2018

A Mobile application to improve tracking and verification of products in supply chain logistics using blockchain technology

Julius Gikonyo Kiano
Faculty of Information Technology (FIT)
Strathmore University

A MOBILE APPLICATION TO IMPROVE TRACKING AND VERIFICATION OF PRODUCTS IN SUPPLY CHAIN LOGISTICS USING BLOCKCHAIN TECHNOLOGY

Julius Gikonyo Kiano

Submitted in partial fulfillment of the requirements of the Degree of Masters of Science in Mobile Telecommunication and Innovation

Faculty of Information Technology
Strathmore University
April, 2018

Declaration

I declare that this work has not been previously submitted and approved for the award of a degree by this or any other University. To the best of my knowledge and belief, the thesis contains no material previously published or written by another person except where due reference is made in the thesis itself.

Julius Gikonyo Kiano
091776

Signature: _____

Date: _____

APPROVAL

The dissertation of Julius Gikonyo Kiano was reviewed and approved by:

Dr. Humphrey Njogu
Faculty of Information Technology
Strathmore University

Signature: _____

Date: _____

Acknowledgments

I acknowledge, with gratitude, my debt of thanks to Safaricom Academy and Strathmore University for an opportunity to undertake my master's degree in their program. Special acknowledgements to the OkHi team for allowing me to conduct this research and Dr. Humphrey Njogu for his guidance throughout the research.

Dedication

I dedicate this dissertation to the late Dr. Julius Gikonyo Kiano, one of the most brilliant minds in our country, my family, mentors, friends, my dissertation supervisor Dr. Humphrey Njogu and the entire Strathmore University fraternity for their support throughout the dissertation period.

Abstract

In Kenya, the generation, distribution and utilisation of fake products has been expanding at an alarming rate. In spite of the fact that there has been numerous related researches concentrating on improving supply chain quality management, major issues are still present due to the lack of trust in a supply chain. The main challenges facing traditional supply chain is the self-interest of supply chain members and the limitations of quality inspections. With vast supply chains it becomes next to impossible to trace the movement of goods as they make their way to a retailer. A retailer then does not have a trusted way of verifying authenticity of goods received.

Blockchain is a promising technology that can be leveraged to solve the aforementioned problems by providing a decentralised system of trust. The purpose of this study is to address the shortcomings of a traditional supply chain by leveraging Blockchain technology. This study has developed a solution that is able to provide an effective, efficient and secure way to track and verify products in a supply chain. The mobile application is able to track the distributions of products among the manufacturers, distributors and consumers. Supporting the mobile application is a network of distributed fault-tolerant validator nodes that utilise the Proof of Stake algorithm to maintain and mutate the state of the Blockchain based on incoming transactions.

This study adopted the Agile Software methodology because it offers a quick and flexible way to conduct development sprints and incorporating user feedback. The developed solution recorded high performance results from the usability tests conducted and the network of distributed validator nodes maintained consistent and accurate Blockchain records, facilitating a decentralised method of trust within a supply chain.

Keywords: Blockchain, Supply Chain Management, Proof-of-Work, Proof-of-Stake

Table of Contents

List of Tables

List of Figures

List of Abbreviations/Acronyms

API – Application program interface

BTF – Byzantine fault tolerance

CPU – Central Processing Unit

iOS – iPhone Operating System

IP – Internet Protocol

JSON – JavaScript Object Notation

P2P – Peer-to-Peer

SMS – Short Message Service

Definition of Terms

Bitcoin – A Peer-to-Peer Electronic Cash System (Nakamoto, 2008).

Block – A record of a valid transaction that has occurred in a Blockchain (Crosby & Pattanayak, 2015).

Blockchain – This is a proper linear, chronological ordering of blocks with every block containing the hash of the previous block (Crosby & Pattanayak, 2015).

Byzantine fault – This is an incorrect operation that occurs in a distributed system that can be caused by a node either failing to return a result, returning an incorrect result or returning a deliberately misleading result (Lamport, 1982).

Contracts – Applications that run exactly as programmed without any possibility of downtime, censorship, fraud or third party interference (Wood, 2018)

Ether – A crypto currency used in the Ethereum Blockchain network (Wood, 2018).

Ethereum – A Blockchain with a built-in fully fledged Turing-complete programming language that can be used to create contracts (Wood, 2018).

Proof-of-Stake – A consensus mechanism for digital currencies which consists of the absence of expensive computations and hence a lower entry barrier for block generation rewards (BitFury Group, 2015).

Proof-of-Work – A consensus mechanism for digital currencies where each node is required to solve a computationally difficult problem to ensure the validity of a new Block in the Blockchain (BitFury Group, 2015).

RESTful API - An application program interface that uses HTTP requests to GET, PUT, POST and DELETE data (Rouse, 2016).

CHAPTER 1: INTRODUCTION

1.1 Background

The spread of counterfeit products has become a global menace in recent years. Similarly, the range of goods subject to counterfeiting has also increased significantly. The main instances of brand and product counterfeiting developed around five decades back (Ergın, 2010). In the past, a small number of manufacturers of specialised items were affected, hence it was assumed that this phenomenon would be of little significance (Ergın, 2010). Unfortunately, counterfeiting has become a widespread phenomenon that has turned into a massive multifaceted problem of global significance.

Research demonstrates that the rapid growth of this trade and the velocity of its development is energised by various components ranging from restricted supply of authentic items, powerlessness to distinguish origin items, high costs of genuine items, poverty, defilement and numbness of the masses (Staake & Fleisch, 2008). As a result, the continuous emergence of counterfeit products and product quality scandals has revealed the importance of quality management from a supply chain perspective. Although there have been many related research projects and studies to resolve the series of problems in supply chain logistics, the absence of trust is as yet a troublesome issue for the solutions utilised these days.

Lack of transparency is one of the most common problems in the traditional supply chain. It is increasingly difficult for consumers and retailers to truly know the worth or authenticity of their products. In a similar way it is extremely difficult to investigate supply chains when there is suspicion of unethical or illegal practices. With vast supply chains it becomes a challenge to maintain, update and reference detailed records as a product moves through a given market. Distributors and retailers also suffer from loss of time and capital when trying to manage the logistics of who needs what, when and how (Marr, 2018).

The emergence of Blockchain technology has brought innovative possibilities to Supply Chain Quality Management. A Blockchain is an incorruptible computerised record of economic exchanges that can be customised to record not simply money related exchanges but rather everything of value (Tapscott & Tapscott, 2016). In a Bitcoin system, Blockchain demonstrates the characteristics such as trust machine, decentralised governance and traceable transactions. It solves the issues of distrust on the basis of unchanged information and traceable records through standardised norms and agreements.

Although Blockchain is typically associated with the use of cryptocurrencies i.e. Bitcoin, in reality the use of a distributed ledger has many applications. It can be used for tracking payments, contracts or agreements. Since a processed transaction is stored in a Block across multiple nodes in a network, it provides a high level of transparency. Since every Block is linked to each other through the use of a cryptographic hash, it is highly secure . There is no central governing authority over it and is extremely efficient and stable (Marr, 2018).

Based on the aforementioned advantages of Blockchain technology, this technology can be used to increase the efficiency and transparency of supply chain logistics and make positive impacts from deliveries, to warehousing, to payments. The very things that are vital for unwavering quality and trustworthiness in a supply chain are provided by Blockchain. Through consensus making there is no dispute in the chain regarding incoming transactions because all nodes have the same version of the ledger. Records on the blockchain cannot be erased which is critical for a transparent supply chain.

1.2 Problem Statement

Traditional supply chain management and particularly logistics is characterised by several challenges that center around issues of trust. Manufacturers lack the transparency of how their products get into the market, and in the case of vast supply chains, suppliers cannot effectively track the arrival of their shipments to various destinations. Consumers to lack an effective way to determine authenticity of purchased goods. This lack of transparency in any supply chain leaves opportunities for the introduction of counterfeit goods in the market, illegal and unethical misconduct by supply chain actors which may negatively affect the economy, as well as introduce health hazards to the population.

1.3 General Objective

Based on aforementioned challenges, this study sought to design an effective and transparent supply chain quality management platform that will leverage on Blockchain technology to improve the tracking and verification of products in a secure and trusted way. The system targets to provide a reliable, trusted and decentralised model that will allow supply chain actors to determine the authenticity of products by effectively tracking them from the manufacturer to the consumer.

1.4 Research Objectives

i. To identify common challenges experienced in supply chain management.
ii. To review existing blockchain based supply chain management systems.
iii. To design, develop and test a mobile application for supply chain management based on Blockchain technology.
iv. To validate the effectiveness of a mobile application for supply chain management by measuring the accuracy and response rates.

1.5 Research Questions

i. What are the common challenges experienced in supply chain management?
ii. What are the existing blockchain based solutions for supply chain management?
iii. How can a mobile based supply chain management application be designed, developed and tested?
iv. Does the solution improve supply chain logistics by providing a transparent and decentralised trust mechanism for supply chains and its actors?

1.6 Justification

When a product changes hands, the transaction could be digitally documented, creating a permanent history of a product, from manufacture to sale. This could dramatically reduce time delays, added costs, and human error that plague transactions today. Moreover, having a shared, indelible ledger with codified rules could potentially reduce the amount of counterfeit goods coming into the country. Wholesalers and distributors will be able to verify their incoming shipment before further distribution, reducing any health public concerns and overall improving the country's economy.

1.7 Scope and Limitations

This study will be focused on using Blockchain technology to manage the product delivery aspects of supply chain logistics, with main actors being manufacturers, distributors, retailers and consumers. The mobile application will run on both Android and iOS platforms so as to have a broad number of users during testing.

CHAPTER 2: LITERATURE REVIEW

2.1 Introduction

This chapter focuses on understanding supply chains, its actors and challenges experienced. It discusses different technologies currently used for supply chain management and dives deep in understanding how Blockchain technology works. It focuses on identifying existing Blockchain based supply chain systems and from it create a model that would improve tracking and verification of products by supply chain stakeholders.

2.2 Supply Chain Management

Supply chain management is a set of approaches used to efficiently distribute products among manufacturers, warehouses, distributors and retailers. It ensures merchandise is delivered to the right destination at an agreed time (Lu, 2011). It can also be defined as the management of flow of products and services, which starts from the origin of products and ends at the product's consumption by an end customer. It also comprises movement and storage of raw materials that are involved in work in progress, inventory and fully furnished goods (Tutorials Point Pvt. Ltd, 2016).

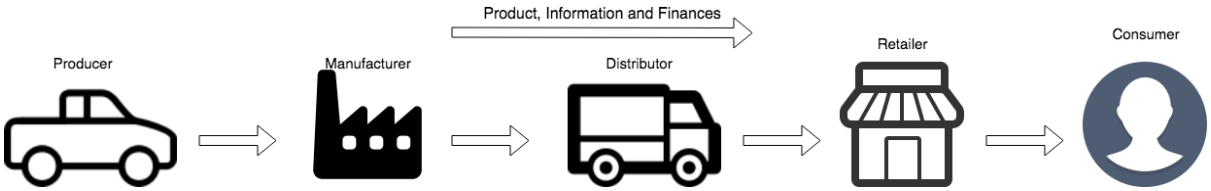

Figure 2.1 Supply Chain Management (Lu, 2011)

Figure 2.1, identifies the flow of products and information from producers to consumers. It illustrates how the product moves from a producer to the manufacturer, who then passes it onwards to a distributor for shipment. The distributor then ships it to a wholesaler or other distributors. Wholesalers then distribute these products to local retailers where customers can easily access these products. As a result of this supply chain management basically manages the supply and demand needs in a market (Lu, 2011).

2.3 Common Challenges in Supply Chain Management

2.3.1 Transparency

For many products, origin is an essential feature of what the customer buys, even if it is an intangible or a difficult-to-verify quality. For some products is it nearly impossible to distinguish one particular brand from alternatives (SCRC SME, 2003). It is equally difficult to determine where products are manufactured or sourced, this facilitates the introduction of illegal or harmful products within a market that can have detrimental health and other hazardous risks to the population (New, 2010).

2.3.2 Traceability

Supply chain intelligence is knowing more than where goods are at any given moment. To find the source of flawed parts or component failures, being able to trace the origin and provenance of previously shipped goods is critical (Marr, 2018). In cases of agricultural products it becomes a difficult task for retailers and wholesalers to pull hazardous products from the shelves as they lack a way of determining where their particular supplier sourced the product. As a result of this companies can suffer major losses in revenue by taking down all products in that particular category due to the lack of confidence they have for it (IBM, 2016).

2.3.3 Trust

The most important factor in a collaboration of supply chain actors is trust. Trust enhances the chances of a successful supply chain relationship. Lack of trust can cause high transaction costs as a result of poor performance (New, 2010). Companies need trust to be agile and flexible. However establishing a system of trust is not only difficult to obtain but even harder to maintain. A manufacturer must be able to trust their providers, distributors must be able to trust their manufacturers, wholesalers and retailers must be able to trust their distributors and finally the end consumer must be able to trust their retailer (SCRC SME, 2003).

2.3.4 Decentralisation and Data Storage

Supply chain actors tend to face both organisations and cultural issues, such as executing operating plans on the basis of corporate goals. Consequently, companies have revoked social contracts, mistreated skilled laborers and underutilised their professional talent assets. Another major disadvantage is that methods of communication tend to vary greatly, with some

companies still relying on manual paperwork. As a result, data storage becomes locked away in in proprietary systems that do not allow for collaboration (Mulay, 2013).

2.4 Application of Different Technologies In Supply Chain Management

2.4.1 Radio Frequency Identification (RFID)

Identified by Robison, 2015, RFID is an essential piece of technology that provides supply chain stakeholders innumerable benefits. They are small chips that are placed of packages and provide a way for individuals to easily track and monitor their inventory. Due to the kind of visibility that RFID provide they substantially improve supply chain efficiencies by immediately detecting problems in real-time, enabling employees to correct them as soon as they are alerted. In addition to this they allow for a much easier and more consistent way for tracking , allowing supply chain stakeholders to have maximum visibility of their products in transit (Robinson, 2015).

2.4.2 Barcodes

A barcode is a machine-readable representation of data. The data is arranged in a series of bars with varying degrees of bar thickness. They have impacted almost every aspect of supply chain logistics. They are used as an identification tool that helps determine products, track them and greatly improve on errors that would otherwise be present with manual physically written identification. They are easy to handle, accurate and affordable. These advantages makes them a widely used tool and accepted globally (McCathie, 2005). Figure 2.2 shows an example of a standard barcode.

Figure 2.2 Barcode example (McCathie, 2005)

2.4.3 Quick Response Codes (QR Codes)

A QR Code is a two-dimensional barcode that can be easily read using a smartphone camera. The information stored can link to websites, emails or contain added text. It was initially designed for the Japan automotive industry but are now used for product tracking, identification of products, time tracking and marketing campaigns (Chipman, 2013).

Figure 2.3 QR Code example (Chipman, 2013)

2.4.4 Internet of Things (IoT)

As published by Global Trade Magazine, 2017, The Internet of Things (IoT) is concerned with using the Internet to connect devices, allowing for the sharing of data and communication between us, our devices and applications. Through the sharing of information, it enables supply chain stakeholders to make accurate decisions. It increases visibility, drawing attention to possible faults in a given supply chain operation and from this enable ways to improve the system process, accuracy and efficiency. IoT is currently being used in the shipping element of the supply chain, as installed sensors are able to track temperature, humidity, and any potential faults that could impact products (Global Trade, 2017).

2.5 Blockchain Technology

A Blockchain uses mutually distributed ledgers that have been built on a series of innovations used for organising and sharing digital data (Nakamoto, 2008). It is a distributed database, which is shared among and agreed upon a peer-to-peer network. It consists of a linked sequence of blocks (a storage unit of transaction), holding time stamped transactions that are secured by public-key and verified by the network community. Once a component is added to the Blockchain, it cannot be changed, transforming a Blockchain into an unchanging record of past activity (Seebacher & Schüritz, 2017). The technology was first introduced in the year 2008 in Nakamoto's whitepaper as the underlying technology of Bitcoin (Nakamoto, 2008).

2.5.1 Structure of a Blockchain

Blockchain is a data structure that is ordered from the transaction information. It can be stored as a file flat (a file that contains a non-relative relationship record), or stored in a simple database. Blockchain is usually regarded as a vertical stack, the first block as the bottom of the first block of the stack, and then each block is placed on top of the other blocks. In order to ensure the traceability of the Blockchain, each block will have a time stamp. The block consists of two parts, the block header which connects with the pre-block as well as providing the integrity of the Blockchain and block body which records the updated data in the Blockchain network (Daniel Tse, 2017). Figure 2.4 shows the organisation structure of Blockchain. Each block links the pre-block through the block head, forming a chain structure.

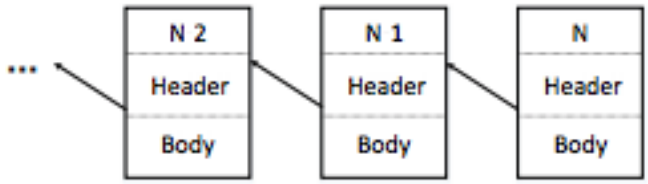

Figure 2.4 Structure of a Blockchain (Nakamoto, 2008)

2.5.2 Blockchain Proof-of-Work Algorithm

As Nakamoto highlighted in his white paper (Nakamoto, 2008), the purpose of proof of work is to implement a distributed timestamp server on a peer-to-peer basis. It involves scanning for a value that when hashed, such as with SHA-256, the hash begins with a number of zero bits. With Proof-of-Work, miners compete against each other to complete transactions on the network and get rewarded. In a network that users send each other digital tokens, a decentralised ledger gathers all the transactions into blocks. However, care should be taken to

confirm the transactions and arrange blocks. This responsibility bears on special nodes called miners, and through a process called mining (Tar, 2018). For a proposed block to be accepted in the Blockchain network, nodes must perform a Proof- of -Work to sign the block. The difficulty of this process is altered dynamically to limit the rate at which new Blocks are generated by the network. (Nakamoto, 2008).

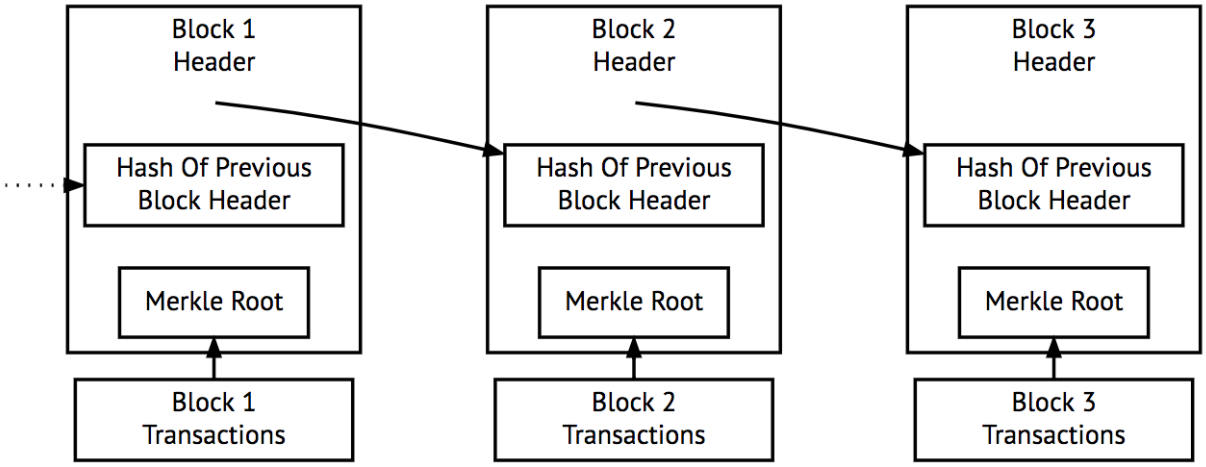

Figure 2.5 Simplified Bitcoin Blockchain (Nakamoto, 2008)

Every transaction has a hash associated with it. In a block, all of the transaction hashes are themselves hashed, sometimes several times, and the result is the Merkle root. The Merkle root is the hash of all the hashes of all the transactions in the block and is included in the block header. With this scheme, it is possible to securely verify that a transaction has been accepted by the network (Nakamoto, 2008).

For a block to be valid it must hash to a value less than the current target; this means that each block indicates that work has been done generating it. Each block contains the hash of the preceding block; thus each block has a chain of blocks that together contain a large amount of work. Changing a block (which can only be done by making a new block containing the same predecessor) requires regenerating all successors and redoing the work they contain. This protects the block chain from tampering (Tapscott & Tapscott, 2016).

2.5.3 Blockchain Proof-of-Stake Algorithm

Due to the increasing computational requirements, unfortunately the concept of the Proof-of-Work based system tends to lean towards eventual self-destruction (Lele, 2017). Proof-of-stake (PoS) aims to replace the way of achieving consensus in a distributed system. Generating a

block involves sending coins to oneself, which proves the ownership. The required amount of coins (also called target) is specified by the network through a difficulty adjustment process similar to Proof-of-Work that ensures an approximate, constant block time.

The initial distribution of the currency is usually obtained through a period of Proof-of-Work mining. The Blockchain keeps track of a set of validators, and anyone who holds the block chain's base crypto currency (in Ethereum's case, ether) can become a validator by sending a special type of transaction that locks up their ether into a deposit (Simantov, 2018). The process of creating and agreeing to new blocks is then done through a consensus algorithm that all current validators can participate in. There are many kinds of consensus algorithms, and many ways to assign rewards to validators who participate in the consensus algorithm, so there are many varieties of proof of stake. From an algorithmic perspective, there are two major types:

i. Chain-Based Proof-of-Stake

The algorithm pseudo-randomly selects a validator during each time slot (e.g. every period of 10 seconds might be a time slot), and assigns that validator the right to create a single block, and this block must point to some previous block (normally the block at the end of the previously longest chain), and so over time most blocks converge into a single constantly growing chain.

ii. BFT-Style Proof-of-Stake

Validators are randomly assigned the right to propose blocks, but agreeing on which block is canonical is done through a multi-round process where every validator sends a "vote" for some specific block during each round, and at the end of the process all (honest and online) validators permanently agree on whether or not any given block is part of the chain. Note that blocks may still be chained together; the key difference is that consensus on a block can come within one block, and does not depend on the length or size of the chain after it (Simantov, 2018). The main declared advantage of Proof-of-Stake approaches is the absence of expensive computations and hence a lower entry barrier for block generation rewards (BitFury, 2015).

2.6 Existing Supply Chain Management Solutions

2.6.1 IBM Supply Chain Management

IBM supply chain management is a solution developed by IBM an American multinational technology company headquartered in Armonk, New York, United States. The solution delivers supply chain planning and execution capabilities across the extended enterprise, enabling companies to anticipate, control and react to demand and supply volatility within the supply chain. It manages how supply chain stakeholders fulfill orders, how much inventory they should store where, and the planning and execution of shipments to meet different wholesalers and retailers commitments (IBM, 2016).

2.6.2 SAP Supply Chain Management

SAP is the world's largest business software, headquartered in Walldorf, Germany. The SAP supply chain management solution is part of their SAP ERP (enterprise resource planning) software. It controls production planning, business forecasting and demand planning. It helps the organisation to manage their supply chain process in a dynamic environment. SAP SCM process helps supply chain stakeholders to connect with each other to manage supply chain process efficiently and effectively (SAP, 2017).

2.6.3 Oracle Supply Chain Management

Oracle is an American multinational computer technology corporation, headquartered in Redwood Shores, California. It offers set of software solutions that manages and oversees the flow of goods, data, and finances as a product or service moves from point of origin to its final destination. The solution encompasses everything from product development to logistics, including production and manufacturing, sourcing, transportation, inventory and warehouse management, and shipping (Oracle, 2016).

2.6.4 JDA Software

JDA Software Group, Inc. is an American software and consultancy company headquartered in Scottsdale, Arizona, United States. The solution offers different software experiences for manufacturers, retailers distributors and the service industry. They also offer cloud based solutions that powers their architecture (JDA Software, 2017).

2.7 Existing Blockchain Based Supply Chain Management Solutions

2.7.1 Provenance

Provenance is a supply-chain traceability application developed using Ethereum. The application tracks yellowfin and skipjack tuna fish in Indonesia. Recipients are able to view the story and journeys of the fish they buy by simply scanning a QR Code. They are able to track the product up to the fisherman that caught the fish. Since its launch provenance has been praised by the Indonesian government for providing this transparency to its citizens. (Allison, 2016).

2.7.2 Everledger

Everledger is a Blockchain application developed for tracking diamonds. The company partnered with Barclays Bank to create a records of diamonds that are registered in its Blockchain. The goal of which is to satisfy that the final cut diamonds was properly sourced from different parts of the world (Roberts, 2017).

2.8 General Blockchain Based Solutions

2.8.1 IBM Blockchain Platform

IBM Blockchain Platform is a commercial-ready solution that addresses the full lifecycle (develop, govern, and operate) of a multi-organisation blockchain network. It provides a highly secure and permissioned blockchain network upon which authenticated members can easily define assets and create the business solutions for modifying and exchanging them. The solution is built on the Hyperledger Fabric code base that leverages a modular architecture to achieve enterprise levels of security, data integrity, scalability, and performance (IBM, 2018).

2.8.2 Ethereum

Ethereum is a public blockchain network built with a fully-fledged Turning complete programming language that can be used to create “contracts” within the network by simply writing a few lines of code. A contract is executed by nodes in the network when a particular condition is met and can be used to create transactions such as transferring tokens, or in Ethereum’s case, Ether from one wallet to another. Using smart contracts, it is possible for anyone to develop solutions that run on the Ethereum network (Buterin, 2015).

2.9 Summary of Existing Solutions

The aforementioned solutions still suffer from lack of transparency and a centralised trust mechanism. They rely on a single governing body to control and maintain the solution. This facilitates the introduction of illegal and counterfeit products as a malicious third party would only have to target a single central repository of records. Furthermore, by not providing transparency to consumers, organisations may partake unethical ways of conducting its distributions. As for the Blockchain solutions identified, they focus on specific kind of products, effectively creating a need for a more robust supply chain quality management solution, that is able to manage any kind of product.

2.10 Conceptual Framework

As discussed in this chapter, the use of Blockchain technology has greatly impacted various supply chains making them more secure and transparent. Manufacturers, distributors, retailers and consumers are able to verify the authenticity of goods by being able to trace the movement of individual items through a supply chain. Introduction of counterfeit products while in transit will be easily detected by any actors in the supply chain effectively cutting down counterfeit goods in a particular market.

This research seeks to develop a robust supply chain management platform that will focus on the traceability of products based using Blockchain technology. It will be able to provide secure and transparent supply chain transactions to manufacturers, distributors and consumers. Supply chain stakeholders will be able to create distributions, verify them and view a products journey as it penetrates the market in a transparent and open way. The platform will be able to cater towards vast supply chains with wide range of products while still providing a decentralised mechanism of managing trust in those supply chains.

For an effective solution the consumer application will support both Android and iOS platforms to ensure any user can verify the authenticity of goods. Supporting the consumer mobile applications will be a network of fault tolerant validator nodes that will utilise the Proof-of-Stake algorithm in order to provide fast transaction speeds and while still remaining cost effective in terms of energy consumption.

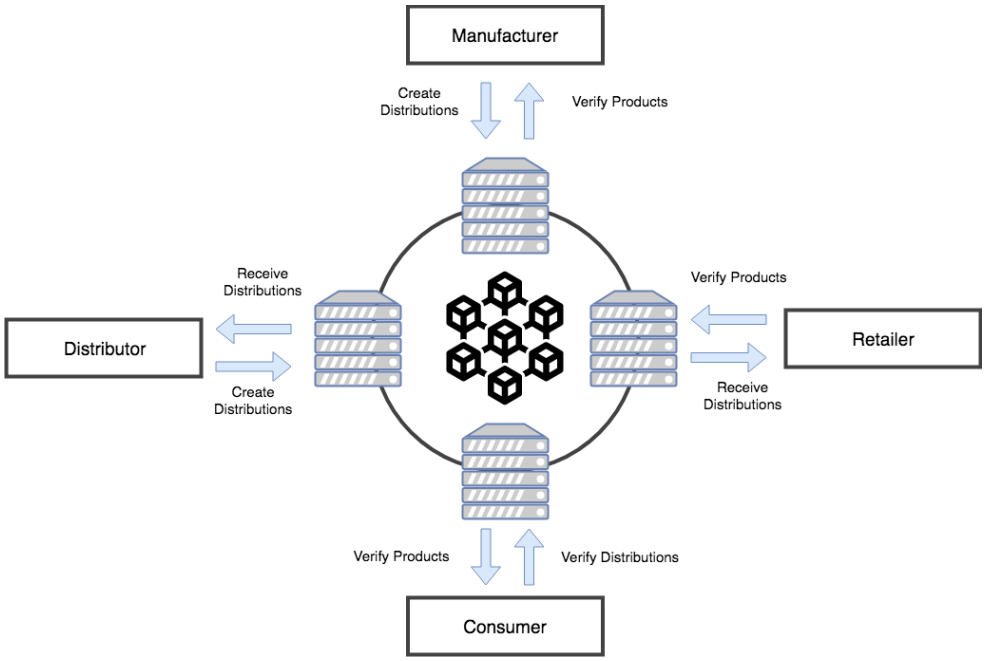

Figure 2.6 Conceptual Model

CHAPTER 3: METHODOLOGY

3.1 Introduction

This chapter discusses about the software methodology used to design and implement an effective supply chain management platform through the use of a consumer based application. The proposed solution was developed using Agile Software development methodology as the framework of choice. This chapter describes this research methodology and how it was used for the development of the mobile application and Blockchain platform.

3.2 Software Development Methodology

The concept of agile development was recommended in 2001 by the agile team, and then later recognized and accepted by various teams and companies. It has been widely used in many projects since its conception (Li, 2010). Agile Methodology suited for this study, as changes could be made to the application or system and not have a significant impact. It encourages user feedback from participants and stakeholders and ultimately improving user acceptance. The proposed system underwent four main phases as shown in Figure 3.1

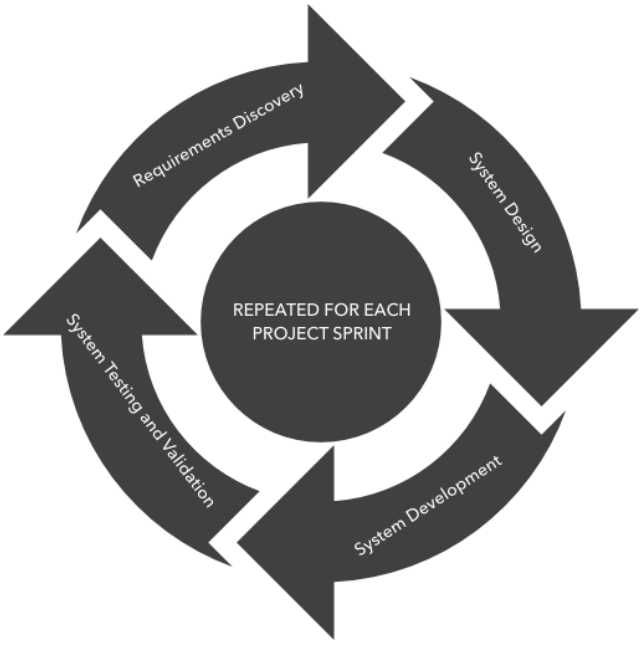

Figure 3.1 Agile Software Methodology adapted from Li (2010)

3.2.1 Requirements Discovery

During this phase, the researcher sought to know various functional requirements and the non-functional requirements of the system. A detailed and thorough review of existing documents on adoption of Blockchain technology in supply chain logistics was conducted to help formulate a solution that improve the tracking and verification of products as they make their way into a given market. This was then documented to facilitate the functionality requirements for the development of the proposed mobile application.

3.2.2 System Design

Following Blockchain convention, the developed solution was designed to be highly transparent and scalable. Anyone with a computer would be able to download the validator program and not only retrieve their copy of their Blockchain but also start verifying transactions. Manufacturers, distributors, and retailers will be able to create transactions thorough the mobile application while consumers will be able to read the information that is stored in the Blockchain. The developed solution would also allow third-party organisations, with their custom business logic to run their solutions on the Blockchain without having to use the developed mobile application by simply interacting with a validator.

For the purpose of obtaining holistic representation of the developed system, Unified Modeling Language (UML) was used for modeling and designing diagrams (Bell, 2004). The study employed the following diagrams:

i. Use Case Diagrams

Provided a high level view of the system. They capture to a certain extent system structures. The diagrams described sequences of actions a system performs that yield an observable result of value to a particular actor (Felici, 2011).

ii. Sequence Diagrams

Was used demonstrate the collaborations between objects in the sequential order that those collaborations happen (Bell, 2004).

iii. Low and High Fidelity Prototypes

Low-fidelity prototyping tools and methods were used for early design just after requirements analysis, to help conceptualize and envision the interface at a high level. These tools supported rough sketching of interface screens by freehand drawing with a mouse or tablet pen. High-

fidelity prototyping tools permitted the creation of a lifelike used for user tests, before the final version was developed.

3.2.3 Systems Development

This study aimed at coming up with a fault tolerant network of validator nodes that would maintain the state of the Blockchain and a mobile application to create transactions to the Blockchain. The mobile application was built for both Android and iOS platforms. To achieve this the researcher utilised the React Native framework for cross platform development (Danielsson, 2016). The Blockchain platform is built on top of the Tendermint Blockchain Consensus framework using JavaScript as the main programming language for validator nodes (Kwon, 2014). All Blockchain data is distributed across the multiple nodes that performs verification, validation of transactions and achieving consensus before mutating the state of the Blockchain. The platform built is open-source in nature allowing anyone to become a validator node or initiate transactions on the Blockchain.

3.2.4 System Testing and Validation

Once the development phase concluded, testing was done on the application and platform with the aim of ensuring that it performs as intended. The system underwent the following tests:

i. Usability Testing

Was done to see how easy it is to use the mobile application by testing it with real users. Users were asked to complete tasks, typically while they are being observed by the researcher, to see where they encounter problems and experience confusion. If more people encounter similar problems, recommendations will be made to overcome these usability issues.

ii. Functionality Testing

This test was done to verify whether the mobile application and Blockchain platform meets both functional and non-functional requirements. The system will be tested by providing it with some related input so that the output can be evaluated to see how it conforms, relates or varies compared to its base requirements.

iii. Compatibility Testing

The mobile application was tested using Firebase's Testlab to verify the application is stable across a wide range of android devices (Firebase, 2018). Finally, a small group of BETA testers will be identified who will provide valuable feedback on the mobile applications performance on their device.

iv. Integration Testing

This involved combining multiple units of the platform and testing it as a group. The purpose of this level of testing is to expose faults in the interaction between integrated units or software components. This was done by monitoring validator nodes in the Blockchain and recording their response and uptimes.

3.3 Ethical Considerations

This study ensured that all respondents and BETA testers acted at will and they were not persuaded in any way. Any private data the respondents chose to share remained private and was only used for analysis purposes. The study also ensured that the solution proposed worked for people who chose to use the service.

3.4 Validation

To validate that the application developed addressed the challenges within supply chain logistics, a local export company in Kenya called Chriven Enterprises was consulted and used the developed solution to manage one of their various shipments. The company was selected due to their 7 year long experience in supply chain logistics and multiple vendors and actors within their supply chain. A usability and validation questionnaire, shown in Appendix A, was prepared and distributed to 15 respondents and the data visualized using Google Sheets.

CHAPTER 4: SYSTEM ANALYSIS AND DESIGN

4.1 Introduction

This chapter presents the analysis, design, implementation and testing procedures adopted in the development of the prototype proposed in the study. The architecture of the developed prototype, its algorithms, and process and database design are discussed in detail. Application wireframes of the prototype interfaces are then presented.

4.2 Functional Requirements

Functional requirements are the capabilities, functions and basic processes that the implemented application must be able to perform.

4.2.1 Manufacturers

i. Product distribution channels: The system should allow manufactures to identify how their product has penetrated a given market.
ii. Product creation: The system should allow manufacturers to create different kinds of products and have them stored on the Blockchain.
iii. Supply chain distribution creation: The system should allow manufacturers to create new shipment orders to an intended wholesaler, retailer or other distributors.
iv. Supply chain distribution verification: The system should allow manufacturers to verify the authenticity and integrity of the shipment that they receive.

4.2.2 Distributors

i. Shipment Information: The system should allow distributors to obtain a report of a particular shipment, its contents and timestamp of when created.
ii. Supply chain distribution creation: The system should allow distributors to create new shipment orders to an intended wholesaler, retailer or other distributors.
iii. Supply chain distribution verification: The system should allow distributors to verify the authenticity and integrity of the shipment that they receive.

4.2.3 Retailers

i. Product verification: The system should enable retailers to verify the authenticity of individual product items that they receive from a distributor.
ii. Supply chain distribution verification: The system should allow retailers to verify the authenticity and integrity of the shipment that they receive from a distributor.

4.2.4 Consumers

i. Product verification: The system should allow enable consumers to verify the authenticity of individual product items that they purchase from a retailer.
ii. Product supply chain tracing: The system should allow the consumer to view a particular product's journey in a supply chain at any given moment.

4.3 Non-Functional Requirements

Non-functional requirements are the requirements that do not affect the core business of the application, the application can still work with or without them, but which are part of the system. They include:

i. Usability: The system should have an easy to use interface.
ii. Reliability and availability: The system should be reliable and always available to perform tasks.
iii. Performance: The system should have an acceptable response time while performing functions.
iv. Scalability: The system's performance should not be adversely affected as the number of users' increases.

4.4 System Architecture

To satisfy the design requirements for providing a decentralised mode of trust within a supply chain, Blockchain technology was used as the primary way of validating transactions and distribution of a shared ledger. Figure 4.1 shows how a transaction instantiated from the mobile application gets processed and added to the Blockchain.

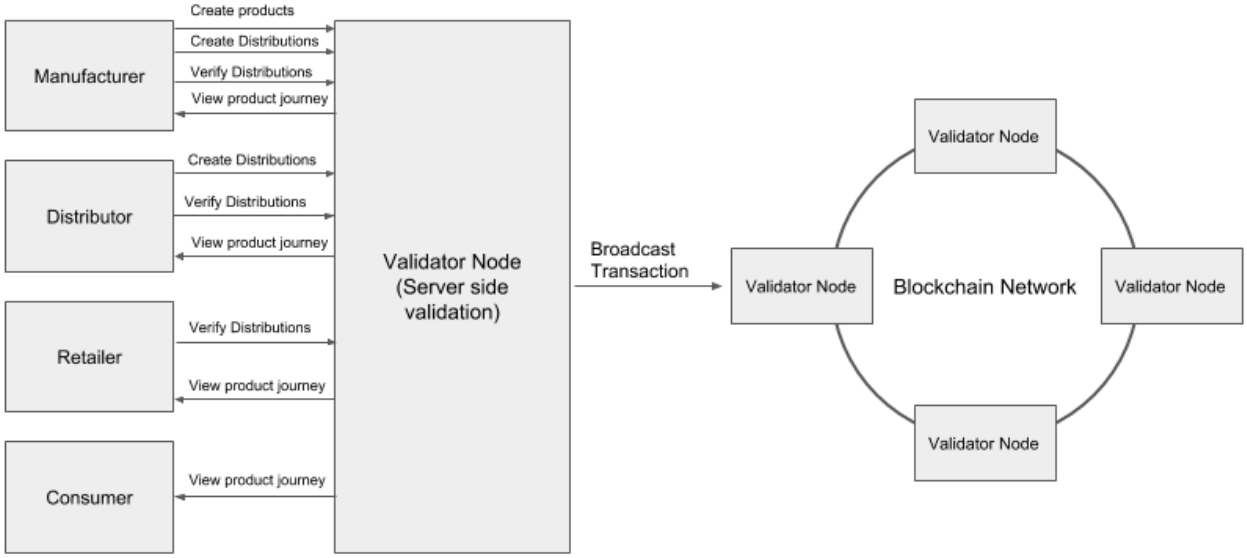

Figure 4.1 System Architecture

To perform any transactions with the system a user must first generate a pair of RSA keys and a public address. This is done during the signing up process of the mobile application. The public address is generated by passing the users public key through a SHA-256 Cryptographic Hash Algorithm and is used within the application to establish a particular distribution point. The private key is used for the purpose of signing messages transmitted to a particular validator node. The public address, public key and private key are all stored in the users device and are used whenever the user wants to create a transaction and only the user's public address and public key is stored on the Blockchain for the purpose of verifying message signatures. A copy of these credentials would then be sent to the user's email address should they choose to login on a different device. Once a user has generated these credentials they are able to create and verify distributions by sharing their public address through the mobile application as well as determine a particular products authenticity by tracing its journey through a supply-chain.

Creating a distribution involves scanning the QR Codes of products that a particular manufacturer and/or distributor wants to distribute. The values of the QR Codes that are scanned are unique identifiers that are used within the Blockchain to distinctly determine a

particular product. Once the user has scanned a set number of products, the mobile application generates and encrypts the message using a validator node's public key and attaches its signature by using the users private key. The message consists of a list of products, receiver's public address, a SHA-256 message digest, and the sender's current location. Once the message has been composed it is ready to be transmitted to a validator node in the Blockchain network.

Validators are nodes within the network that participate in consensus whenever there is an incoming transaction by broadcasting cryptographic signatures or votes. Each validator has a voting power that is the equivalent to cryptographic coins during the Proof-of-Stake algorithm. A set of validators with at least $\frac{2}{3}$ of the total voting power is called *majority of validators* and a set of validators with at least $\frac{1}{3}$ of the total voting power is called *minority of validators*. A block is only committed if $\frac{2}{3}$ majority of validators sign commit votes for that block.

Once a validator node receives the message, it first decrypts it using its private key. After the message has been decrypted the node validates the integrity of the message by generating a SHA-256 message digest comparing it with what is attached. Once the message integrity has been verified the validator node checks the message signature to prove that the message actually came from the user. Finally, the node determines whether the user is capable of performing the requested transaction i.e. whether the user owns the products they want to distribute.

After the validation procedures, the node broadcasts the transactions to all available validator nodes, the purpose of which is to reach a consensus in determining whether the suggested transaction is valid and how the Blockchain should be mutated. Each validator node has an assigned voting power that is used to drive the consensus decisions. All validator nodes use the Tendermint Blockchain consensus framework that utilises the Proof-of-Stake algorithm to determine Blocks in a Blockchain allowing the transaction to be processed nearly instantaneous due to the elimination of the mining process. Once the transaction is complete the receiving user is notified via push notification regarding their incoming distribution.

4.4.1 Message Transmission and Structure

To create a transaction on the Blockchain, supply chain actors must construct an encrypted and signed message to send to a particular validator node. All messages are encrypted using a validator node's public key and signed using the initiator's private key that they obtain after successful registration on the system. There are three distinct transactions that can occur. These include:

i. Product creation

This transaction is only initiated by the manufacturer. The message consists of product information e.g. product name, the signature of the manufacturer and the manufacturer's public address. The message is then encrypted using a particular validator node's public key. The validator node would then decrypt the message using its own private key and verify the message signature by using the manufacturers public key that is stored on the Blockchain network. The validator node would then determine whether the user can perform this transaction by referencing the manufacturers stored in the Blockchain that match the received public address. A hash of the transaction is then constructed by using the product information and manufactures public key. The transaction is added to the Blockchain after validator nodes achieve consensus.

ii. Distribution creation

This transaction is only initiated by manufacturers and distributors. The message consists of distribution information such as name of the distribution and products in the distribution. The signature and public address of the initiator is also attached. The message is then encrypted using a particular validator node's public key. The validator node then decrypts the message using its own private key and verifies the message signature by using the initiators public key that is stored on the Blockchain network. The validator node would then determine whether the user can perform this transaction by referencing the manufacturers and distributors stored in the Blockchain that match the received public address. A hash of the transaction is then constructed by using the distribution information and initiator's public key. The transaction is added to the Blockchain after validator nodes achieve consensus.

iii. Distribution verification

This transaction is only initiated by manufacturers, distributors and retailers. The message consists of the unique distribution identifier, the signature and public address of the initiator. The message is then encrypted using a particular validator node's public key. The validator

node then decrypts the message using its own private key and verifies the message signature by using the initiators public key that is stored on the Blockchain network. The validator node would then determine whether the user can perform this transaction by referencing the manufacturers, distributors and retailers stored in the Blockchain that match the received public address. A hash of the transaction is then constructed by using the unique distribution identifier and initiator's public key. The transaction is added to the Blockchain after validator nodes achieve consensus.

4.4.2 Consensus

The solution was developed using the Tendermint Blockchain consensus framework and handles the consensus protocols of the established validator nodes. The validator nodes take turns in proposing blocks of transactions and voting on them. Blocks are committed in a chain, with one block at each height. A block may fail to be committed, in which case the protocol moves to the next round, and a new validator gets to propose a block for that height. Two stages of voting are required to successfully commit a block, these are called pre-vote and pre-commit. As shown in Figure 4.2, a block is committed when more than 2/3 of validators pre-commit for the same block in the same round (Kwon, 2014).

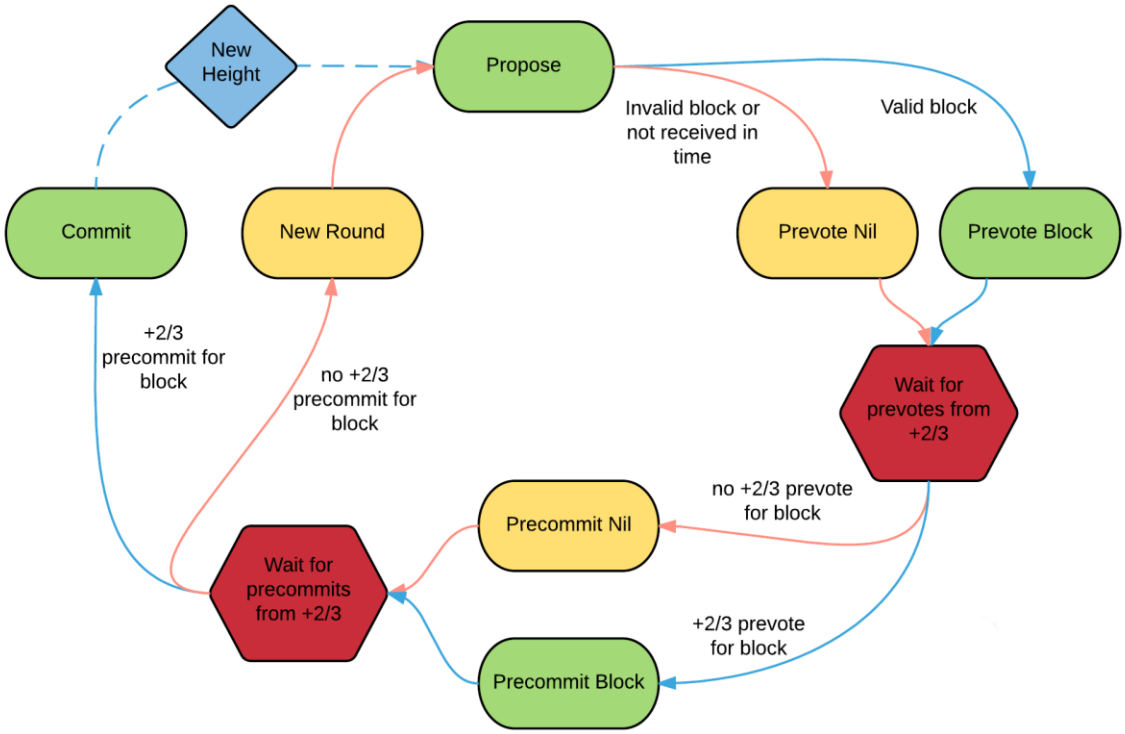

Figure 4.2 Tendermint Consensus Protocol (Kwon, 2014)

4.4.3 Proof-of-Stake

Each validator node has an assigned voting power that is used during consensus. The voting power in this case is used as "stake" during consensus and can be considered as currency. Validators are then forced to bond their stake to the network during the consensus protocol. If a validator acts maliciously their stake is destroyed. A validator will be rewarded by the network by only if they are able to achieve consensus as the network dictates. This effectively creates a crypto-currency within the network.

4.4.4 QR Code Generation

QR Codes are generated by the manufacturers for the purpose of identifying each product uniquely. They do this through interacting with a validator node through a RESTful API. The API gives manufacturers the ability to specify the number of QR Codes they wish and each QR Code returned will identify a product uniquely in the Blockchain. Due to the 3 kilobyte maximum capacity that QR Codes can hold, only the unique product identifier is encoded in the QR Code (Kieseberg, 2016). The QR Codes are then attached to the different products that the manufacturer wants to distribute. When creating a distribution from within the application, the manufacturer can then add the relevant product information such as product name and description which gets stored in the Blockchain and is associated with the unique product identifier that is encoded in the QR Code. This code can be scanned by any actor in the supply chain to obtain the relevant product information as well as trace back the product to the manufacturer.

4.4.5 Distributed Data Storage

Once a validator node is active on the Blockchain network, it immediately retrieves its own copy of the Blockchain. The Blockchain data is then stored locally on the validator node's hard disk drive. Information stored is of a NoSQL, JSON structure and can be accessed programmatically via a RESTful framework. When a user causes a transaction, it mutates the state of the Blockchain by generating and adding new Blocks. The consensus algorithm ensures that all validator nodes have identical copies of the Blockchain and the data stored in each node is consistent.

4.5 System Design Tools

4.5.1 Context Diagram

Figure 4.3 shows the boundary between the Blockchain and its environment along with the entities that interact with it.

i. Manufactures create transactions on the Blockchain by creating products, creating distributions and verifying incoming distributions. They are also able to read from the Blockchain how their products penetrate a market by following a trail of distributions.

ii. Distributors create transactions by creating and verifying distributions. They are also able to read from the Blockchain product information and determine its authenticity by tracing it back to the manufacturer.

iii. Retailers create transactions by verifying incoming shipment from distributors. They can also retrieve from the Blockchain relevant product information and trace back the product to the manufacturer.

iv. Consumers are able to read relevant product information from the Blockchain and determine the authenticity of their purchased goods by tracing it back to the manufacturer.

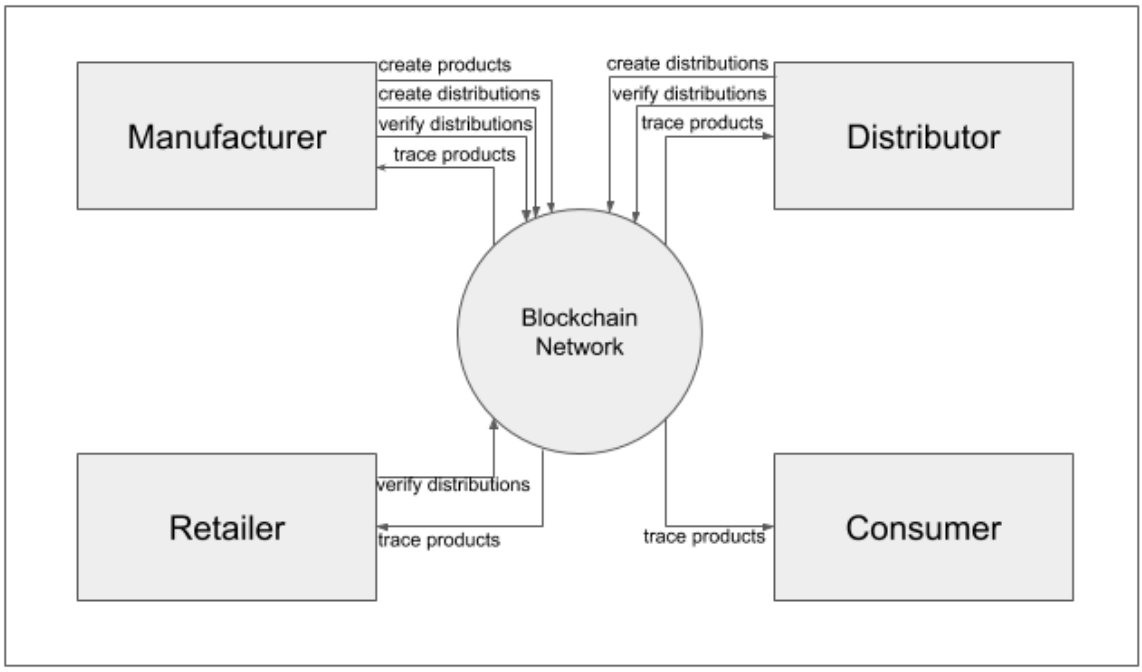

Figure 4.3 Context Diagram

4.5.2 Use Case Diagram and Descriptions

Figure 4.4 gives an illustration of the major interactions that the new system underwent with the various actors and other sub-systems. What follows are the Use Case Descriptions.

Figure 4.4 Use Case Diagram

The following are the Use Case Descriptions:

Table 4.1 Verify Distribution

Use Case: Verify Distribution	
Primary Actors:	Distributors, Retailers
Stakeholders:	Manufacturer
Precondition	Need to verify an already dispatched distribution.
Post condition	Verify distribution, view verification results that determine the authenticity of products dispatched
Main success scenario	
Actor	**System**
1. User receives distribution 2. User selects scan 3. User reads QR codes of the products received.	3.1 System validates, determines the authenticity of the products and displays results to the user.
Alternative Flow: At step 2, user selects the item scanned from the menu. • User views product information e.g. weight, size, color etc.	• System retrieves single product information

Table 4.2 View Product Journey

Use Case: View Product Journey	
Primary Actors:	Customer, Retailer, Distributors
Stakeholders:	Manufacturer
Precondition	Need to view product journey in supply chain User has a product with QR Code
Post condition	User views product journey
Main success scenario	
Actor	**System**
User scans an individual product	System displays product journey through a supply chain

Table 4.3 Create An Account

Use Case: Create An Account	
Primary Actors:	Customer, Retailer, Distributors, Manufacturer
Stakeholders:	
Precondition	Need to manage a supply chain and verify the authenticity of products
Post condition	User generates a pair of RSA Keys and a public address
Main success scenario	
Actor	**System**
User submits registration details	Account created and user owns a public address

Table 4.4 Generate QR Code

Use Case: Generate QR Code	
Primary Actors:	Manufacturer
Stakeholders:	
Precondition	Manufacturer has a public address Manufacturer has a unique product identifier
Post condition	Generate QR Code
Main success scenario	
Actor	**System**
Submit unique product identifier	QR Code is successfully generated.

4.5.3 Sequence Diagram

The sequence diagram shows the flow of information between the main entities in the system. Figure 4.5 depicts how users interact with the system, how they are able to verify the authenticity of the product.

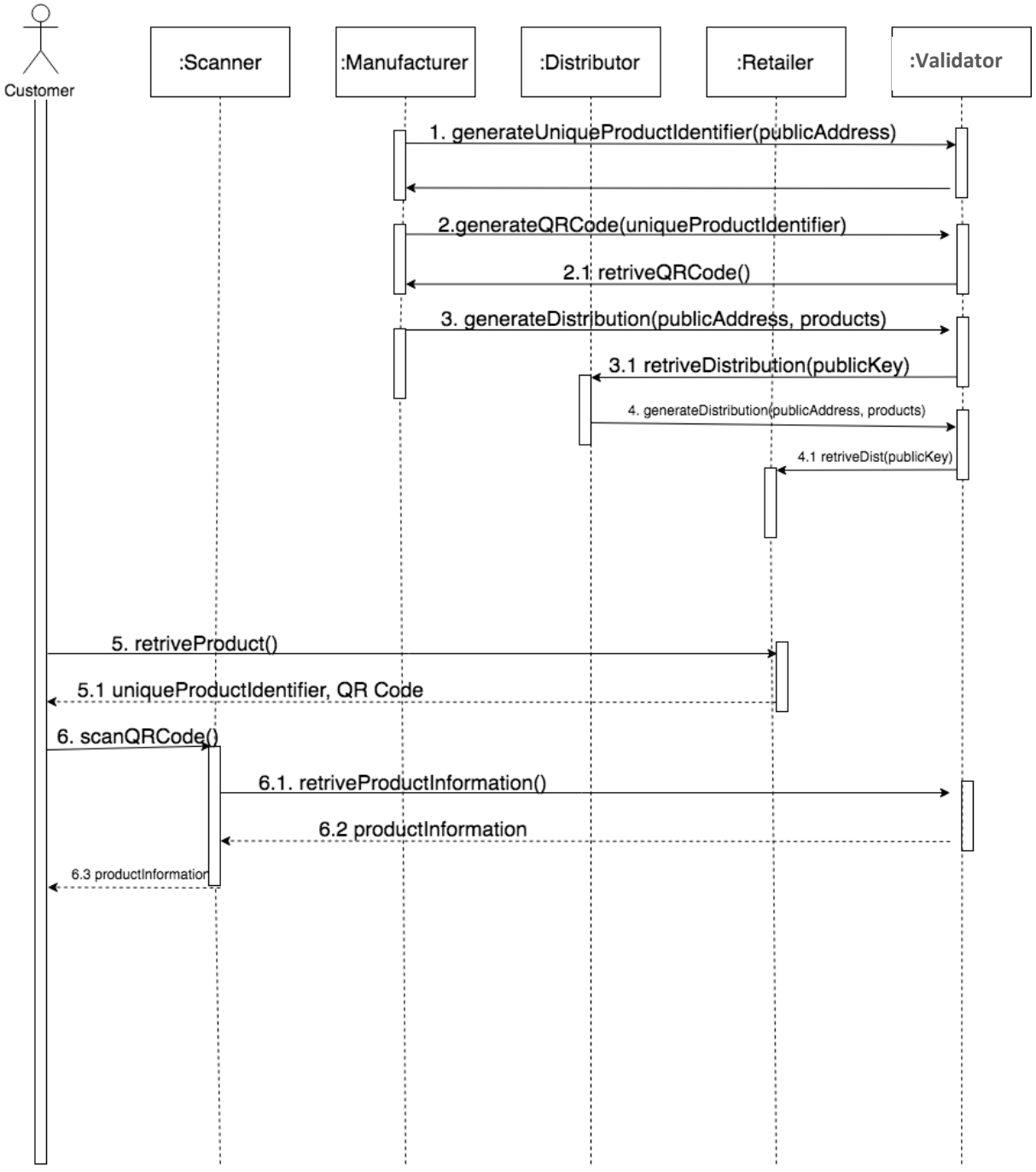

Figure 4.5 Sequence Diagram

4.5.4 Class Diagram

Figure 4.6 is a design class diagram that shows all interactions between classes, their corresponding methods and attributes.

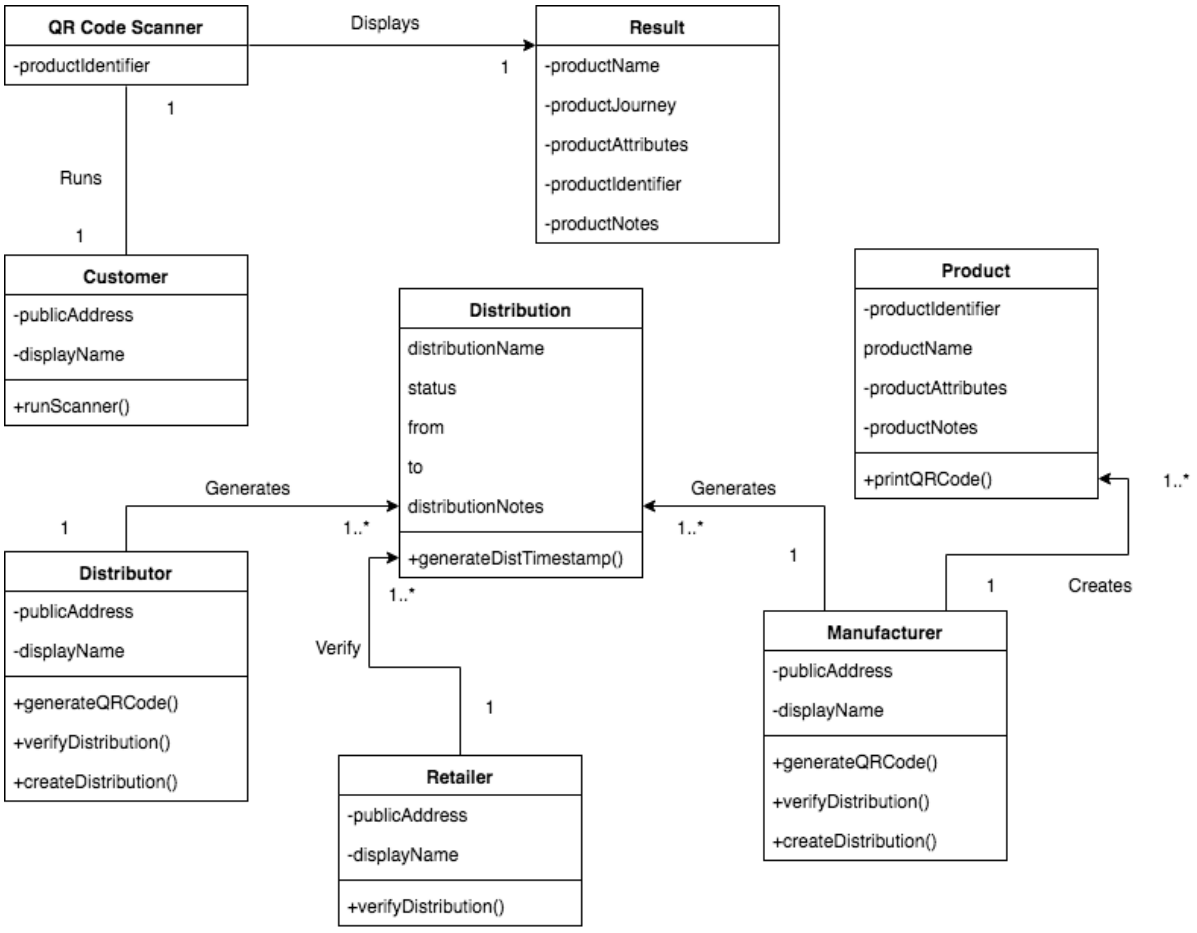

Figure 4.6 Class Diagram

4.6 Security Design

4.6.1 Transaction Message Transmissions

To conduct any transactions on the Blockchain users have to generate a pair of RSA keys. From the RSA keys a public address is generated by hashing the public key using the SHA-256 hashing algorithm. The public address is used to identify a user uniquely in the Blockchain and the public key is used by the validator nodes to verify a message signature. To initiate a transaction, the mobile application encrypts the transaction using a particular validators public key and attaches a signature to the message. The signature is created using the user's private key that only they have access to. A particular validator will then decrypt the message and verify the signature and only then broadcast the transaction to peer validator nodes. Figure 4.7 shows an example of a pair of RSA keys and a public address.

Figure 4.7 RSA Keys and Public Address

4.6.2 Blockchain Structure

The Blockchain is maintained and mutated by connected validator nodes. The data stored is of a NoSQL structure. To conform to Blockchain architecture each collection of record stored maintains a *previousHash* and *hash* properties. The *previousHash* points to the previous Block in the chain and the *hash* property is the SHA-256 value of the data stored in the current Block. This ensures data in each Block cannot be tampered with. If a malicious individual wanted to alter the information in a particular Block they would have to re-calculate hashes for each and every Block in the chain for every available validator node in the network. This maintains a system of trust within the network and provides a decentralised architecture for the supply chain network.

4.6.3 Hashing Algorithm

The primary hashing algorithm used is SHA-256. It is used to generate public addresses and is used to maintain the integrity of the information stored in each Block of the Blockchain. It was used since it features a higher level of security than its predecessor and can be easily computed by validator nodes without much processor requirements.

4.6.4 Byzantine Fault Tolerance Validator Nodes

Blockchains are inherently decentralised systems which consist of different actors who act depending on their incentives and on the information that is available to them. Whenever a new transaction gets broadcasted to the network, nodes have the option to include that transaction to their copy of their ledger or to ignore it. When the majority of the actors which comprise the network decide on a single state, consensus is achieved. A fundamental problem in distributed computing and multi-agent systems is to achieve overall system reliability in the presence of a number of faulty processes. This often requires processes to agree on some data value that is needed during computation.

These processes are described as consensus. Some of the question this raises are:

- What happens when an actor decides to not follow the rules and to tamper with the state of his ledger?
- What happens when these actors are a large part of the network, but not the majority?

In order to create a secure consensus protocol, it must be fault tolerant. Blockchains are decentralised ledgers which, by definition, are not controlled by a central authority. Due to the value stored in these ledgers, bad actors have huge economic incentives to try and cause faults. To mitigate this and provide reliability and integrity of information in the Blockchain every validator node runs on the Tendermint framework. This ensures that transactions are processed and consensus achieved by at least two thirds of the network. This allows a third of the network to be corrupted but still maintain overall information integrity. If a malicious node tries to incorrectly mutate the Blockchain only their local copy of the ledger is corrupted and their vote is ignored by the majority of the network.

4.7 Network Design

To achieve decentralisation in the Blockchain, remote validator nodes need to be able to communicate and achieve consensus. When a validator node comes online it first performs a peer discovery lookup. It attempts to discover all available validator nodes and if two thirds of the network are available, transactions can occur. A validator node will first attempt to connect to a particular genesis validator node and from it announce its availability in the network. Genesis validator nodes are nodes in the Blockchain whose public IP addresses are known and publicly available. They also carry majority of the voting power in the Blockchain, however they can still be overruled by other validator nodes if compromised.

A validator node represents nodes in the network who's IP is not known. It represents anyone who has downloaded the validator program and actively becomes a node in the network and begins validating transactions. The mobile application sends a transaction to a particular validator node via a secure HTTPS channel. The node then broadcasts the transactions to all peers, including genesis nodes. Every node in the Blockchain has a voting power that they use to achieves consensus via a secure P2P Gossip Protocol (Kwon, 2014). This voting power can be increased or decreased programmatically depending on the business logic of the network. Figure 4.8 shows a network of validator nodes including known genesis nodes.

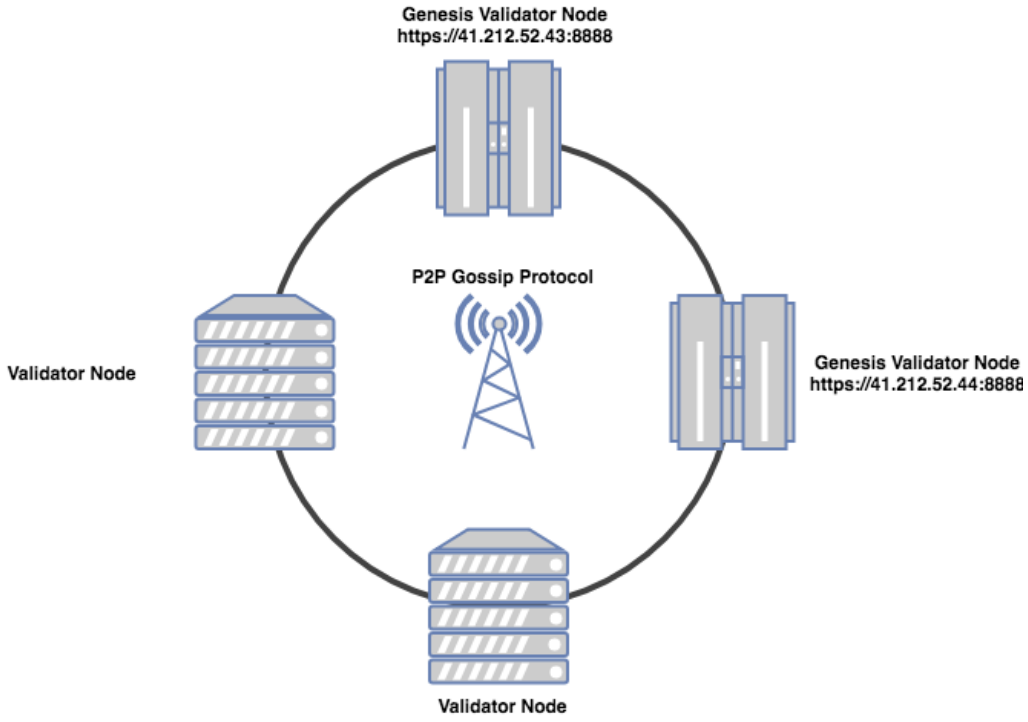

Figure 4.8 Validator Node Network

4.8 Wireframes

This section shows the user interface flow diagrams which include mobile application wireframes.

4.8.1 Generating Keys Wireframe

Figure 4.9 illustrates how users will be able to generate their public and private keys as well as public address.

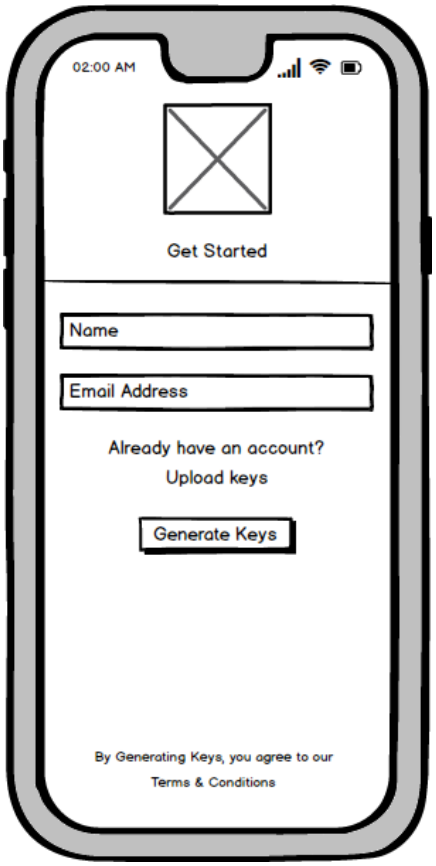

Figure 4.9 Generating Keys Wireframe

4.8.2 Distribution History Wireframe

Figure 4.10 illustrates how manufacturers, distributors and retailers will be able to view a listing of past and incoming shipment.

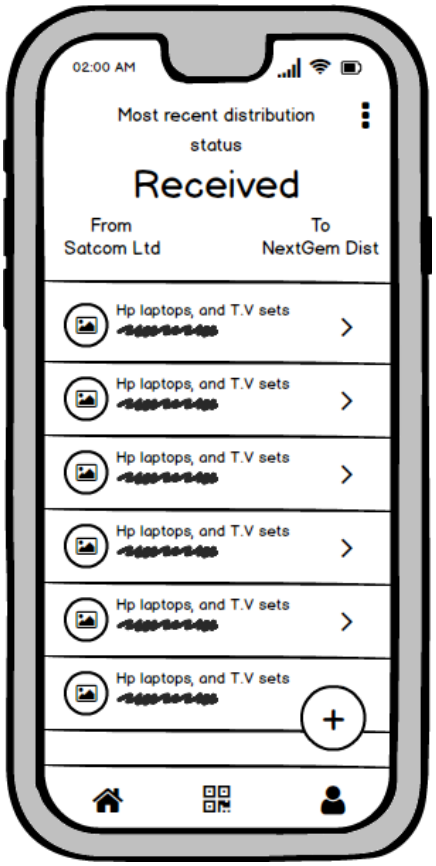

Figure 4.10 Distribution History Wireframe

4.8.3 Create Distribution Wireframe

Figure 4.11 illustrates how manufacturers and distributors will be able to create distributions by scanning the QR Codes of products.

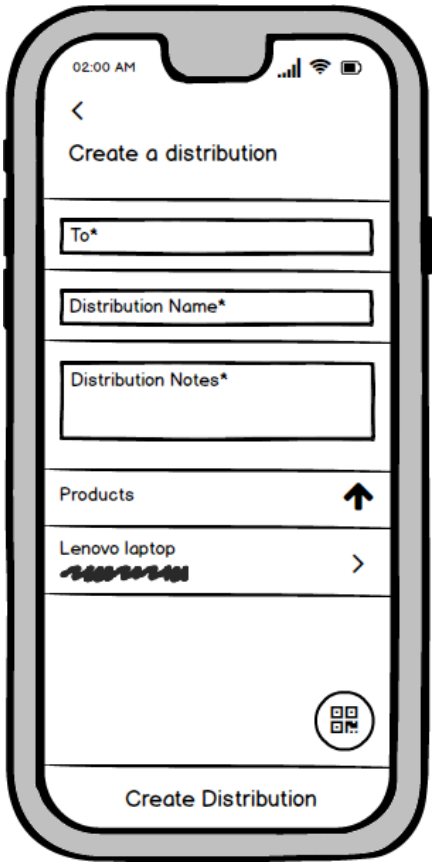

Figure 4.11 Create Distribution Wireframe

4.8.4 Product Journey Wireframe

Figure 4.12 illustrates how manufacturers, distributors, retailers and consumers will be able to trace a scanned product back to particular manufacturer.

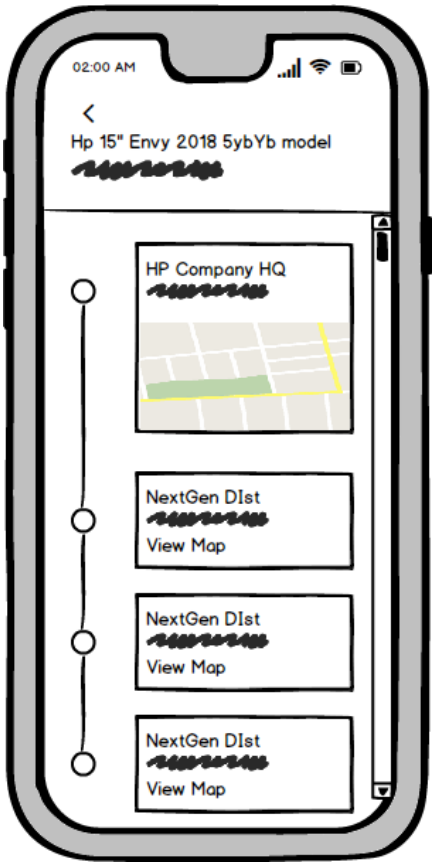

Figure 4.12 Product Journey Wireframe

4.9 Conclusions

Data collected from the respondents was analysed and used to come up with informed conclusions. The proposed solution should be built for both Android and iOS platforms, features like QR code scanner, creating distributions, verifying distributions and viewing product journeys offered. All transactions shall be carried out by decentralised remote nodes ensuring transparency among supply-chain stakeholders and users. The Blockchain would be decoupled from the mobile application developed allowing different organisations to come up with their own custom solutions for their supply chain and have that information transparent to all their stakeholders.

System analysis and design helped to fine-tune the object requirements definition pinpointed in requirements analysis and to determine design specific objects. It was useful at characterising the design, segments, modules, interfaces and information for the proposed system which helped satisfy the requirements. The next chapter explains the prototype building and testing.

CHAPTER 5: SYSTEM IMPLEMENTATION AND TESTING

5.1 Introduction

This chapter focuses on prototype building, testing and validation of the proposed system. Implementation part involves exploring various modules of the system, how implementation was done and how they function. Testing and validation involves functional testing and usability testing to check if the system fulfilled the objectives of the proposed solution.

5.2 Software Environment

The system, named Rinku consists of a single mobile application that runs on both Android and iOS mobile operating systems and a network of connected validator nodes that maintain and manipulate the Blockchain. The mobile application was built using Facebook's React Native platform that facilitates the development of cross-platform mobile applications using JavaScript and React (Danielsson, 2016). Tendermint Blockchain consensus framework was used to develop the program that runs the validator nodes. It facilitates the development of Byzantine fault-tolerant replicated state machines in any programming language (Kwon, 2014). As a result of this, the program that runs on the validator nodes is entirely written in JavaScript. All validator nodes require NodeJS v9 installed.

5.2.1 Encryption

RSA keys are generated by validator nodes which use the crypto library, natively accessible in NodeJS server environments (Node.js, 2016). Once a user signs up using the mobile application a validator node issues them with their public key, private key and public address. The public address is generated by hashing the public key using the SHA256 hashing algorithm. These credentials are stored on the users device and only the only the public key and public address is stored in the Blockchain for the purpose of verifying message signatures. Users are able to share their public address via the mobile application.

5.3 Hardware Requirements

The mobile application runs on any Android or iOS device with at least 512MB of RAM and 2GB of internal storage. Validator nodes require at least 1GB of RAM and a single core to run. The memory allocation depends on the size of the Blockchain, during the development of this solution validator nodes required 4GB worth of memory to effectively maintain the Blockchain.

5.4 Network Requirements

The mobile application requires a stable Internet connection, at least 512kb/s to make any transactions to the Blockchain. Validator nodes require the public addresses of Genesis nodes to perform a peer discovery look up to achieve consensus on incoming transactions.

5.5 System Modules

5.5.1 Rinku Mobile Application

This application is designed to run on both Android and iOS mobile phones and requires a camera, Internet connection and GPS information.

Sign Up

Figure 5.1 shows how a user generates their RSA Keys and public address to be used in creating transactions in the Blockchain. RSA keys are generated by interacting with a validator node through a RESTful API. The public key, private key and public address are then stored on the users device and a copy is sent to their email address. Only the public key and public address gets stored on the Blockchain for the purpose of verifying message signatures. Users are able to share their public address through the mobile application to an intended recipient.

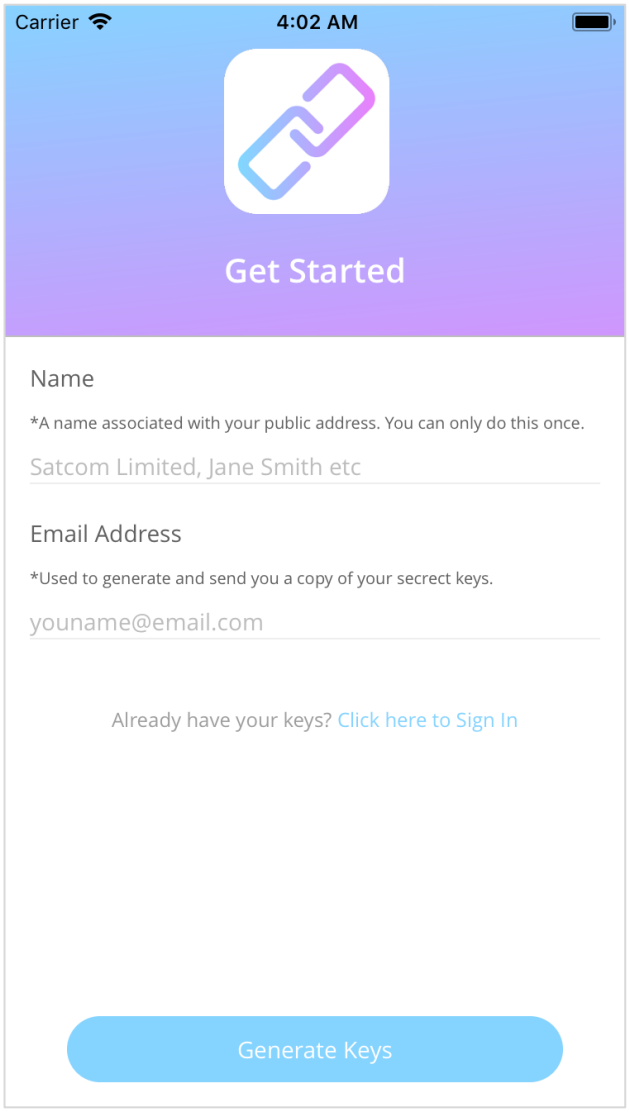

Figure 5.1 Sign Up

History Distributions

Figure 5.2 shows a user's history distribution transactions obtained from querying the state of the Blockchain.

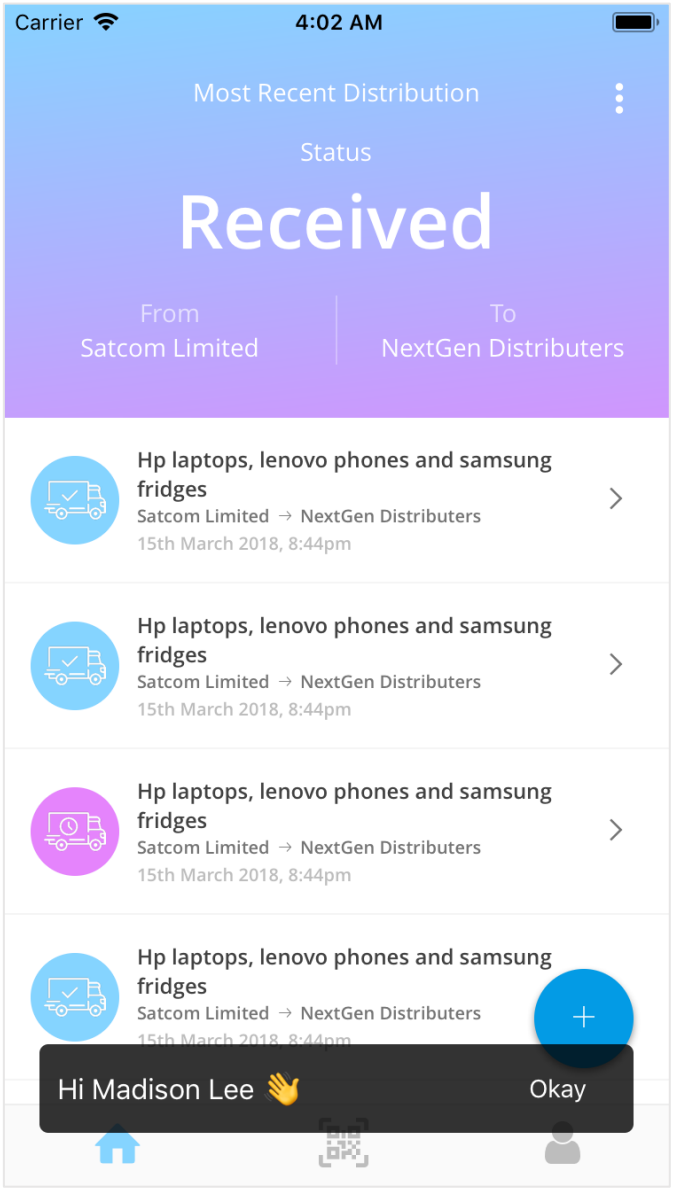

Figure 5.2 History Distributions

Scan History

Figure 5.3 shows a history of recently scanned products by the user.

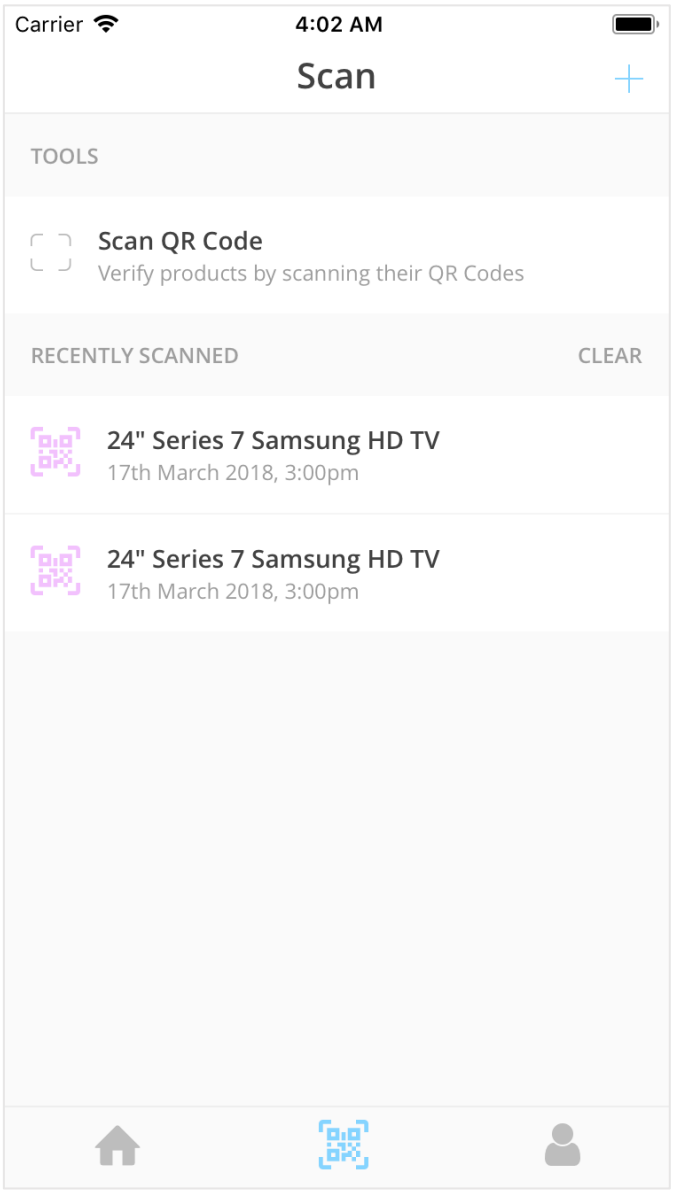

Figure 5.3 Scan History

Verifying Distributions

Figure 5.4 shows how a user can verify received distribution via scanning individual products that they have received.

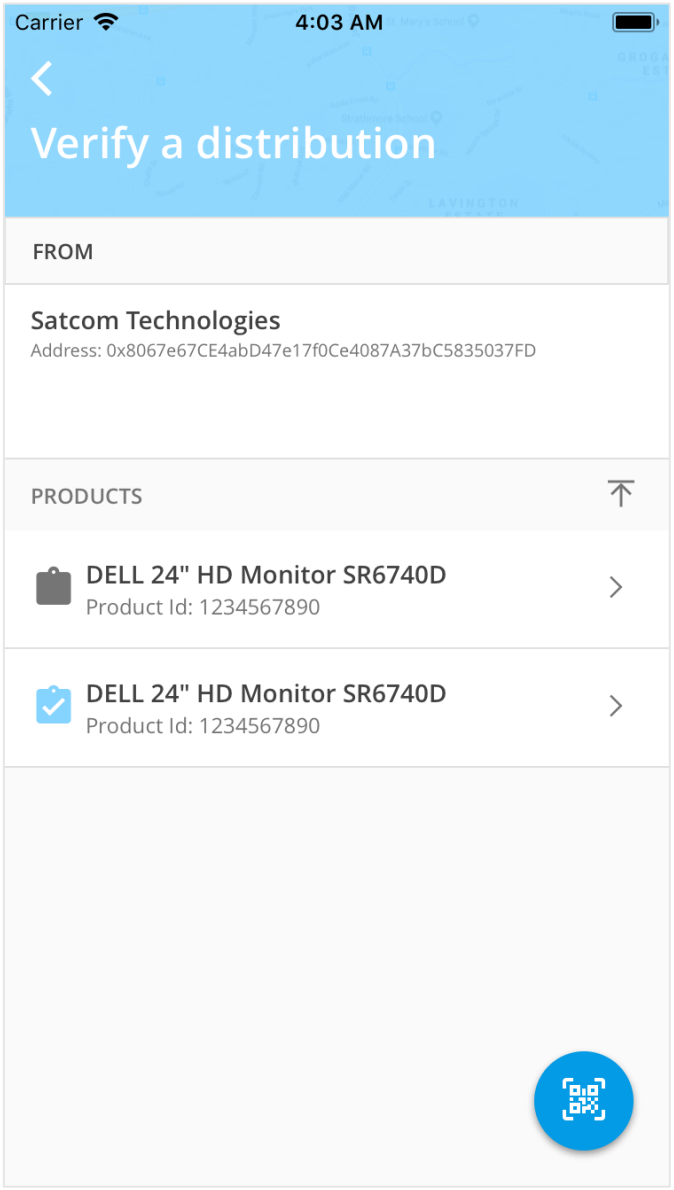

Figure 5.4 Verifying Distributions

QR Code Scanner

Figure 5.5 displays the mobile application's in built QR Code scanner that users will utilise to scan different products. QR Codes are generated by manufacturers through interacting with a validator node via a RESTful API. Each QR Code identifies a product uniquely in the Blockchain. Manufacturers will also create product information through the mobile application that will be associated with the generated QR Code which will be stored on the Blockchain. They will then attach these QR Codes on their products and can be scanned by all supply chain actors running the mobile application.

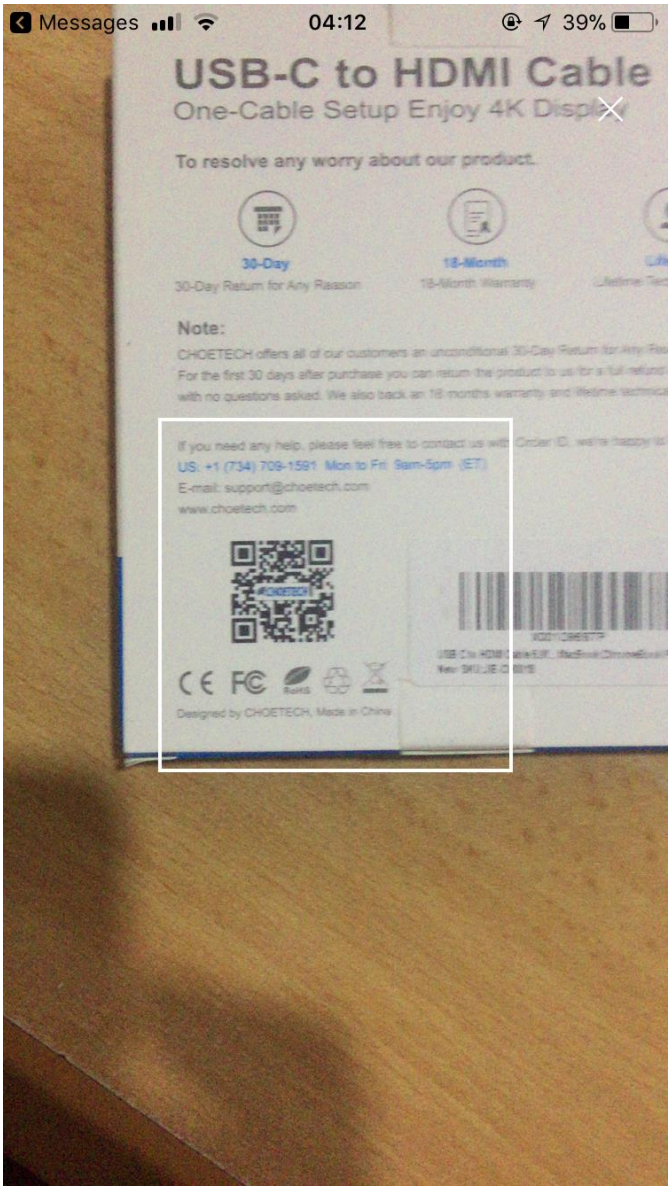

Figure 5.5 QR Code Scanner

5.5.2 Validator Nodes

Figure 5.6 displays log messages from a validator nodes during an incoming transaction from the mobile application. These sequence of procedures happen for every single node in the Blockchain network. Once a validator node has verified the transaction, it attempts to mutate the state of the Blockchain by taking part in the consensus protocol highlighted in Chapter 4. Once consensus is reached the validator nodes mutates its own copy of the leger ensuring consistency and in the records stored.

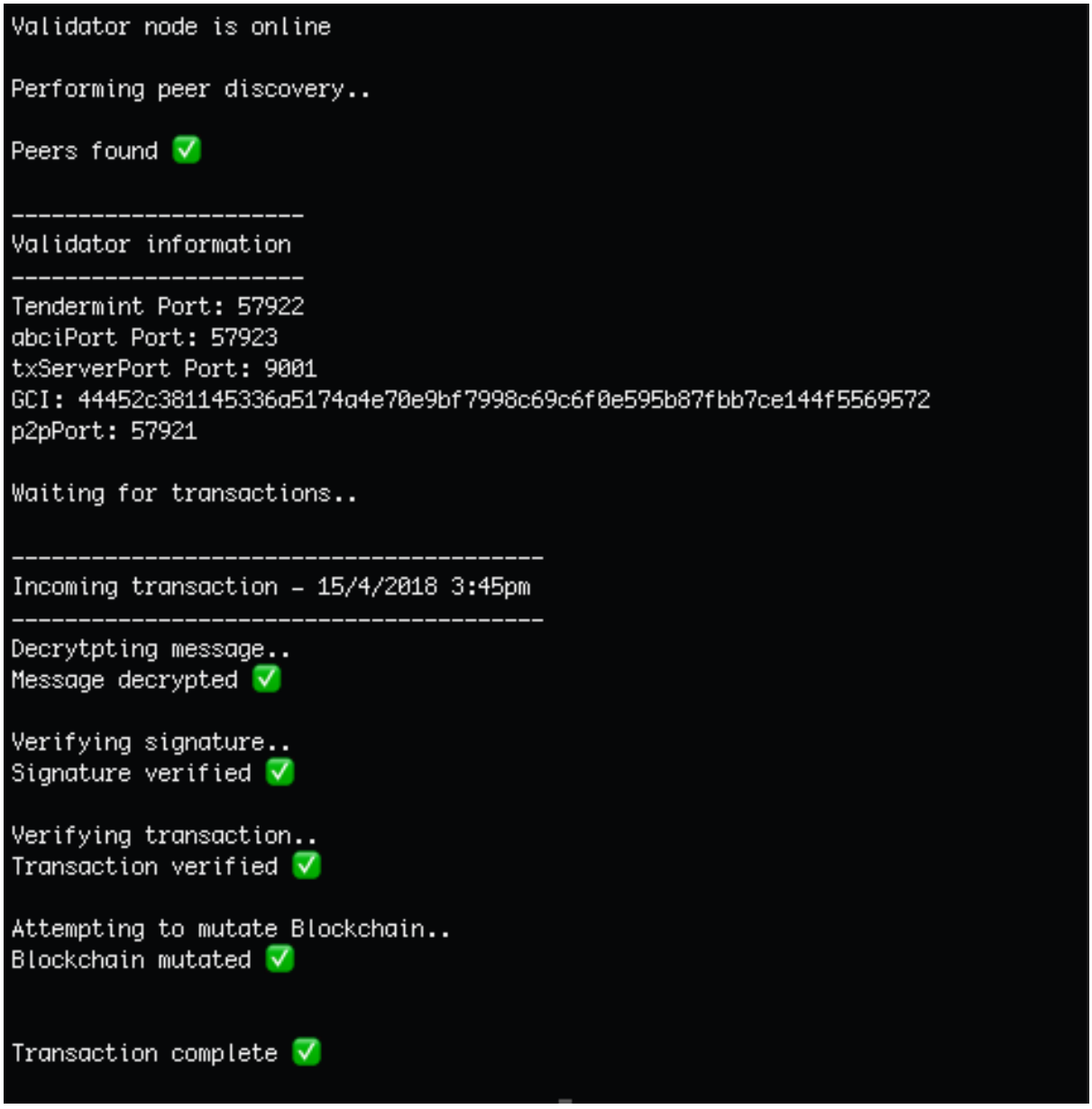

Figure 5.6 Validator Node

5.6 System Testing

The implemented system was developed using the Agile software methodology and tested using Agile testing. This is an approach where the system is tested for any performance issues and glitches. This testing approach was continuously applied during the development process to make sure during each subsequent iteration the changes and features were well implemented.

5.6.1 Compatibility Testing

Compatibility testing was carried out to make sure that the developed mobile application is compatible with both the Android and iOS platforms. To make the mobile application accessible to most users, it was developed for both Android and iOS platforms. To determine its compatibility, the mobile application was tested on Android devices from software version 4.4 to 7.1.2 and iOS software version 9.0 to 11.0. The mobile application passed all compatibility tests and users are able to use the application across all the tested software versions.

Android Platform Compatibility Testing

Table 5.1 Android Platform Compatibility Test

Android Version	Compatibility Status
Android 4.4 - 4.4.4 (KitKat)	Yes
Android 5.0 - 5.1.1 (Lollipop)	Yes
Android 6.0 – 6.0.1 (Marshmallow)	Yes
Android 7.0 – 7.1.2 (Nougat)	Yes

iOS Platform Compatibility Testing

Table 5.2 iOS Platform Compatibility Test

iOS Version	Compatibility Status
iOS 9.0	Yes
iOS 10.0	Yes
iOS 11.0	Yes

5.6.2 Usability Testing Results

The developed solution was tested by a local export company in Kenya called Chriven Enterprises. This company was selected for testing as they have multiple touchpoints in their supply chain and have been in the export business for over 7 years. The company provides the necessary supply chain work experience required for this research. A usability and validation questionnaire was prepared and distributed to 15 respondents and the data visualized using Google Sheets.

Usability testing was conducted to determine whether the application was user friendly. It was used to ascertain that users could navigate through and understand the applications functionality. The major things that were tested included: Signing up, generating a public address, scanning a product, creating distributions and verifying distributions. All 15 respondents were able to perform these actions within the application, obtaining a 100% success rate for each of the tested actions.

Signing Up

As illustrated in Figure 5.7, all the respondents were able to successfully sign up and generate a pair of RSA keys.

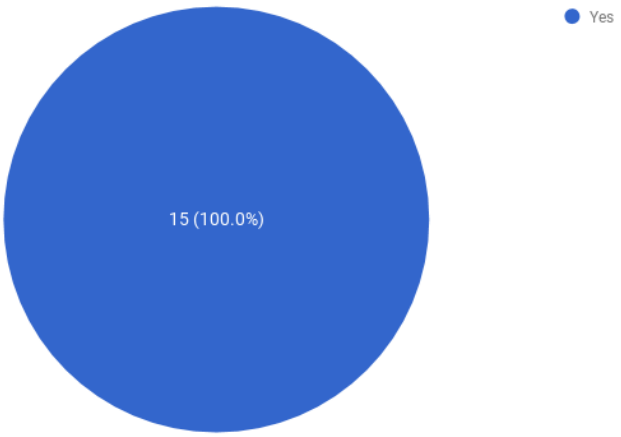

Figure 5.7 Signing Up

Generating a public address

As depicted in Figure 5.8, all the respondents were able to successfully generate their public address that they used to create and verify distributions.

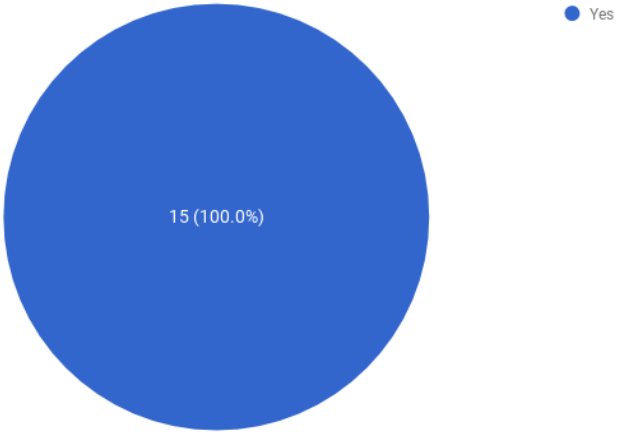

Figure 5.8 Generating a public address

Scanning a product

As shown in Figure 5.9, all respondents were able to use their phones to scan QR Codes to verify its authenticity.

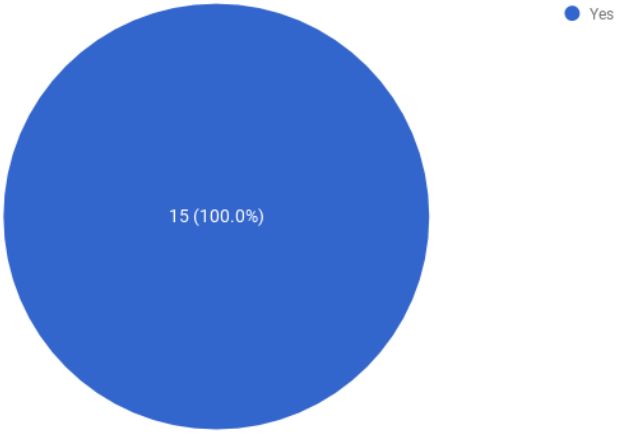

Figure 5.9 Scanning a product

Creating and verifying distributions

Using their public addresses and pair of RSA Keys the all the respondents, as shown in Figure 5.10, were able to create and verify multiple distributions.

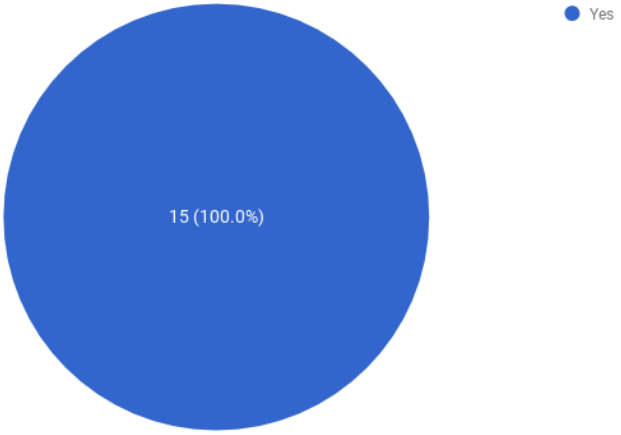

Figure 5.10 Creating and verifying distributions

5.6.3 Validator Nodes Accuracy and Response Rates

To test the accuracy and response rates of the validator nodes, two remote servers and two local computers were used. The first test was conducted to determine how fast the validator nodes would achieve consensus and the second test was to determine the accuracy of the data stored in all computers. A total of twenty test cycles was performed for each of the tests. The goal for this test was to ensure that every validator node is able to perform the consensus procedure accurately and each have an exact copy of the distributed ledger.

The test involved carrying out different transactions from the mobile application and recording the results. Transactions tested includes: creating distributions, verifying distributions and creating products. All validator nodes were able to achieve consensus during each test cycle and have an identical copy of the distributed ledger. Due to the Proof-of-Stake algorithm, consensus was achieved, on average 1.2 seconds in each test cycle.

Validator Nodes Accuracy

Figure 5.11 shows that during the twenty rounds of testing the validator nodes achieved 100% accuracy, meaning the data stored across all nodes were identical after each transaction.

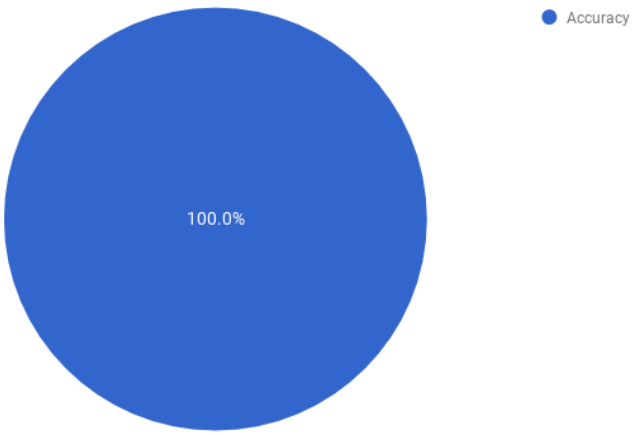

Figure 5.11 Validator Nodes Accuracy

Validator Nodes Response Rate

Figure 5.12 shows the fluctuation of time taken by validator nodes to achieve consensus. From the testing done it take s on average 1.2 seconds for the validator nodes to achieve consensus. The reason for the fluctuation is varying Internet connection speeds among the different nodes.

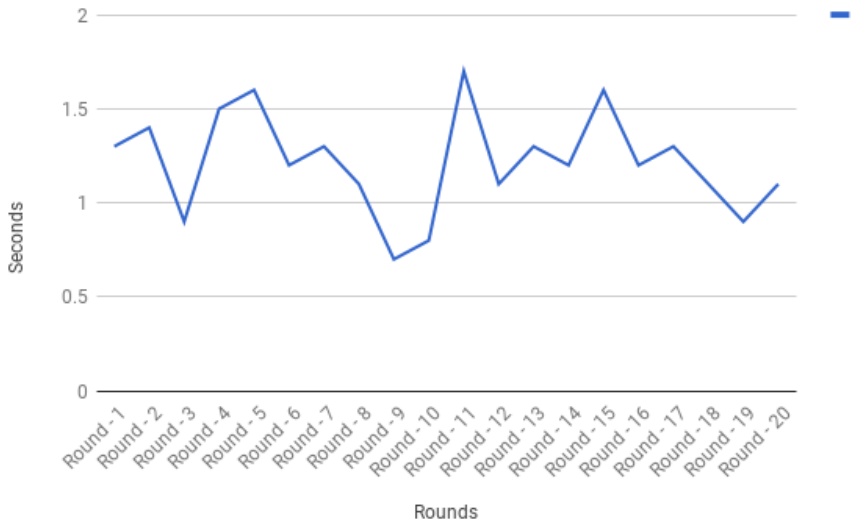

Figure 5.12 Validator Nodes Response Rates

5.7 Validation

Validation was carried out so as to check whether the implemented system addressed the challenges that existed as far as providing a decentralised system of trust within supply-chains. A questionnaire was designed and distributed among the 15 respondents in Chriven Enterprise to validate whether the solution developed improves their supply chain logistics by providing transparency to their stakeholders and end consumers.

After extensive use of the developed solution, as shown in Figure 5.13, 100% of the respondents validated that the proposed system improved their supply chain logistics.

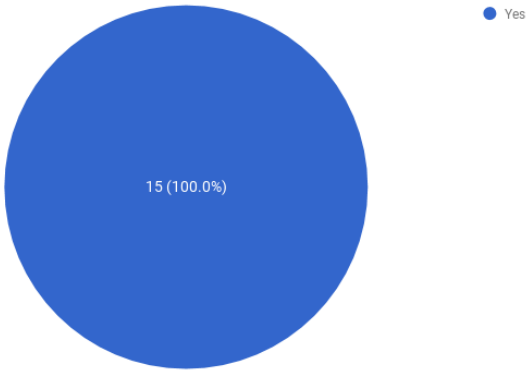

Figure 5.13 Does the solution improve supply chain logistics

The respondents were then asked whether they would recommend developed system to other companies. As illustrated by Figure 5.14, 100% of the respondents concluded that they would indeed recommend the system to various other companies.

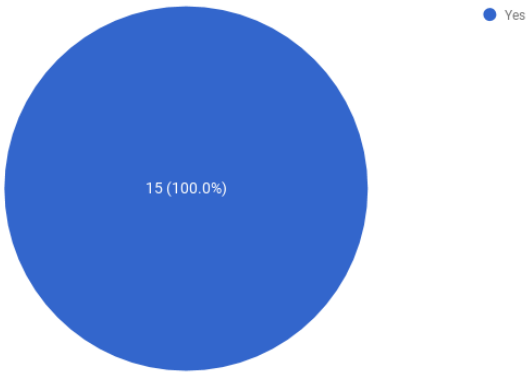

Figure 5.14 Recommendation of the developed solution

5.8 Conclusions

The system design process gave information on how the mobile application and Blockchain implementation was done. All the research objectives were also considered so as to ensure that the system implemented met the user requirements of potential users. The entire system was implemented based on the objectives.

CHAPTER 6: DISCUSSION OF RESULTS

6.1 Introduction

This chapter reviews how the research objectives were achieved by mentioning the findings that were obtained and the achievements. It also reviews the solution that was developed and mentions its advantages and disadvantages.

6.2 Findings and Achievements

In order to develop a viable solution, the results from the research conducted were used to identify the most appropriate technology. One of the objectives of this research was to develop a Blockchain based supply chain management system that improved traceability and verification of products. As covered in Chapter 2, Blockchain technology allows multiple remote client side computers to maintain a digital ledger (Tapscott & Tapscott, 2016). This allows all transactions made from the developed supply-chain system to be decentralise and prevent single points of failure due to its distributed architecture.

The mobile application developed allowed manufacturers to create products, send and receive distributions as well as track their products as they propagate through the market. Distributors are able to manage their distribution channels by sending and receiving distributions and verifying the authenticity of the goods that they transact with. Retailers are able to verify incoming shipment and finally consumers have the ability to trace the movements of their purchased products, verifying its authenticity.

Achieving the aforementioned advantages required extensive testing and iteration from user feedback from different stakeholders in a supply chain. To test the effectiveness of the solution, the mobile application was used to manage a shipment of agricultural products in a local Kenyan export company called Chriven Enterprises. The company was chosen due to the availability of multiple touchpoints in their supply chain.

The mobile application's usability among 15 different respondents was tested. 100% of the respondents were able to verify a products authenticity by simply scanning a QR Code and viewing results. 100% of the respondents validated the implemented system improved their supply chain logistics and they also concluded that they would recommend the solution to other companies. These findings show how effective the different supply chain stakeholders found

the developed solution to be. In addition, the respondents proposed several new ways to track different shipments.

6.3 Review of Research Objectives in Relation to the Mobile Application

In reference to section 1.3, the first objective of this research was to identify common supply chain management challenges. According to the study done in Chapter 2, traditional supply chains suffer from lack of transparency, traceability trust that stem from a lack of a decentralised point of reference. The challenges identified facilitate the introduction of counterfeit and illegal products into a market than can have serious health and economic implications for a given market.

The second objective was to review existing blockchain based supply chain management solutions and platforms. According to the study done in literature review section, the already existing Blockchain based supply chain systems e.g. Provenance and Everledger have excelled in their implementations and are currently being used to provide transparency to their consumers. It is from this basis that creates a gap for a more robust Blockchain supply chain system that is capable of scaling and adapting to multiple kinds of supply-chains.

The third objective was to design, develop and test a mobile application used for supply chain management based on Blockchain technology. The developed mobile application performs transactions on a single node, that broadcasts the requested transaction to the network of nodes. Each node contains its own separate copy of the supply-chain information and participates in consensus when validating transactions. As a result the supply-chain becomes decentralised and anyone with a computer is able to start verifying its transactions by running the validator program. The mobile application was tested by distributing a usability questionnaire to 15 respondents.

The final objective was to validate the effectiveness of a mobile application for supply chain management by measuring the accuracy and response rates. This was done by performing accuracy and response rates testing on the different validator nodes and usability tests done by the professional BETA testers. The validator nodes in all testing cycles achieved consensus in 1.2 seconds and all had the same information stored, achieving 100% accuracy. Response rate feedback from the professional BETA testers was also taken into consideration. 93.33% of the respondents found the applications core functionality which is verifying and tracking distributions and products to be the most useful feature in the application. Some of the

respondents provided valuable feedback that was incorporated within the application and are looking forward for conducting more trials before adopting the solution.

6.4 Advantages of the Application

Compared to the current centralised trust mechanism that existing supply-chain systems have, the proposed solution offers a decentralised trust mechanism where all supply-chain information is held on a network of validator nodes. This provides users and supply-chain stakeholders the necessary transparency they need to trace and verify the authenticity of distributed products as the data stored on these nodes cannot be tampered with by a malicious third party for their own self-interest. To further enhance transparency, anyone with a computer can easily become a validator node, validate transactions and view the state of the Blockchain by simply running the validator program. The proposed solution utilises the Proof-of-Stake algorithm which not only makes conducting transactions nearly instantaneous but saves energy by eliminating the process of mining that is used by typical Blockchains for purpose of singing blocks.

6.5 Limitations of the Application

The current system requires all product to have unique identifiers. This requires manufacturers to generate QR Code beforehand and attaching it to their products. Secondly only users with mobile phones running either Android or iOS operating system can use the solution. The mobile application solely relies on validator nodes to perform transactions which requires a network of nodes to be available to validate a particular transaction.

CHAPTER 7: CONCLUSIONS, RECOMMENDATIONS AND FUTURE WORK

7.1 Introduction

In this chapter, conclusions, recommendations and future work are discussed. As for the conclusions, all the objectives are reviewed briefly by looking at how the research questions were answered. In recommendation, the researcher gives some recommendations to users and stakeholders of the system. Future work entails something that was not implemented in the system but can be implemented in the future.

7.2 Conclusions

This research found out that Blockchain technology can be used to manage supply chains by providing a transparent and trusted way for users to trace the origins of their products. It is able to provide a supply-chain the necessary transparency that would give consumers confidence in the products they purchase and in-turn cause a reduction of counterfeit goods that are in the market. The study exposes the shortcomings of the current centralised trust mechanism that traditional supply-chains employ and how counterfeit products are introduced to the market because of it.

The challenges identified in traditional supply chains led to the development of a Blockchain based supply chain management system that enables transparency and enforces integrity. As a result of this, information is stored in a network of computers connected using Peer-to-Peer Gossip protocols for communication and consensus making. This facilitates anyone with a computer to start validating transaction by running the validator program. Agile software development methodology was used to develop the system because it allows for iterative build in terms of requirements such that the final build supports all the features needed by the customer. Testing and validation was done using a questionnaire that was distributed to 15 respondents.

7.3 Recommendations

Counterfeit goods are a serious problem in our country. It damages economies and in more cases than not lead to health hazards. This stems as a result of the centralised trust mechanism that are in place with existing supply-chains. Having a decentralised trust mechanisms ensures the integrity of the data stored and provides transparency to the supply-chain stakeholders. From the finding of this research, users obtain more confidence and have a sense of security in products they buy if they have a sure way of determining whether a product is authentic. This

in turn can lead to a brand being trusted more due to the fact that the provide transparency of how they manage their distributions. Therefore, my recommendation is that manufactures should adopt this system in order to manage the quality of their supply chain and provide their consumers with the necessary transparency they require. The mobile application can be downloaded for free on both Android and iOS stores by users and stakeholders of a supply chain. They can set up validator nodes so as to maintain the integrity of the Blockchain.

7.4 Future Work

The researcher has identified features and enhancements that can be used to expand the proposed solution. The proposed solution consists of a single mobile application that is used for the creation and verification of a distribution. To enhance this a web application can be developed to manage larger supply-chains. The proposed solution utilises a restful design to instantiate transaction. This restful frameworks can be used by IoT (Internet of Things) devices and system for automated transactions and verifications. A public key infrastructure can be developed to manage and verify public addresses of users.

REFERENCES

Allison, I. (2016, January 13). *Provenance has a big year ahead delivering supply chain transparency with Bitcoin and Ethereum*. Retrieved February 22, 2018, from http://www.ibtimes.co.uk/: http://www.ibtimes.co.uk/provenance-has-big-year-ahead-delivering-supply-chain-transparency-bitcoin-ethereum-1537237

Baker, R. (2017). *Transnational Crime and the Developing World.* Global Financial Integrity.

Bell, D. (2004). *UML's Sequence Diagram.* IBM, IT Specialist. IBM.

BitFury Group. (2015). *Proof of Stake versus Proof of Work.* San Francisco: BitFury Group.

Buterin, V. (2015). *A Next Generation Smart Contract & Decentralized Application Platform.* Ethereum.

Chipman, M. (2013, 4 23). *The future of the QR Code in Supply Chain Marketing*. Retrieved February 22, 2018, from TSB Supply Chain: http://www.tsbsupplychain.com/news/the-future-of-the-qr-code-in-supply-chain-marketing#.WuKwKlOFNhE

Crosby, M., & Pattanayak, P. (2015). *BlockChain Technology: Beyond Bitcoin.* Sutardja Center for Entrepreneurship & Technology, Berkeley Engineering. Berkeley: Sutardja Center for Entrepreneurship & Technology.

Daniel Tse, B. Z. (2017). *Blockchain Application in Food Supply Information Security* . University of Hong Kong, Department of Information Systems, Hong Kong.

Danielsson, W. (2016). *React Native application development.* Linköping: Linköping University.

Deloitte UK. (2016). *What is a blockchain?* London: Deloitte UK.

Engelberg, D., & Seffah, A. (2002). *A Framework for Rapid Mid-Fidelity Prototyping of Web Sites.* Concordia University, Human-Centred Software Engineering Group. Toronto: Kluwer Academic Publishers.

Ergın, E. A. (2010). *The rise in the sales of counterfeit brands: The case of Turkish consumers.* Cankaya University, Department of Management. Yukarıyurtçu Mahallesi: frican Journal of Business Management Vol. 4(10).

Felici, M. (2011). *Use Cases.* School of informatics.

Francisco, K., & Swanson, D. (2018). *The Supply Chain Has No Clothes: Technology Adoption of Blockchain for Supply Chain Transparency.* University of North Florida, Department of Marketing & Logistics, Florida.

Global Trade. (2017, 11 20). *How is Technology Enhancing Supply Chain Management?* Retrieved February 22, 2018, from Global Trade Mag:

http://www.globaltrademag.com/global-logistics/infographic-technology-enhancing-supply-chain-management

IBM. (2016). *Transform supply chain transparency with ibm blockchain.* New York: IBM.

IBM. (2018). *IBM Blockchain Platform, Technical Overview* . New York: IBM.

JDA Software. (2017). *About JDA Software*. Retrieved February 22, 2018, from JDA Software: https://jda.com/about

Kieseberg, P. (2016). *QR Code Security.* Wien: SBA Research.

Kwon, J. (2014). *Tendermint: Consensus without Mining.* San Francisco: Tendermint.

L. , M., & K., M. (n.d.). *Is it the End of Barcodes in Supply Chain Management?*

Lamport, L. (1982). *The Byzantine Generals Problem.* SRI International. New York: ACM Transactions on Programming Languages and Systems (TOPLAS) .

Lele. (2017). *LELE Whitepaper.* LELE community.

Li, J. (2010). *Agile Software Development.* Technische Universitt Berlin. Berlin: Technische Universitt Berlin.

Lu, D. D. (2011). *Fundamentals in supply chain management.* Ventus Publishing Aps.

Mallo, J., Barnes, J., & Bowers, T. (2004). *Business Law: The Ethical, Global, and E-commerce Environment.* Indiana: McGraw-Hill/Irwin, 2004.

Marr, B. (2018, March 23). *How Blockchain Will Transform The Supply Chain And Logistics Industry*. Retrieved February 22, 2018, from Forbes: https://www.forbes.com/sites/bernardmarr/2018/03/23/how-blockchain-will-transform-the-supply-chain-and-logistics-industry/#44b0daad5fec

McCathie. (2005). *Is it the End of Barcodes in Supply Chain Management?* United Arab Emirates: University of Wollongong.

Mulay, A. (2013, 11 10). *Decentralize to Improve Supply Chain Efficiency*. Retrieved February 22, 2018, from Ebnonline: https://www.ebnonline.com/author.asp?section_id=3315&doc_id=268703

Munassar, A., & Govardhan, A. (2010). *A Comparison Between Five Models Of Software Engineering* . Jawahrlal Nehru Technological University, Principal JNTUH of Engineering College. Hyderabad: Jawahrlal Nehru Technological University.

Nakamoto, S. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System.* Satoshi Nakamoto.

New, S. (2010, 10). *The Transparent Supply Chain*. Retrieved February 22, 2018, from Harvard Business Review: https://hbr.org/2010/10/the-transparent-supply-chain

Oracle. (2016). *The future for cloud-based supply chain management solutions.* California: Oracle.

Patroba, H. (2015). *China in Kenya: Addressing Counterfeit Goods and Construction Sector Imbalances.* Johannesburg: South African Institute of International Affairs.

Pollinger, Z. (2008). *Counterfeit Goods and Their Potential Financing of International Terrorism.* Harvard University.

Roberts, J. (2017, September 12). *The Diamond Industry Is Obsessed With the Blockchain*. Retrieved February 22, 2018, from http://fortune.com/: http://fortune.com/2017/09/12/diamond-blockchain-everledger/

Robinson, A. (2015, 10 14). *Uses of Supply Chain Technology Applications Moving Shippers into the Future of Effective Management*. Retrieved February 22, 2018, from Cerasis: http://cerasis.com/2015/10/14/supply-chain-technology-applications/

Rouse, M. (2016, December). *RESTful API.* Retrieved February 22, 2018, from techtarget.com: https://searchmicroservices.techtarget.com/definition/RESTful-API

SAP. (2017). *SAP ERP*. Retrieved February 22, 2018, from SAP: https://www.sap.com/africa/products/enterprise-management-erp.html#item_0

SCRC SME. (2003, 5 11). *Trust in Supply Chain Relationships: What Does It Mean to Trust*. Retrieved February 22, 2018, from Supply Chain Resource Cooperative: https://scm.ncsu.edu/scm-articles/article/a-sustainable-energy-platform-for-the-eu-and-the-world-2

Seebacher, S., & Schüritz, R. (2017). *Blockchain Technology as an Enabler of Service Systems: A Structured Literature Review.* Karlsruhe Institute of Technology, Kaiserstr. Karlsruhe: Karlsruhe Institute of Technology.

Simantov, M. (2018). *Proof of Stake.* New York: Ethereum.

Staake, T., & Fleisch, E. (2008). *Countering Counterfeit Trade: Illicit Market Insights, Best-Practice Strategies, and Management Toolbox.* Zurich: Springer Science & Business Media.

Tao, Y. (2015). *Entity Relationship Diagram.* Chinese University of Hong Kong, Department of Computer Science and Engineering. Hong Kong: Chinese University of Hong Kong.

Tapscott, D., & Tapscott, A. (2016). *Blockchain Revolution: How the Technology Behind Bitcoin Is Changing Money, Business, and the World.* New York: Pengiun Random House, LLC.

Tar, A. (2018, Jan 17). *Proof-of-Work, Explained.* Retrieved Feb 19, 2018, from Cointelegraph: https://cointelegraph.com/explained/proof-of-work-explained

Tutorials Point Pvt. Ltd. (2016). *Supply Chain Managament.* India: Tutorials Point Pvt. Ltd.

Vasin, P. (2017). *BlackCoin's Proof-of-Stake Protocol v2*. https://blackcoin.co.

Wood, D. G. (2018). *Ethereum: A Secure Decentralised Generalised Transaction Ledger.* San Francisco: Ethereum.

Wright, A. (2015). *Decentralized Blockchain Technology and the Rise of Lex Cryptographia.* Yeshiva University, Benjamin N. Cardozo School of Law, New York.

APPENDICES

Appendix A: Usability and Validation Questionnaire

*Required

Section A: Usability Testing

A1. Were you able to sign up? (Choose One)*

- o Yes
- o No

A2. Were you able to generate your public address? (Choose One)*

- o Yes
- o No

A3. Were you able to scan a product? (Choose One)*

- o Yes
- o No

A4. Were you able to create a distribution? (Choose One)*

- o Yes
- o No

A5. Were you able to verify a distribution? (Choose One)*

- o Yes
- o No

A6. If any of your answer above is 'No' please list the problems you encountered?

A7. How would you rate the whole application? (Choose One per row)*

	Poor	Fair	Good	Very Good	Excellent
Navigation	o	o	o	o	o
User Interface & Experience	o	o	o	o	o
Core functionality	o	o	o	o	o
Responsiveness	o	o	o	o	o

A8. What feature did you find most useful?

A9. Do you have any suggestions, comments and recommendations about this application?

Section B: Validation

B1. Does the developed solution improve your supply chain logistics?

- Yes
- No

B2. Would you recommend this application to other companies?

- Yes
- No

Thank you for your time.

Appendix B: Extra Application Screenshots

Onboarding Tutorial

Figure B.1 shows an onboarding tutorial for new users. It displays, in 3 transitions, all the basic functionalities they should expect from the application.

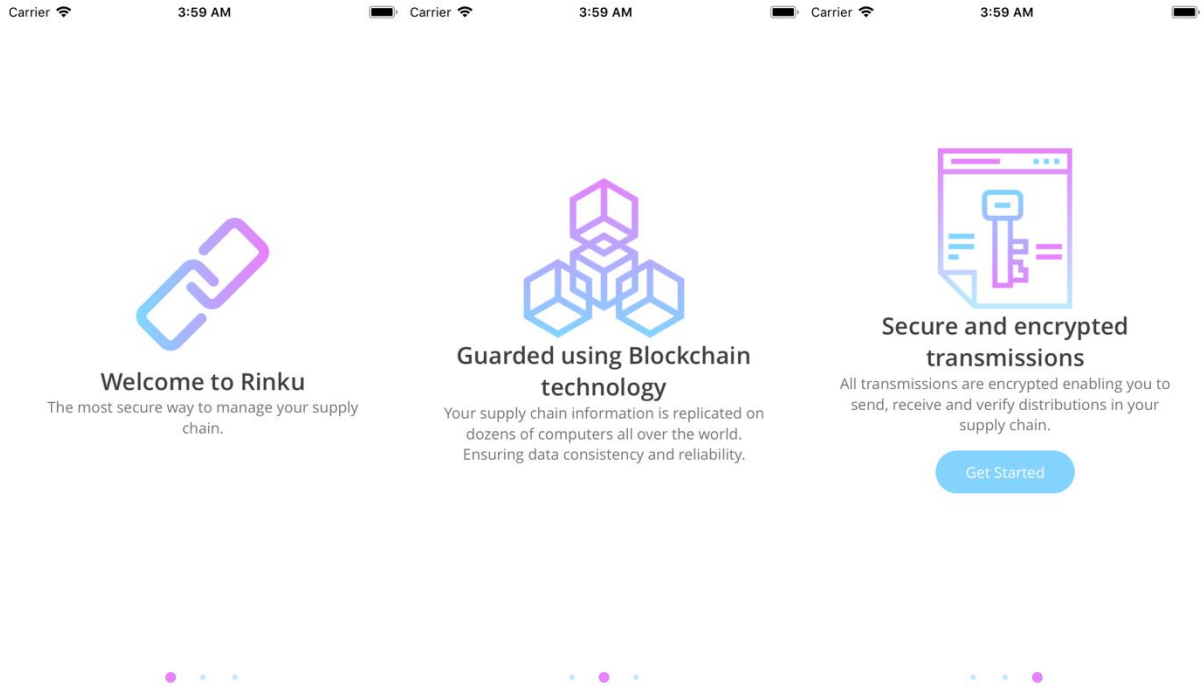

Figure B.1 Onboarding Tutorial

Application Settings

Figure B.2 shows the settings section of the application where the user can choose to turn off fingerprint authentication, logout and copy their public address to their clipboard.

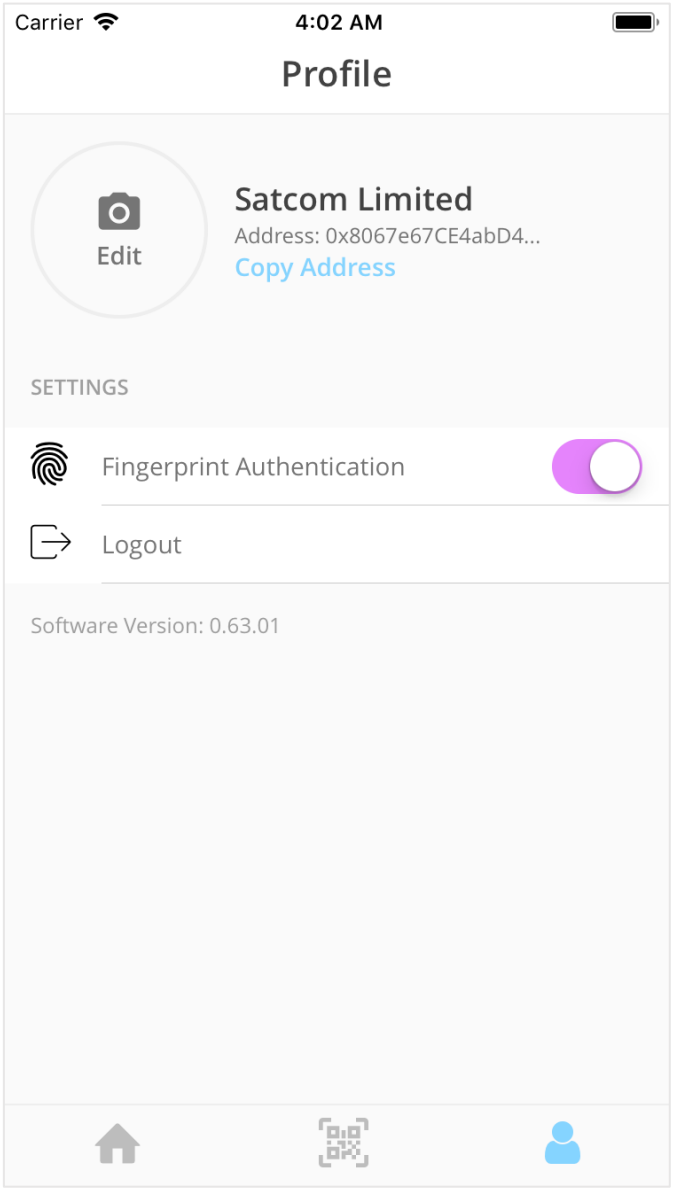

Figure B.2 Application Settings

Biometric Authentication

Figure B.3 shows how the mobile application utilises biometric fingerprint authentication to login the user.

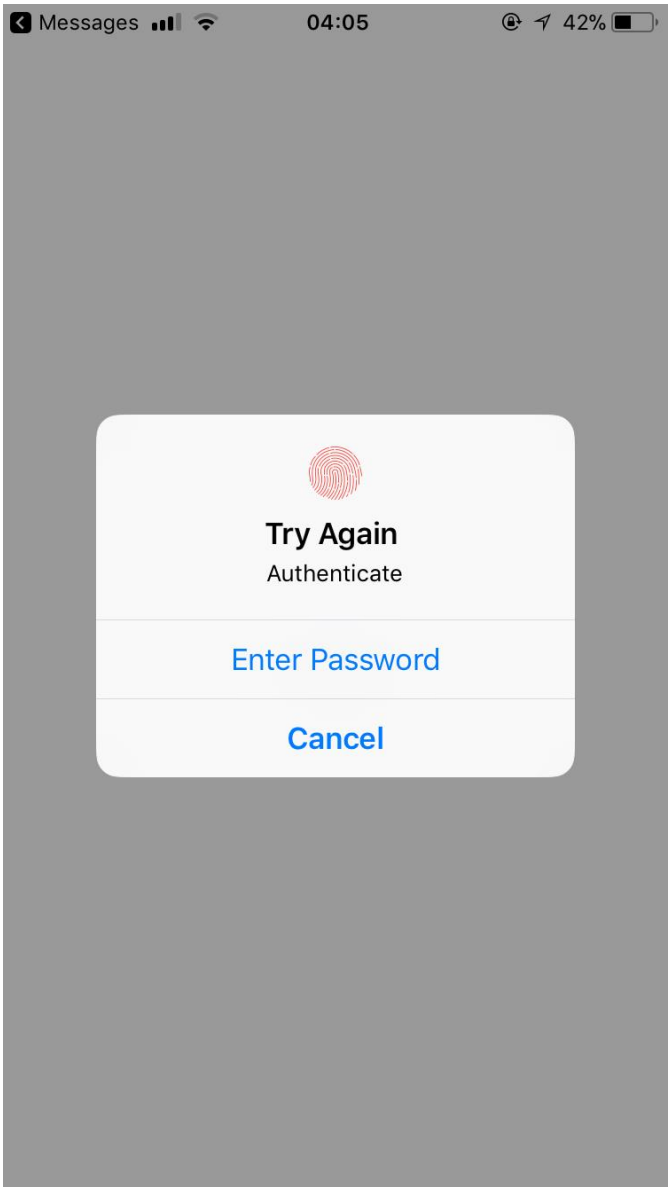

Figure B.3 Biometric Authentication

Appendix C: Turnitin Report

Figure C.1 shows the originality report from the Turnitin online application.

Figure C.1 Turnitin Report