
    if (resultPrescptionOTPCheck) {
        //array [id, hub, healthFacility, medicineName, doses, DrNotes, passphrase, otpCode, status]
        const OTPCheckChecout = result[7];
        if(OTPCheckChecout != formOTPCodeCheckout){
            alert('Invalid or Expired OTP');
            location.reload();
            return;
        } else {


         ////////////// UPDATING DOSES IN THE FACILITY //////////////

    web3.eth.requestAccounts()
    .then((accounts) => {
        const senderAddress = accounts[0];

        // Calling the Solidity function to update medicine doses
        return contract.methods.updateMedicineDoses(readMedId, updateMedDoses)
        .send({ from: senderAddress });
    })
    .then((receipt) => {
        // Transaction was successful, display alert
        alert('Inventory update complete! Transaction hash: ' + receipt.transactionHash);
    })
    .catch((error) => {
        // Transaction failed, display error alert
        alert('Update failed. Error: ' + error.message);
        location.reload();
        return;
```

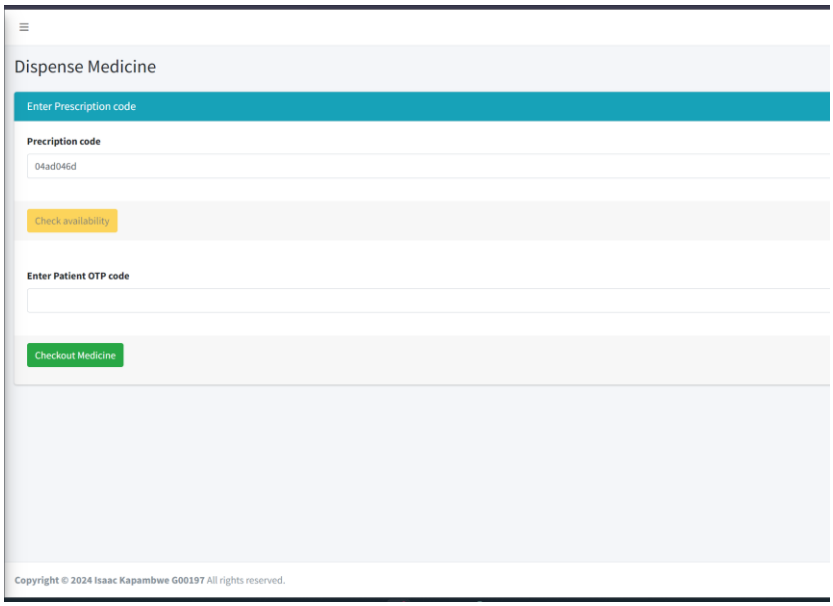
```
        // Transaction failed, display error alert
        alert('Update failed. Error: ' + error.message);
        location.reload();
        return;
    });

    ////////////// UPDATING PRESCRIPTION //////////////
    web3.eth.requestAccounts()
    .then((accounts) => {
        const senderAddress = accounts[0];

        // Calling the Solidity function to update prescription status
        return contract.methods.updatePrescription(prescriptionCode, 'OTP_EXPIRED_PRESCRIPTION_CLOSED','PrescriptionCompletedAndClosed')
        .send({ from: senderAddress });
    })
    .then((receipt) => {
        // prescription Transaction was successful, display alert
        alert('Prescription has been updated! Transaction hash: ' + receipt.transactionHash);
    //Displaying Doctors Notes
    var viewDocsNotes = document.getElementById('showDocNotes');
    //viewDocsNotes.classList.remove('d-none');
    const displayDocNotes = '<br><b>Prescription:</b><br><ul><li><b>Medicine Name:</b> '+pMedName+' </li><li><b>Doses:</b> '+ pDoses + '</li><li><b>Doctors Notes:</b> '+pDocNotes+' <
    viewDocsNotes.innerHTML = displayDocNotes;

        //Disable OTP button
        document.getElementById('btnMedCheckout').classList.add('disabled');
        document.getElementById('btnMedCheckout').disabled = true;
    })
    .catch((error) => {
        // prescription Transaction failed, display error alert
        alert('Update failed. Error: ' + error.message);
        location.reload();
        return;
    });

     }
    }else{

    //////////////////////////

    }
```

Output (Valid Passphrase to check for availability)

The OTP section only appears once the availability is confirmed (and after the user clicks the alert shown below)

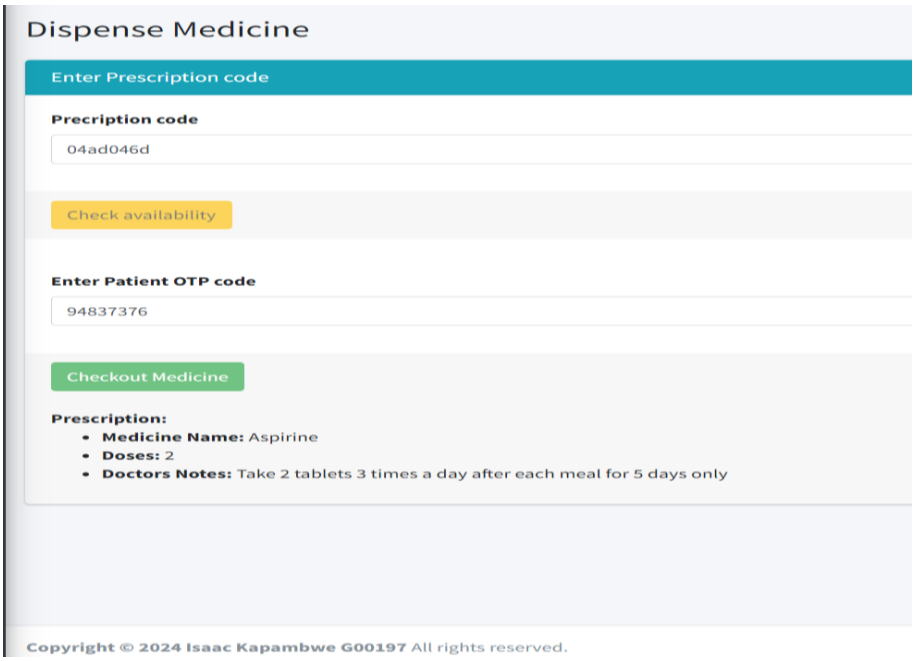


OTP Form Appears and button to check availability is disabled (greyed out)



OTP Processing to confirm checkout.

Once the OTP is entered in the form (the one that appeared after confirmation of availability) the prescription will appear with the Doctors instructions on how to take the medication (no patient information is revealed). The button to check OTP gets disabled (greyed out). The blockchain ledger is also updated to close the prescription (can't be reused) and keep a record of the transaction.



Inventory update

Hub inventory (doses) are updated

Copy CSV Excel PDF Print Column visibility Search:

Name	Doses
Aspirine	398
Panado	999
Coartem	257
Name	**Doses**

Showing 1 to 1 of 1 entries Previous 1 Next

Medicine requisition, approval and supply.

This flowchart demonstrates how medicine requisitions are made, verified and approved in a decentralised manner without requiring a central authority yet being trustworthy due to the use of smart contracts.

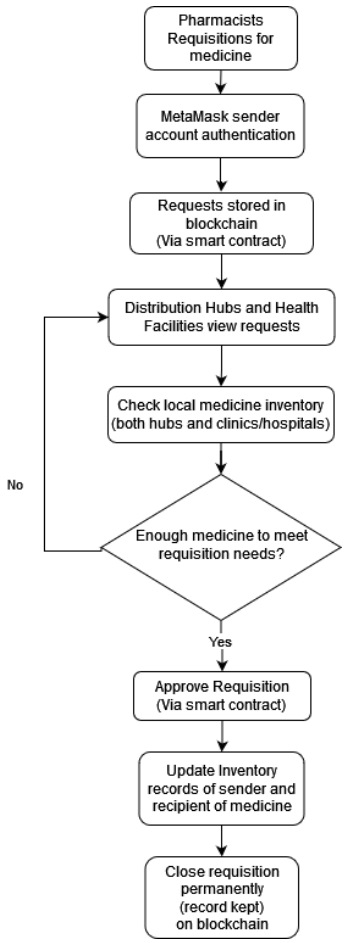


Figure 4.3 - Medicine supply flowchart

Code Snippets

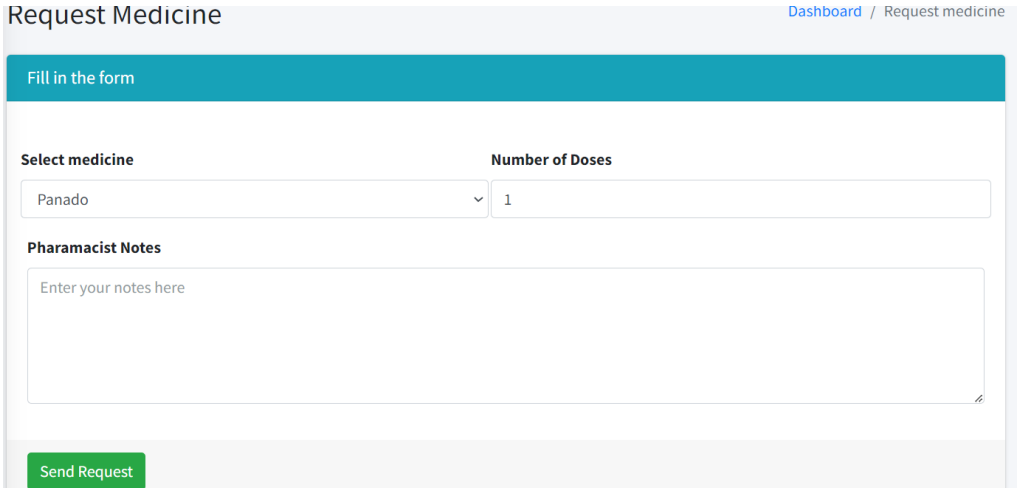
Solidity smart contract to create a request (requisition for medicine)

```
Request[] public requests;

function createRequest(string memory _pharmacist, string memory _medicine, uint _doses, string memory _notes, string memory _hub) public {
    Request memory newRequest = Request({
        pharmacist: _pharmacist,
        medicine: _medicine,
        doses: _doses,
        notes: _notes,
        hub: _hub,
        status: RequestStatus.PendingDelivery,
        deliveryHub: ""
    });
```

UI Form

```
<form id="frmRequest">
  <div class="card-body">

    <div class="form-group">
      <!--  <button type="button" name="btnAddMedicine" id="btnAddMedicine" class="btn btn-warning">Add another drug</button> -->
        <div class="row">
        <table id="enterMedicines" class="col-md-12">
            <tr>
                <td>
                    <br>
                    <label for="selPrescriptionMedicine1">Select medicine</label>
                    <select class="form-control" id="selPrescriptionMedicine1" style="width: 100%;">
                        <option value="panado" selected>Panado</option>
                        <option value="Coartem">Coartem</option>
                    </select>
                </td>
                <td>
                    <br>
                    <label for="numDose1">Number of Doses</label>
                    <input type="number" name="numDose1" class="form-control" id="numDose1" min="1" max="9999" value="1" required>
                </td>
            </tr>
        </table>
        </div>
    </div>

      <div class="form-group">
        <label for="notes">Pharamacist Notes</label>
        <textarea rows="5" name="notes" class="form-control" id="notes" placeholder="Enter your notes here" required></textarea>
      </div>
  </div>

  <div class="card-footer">
          <button type="submit" id="btnRequest" name="btnRequest" class="btn btn-success">Send Request</button></div>
</form>
```

Form output



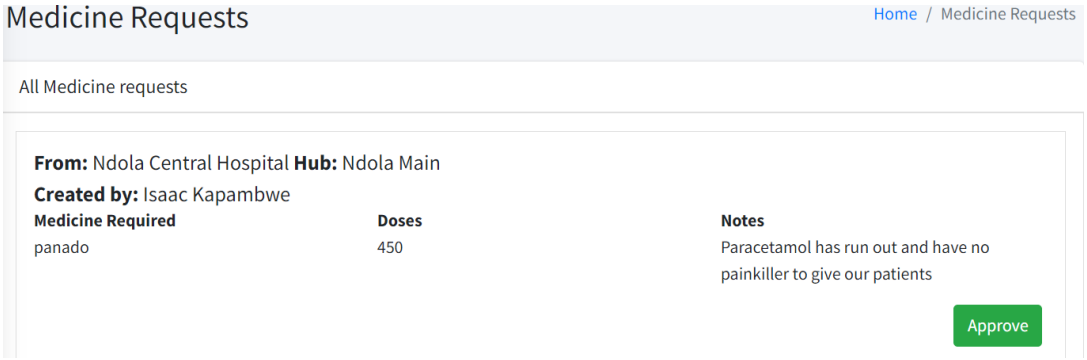
Processing form

The “createRequest” solidity contract method (shown above) is called, authentication is carried out using MetaMask and the values from the form are passed into the solidity smart contract which in turn updates the blockchain.

```
// Call the createRequest function from the smart contract
async function createRequest(pharmacist, medicine, doses, notes, hub) {
    const account = await connectAccount();
    contract.methods.createRequest(pharmacist, medicine, doses, notes, hub).send({ from: account })
        .on('receipt', function(receipt){
            console.log(receipt);
        })
        .on('error', function(error, receipt) {
            console.log(error);
        });
}
```

Output

Approve button updates the blockchain ledger via a smart contract to update the inventory of the 2 participating peers



CHAPTER 5

RESULTS AND DISCUSSIONS

This chapter covers the results of various evaluation methods and a discussion of relevant evaluation metrics.

5.1 Results Presentation

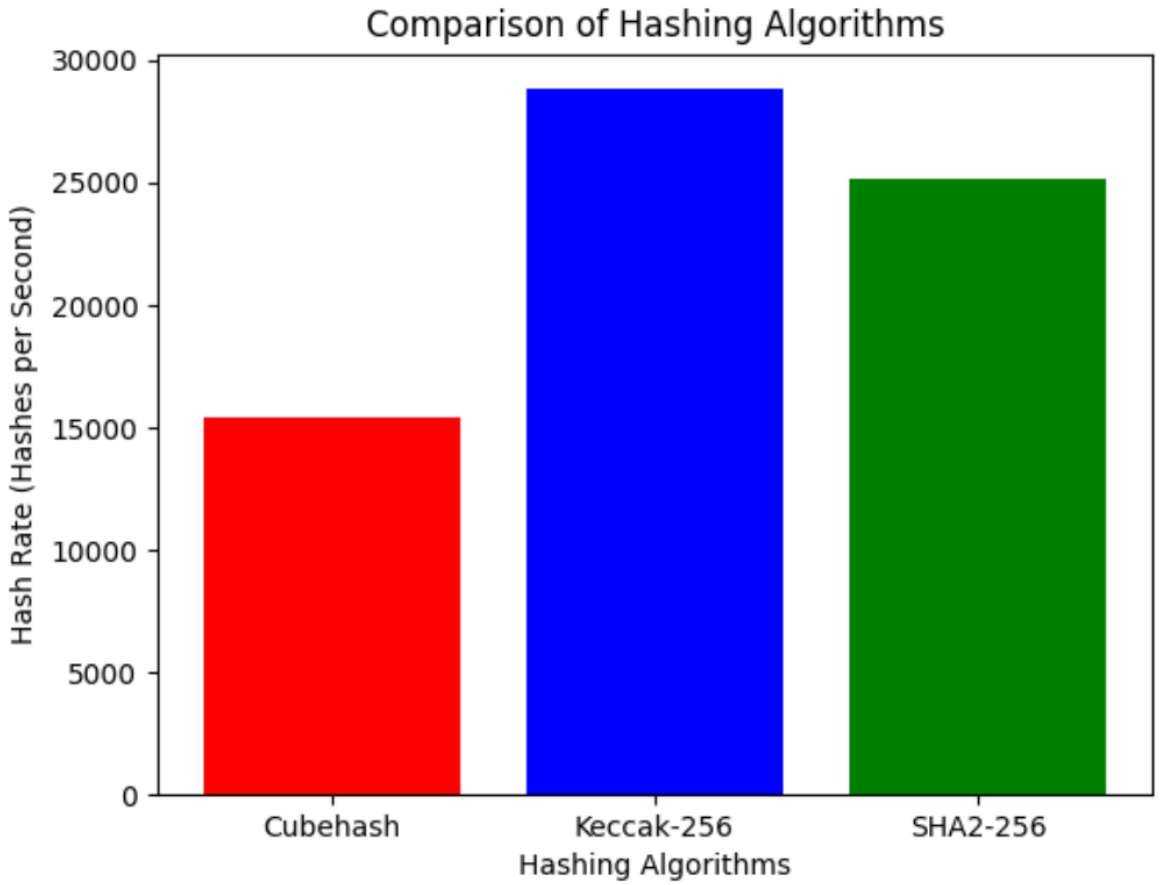
Comparison of number of generated hash codes per second (KHash/s) between Keccak-256, Cube hash and SHA2-256.

Khash/s

Cube hash: 15435

Keccak-256: 28829

SHA2-256: 25198



5.2 Analysis of Results

Keccak-256: Hash Rate: 28,829 KHash/s

Keccak-256 is the fastest among the three hashing algorithms, generating the highest number of hash codes per second. This is a notable strength, especially in scenarios where high performance and speed are crucial such as blockchain transaction processing.

CubeHash: Hash Rate: 15,435 KHash/s

CubeHash has a lower hash rate compared to Keccak-256 but is still a presented a relatively fast hash rate. It can be used reliably for security requirements but will be perform worser than Keccak-256 in time sensitive applications.

SHA-256: Hash Rate: 25,198 KHash/s

SHA-256, while not as fast as Keccak-256 in this comparison, is still a widely used and secure hashing algorithm. Its balance between speed and security makes it a popular choice for various cryptographic applications such as Bitcoin.

5.4 Implications of Results

Keccak-256 stands out for its high hash rate, making it the fastest among the three and the most suitable for time sensitive tasks such as managing a blockchain network. SHA-256, despite being slightly slower than Keccak-256, is a well-established and widely adopted hashing algorithm known for its security. CubeHash, while not as fast as Keccak-256 or SHA-256 in this comparison, may still be suitable depending on specific requirements.

CHAPTER 6

SUMMARY AND CONCLUSION

This chapter presents the summary and conclusion of the research project, which aimed to develop a blockchain and zero knowledge proof model for decentralised drug distribution and stock transfer in public health care facilities in Zambia. The chapter also discusses the main findings, contributions, limitations, and future works of the project.

6.1 Summary of Main Findings

This section summarises the main findings of the project, which include:

The identification of the primary challenges and limitations of the current drug distribution model in public health care facilities in Zambia, such as inefficiency, delays, fraud, theft, and lack of transparency and accountability.

The development of a decentralised blockchain and zero knowledge proof model for drug distribution and stock transfer, which leverages the features of blockchain technology, such as security, transparency, immutability, and smart contracts, and the features of zero knowledge proofs, such as privacy, confidentiality, and verification, to improve the efficiency, security, privacy, and transparency of the drug distribution and stock transfer processes.

The development of a scalable decentralised proof of concept application using Ethereum blockchain and zero knowledge proofs technologies for drug distribution and stock transfer in public health care facilities in Zambia, which demonstrates the feasibility and functionality of the proposed model.

The evaluation of the model using relevant performance metrics for blockchain, zero knowledge proof, distribution, and stock transfer, such as scalability, reliability, security, privacy, efficiency, and cost-effectiveness, which show the advantages and benefits of the proposed model over the current model.

6.2 Contribution to the body of knowledge

The development of a novel and innovative model that integrates blockchain and zero knowledge proofs technologies for decentralised drug distribution and stock transfer in public health care facilities, which addresses the challenges and limitations of the current model and provides a solution that is more efficient, secure, private, and transparent.

The application of the model to the Zambian health sector, which is a context that has not been explored before in the literature and has a high potential for impact and social good, as it can improve the access and availability of essential drugs to patients who need them the most, reduce the wastage and losses of drugs due to expiry, fraud, and theft, and increase the donor confidence and funding for drug procurement.

The advancement of the theoretical and conceptual framework that supports the proposed model, which draws from various disciplines, such as computer science, cryptography and supply chain management and applies various theories, such as distributed systems theory, game theory, and complex systems theory, to analyse and explain the design, performance, and properties of the proposed model.

6.3 Limitations of the system

The main limitation of the system is lack of biometric functionality to generate Zero Knowledge proofs, the PoC utilises phone number and email address which still enable the model to operate as intended but not to the highest level of security. Due to the sensitivity of the data in medicine distribution, datasets where limited (often not relevant to the research), therefore there is a reliance on processed secondary.

Lack of tools for evaluating and testing Zero Knowledge Proofs due to it's limited adoption.

6.4 Future works

Exploring the development of Decentralised Applications in Pharmacy Management Systems, Logistics Management Systems for a fully integrated decentralised supply chain.

Investigating other blockchain platforms and consensus mechanisms that may offer better performance, scalability, and security for the proposed model, such as Hyperledger Fabric, Corda, or Algorand.

Incorporating other features and functionalities that may enhance the proposed model, such as biometrics for zero knowledge proofs, digital drug serialisation, machine learning, and artificial intelligence, to enable more accurate and efficient drug tracking, verification, and distribution.

REFERENCES

Al-Aswad, H., El-Medany, W. M., Balakrishna, C., Ababneh, N., & Curran, K. (2021). BZKP: Blockchain-based zero-knowledge proof model for enhancing healthcare security in Bahrain IoT smart cities and COVID-19 risk mitigation. *Arab Journal of Basic and Applied Sciences*, *28*(1), 154–171. https://doi.org/10.1080/25765299.2020.1870812

Baboli, A., Fondrevelle, J., Tavakkoli-Moghaddam, R., & Mehrabi, A. (2011). A replenishment policy based on joint optimization in a downstream pharmaceutical supply chain: Centralized vs. decentralized replenishment. *The International Journal of Advanced Manufacturing Technology*, *57*(1), 367–378. https://doi.org/10.1007/s00170-011-3290-x

Bvuchete, M., Grobbelaar, S. S., & Van, E. J. (2020). Best practices for demand-driven supply chain management in public healthcare sector: A systematic literature review. *South African Journal of Industrial Engineering*, *31*(2), 11–27. https://doi.org/10.7166/31-2-2006

Chileshe, M. (2021). *Widespread Fraud in Emerging Economies Public Sector: Evidence from the Republic of Zambia - ProQuest* [Nothcentral University]. https://www.proquest.com/openview/d867e78938042e4edea3ba4a4bcc677f/1?pq-origsite=gscholar&cbl=18750&diss=y

Dawkins, C. E., & Barker, J. R. (2020). A Complexity Theory Framework of Issue Movement. *Business & Society*, *59*(6), 1110–1150. https://doi.org/10.1177/0007650318762404

De Giovanni, P. (2020). Blockchain and smart contracts in supply chain management: A game theoretic model. *International Journal of Production Economics*, *228*, 107855. https://doi.org/10.1016/j.ijpe.2020.107855

Dick-Sagoe, C., Asare-Nuamah, P., & Dick-Sagoe, A. D. (2021). Public choice and decentralised healthcare service delivery in Lesotho: Assessing improvement and efficiency in service delivery. *Cogent Social Sciences*, *7*(1), 1969737. https://doi.org/10.1080/23311886.2021.1969737

Dos Santos, R. P. (2017). On the Philosophy of Bitcoin/Blockchain Technology: Is it a Chaotic, Complex System? *Metaphilosophy*, *48*(5), 620–633. https://doi.org/10.1111/meta.12266

Gaba, G. S., Hedabou, M., Kumar, P., Braeken, A., Liyanage, M., & Alazab, M. (2022). Zero knowledge proofs based authenticated key agreement protocol for sustainable

healthcare. *Sustainable Cities and Society*, *80*, 103766. https://doi.org/10.1016/j.scs.2022.103766

Gallien, J., Leung, N.-H. Z., & Yadav, P. (2021). Inventory Policies for Pharmaceutical Distribution in Zambia: Improving Availability and Access Equity. *Production and Operations Management*, *30*(12), 4501–4521. https://doi.org/10.1111/poms.13541

Ghosh, R. K., & Ghosh, H. (2023). *Distributed Systems: Theory and Applications*. John Wiley & Sons.

Hamilton, M. (2020). Blockchain distributed ledger technology: An introduction and focus on smart contracts. *Journal of Corporate Accounting & Finance*, *31*(2), 7–12. https://doi.org/10.1002/jcaf.22421

HEART. (2016). *Comparative advantages and disadvantages of "push" and "pull" mechanisms in pharmaceutical management*. https://assets.publishing.service.gov.uk/media/58b544e1e5274a2a5c000084/pharmaceutical-management-Push-and-Pull-Systems-HEART-Helpdesk-.pdf

IDC. (2017). *Medical Stores Limited – Industrial Development Corporation (IDC) Zambia Limited*. https://www.idc.co.zm/industry-sectors/tourism-2/medical-stores-limited/

Iqbal, M., Ishaq, G., & Dar, P. (2017). Medicines Management in Hospitals: A Supply Chain Perspective. *Systematic Reviews in Pharmacy*, *8*, 80–85. https://doi.org/10.5530/srp.2017.1.14

Kaiser, A. H., Hehman, L., Forsberg, B. C., Simangolwa, W. M., & Sundewall, J. (2019). Availability, prices and affordability of essential medicines for treatment of diabetes and hypertension in private pharmacies in Zambia. *PLOS ONE*, *14*(12), e0226169. https://doi.org/10.1371/journal.pone.0226169

Khan, S. N., Loukil, F., Ghedira-Guegan, C., Benkhelifa, E., & Bani-Hani, A. (2021). Blockchain smart contracts: Applications, challenges, and future trends. *Peer-to-Peer Networking and Applications*, *14*(5), 2901–2925. https://doi.org/10.1007/s12083-021-01127-0

Khatoon, A. (2020). A Blockchain-Based Smart Contract System for Healthcare Management. *Electronics*, *9*(1), Article 1. https://doi.org/10.3390/electronics9010094

Kim, D. (2005). An Integrated Supply Chain Management System: A Case Study in Healthcare Sector. In K. Bauknecht, B. Pröll, & H. Werthner (Eds.), *E-Commerce and Web Technologies* (pp. 218–227). Springer. https://doi.org/10.1007/11545163_22

Ko, Y. J., Kim, Y. K., Kim, T., Arai, A., Rhee, Y. C., & Park, C. (2020). The impact of perceived trustworthiness on trust and commitment: A case of boosters in a university

athletic programme. *Sport in Society*, *23*(2), 180–203. https://doi.org/10.1080/17430437.2019.1680640

Kumar, G. (2023). Securing pharmaceutical supply chain using digital drug serialization. *World Journal of Advanced Engineering Technology and Sciences*, *10*, 015–020. https://doi.org/10.30574/wjaets.2023.10.1.0244

Maciejewski, M. L. (2020). Quasi-experimental design. *Biostatistics & Epidemiology*, *4*(1), 38–47. https://doi.org/10.1080/24709360.2018.1477468

Mackey, T. K., & Cuomo, R. E. (2020). An interdisciplinary review of digital technologies to facilitate anti-corruption, transparency and accountability in medicines procurement. *Global Health Action*, *13*(sup1), 1695241. https://doi.org/10.1080/16549716.2019.1695241

Mackey, T. K., & Liang, B. A. (2012). Combating healthcare corruption and fraud with improved global health governance. *BMC International Health and Human Rights*, *12*(1), 23. https://doi.org/10.1186/1472-698X-12-23

Ministry of Finance and National Planning. (2022). *Eighth National Development Plan (8NDP)*. Ministry of Finance and National Planning. https://www.fao.org/faolex/results/details/en/c/LEX-FAOC210616

Peltoniemi, T. (2021). *The digitalization of medicine supply chain: How to re-aim the shots in the dark?*

Priyan, S., & Uthayakumar, R. (2014). Optimal inventory management strategies for pharmaceutical company and hospital supply chain in a fuzzy–stochastic environment. *Operations Research for Health Care*, *3*(4), 177–190. https://doi.org/10.1016/j.orhc.2014.08.001

Rawat, R. (2022). A SYSTEMATIC REVIEW OF BLOCKCHAIN TECHNOLOGY USE IN E-SUPPLY CHAIN IN INTERNET OF MEDICAL THINGS (IOMT). *International Journal of Computations, Information and Manufacturing (IJCIM)*, *2*(2), Article 2. https://doi.org/10.54489/ijcim.v2i2.119

Seyed-Nezhad, M., Ahmadi, B., & Akbari-Sari, A. (2021). Factors affecting the successful implementation of the referral system: A scoping review. *Journal of Family Medicine and Primary Care*, *10*(12), 4364–4375. https://doi.org/10.4103/jfmpc.jfmpc_514_21

Sharma, A., Sarishma, Tomar, R., Chilamkurti, N., & Kim, B.-G. (2020). Blockchain Based Smart Contracts for Internet of Medical Things in e-Healthcare. *Electronics*, *9*(10), Article 10. https://doi.org/10.3390/electronics9101609

Shukar, S., Zahoor, F., Hayat, K., Saeed, A., Gillani, A. H., Omer, S., Hu, S., Babar, Z.-U.-D., Fang, Y., & Yang, C. (2021). Drug Shortage: Causes, Impact, and Mitigation Strategies. *Frontiers in Pharmacology*, *12*. https://www.frontiersin.org/articles/10.3389/fphar.2021.693426

Siyal, A. A., Junejo, A. Z., Zawish, M., Ahmed, K., Khalil, A., & Soursou, G. (2019). Applications of Blockchain Technology in Medicine and Healthcare: Challenges and Future Perspectives. *Cryptography*, *3*(1), Article 1. https://doi.org/10.3390/cryptography3010003

Stecca, G., Baffo, I., & Kaihara, T. (2016). Design and operation of strategic inventory control system for drug delivery in healthcare industry. *IFAC-PapersOnLine*, *49*(12), 904–909. https://doi.org/10.1016/j.ifacol.2016.07.890

Sun, X., Yu, F. R., Zhang, P., Sun, Z., Xie, W., & Peng, X. (2021). A Survey on Zero-Knowledge Proof in Blockchain. *IEEE Network*, *35*(4), 198–205. https://doi.org/10.1109/MNET.011.2000473

Tembo Mwanaumo, E., Kabwe, D., Mutono Mwanza, B. G., & Mishengu Mwanaumo, E. (2023, April 4). Assessing the Last Mile delivery logistics of the Zambia Medicines and Medical Supplies Agency. *Proceedings of the International Conference on Industrial Engineering and Operations Management*. 4th African International Conference on Industrial Engineering and Operations Management, Lusaka, Zambia. https://doi.org/10.46254/AF04.20230151

Tezel, A., Febrero, P., Papadonikolaki, E., & Yitmen, I. (2021). Insights into Blockchain Implementation in Construction: Models for Supply Chain Management. *Journal of Management in Engineering*, *37*(4), 04021038. https://doi.org/10.1061/(ASCE)ME.1943-5479.0000939

Toscano, F., O'Donnell, E., Unruh, M., Golinelli, D., Carullo, G., Messina, G., & Casalino, L. (2018). Electronic health records implementation: Can the European Union learn from the United States? *European Journal of Public Health*, *28*(suppl_4), cky213.401. https://doi.org/10.1093/eurpub/cky213.401

UNICEF - Malaria. (2023, February). UNICEF DATA. https://data.unicef.org/topic/child-health/malaria/

USAID. (2021, December). *Zambia Connects All Provincial Hubs to Improve Data Visibility | USAID Global Health Supply Chain ProgramZambia Connects All Provincial Hubs to Improve Data Visibility*. USAID Global Supply Chain Program.

https://www.ghsupplychain.org/news/zambia-connects-all-provincial-hubs-improve-data-visibility

Uthayakumar, R., & Priyan, S. (2013). Pharmaceutical supply chain and inventory management strategies: Optimization for a pharmaceutical company and a hospital. *Operations Research for Health Care*, *2*(3), 52–64. https://doi.org/10.1016/j.orhc.2013.08.001

Vledder, M., Friedman, J., Sjöblom, M., Brown, T., & Yadav, P. (2015). *Optimal Supply Chain Structure for Distributing Essential Drugs in Low Income Countries: Results from a Randomized Experiment* (SSRN Scholarly Paper 2585671). https://doi.org/10.2139/ssrn.2585671

Walter, T. F. (2018). *The Spatial Distribution of Health Services in Zambia*.

WHO. (2014, November). *MEDICINES IN HEALTH CARE DELIVERY*. https://cdn.who.int/media/docs/default-source/searo/hsd/edm/csa-myanmar-2014.pdf?sfvrsn=4a2967da_2

World Health Organisation. (2023). *World health statistics 2023: Monitoring health for the SDGs, sustainable development goals*. https://www.who.int/publications-detail-redirect/9789240074323

Zambia Statistics Agency. (2022). *2022 CENSUS OF POPULATION AND HOUSING*. https://www.zamstats.gov.zm/wp-content/uploads/2023/05/2022-Census-of-Population-and-Housing-Preliminary.pdf

Zhang, C., Wu, C., & Wang, X. (2020). Overview of Blockchain Consensus Mechanism. *Proceedings of the 2020 2nd International Conference on Big Data Engineering*, 7–12. https://doi.org/10.1145/3404512.3404522