2020

An agency core banking application using blockchain technology.

Kamau, John Kibathi
Faculty of Information Technology
Strathmore University

AN AGENCY CORE BANKING APPLICATION USING BLOCKCHAIN TECHNOLOGY

By

John Kibathi Kamau

111001

A Thesis Submitted to the Faculty of Information Technology as a partial requirement for the award of a Master degree in Information Technology.

November 2020

DECLARATION AND APPROVAL

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.

John Kibathi Kamau

…….....

Wednesday, 11 November 2020

Approval

The thesis of John Kibathi Kamau was reviewed and approved by the following:

Dr. Joseph Orero, PhD

Senior Lecturer,

Faculty of Information Technology,

Strathmore University.

Dr. Bernard Shibwabo,

Director of Graduate Studies,

Strathmore University

ACKNOWLEDGEMENTS

It is with great honour that is take this opportunity acknowledge the support I have received from my supervisor Dr Orero, in the various stages culminating to this research proposal.

His words of wisdom and advice led to the successful completion of this project. I also acknowledge my family for their immense help, advice and encouragement. I also acknowledge the moral support from my friends and colleagues for their relenting support. I am grateful and thankful to them all.

DEDICATION

This project is a dedication to my parents Mr & Mrs James Kibathi Kamau and my brothers Alan and Patrick for their support & encouragement during the preparation of this project. May God bless them in abundance.

TABLE OF CONTENTS

TABLE OF FIGURES

ABBREVIATIONS

ATM - Automated Teller Machine

CBK - Central Bank of Kenya

KYC - Know-Your-Customer

POS - Point-of-Sale

VPN – Virtual Private Network

CBS – Core banking system

DES -Algorithm – Data Encryption Standard

DNS – Domain Name System

DOS – Denial of Service

DDOS – Distributed Denial of Service

SQL – Structured Query Language

PCI DSS - Payment Card Industry Data Security Standard

OS – Operating System

POW - proof-of-work

PBFT - Practical Byzantine Fault Tolerance.

ABSTRACT

Cut throat competition between various institutions in the financial sector in Kenya particularly banks have pushed them into adopting innovative ways to serve their customers and generate revenue. One of the innovations that banks have come up with is the use of agency banking channels to serve their customers. This channel has proved to be very successful of over the years since its launch and has seen many banks take up the channel. However, this channel has opened up a new avenue for frauds and theft by criminals. This has pushed the banks into adopting new security techniques to combat these criminals. Software related security mechanisms have been installed to curb fraud for example the use of Encryption techniques such as Data Encryption Standard (DES) encryption. Although it has shown great promise in securing end to end connection with the bank servers, Data Encryption techniques have multiple weaknesses that we hope the adoption of block chain technology will resolve. The purpose of this project was to come up with an agency banking application that will use block chain technology to assist banks in curbing the vice of fraudulent transactions initiated by fraudulent cards. The model works by replacing the current architecture is use and replacing it with one that uses block chain technology. In order to secure agency banking transactions, the transactions are stored in an immutable ledger which are then chained together to form the block chain. The block chain forms the database because it stores information in a digital ledger in data structures referred to as blocks. In the model, every bank maintains a copy of this Ledger to form a decentralized system that is more secure as opposed to the existing one that is central and is prone to security breaches. This blocks use hashing algorithm to identify each transaction securely. The network is a permissioned network hence only authorized nodes are allowed to process transactions. The model was tested and a transaction was sent to from an agent's point of sale network to the peer to peer network to the validating nodes where it was successfully validated and the result want sent to the customer via the agent Point of Sale terminal.

INTRODUCTION

1.1 Background

Cut throat competition amongst financial institutions in Kenya particularly banks have pushed them into adopting more and more innovative ways to serve their customers and generate revenue. These innovations include use of ATMs, Prepaid and post-paid debit cards, credit cards, mobile lending via mobile banking, zero interest accounts and finally the latest which forms the basis of our study which is agency banking (Barasa & Mwirigi, 2013).

The agency banking model is a form of alternative banking system, in which banks provide banking services via non-bank agents (Central Bank of Kenya, 2013). This may include local grocery shops, supermarkets, stalls, pharmacies or kiosks. The channel allows banks to extend their established services to areas where they don't have the capacity to create a fully operational branch, especially in rural and remote areas where a relatively large percentage of people remain unbanked. Agency banking particularly in the rural areas has become the primary use of accessing banking facilities in the absence of bank branches. Agency banking ensures efficient and quick access to banking facilities away from the presence of banks in those areas (Barasa & Mwirigi, 2013). A licensed financial institution such as a bank is involved in the provision of financial services through a retail agent to its clients. Usually, the bank offers these customer-friendly products and services in branches, however it also delegates the responsibility of service delivery of the same to an agent (Vutsengwa & Ngugi, 2013).

Agency banking has yielded great results since it was introduced in the banking industry way back in 2010 boasting higher traffic than banking halls and wide range of banking services previously found only in banking halls (Vutsengwa & Ngugi, 2013). Brazil is often recognized as a global pioneer in this field since it was an early adopter of the agency banking model and over the years has grown larger and developed a network of agent banks covering more than 99% of the country's municipalities (Alliance for Financial Inclusion, 2012). Other countries in Latin America which have done the same, include Mexico (2009), Peru (2005), Colombia (2006), Ecuador (2008), Venezuela (2009), Argentina (2010), and Bolivia (2006) (Alliance for Financial Inclusion, 2012).

With the increased traffic of agency banking transactions, frauds such as card skimming, card theft, have increased excessively in recent years (Gichungu & Oloko, 2015). Fraud detection & prevention techniques include analysing of the spending

patterns and behaviour of bank customers. This particular problem is now affecting the new agency banking channels affecting customer experience and business for bank agents alike.

1.2 Problem Statement

Traditional database technology is also prone to various threats including, accidental losses, theft and fraud, loss of privacy and confidentiality, loss of data integrity and availability, Malware, Ransomware, brute force attack and stolen or unsecured backups. Agency banking software relies on applications that make use of various database technologies. In this new approach, we seek to improve database security using blockchain technology.

Blockchain introduces digital immutable ledgers that that guarantee data integrity. Also blockchain stores this ledgers in peers or nodes that ensure availability. Coupled together with existing authentication techniques will ensure unauthorized access to the data stored in the blockchain is not permitted.

1.3 Objectives

1.3.1 Aim

The main aim of this project is to create an application that will secure agency banking transactions by introducing block chain technology meaning that transactions will now be stored in an immutable ledger which is more secure.

1.3.2 Specific objectives

i) To investigate the problems associated with the current agency banking
ii) To analyse how block chain can be implemented in agency banking and its security applications within the banking sector.
iii) To develop an application that will use block chain technology to secure data storage in agency banking database and curb fraud.
iv) To test the success of the proposed agency banking block chain application.

1.4 Research Questions

This research will answer the following investigative questions.

i.) What are the problems associated with agency banking security protocols?
ii.) Can block chain technology be used to secure transaction in an agency banking database?

iii.) Can the agency banking blockchain solution be constructed using open source integrated development environments thereby reducing the initial cost of procuring an agency banking application for banks?

iv.) How is the proposed block chain application to be tested?

1.5 Justification

This research will assist in developing an application that will be used by banks to transact on the agency banking platform securely.

There are many cases whereby there has been loss of customer account data and consequently has costed the organization heavy legal fees and fines worth millions of shillings. Including the brand damage associated with these breaches. Sometimes the institution that was processing cardholder data recently passed a Payment Card Industry (PCI) audit and was subsequently certified. Payment Card Industry Data Security Standard (PCI DSS) is a one off audit and unfortunately, sophisticated cybercriminals nowadays continue to find ways to work around this audit.

Banks that are aspiring to enter this space will be able to use the application to secure the agency banking transactions and increase the feasibility to invest in agency banking. The application will also assist aspiring banks to reduce the amount of security capital they require to invest to achieve maximum profitability without wastage.

1.6 Scope and Limitation

The purpose of this research is to create an application using block chain technology that addresses information security as well as securely stores agency banking transactions in a blockchain. This will provide a minimum set of requirements that must be adhered to during the storage of agency banking related data.

2 LITERATURE REVIEW

2.1 Introduction

This section looks at a theoretical literature review of blockchain-based applications across multiple use cases. The goal is to examine the current state of blockchain technology, its various implementations as well as demonstrate how agency banking activities in Kenya can be revolutionized by features of this disruptive technology. Based on these findings, we shall determine the various research gaps and future areas of study that are anticipated to be of significant value to both for agents and customers alike.

2.2 Agency Banking in Kenya

The agency banking model is a form of alternative banking system, in which banks provide banking services via non-bank agents (Central Bank of Kenya, 2013). This may include local grocery shops, supermarkets, stalls, pharmacies or kiosks. The channel allows banks to extend their established services to areas where they don't have the capacity to open a fully operational branch, especially in rural and remote areas where a relatively large percentage of people remain sparsely populated. In recent years since its introduction in 2010, agency banking has been adopted and implemented by many developing countries, particularly within East Africa and Latin America (Central Bank of Kenya, 2011).

Agency banking model was first introduced in Kenya in 2010 as one of the alternate banking channels (Central Bank of Kenya, 2011). Since then, various banks in Kenya have embraced the agency banking channel with the numbers growing to 13 commercial banks by the end of September 2013 which represents 29% of the 44 banks. Other banks which have registered for agency banking are yet to roll out the channel. This expansion of the use of information technology to offer banking services away from traditional banking halls as well as increased investment by telecommunication companies in Kenya has led to the adoption of agency banking across the country with banks using various trading names such as Equity Bank (Equity Mashinani), Kenya Commercial Bank (KCB Mtaani), Post Bank (Benki Yangu), Cooperative Bank (Co-op KwaJirani). This has been authorized by central bank of Kenya (CBK) to offer services on behalf of the institution, (Central Bank of Kenya, 2010). Most of these banks are local banks, which shows that main international banks in Kenya like

Standard Chartered and Barclays have not yet ventured into this mode of banking channel. This particularly favours retail banks because of their high volume of transactions and customer numbers. Investments banks may not find it feasible to invest or venture into agency banking because of their clientele**.**

Various other countries including Latin America have adopted agency banking including Ecuador (2008), Mexico (2009), Argentina (2010), Colombia (2006), Venezuela (2009), Peru (2005), and Bolivia (2006) (AFI, 2012).

A link exists between the number of years of experience a country has with introducing agent banking and the number of agents the country has (Rizzo, 2017). Using only years of experience as a predictive variable between these limited samples of five countries the linear regression model indicates that one country will gain 0.69 additional agents per 10,000 adults for each additional year of experience. While Mexico has fallen short of the projected number of agents in its first year (2010), it is expected to exceed the anticipated number of agents in 2011. (Central Bank of Brazil, 2010)

Kenya has approximately 9,000 bank agents with a smaller adult population than Mexico, this signifies nearly four agents per every 10,000 adults in Kenya (Central Bank of Kenya, 2010). Kenya attributes its quick start to the already developed network of agents used in Kenya's highly successful mobile banking model, M-PESA, whereby agency banking borrowed in the initial implementation of the agent banking model (AFI, 2012).

2.3 Risks and challenges associated with agency banking

According to Mas's (2009) work on the economics of branchless banking, some agents have been found to disclose customer information to third parties. The bank has a duty of confidentiality with respect to customers and a violation of that obligation has led customers to take legal action against the parent banks. Security and trustworthiness has been termed as one of the most important factors when deciding on the use of a banking service delivery channel (Valluri, 2012).

Lack of mobile network services is another challenge that agency banking is experiencing. Agency banking requires a strong connection to the internet in order for the terminal to connect to the banks servers via the banks VPN.

Issues of card security is another agency banking challenge (Mwirigi, 2013). Insecurity comes in very many formats including fraudsters. This has led many

investors to shy away from the agency banking business. Lastly is the fear of robbery. Unlike branches which usually have armed security guards on standby. Agencies do not share this luxury. They have to rely on quick response alarms, watchmen, strong rooms which have often in the past proved to be inefficient at deterring criminals from stealing money (Barasa, 2013).

The main objective of this agency banking blockchain application is to increase the level of security of the platform by storing this transaction in a block chain instead of the conventional database.

2.4 Block Chain Technology

Well-known implementations of public blockchains include Bitcoin, Ethereum, Litecoin and, in general, most cryptocurrencies (Nakamoto, 2008, Haferkorn and Quintana Diaz, 2015). In private blockchain, the main applications include database management, auditing and, in general, performance demanding solutions (Zheng et al., 2016). The modern internet deals with assets, which we consider most valuable. These assets can be stored in encoded form on a peer to peer network chain called a block chain or ledger, where each participant shares transaction information transparently (Barasa, 2013). This decentralized block chain system is going to change the way we use data and information including business or personal, all the way to the way we use our Internet of Things devices (IOT), conduct political elections, public transport, and even personal authentication It will also change banks and other financial institutions, hospitals, companies and governments among other industries along the way.

A block chain-based point-of-sales solution could bring more reliability and traceability to the agency banking business. There are some application areas whereby block chain has already proved to be very successful. In the application of Point of sale systems, Information related to billings, taxes, and customer's ratings and finally inventory can be stored and distributed across the blocks within the chain (Cachin, 2015). Smart contracts may be used trigger processing of incoming data and to ensure taxes, regulations, and other compliance guidelines are maintained before any transaction occurs.

2.5 Block Chain Technology Algorithm in Agency banking

Each agent bank in the block chain will store a copy of the ledger. Since it is decentralized, a block chain-based structure will take protection further, making it harder for hackers to identify and exploit single vulnerability points currently found in

the existing agency banking architecture (Faruk, 2013). The customer's account information is stored immutably on a distributed ledger, and the connection can be supported by immutable smart contracts between agents and agency banks. Usually, the block chain is run by a peer-to-peer network working together to solve complex mathematical problems to validate new blocks in the network (Swanson, 2015). Once maintained in the agency banking network, the data cannot be changed in any given block without modifying all subsequent blocks, which requires approval from most of the agent banks in the agency banking network. This is the key reason why the agency banking block chain application is safe and not hackable or breakable. All block chains use a hash which are long series of random strings used to track block chain transactions (Swanson, 2015). This was incorporated in the model to secure the agency banking network.

2.5.1 Insecure DNS

DNS is presently largely centralized. Therefore, hackers can break into the connection between point of sale terminals and bank servers and wreak havoc. They can route point of sale terminals to scam servers to steal card data or simply make an agent of a group of agents unavailable (Atandi, 2013). They can also combine DNS attacks with DDoS attacks to make bank servers unusable for prolonged time. The current most effective solution to such problems is tailoring log files and allowing real-time alerts for suspicious network activities. The customer's data can be stored intact on a distributed ledger and making it more secure from this type of attack

2.5.2 Identity and Access Management

Blockchain identity management does not just stop at user identities but also extends to Point Of Sale devices and services. To facilitate machine to machine (M2M) communication securely will require reliable protocols to establish trusted access control between Point Of Sale devices and network resources. The Point Of Sale device will be uniquely identifiable to enable authenticity and prevent security breaches.

2.5.3 Database Management

Data, is already known as the universal currency. Traditional databases storing data including storing customer related data use CRUD (Create, Read, Update, and Delete) operations (Xiawei, 2008). By comparison, the block chain only allows transactional data to be appended and retrieved in a block chain, so the data cannot be removed erroneously. Under the new agency banking model, every node has access to

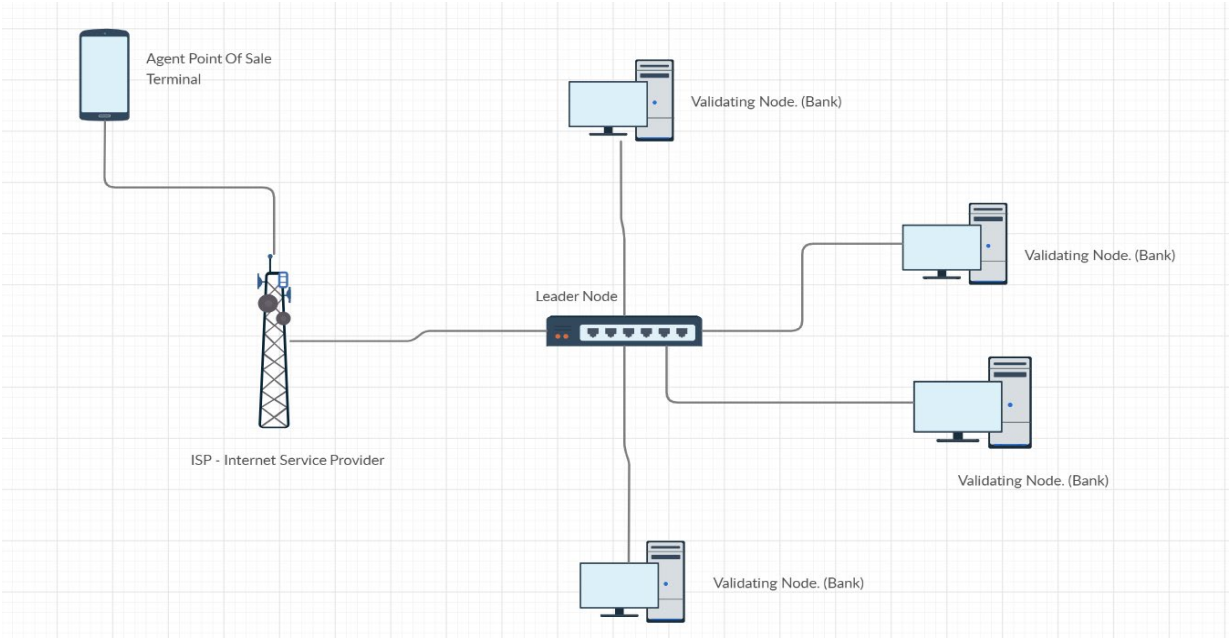
a ledger and can test and verify if the ledger has been tampered with or whether the transaction was improperly changed in any of the blocks. It would be achieved by determining the hash value of the block data mathematically and then comparing it to the previous hash value stored in the next block.

2.5.4 Securing Edge Devices with Authentication.

Block chain technology can help secure Point of Sale devices. Point of Sale devices will be designed to communicate with private block chain nodes in the cloud over a protected API in the proposed model. Incorporating block chain technology into a Point of Sale system allows Point of Sale devices to safely discover each other, encrypt machine-to-machine transactions using distributed key management techniques, and verify software update validity and authenticity, and policy changes.

2.6 Conceptual Framework

The conceptual framework above illustrated the new blockchain based agency banking application. The solution seeks to bring together various components to secure agency banking transactions. As shown above the agent will be able to access the blockchain network using the point of sale terminal which will be running an application which we have developed. The solution will take input from the customer and send the transaction to the agency banking network via an internet connection provided by the internet service provider. From there, the transaction will be received by the leader node who will then forward the same to the validating nodes who will then mine the transaction and add it in the blockchain. The process of mining starts when new transactions are propagated and advertised to all nodes (Agent banks). Then, every miner node collects new transactions into a block. The nodes then look for proof of work. When a node finds a proof of work it broadcasts the block to all nodes. Nodes accept the block if the transactions in it are valid and not already spent. Nodes accept the block by working on creating the next block in the chain, using the hash of the accepted blocks in the previous hash.



2-1 Agency Banking Conceptual Framework

3 RESEARCH METHODOLOGY

3.1 Introduction

This chapter discusses the methods used to perform the study as well as the design and implementation of the proposed security policy as well as the research design, location of study, targeted population, sampling design, data collection tools, pilot testing and finally data analysis.

3.2 Research Design

This study uses a Causal-comparative or quasi experimental. A causal-comparative design is a research design that seeks to find relationships between independent and dependent variables after an action or event has already occurred (Neil J. Salkind, 2010). The researcher's goal is to determine whether the independent variable affected the outcome, or dependent variable, by comparing security that is offered by blockchain and the security that is offered by the current encryption methods .

Causal-comparative research design is appropriate for this particular research due to the fact it allowed analysis and relation of variables. This is a cross-sectional study (can involve one-time interactions with banks and their agents) as opposed to longitudinal study (study that usually follow these individuals over a given period of time).

3.3 Location of the Study

The study is conducted in Nairobi which is where the participating has their head office. Agency banking is also more popular here than in any other county in Kenya. This will assist it taking into account that card fraud can take place in any part of the country

3.4 Target Population and Sampling

The target population is the specific population about which information is desired. According to (Gschu, 2004), a population is a well-defined collection of individuals, facilities, items, events and community of things or households under investigation. The target population are the people of Nairobi county who are the most technologically advanced people in the country and among them there are high tech fraudsters who have the knowledge to carry out information technology based attacks on the agency banking platform, includes the all the stakeholders of the agency banking industry including bank agents, customers and agent banks.

This study involved 2 sample financial institutions; each institution will have 5 participants. Namely, one customer, an agent, bank manager, agent bank and system

administrator. The total number of the people who shall be involved in this study are 10.

3.5 Data Collection

Sample transactions will be initiated from a point of sale terminal. These transactions will enable us to observe the movement of data through the agency banking block-chain solution and analyse its effectiveness in encrypting as well as secure transmission of transactional data. (Erickson and Wiedersheim, 1997) state that there are two sources of data: primary sources and secondary sources. The selection of an appropriate method of data collection depends on the research problem, design and categories of data requirements. The study used primary data.

The Primary source of date is the transaction that will be initiated by the customer at the agent's premises using the agent's point of sale terminal. Primary data is collected to allow the researcher document a report on how well the system was able to meet the objectives that were set out in the first chapter. This was collected from the experiment setup that the researcher had proposed and had been actualized as shown in the next chapter.

This data was collected through observation of the results that were displayed by the tkinter application interface written in Python language. This primary data was collected and was used to make sense of the research and prove its a liability as the expected outcome, the researcher compared it to the already existing knowledge in the field of information and agency banking network security to see if the system was able to enhance knowledge in the area and to the conformed the set of standards as guided by the industry regulator which is the Central Bank of Kenya.

3.6 Data Analysis

To this end we used encryption to achieve the following 3 principles: Accountability, Confidentially and Integrity.

When a user creates a transaction record as the POS, he/she encrypts their data with his private key and post the data to Block chain Database. Block chain Database API decrypts the data with the user's public key. In this process, the user's identity has been confirmed. It achieves the objective of accountability and confidentially.

Block chain Server API calculates the transaction hash value with nonce, i.e. random string, and the previous hash. Block chain Database API inserts the

transaction, nonce and hash to the database. To detect any unauthorized change, Block chain Database API re-calculates the hash value based on the information of the previous hash, transaction and nonce. When any changes are made the hash value will change and inform the API. Then the data integrity would be guaranteed.

3.7 System Development Methodology

The methodology I propose to use in this model is the waterfall methodology. In a Waterfall model, each phase must be completed before the next phase can begin and there is no overlapping in the phases.

In "***The Waterfall***" methodology, the entire software development process was split into different phases. The one-step outcome acted as the reference to the next process. This means that every stage in the development cycle has been decided by the completion of the previous phase. The waterfall model is a design process whereby progress is seen as flowing steadily waterfall through the phases of Conception, followed by Analysis process, Elicitation, validation step, specification step, Design process, Construction, Testing, Production or Implementation and finally Maintenance.

3.7.1 System Analysis

During this stage we propose to go through the following steps:

i.) Elicitation step:

During the Elicitation step, we gathered the requirements from the banks using a questionnaire. Then, the specifications of the agency banking application were captured and documented in a requirement specification document.

The tool I used for this step is the use case diagram. This tool helped to visually show the system's engagement with its users.

ii.) **Validation step**

During the Validation step is where the "analysing" actually started. The main purpose of this step was to ensure information conveyed during elicitation will accurately represent expectations of the researcher and stakeholders. The research here involved consolidating the security criteria used in agency banking, rationalizing them, searching for overlaps and differences and developing templates to aid with process visualization.

The tools I used for this step is the validation board. The tool was useful for a systematic and active way to set goals and make decisions about whether we should proceed with the idea or pivot.

iii.) **Specification step**

During this step, we prioritized and formally documented the requirements properly in a Requirements Definition Report. This specifications were numbered allowing monitoring during the rest of the lifecycle. They were also be reviewed to ensure they can be verified.

iv.) **Verification step**

This was the final step in the process of collecting requirements, and includes verifying documented requirements accurately and communicating the client's needs and expectations. We developed acceptance criteria during this phase, and started writing test cases for the final solution.

3.7.2 System Design

This is the stage where the gap between the problem domain and the current structure was bridged. We converted the SRS document into a format that was implemented in this phase and decided how the system will operate. We divided the system development activity into several smaller activities that we coordinated with one another to achieve the main goal of system implementation.

i.) **Identify system goals**

This goals include the objectives and the functionalities that the banks will want from the proposed system.

ii.) **System decomposition**

In this step we sub divided complex problem of the system into smaller parts that are easier to work with. These smaller parts were examined and designed individually, making them more manageable. This included the architectural elements, interface design elements, component level elements and deployment level elements

iii.) **Hardware allocation**

In this phase we identified the system's core physical components and how they are interrelated. This helped us to design and better understand how their

components fit into the system architecture and provide important information to software designers about software creation and integration.

iv.) **Data management**

After the system design stage was complete we achieved the following outputs:

- The new program includes technology and organizational improvements.
- A data schema in the form of a blockchain.
- A functional hierarchy diagram and web page map that describes the program structure in a graphical way.
- Pseudo code for each of the modules in the program.
- A working prototype for the proposed agency banking blockchain system.

3.7.3 System Implementation

Here we ensured that the alternate banking system was operational. And a simulated delivery of the new systems to the agent banks was done. This allowed will allow users i.e. business teams to take over its operation for use and evaluation in the real world environment. The activities to be expected in the real world scenario would involve training the front end and backend users to handle the system, piloting of the new solution with agents, file conversion of existing files stored in the traditional database will be added into the blockchain and lastly conduct a Post-Implementation Evaluation Review (PIER).

3.7.3.1 Programming Language: Python

Python is used because it is a high-level, interpreted and dynamic programming language used globally for scripting that focuses on code readability. The Python syntax helped us code in less steps compared to another programming language like C++. Python is relatively easy to learn hence training of new users and system administrators will be easier once new banks adopt the model. Since it is very clear and straightforward, it will be easy to understand the program code. It is both free and open-source. This will help keep the project costs lower.

Cross-platform - It on most operating systems like Microsoft Windows, Linux, and Mac OS X. hence fewer integration challenges will be experienced.

3.7.3.2 Star UML – software modelling tool

This is an open source software tool that supports UML used for modelling. We used this tool during the design phase to create the software modelling diagrams that was used to model the software. It was also used because it has excellent extensibility and since its open-source, this helped keep the project costs lower

3.9 Research Quality

The quality of the research was guaranteed in the following ways

3.9.1 Relevance

Relevance was identified based on the significance and relevance of the aims, procedures, and results of the research project to the context of the agency banking security problem. This includes the appropriateness of the questions being posed, their results and the scope of the research discussed in relation to the issue of the agency banking.

3.9.2 Credibility

The study findings are reliable, and the knowledge it has produced is scientifically reliable. This includes explicit proof of data adequacy, explanation of well-presented methods and analysis of the findings.

3.9.3 Legitimacy

Steps have been taken to ensure end-users view the testing process as fair and ethical. That is, it will be acceptable and trustworthy. This includes the correct consideration of various principles.

3.9.4 Effectiveness

We have undertaken to ensure that this research will contribute positively in the security problem within the agency banking space. At the proposal stage and during the research process, the study was evaluated through: a strong and articulated aim to resolve and contribute to the systemic security issue facing agency banking. The establishment of a systematic research process was set and objectives in relation to the agency banking problem context, and the continuous reflection on the usefulness of the research findings in relation agency banking product.

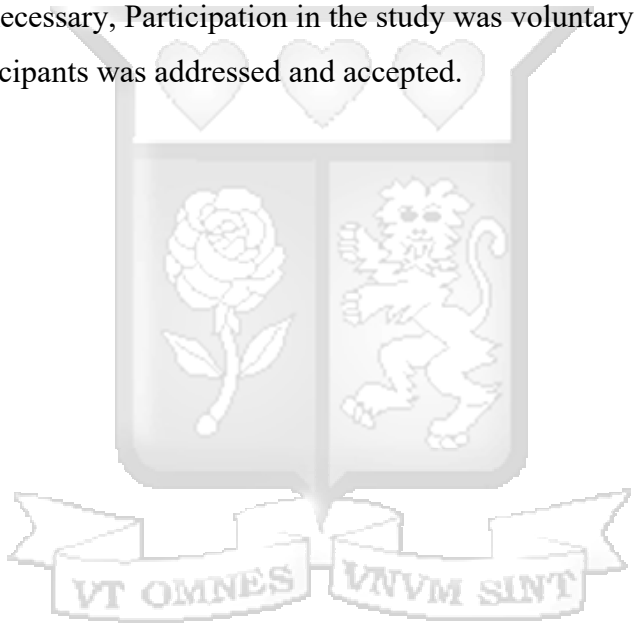
3.9.5 Ethical Considerations

This research project was carried out in full accordance with the research ethics norms and specifically with the defined codes and practices established within the national commission for science technology and innovation's Statement of Ethical

Practice and the LSE Research Ethics Policy. The research involved human participants and conducted a face-to-face door-to-door survey of the effects of the research problem.

The researcher took on a greater obligation to explain in depth what the study was about for all the participants concerned. Every research participant obtained a one-page detailed 'project information sheet' that describes the study's purpose, its undertaking and as well as financing, and how the research findings it will be distributed and utilized.

The project information sheet includes contact details in case any participants need additional information or they may wish to withdraw their participation in the project at any time further, it explained how anonymity and confidentially would be observed. Where necessary, Participation in the study was voluntary and informed consent of all participants was addressed and accepted.



4 SYSTEM ANALYSIS AND DESIGN.

4.1 Introduction

This chapter elaborates on the steps under taken by the researcher during the design and implementation phase of the project. This chapter starts by looking at the requirement analysis, which encompasses a discussion of the functional and non-functional requirements of the system. The chapter analyses the optimal environment for setting up the system for securing agency banking transactions using block chain technology. This discussion is supported by the analysis of the security engines the researcher used i.e. Block Chain. Finally, the research outlines the system operations in a series of use case and sequence diagrams.

4.2 Requirement Analysis

The project aims to model a system that is designed to meet the set of requirements as described below. This model is a System to secure agency banking transactions using block chain technology. This requirement analysis is based on the findings in the literature review. The researcher came up with requirements which were based on their actions, abilities, and testability.

4.2.1 Functional Requirements

1. The system should be able to allow users to create custom rules on the peer to peer network.
2. The system should be able to detect and flag any suspicious traffic on the network.
3. The system should be able to store the store the transactions in an immutable ledger.
4. The system should allow the interface with agency banking blockchain system to display the transaction logs on a web interface

4.2.2 Non-Functional Requirements

1. The system should have fewer downtimes because the proposed system is designed to work on a peer-to-peer network. All nodes on the network will store a copy of the ledger which will allow the creation and customization of rules and to be able to implement the rules on incoming transactions from the POS terminal at all times.
2. The system should be able to respond to the incoming transactions in a timely manner. The researcher foresees a quick response time whereby the system

will be deployed and tested so as to not experience any further latency added to the transaction processing time.

3. The system should be scalable. This means that after implementation, the system can be ported with very minor modifications to any bank that wishes to adopt this application. The fact that the researcher demonstrated the operation of the system on a virtual machine, it is pre-empted that the system would still work the same way when plugged in to a real-world scenario.

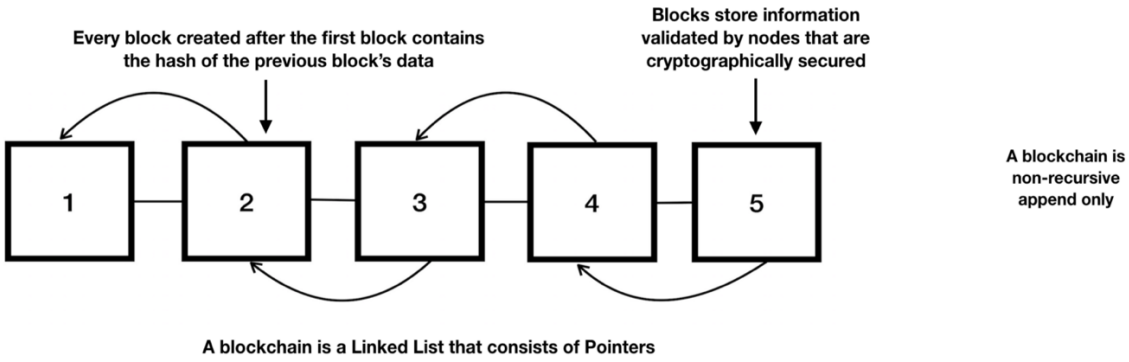
4.2.3 Environment to Secure Agency Banking Transactions using Block Chain Technology

In order to come up with this System that secures agency banking transactions using block chain technology, the researcher needed a platform that provides an opportunity for customizing of the security tools in use. The system was implemented in a windows based environment running windows 10. The choice of the environment was made based on the flexible nature of the OS and its ability to allow supporting components to be integrated with other security tools and features so as to build the agency banking application. In this work, we used Pycharm which is an open-source IDE for python which can be used to construct a distributed ledger platform for running smart contracts in a modular architecture.

4.3 Block Chain Analysis and Architecture

A block chain is a database because it stores information in a digital ledger in data structures referred to as blocks. Transactions were stored in this blocks to further enhance their security.

The agency banking blockchain stores information in uniformly sized blocks. Each block contains hashed information derived from the previous block this way it provides cryptographic based security. The hashing within these blocks uses SHA256 which is usually one-way hash function. This hashed information contains data as well as digital signature from the previous block, and these hashes of previous blocks goes all the way backwards to the first block produced in the blockchain which is referred to as a “genesis block”. These information is passed through a hash function which points to the address of the previous block.



4-1 Agency Banking Block chain architecture diagram

4.4 Overview and Architecture of the Core Components of Agency Banking Blockchain

Here are the core agency banking blockchain architecture components that the researcher used:

- **Node** – Agent's Point Of Sale terminal and bank server within the blockchain architecture. This can also be referred to as the member node.
- **Transaction** –This forms the building block of a the agency banking block chain system that is initiated by the agent via the Point Of Sale terminal it contains, customer records, transaction information, etc. it serves as the purpose of the agency banking blockchain.
- **Block** – This is a set of immutable ledgers containing transactions. This data structure was utilized for storing a set of transactions uniformly which were distributed to all validating nodes in the network which is constituted by agent banks.
- **Chain** – This is referred to as a sequence of blocks uniformly placed in a specific order.
- **Miners** – This are the agent bank mining nodes which do block verification and validation process before adding any transaction information to the blockchain. Each agent bank independently stores a copy of the entire blockchain ledger
- **Consensus (consensus protocol)** – This is an agreed set of rules laid out by agent banks that was used to carry out agency banking operations.

Below shows exactly what is in an individual block in an agency banking blockchain. They include:

- Transaction and customer data
- the hash of the block
- the hash from the previous block

The data that is stored inside an individual block depends on the type of blockchain. In this particular instance, in the agency banking blockchain, the block stores data about the agent, client, receiver, sender, and the amount of float. A hash is a fingerprint that contains a long record consisting of digits and letters. Each block hash is generated using a cryptographic hash algorithm (SHA 256). This helps to identify each block in the agency banking blockchain structure. When a block is created, it automatically attaches a hash, while changes appended to a block affect the hash as well. These hashes assist to detect any changes in blocks thereby enhancing security. The last element within the block is the hash derived from the previous block. This creates a chain of blocks and is the core element supporting the agency banking blockchain architecture's cryptographic security. The very first block in a blockchain is unique in that, all confirmed and validated blocks come from the genesis block. Any attempt to make the blocks to change will result in all the following blocks to maintain incorrect information and ultimately render the whole blockchain system invalid this further enhances integrity.

On the other hand, in theory, it could be possible for hackers and fraudsters to adjust all the blocks with the help of powerful computer processors. However, there is a solution that eliminates this possibility known as the proof-of-work. This allows a user to slow down the process of creation of new blocks. In agency banking blockchain architecture, it takes around 3 minutes to determine the necessary proof-of-work and add a new block to the chain. This work is done by agent banks who act as miners who will get to keep the transaction fees from the block that they verified as a reward.

Each new bank that will be rolling out agency banking will be joining the peer-to-peer network as a new node and will go ahead and receive a full copy of the blockchain. Once a new block is created by an agent bank, it is sent to each of the nodes within the agency banking blockchain system. Then, each node or agent bank verifies the block and confirm if the transaction may be completed. If everything is

alright and all rules have been adhered to, the block is appended to the blockchain in each node.

All the agent banks which act as nodes inside the agency banking blockchain architecture create what is known as a consensus protocol. A consensus system can be defined as a set of network rules which everyone abides by and are self-enforced inside the agency blockchain. This architecture makes sure that agency banking blockchain technology immutable and cryptographically secure by eliminating any other third-parties. It is impossible to tamper with the integrity of the blockchain system; as it would be necessary to tamper with all of its blocks, recalculate the proof-of-work for each block, and also control more than 50% of all the nodes in the agency banking peer-to-peer network

4.5 Agency Banking Block Chain Transaction Management Overview

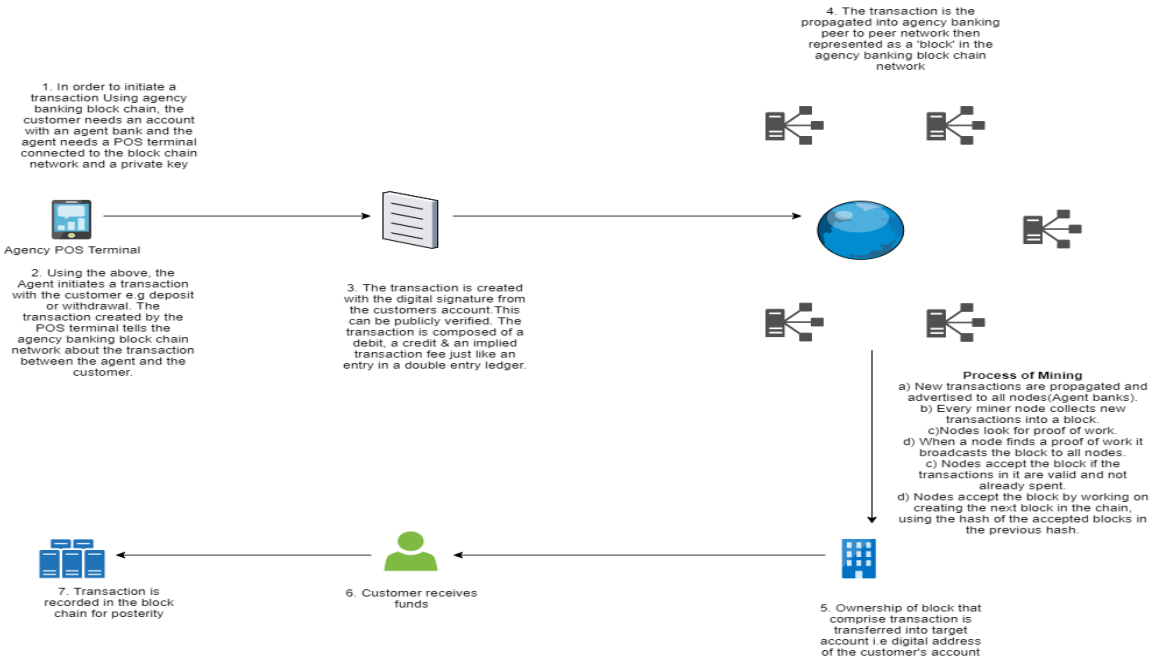
Computer servers that are in the various banks conducting agency banking business which function as mining nodes in the network are known as “miners” and they must compete with each another in order to find a value sourced from the hash function known as the nonce. The agency banking miners utilize their computing resources to solve this value, and this requires procurement of powerful computer hardware or servers by the banks. A protocol built into the blockchain was used to solve the value based on what is called the total hashing power in the network.

This means the more agency banks there are, the more miners they will be. Thereby translating to a higher level of difficulty. This is because with more miners, there will be more computing resources on the agency network which in turn increases the hashing power, measured in hashes per second. Once an agency bank has validated a block, they will receive a reward as an incentive for providing their computing resources to the agency network. The incentives are the motivation for agency banks to mine transaction blocks since they get rewards in the form of transaction fees which translated to profits for the bank. This is known as a Proof-of-Work consensus algorithm.

As shown above, a blockchain agency network uses a distributed network of nodes hosted by agent banks which are decentralized. This means that all agent banks on the agency network store a copy of the transaction blockchain. The nodes or agency banks, will store a complete copy of the blockchain as well as perform mining operations. There will be is no single administrator or core agency banking system to validate a block of transactions. Instead miners or agent banks that perform this

verification will be in place by solving cryptographic puzzles based on a difficulty level proportional to the combined agency banking's network hashing power available. Once the block has been added to the blockchain, this information is immutable and transparent to all agent banks. Blockchain transactions are non-recursive, hence they cannot be repeated once they have been validated into a block. A blockchain is also fault tolerant. If one or more nodes or agent bank is down, there will always be another agent bank or nodes available that run the blockchain. Another benefit of decentralizing agency banking is that it will be permission less and trust less, allowing people including customers, agents and banks who don't know or trust one other to conduct financial transactions. The blockchain provides trust through transparency by recording the transaction while providing a cryptographically secure way to exchange value.

4.6 Diagrammatic Representation of the Agency banking blockchain Network



4-2 Block Chain network

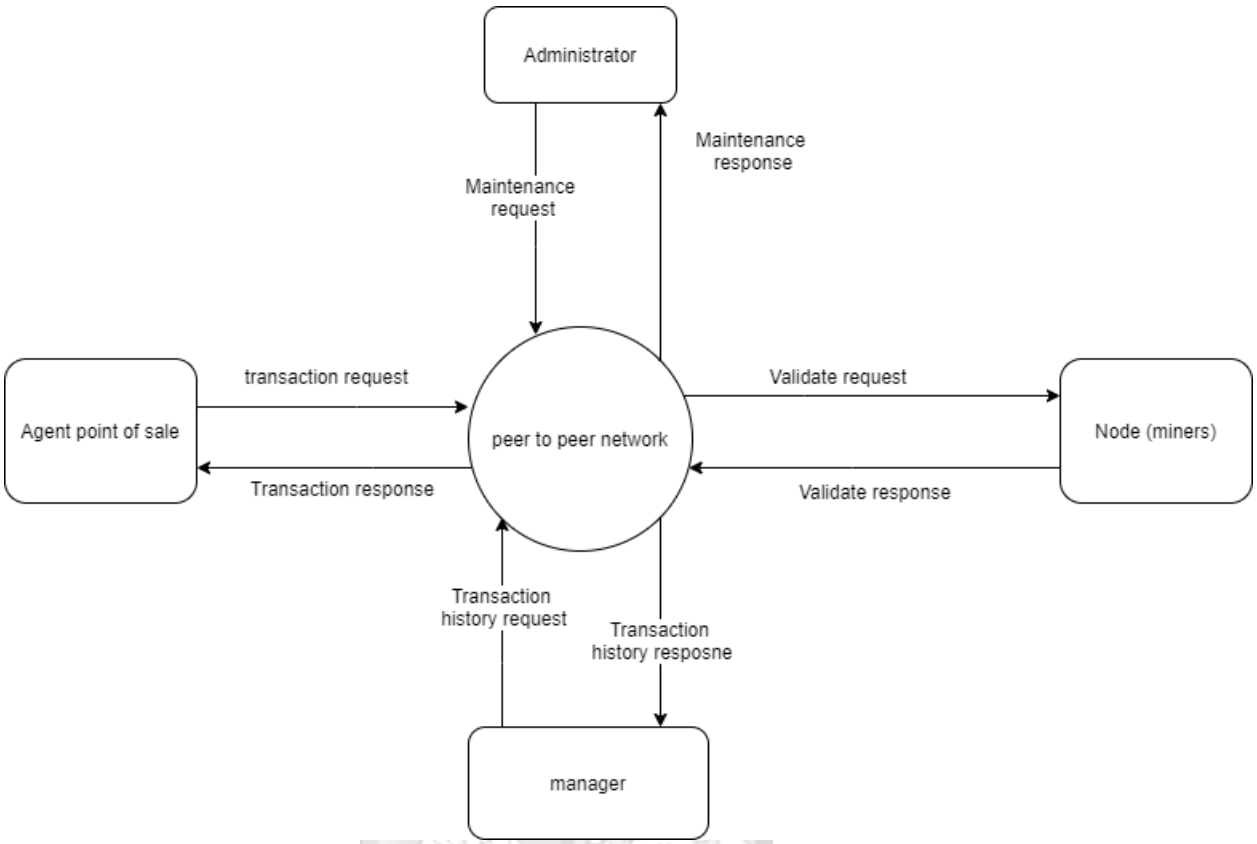
The figure 4-2 outlines the blueprint of the operation and design of the system. From the outlook, the researcher has presented the customer who initiates the transaction and an agent who connects to the network via a Point Of Sale terminal. This machine communicates to the peer to peer network running agency banking blockchain solution which connects to the application running in the mining nodes i.e. agent banks. The agency banking application is hosted in the mining nodes running Windows OS which is connected to all the agency banking blockchain components in

the blockchain networks on is fetch data and display the performance of the network which can be analysed by the researcher and present his findings.

4.6.1 System Architecture

In a public blockchain network for example as Bitcoin or Ether, anyone can join the blockchain network, which exposes the users to Sybil type attack. Bitcoin usually resolves problem this by making it computationally expensive for a peer to introduce a new block of transactions using proof-of-work (POW). Although crypto-currency is an established application of blockchain technology , its performance is limited, with time estimated to confirmation of a transaction estimated to be ten minutes or more, thereby achieving a high throughput of 7 transactions per second (K. Croman, C. Decker,2016). In the agency banking blockchain network, all the participants are whitelisted and bounded by strict contractual obligations and more efficient consensus protocols such as Practical Byzantine Fault Tolerance (PBFT) are in use (M. Castro and B. Liskov, Nov, 2002). PBFT works on based on the assumption that one-third or less of the peers are faulty (f), meaning that the agency banking network consists of at least $n = 3f + 1$ peers to accept f faulty peers. Thus $f=[(n-1)/3]$. The network therefore requires $2f + 1$ peers to come to a consensus on the block of transactions.

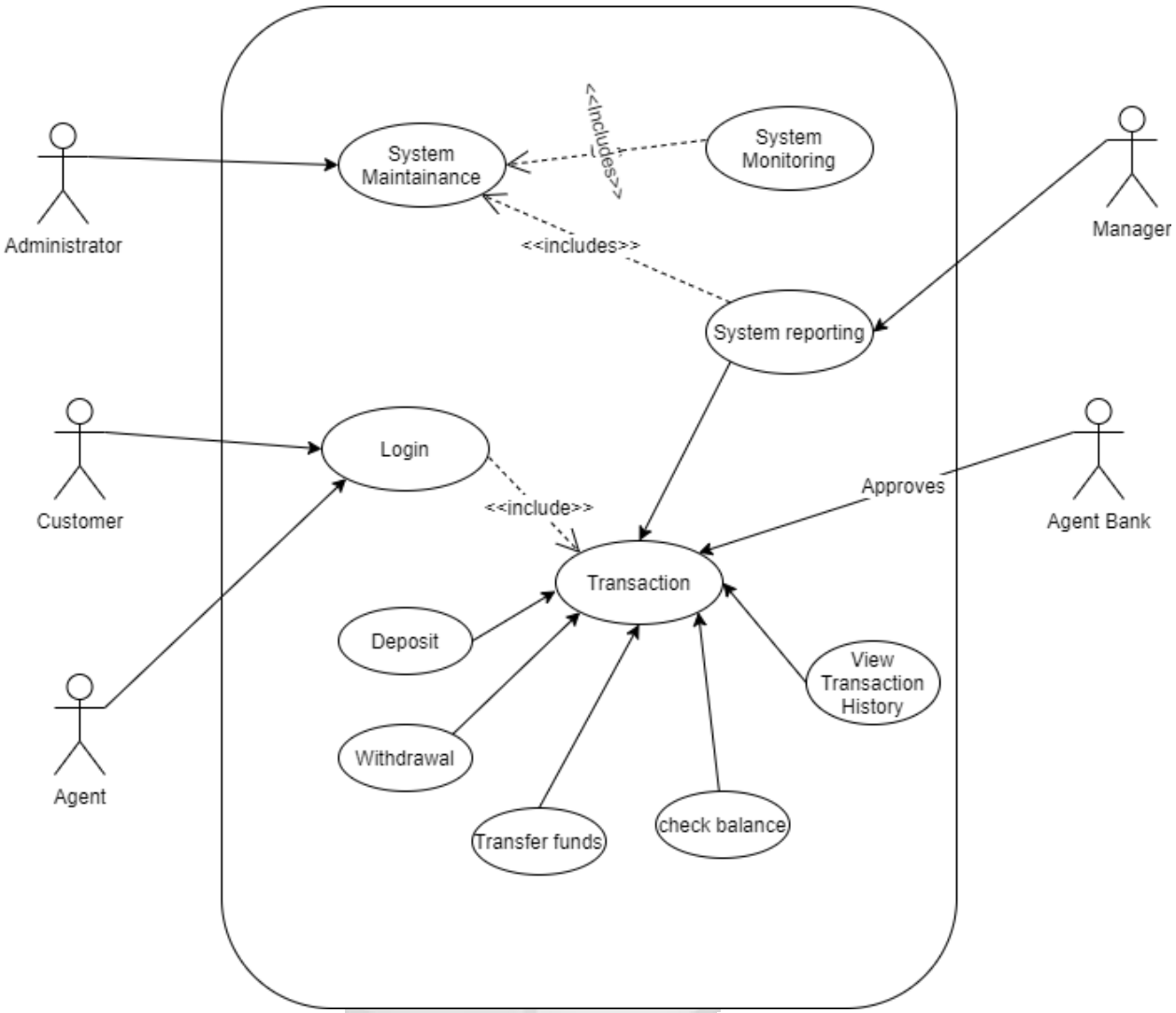
4.6.2 Context Diagram



4-3 Context Diagram

The data input and output modules for this research are point of sale transaction inputs from the bank agent. The input in this case are used to feed data to the agency banking peer to peer network which gathers up this data and sends it to the miners. The miners validate this input against the ledgers and give back output through the peer to peer network back to agent who will present the transaction result to the user (Customer).

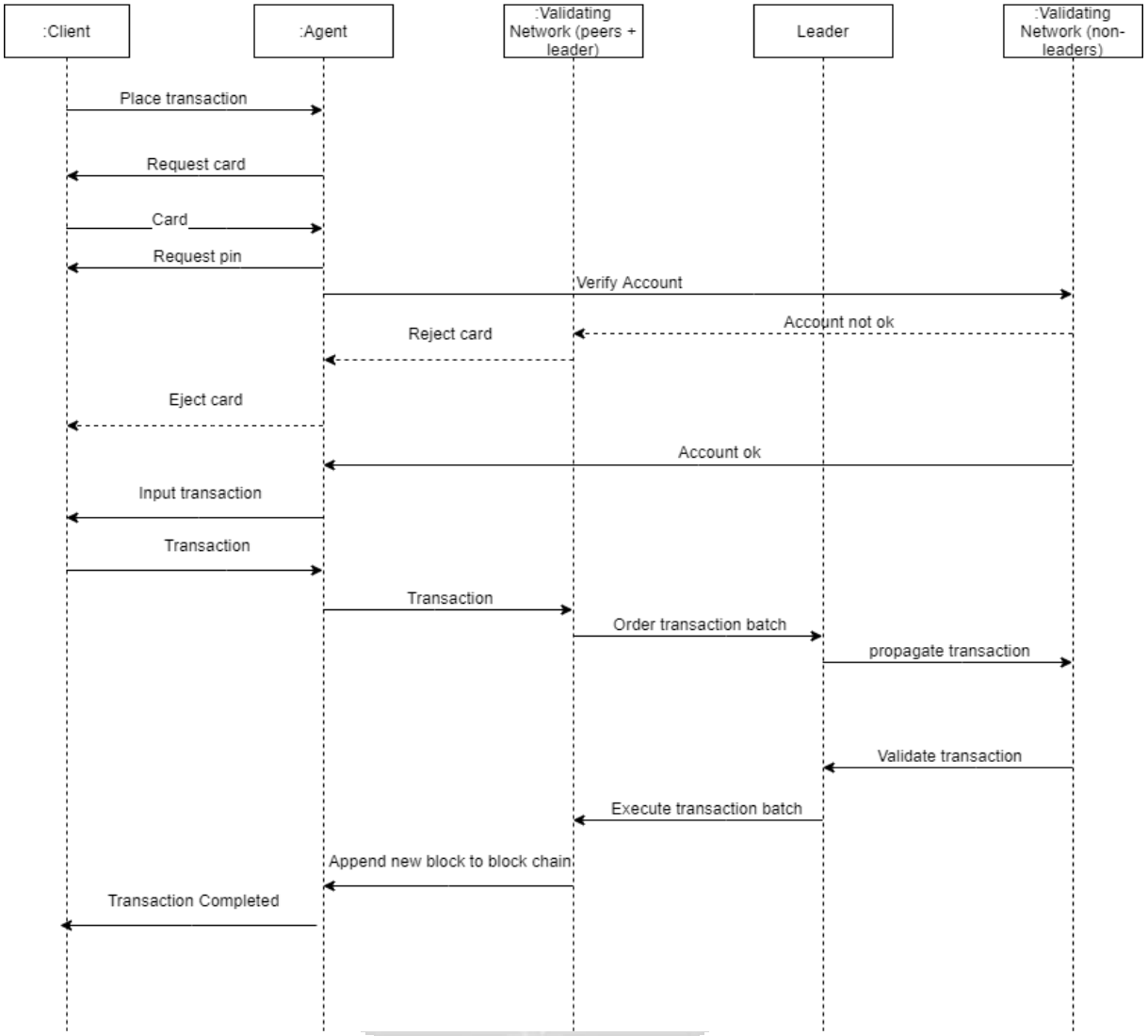
4.6.3 Use case Diagram



4-4 Use case Diagram

The figure 4-4 shows how the different actors interact with the system to make the Model for Securing Agency Banking Transactions using Block Chain Technology. The use case describes five actors. The administrator is identified as an actor because he interacts with the software and hardware components to facilitate maintenance and resolve any technical issue. The agent is identified as an actor because he is to be involved in the initiation of transactions using a Point Of Sale system. The customer is identified as an actor because he is involved as the initiator and recipient of the results of the transaction. Agent bank is identified as an actor in the system because it acts as a mining node used for mining the transaction blocks in the system. The manager is identified as an actor as he plays an over sight role in managing the system. The researcher who takes the role of administrator does the population of rules into the system as agreed upon by the member agent banks. Custom rules are created at this point.

4.6.4 System sequence Diagram



4-5 System Sequence Diagram

Figure 1illustrates a high-level overview of a permissioned agency banking blockchain network. Each participating bank is a Validating Peer (VP), one of which is selected to be the leader. The clients make transaction requests to their respective banking institution's Validating Peer or node, which then validates the transaction and broadcasts it to other Validating Peers. After a few seconds which are defined in batch the timeout rule or after a set number of pending transactions, the leader then creates a block of the pending transactions, maintaining the order by timestamp. Then it proceeds to broadcast this candidate block to other Validating Peers in order to obtain a consensus on the block using PBFT. If 2f +1 peers agree, then each Validating Peer executes all the transactions and appends the block as the next block on their private ledger. Each block is then hashed with the value of the previous block in the blockchain, creating a chain of blocks, and hence the name agency banking blockchain.

5 IMPLEMENTATION AND TESTING

5.1 Introduction

This chapter builds up on the design and analysis from the previous chapter. The outline of this chapter is as follows; the models that were brought together to build the system are discussed. Both hardware and software components are discussed and elaborated. The chapter then describes the setup of the experiment. It outlines all the steps that were taken by the researcher to setup the environment. The chapter then goes through a walkthrough of the implementation phase. Finally, the system is tested and the test results are presented.

5.2 Hardware, Software and Model Components

The software and hardware components that were used to conduct the experiment to be carried out in this research were informed by the nature of the tests to be conducted to achieve the objectives set out by the research.

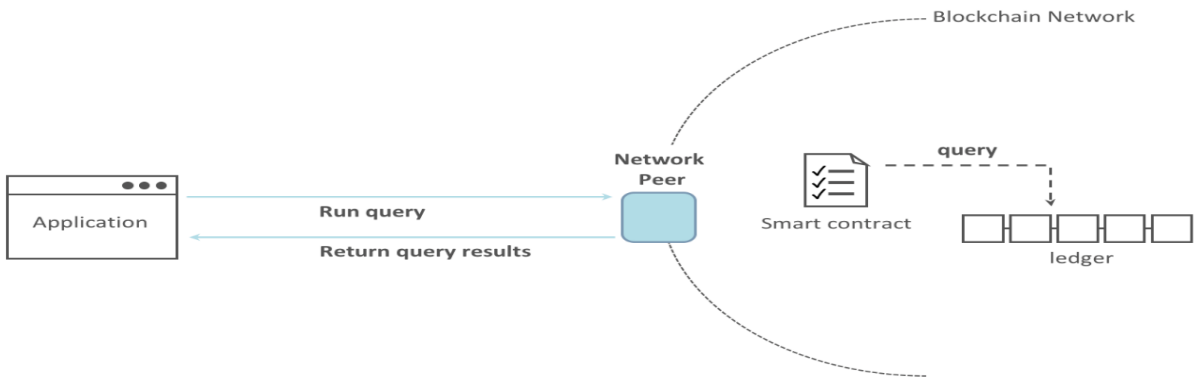
1. Hardware components, A Personal Computer

    a. 16 Gigabyte (GB) Random Access Memory (RAM)
    b. 1TB hard drive disk storage
    c. Intel(R) Core(TM) i7-7550U CPU @ 1.70GHz, 1992 MHz, 4 Core(s), 7 Logical Processor(s) of processing speed

2. Software Components

    i. Windows 10 Host Operating System
    ii. PyCharm

3. Model Components



5-1 Model Components

5.3 Experiment Setup

The experiment to develop the agency banking application using Block Chain Technology to was done on a Windows 10 machine that was customized to meet the needs and objectives of the research. PyCharm was used to create the function that was used to send blocks in the network. It was very important for the researcher to make sure the agency bank application is configured as a framework.

5.3.1 The Steps followed to set up the experiment

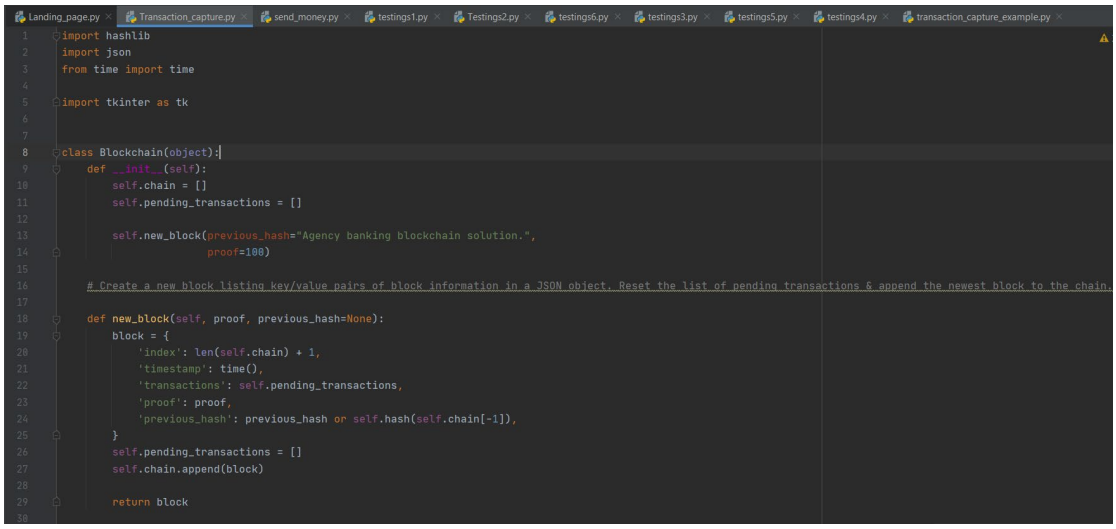
This section will highlight the steps taken to setup environment including the machine where the experiment will take place as well as the mining nodes that will be used to house the agency banking application.

To get started windows 10 and its extension pack were downloaded and installed on Windows to create the test environment. The next step was to install and customize PyCharm. Secondly we had all Prerequisites installed on the platform(s) on which we'll be developing the agency banking blockchain application. The agency banking blockchain application is written in python, which had to be downloaded and installed. Once we had the prerequisites installed, we were ready to write the script that support the user interface and the back end modules.

Landing_page.py | Transaction_capture.py | send_money.py | testings1.py | Testings2.py | testings6.py | testings3.py | testings5.py | testings4.py

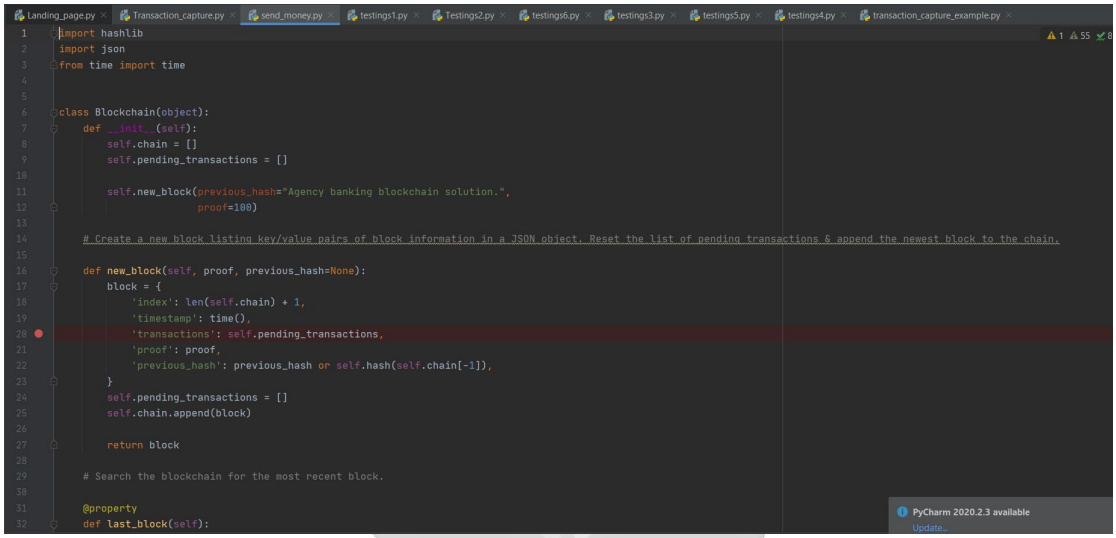
```
import sys
import os
from tkinter import *
from tkinter import messagebox

root = Tk()
root.geometry('500x500')
root.title("Agency Banking Core Banking system")

label_0 = Label(root, text="Select a Transaction Below", width=20, font=("bold", 20))
label_0.place(x=90, y=53)


# label_1 = Label(root, text="Full Names", width=20, font=("bold", 10))
# label_1.place(x=80, y=130)

def deposits():
    os.system('python Transaction_capture.py')


button = Button(root, text='Deposit or Withdraw Cash', width=20, bg='brown', fg='white', command=deposits).place(x=80, y=130)

def sendmoney():
    os.system('python send_money.py')


# Button(root, command=showMsg(), text='Submit', width=20, bg='brown', fg='white').place(x=180, y=380)

button = Button(root, text='Send Money', width=20, bg='brown', fg='white', command=sendmoney).place(x=240, y=130)

root.mainloop()
```

5-2 Landing Page Configuration



```
import hashlib
import json
from time import time

import tkinter as tk


class Blockchain(object):
    def __init__(self):
        self.chain = []
        self.pending_transactions = []

        self.new_block(previous_hash="Agency banking blockchain solution.",
                       proof=100)

    # Create a new block listing key/value pairs of block information in a JSON object. Reset the list of pending transactions & append the newest block to the chain.

    def new_block(self, proof, previous_hash=None):
        block = {
            'index': len(self.chain) + 1,
            'timestamp': time(),
            'transactions': self.pending_transactions,
            'proof': proof,
            'previous_hash': previous_hash or self.hash(self.chain[-1]),
        }
        self.pending_transactions = []
        self.chain.append(block)

        return block
```

5-3 Transaction Capture configuration



```
import hashlib
import json
from time import time


class Blockchain(object):
    def __init__(self):
        self.chain = []
        self.pending_transactions = []

        self.new_block(previous_hash="Agency banking blockchain solution.",
                       proof=100)

    # Create a new block listing key/value pairs of block information in a JSON object. Reset the list of pending transactions & append the newest block to the chain.

    def new_block(self, proof, previous_hash=None):
        block = {
            'index': len(self.chain) + 1,
            'timestamp': time(),
            'transactions': self.pending_transactions,
            'proof': proof,
            'previous_hash': previous_hash or self.hash(self.chain[-1]),
        }
        self.pending_transactions = []
        self.chain.append(block)

        return block

    # Search the blockchain for the most recent block.

    @property
    def last_block(self):
```

5-4 Send Money configuration

5.4 System Implementation

5.4.1 Setting up the peer to peer network interfaces

Unlike a public blockchain for example bitcoin, the agency banking blockchain is a permissioned blockchain or private network, whereby only entities defined in the network can interact with each other. In the permissioned agency banking blockchain, we introduce “Channels” where banks that are part of a blockchain can create separate transactions privately with their respective agents and then pass the final state to the be appended on the main blockchain. Participating agency banks must have identities. Identity will be issued by a Certificate Authority (CA) as crypto-material. Agency banking blockchain uses typical Proof of Work or Proof mechanisms to achieve consensus. Because it’s highly permissioned, it uses a sequence of verified transactions. In order to configure and launch the agency banking

network 3 files are required: configtx.yaml, crypto-config.yaml, and docker-compose.yaml.

The ‘Configtx.yaml’ defines which elements to be used with the agency banking network and are passed onto to ‘configtxgen’ in order to create genesis block and channel artefacts. We split the configtx.yaml file into 5 different blocks; Organizations block, Orderer block, Applications block, Profiles block, Capabilities block. The Orderer block is a messaging system in the agency banking blockchain network, its main purpose is a delivery guarantee, such as atomic or total order broadcast. Profile bock defines which elements we have used with our network and are passed to configtxgen in order to create genesis block and channel artefacts. In this section also, we defined the name of orderer in our network, organizations that are part of the agency banking network. The crypto-config.yaml file was created from ‘ordererOrgs’ and ‘peerOrgs’.

We used a Cryptogen tool to generate the cryptographic material for our network entities. This tool is a utility for generating cryptographic key material. Finally to finish the initialization of our agency blockchain we created:

I. The orderer genesis block. Its purposes as the name indicates is to correctly initialize transaction orders.
II. A channel genesis block. The channel is a private network inside the main network which banks will be able to use to communicate securely with their own customers without the other banks in the blockchain knowing. This allows us to initialize agency banking peers to join a channel.
III. An anchor peer. It’s a peer node with which allows all other peers to discover and communicate with it.

5.4.2 Certificates and artefacts setup

A python script was used to created 2 organizations representing 2 banks, these organizations represent the peers that will house the agency banking application, the smart contracts as well as the ledger.in the above script we also created 1 peer per organization connection between organization 1 and organization 2. We also created certificates to be used for each of the above organization, so that each transaction can be signed by them and we will be able to know who created and signed the transactions we created a genesis block which will act as the starting block for the blockchain.

5.4.3 Connecting the components of the network

In the above script we joined the first peer of the first bank. We also fetch config block for the second bank. We also integrated the first peer of our second bank and updated the environment variables to recognize it. We made these two peers the Anchor Peers of each bank so new peers can communicate to them.

5.4.4 Smart Contracts and Ledgers Installation and setup

Before banks in the agency banking blockchain can transact with each other within the peer to peer network, they define a common set of contracts covering common agreed upon terms this includes, data, rules, concept definitions, and processes. When put together, these contracts guide the business model that govern all of the interactions between the transacting parties. The scripts to write this smart contracts are as shown below

5.5 System Testing

This section highlights the experiments that were conducted by the researcher in order to come up with a blockchain network that is secure and which allows security administrators to run custom rules that can run on agency banking blockchain platform. The rules that were written were supposed to govern the transaction flow from the Point of sale terminal through the peer to peer network onwards to the bank mining nodes for validation and back to the Point Of Sale terminal.

5.5.1 Custom rules definition

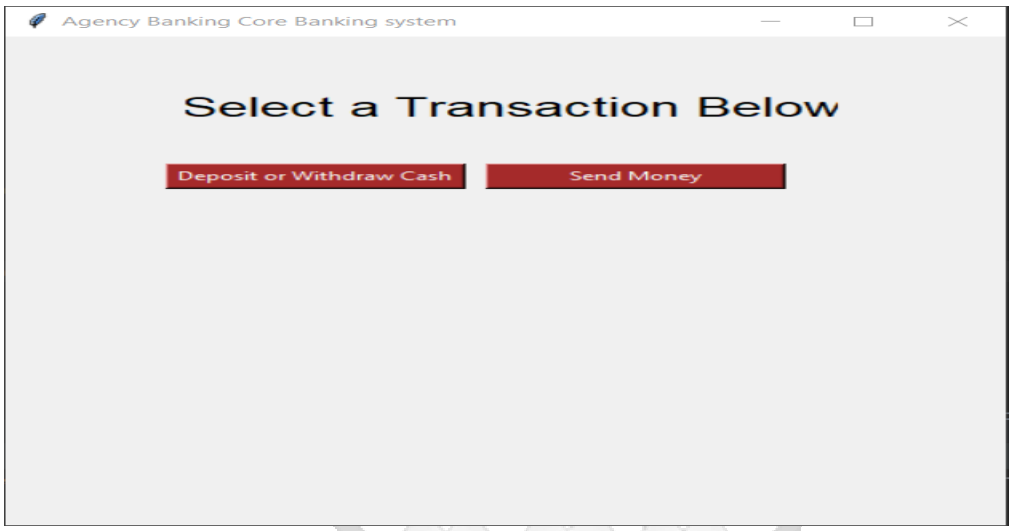
When a transaction initiated by a point of sale terminal is validated at time of commit, whereby the peer performs various checks before applying the state instructions that contained within the transaction itself. This checks include:

- Validating the various identities including the credentials entered by the customer and agent that signed the transaction.
- Verifying that the various signatures of the endorsers on the transaction.
- Ensuring that the transaction satisfies the endorsement policies as stipulated by namespaces of the respective chaincodes.

Agency banking blockchain solution is used to implement and deploy custom endorsement and validation logic into the peer to be associated with the relevant chaincode handling it. This logic is compiled and deployed alongside the peer as a plugin. The scripts to write this custom rules are shown below:

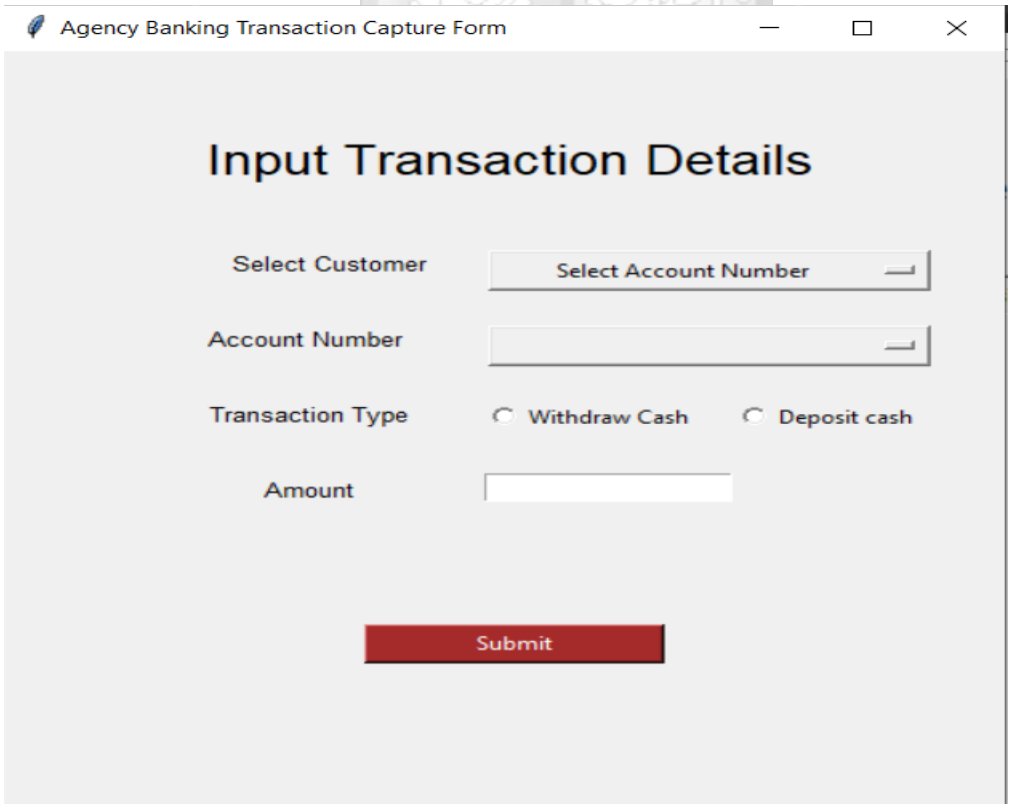
5.5.2 A sample Transaction request

For a transaction to occur in the agency banking block chain system the agent logs in into the application where he or she selects the transaction to be performed



5-5 Landing Page GUI

If the agent selects the Deposit or withdraw cash he or she is presented with the interface to select the customer's account number and transaction type



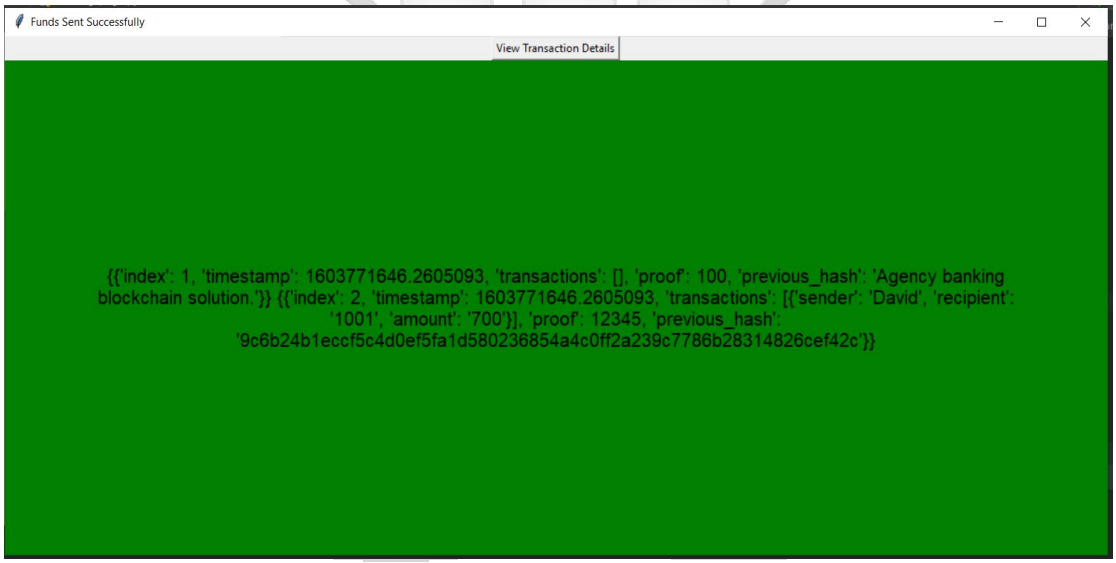
5-6 Transaction capture GUI

If the agent selects the send money GUI, he or she is presented with the interface to fill in the details of the sender and recipient.

The chaincode, which contains a set of key value pairs representing the first state of the agency banking network is installed into the peers and instantiated on the respective bank channel. The chaincode contains the logic defining a set of instructions pertaining to the transactions and the agreed upon price for a transaction. An endorsement policy has also layed out for this chaincode, stating that bank peers must endorse any of the transactions.

5.5.3 Console Results to Demonstrate Block Chain and Encryption Capabilities

A console was used by the researcher to display the results of the experiment and is one of the components of the agency banking blockchain solution. This data displays the number of blocks presently in the blockchain, the total number of transactions that have been initiated and processed.



5-7 Agency Banking Explorer Console

5.5.4 System Testing Classes

The following test cases were conducted by the researcher and the results were as follows

Test Case	Inspection check	Priority
Functional	Were there any custom rules created? In addition, did the rules take effect in the blockchain system to allow it route transactions	High

	to the peers based on the customized rules?	
Functional	Was the system able to detect and drop any suspicious traffic on the network	High
Functional	Was the system able to store the logs of the activity in Level database that can be accessed by third-party applications after referencing to it?	Medium
Non-Functional	Was the system responsive enough to respond to the incoming transaction in a timely manner and update the blockchain in a real time fashion?	Medium

5-8 System Testing Classes

Table 5.1 System testing classes

5.5.5 System testing results

Test Class	Test Results	Comment
Functional	Pass	Suspicious transactions were able to be detected in the network. The nodes did not validate these transactions. They were dropped and flagged as invalid.
Non-Functional	Pass	There was acceptable responsiveness from the system during the implementation as it was

		able to post transactions in real time in the blockchain.

5-9 System testing results

5.6 Usability Questionnaire

Questionnaires were created and distributed amongst 20 users of the agency banking platform. Both users and non-users. The summary that we obtained from the participants were as follows:

	AGENCY BANKING USERS	
NO	Use case	Results
1	Usability	10 out of the 20 participants stated that they use agency banking more than twice a month
2	Popular Services	The most popular service found amongst the active participants was Deposits
3	Security Importance	18 out of the 20 participants indicated that they felt that the security was important
4	Security threats scale	10 out the 2 participants stated that Data leakage was the most risky part of Agency Banking while Doxing was the least with only 1 participant stating it as risky
5	Agency Banking Concerns	12 out of the 20 participants were concerned that the Point of Sale terminal may be infected with a malware.
6	Access to Agency Banking services	18 out 20 participants indicated that they could access agency banking services out of town
7	Agency Banking experience	15 out of the 20 participants stated that they are intermediate users
8	Non-Usability	5 of those who stated the reason why they don't use agency banking said

		they were not aware that their respective banks provided the service
9	Training	12 out of the 20 participants stated that they would require additional training to use the service
10	Agency Banking Importance	15 out of 20 said they consider agency banking services to be vital
11	Resident of Nairobi?	8 of the participants said they reside in the Nairobi area.
12	Possesses a bank account	All participant had a bank account
13	Gender	10 participants were male 10 were female
14	Employment status	10 out of the 20 were employees, 5 were self-employed, 3 were unemployed, 2 were students
15	Age Group	The age group of the participant ranged from 22yrs to 60years of age
16	Ethnicity	18 were Black Africans 2 were Indians
17	Disability	2 out of the 20 participants had a permanent disability

5-10 Usability Questionnaire

5.7 Challenges faced

The implementation and testing of the system presented by the researcher was faced with a number of challenges. This includes the complexity of customizing the windows 10 and making sure that components that allowed the implementation of an agency banking blockchain system was faced. Allowing the prerequisites, tkinter and hashlib library to work in harmony with Python required a lot of tenacity and research to understand their different functionality. Besides that, another complexity that the researcher was faced with was the configuration of the Agency banking blockchain solution dependency packages.

The other challenge that the research posed during the implementation was constantly changing the agency banking blockchain file to capture any new network configuration that was presented in the blockchain network. This meant that the researcher was always aware of the changes or any negligence whenever that would make the system not function properly.

VT OMNES
VNVM SINT

6 CONCLUSIONS AND FUTURE WORK

6.1 Overview

This chapter dissects the findings that were presented in chapter 5 of this study. It analyses the experiment results in detail and sheds more light between the research topics and the findings that were presented. The chapter also looks at the future research work that could be conducted in the same area by drawing conclusions as well as making recommendations drawn from the research findings.

6.2 Discussion

Data collected in chapter five brings into perspective why integration of various security operations including threat detection, alert system, analysis and response are very important in agency banking. From the test results drawn the researcher was able to send a transaction from a bank's agent using a point of sale terminal and send the transaction to the peer to peer network and onwards to the bank specific peers using dedicated channels within the peer to peer network that allowed for private communications prom the POSS to the banks servers. The transaction was hereby processed and the transaction was then completed and the result was returned to the customer. The transaction was also updated in the blockchain ledger.

Agency banking blockchain solution was able to create a genesis block which acted as the beginning of the transaction, then using the channel block this transaction was send to the card holder's specific bank (node) for validation via a channel. The anchor peer received this transaction on behalf of the bank and forwarded the transaction for validation. The transaction was then proceed and the result of the transaction updated on the blockchain.

Agency banking solution on the other hand was used to provide a good GUI using tkinter to allow the researcher to display the transactions in a more organized approach. This can also be used by a bank supervisor and maintenance crew to monitor the status of transactions.

6.3 Conclusion

The system was designed primarily to send and store agency banking transactions securely through a blockchain network. Combining the various components that have been discussed in chapter four of the research, this gave us the work an upper hand in the design and integration of an agency banking blockchain model that would achieve the objectives set out in chapter one.

Chapter two of this research presented the different applications of the blockchain technology and the success they have achieved in those applications. This application paved way for its adoption in various areas within the banking industry. And one such are that needs the security offered by blockchain is Alternate Banking Channels. Of particular interest to this research was agency banking channel. Python was the platform chosen by the researcher to design and implement the agency banking blockchain model due to its success in various blockchain implementations. These were the findings that informed the researcher to settle on the selected research approach that he adopted in chapter 3 and perform similar software modelling techniques that were employed by the previous works in the field of integrating software components to the agency banking blockchain solution.

6.4 Recommendations

This research recommends that for a similar application to be used in a live or commercial setup, security engineers should implement their models on a Linux based environment. This is because of the hardened nature of the Linux based operating system. This means that the researchers were confident about the security of the agency banking blockchain network.

Lastly, the paper recommends that the blockchain based peer to peer rules that come pre-packaged by the python language are a very good starting point for out of the box implementation as this means that the developer only needs to add the number of organizations. However, it is advised that the security administrators go out of their way to come up with new blockchain rules that locally apply to their integration and are custom - made to the banking industry. This makes it easier for them to know what each node does and why the rules that have been set to govern those nodes have been written in that particular way. Besides that, it is also important for the security administrators to familiarize themselves with existing blockchain applications in the financial industry and know what they mean before adopting inheriting any technology used in them.

6.5 Future Research Work

This research focussed on deploying the solution in an agency bank channel only. In future the researcher recommends the solution be deployed in other alternate banking channels including ATMS, POS terminals, Mobile banking and internet banking. This can be achieved by making this devices in this other channels to act as nodes. This means that you do not need to have multiple infrastructures including

software, hardware and personnel to support this channels. The Alternate banking channels team in each banks only needs one team to man all the alternate banking channels network.

REFERENCES

1. Lozano, D. M. A. & Mandrile, M. (2010). *A New Agent Model for Branchless Banking in Colombia*. International Development Law Organization (IDLO) . https://www.findevgateway.org/paper/2010/07/new-agent-model-branchless-banking-colombia

2. Buchenau, Juan, (2010). *Nuevas Tecnologías Y Canales Para La Inclusión Financiera*.

3. Al Alcance Mundial De Todos. (2012). *Agent banking in Latin America. Discussion Paper. Alliance for Financial Inclusion*.

4. Braintechteam, (2015). *Crypto Wallets*. https://blockchaintechteam.com/web/image/721/Asset%209@4x.png.

5. Atandi, F. G. (2013), Challenges of Agent Banking Experiences in Kenya. *International Journal of Academic Research in Business and Social Sciences,* 3(7), 397 – 412.

6. Barasa, D. A. &Mwirigi, F. M. (2013). The Role of Agency Banking in Enhancing Financial Sector Deepening in Emerging Markets: *Lessons from the Kenyan Experience*. European Journal of Business and Management, 5(21), 27-34.

7. Central Bank of Brazil. (2010). *Relatório De Inclusão Financeira*. Brasilia: Central Bank of Brazil. 3(22), 45-46

8. Central Bank of Kenya. (2016). Commercial Banks & Mortgage Finance Institutions. https://www.centralbank.go.ke/index.php/banksupervision/commercial-banks-mortgage-finance-institutions

9. Nyaketcho, Doreen Dale Lindskog, and Ron Ruhl. (2017). *STK implementation in SMS banking in M-pesa-Kenya, exploits and feasible solutions*.

10. Faruk & Noman (2013). *Agent Banking in Bangladesh - A New Era in Financial Institution by Enhancing Customers' Accessibility and Profitability of Banks*. The International Journal of Business & Management, 3(3), 206-210)

11. Gardner M.J, Mills D.L & Cooperman E.S (2000). "*Managing Financial Institutions Anassets Liability Approach"*, (4th Ed.) Malasya, Asia. John Wiley & Sons)

12. Ipspecialist (2010). Cryptocurrency. Retrieved 13 April 2020 from https://ipspecialist.net/wp-content/uploads/2019/10/how-blockchain-technology-work.png>

13. K. Croman, C. Decker, I. Eyal, A. E. Gencer, A. Juels, A. Kosba, A. Miller, P. Saxena, E. Shi, E. G¨un Sirer, D. Song, and R. Wattenhofer (2016). *On Scaling Decentralized Blockchains.* Springer Berlin Heidelberg, pp. 106–125.

14. M. Haferkorn, J.M. Quintana Diaz *(2015).* **Seasonality and Interconnectivity Within Cryptocurrencies – An Analysis on the Basis of Bitcoin, Litecoin and Namecoin** *Springer International Publishing, Cham (pp. 106–120)*

15. M. Castro and B. Liskov (Nov, 2002). *Practical Byzantine Fault Tolerance and*
Proactive Recovery. ACM Trans. Comput. Syst., vol. 20, no. 4, pp. 397–461.

16. Medium (2003). *Smart Contracts*. https://miro.medium.com/max/1247/1*A9_uIE6gwUpBezf6ugpKVw.png.
17. Neil Salkind (2010). Encyclopaedia of Research Design

18. Rizzo, P. (2017) NASDAQ and Citi Announce Pioneering Blockchain and Global Banking Integration, http://www.nasdaq.com/article/nasdaq-and-citi-announce-pioneering-blockchain-and-global-banking-integration-cm792544.

19. T. Swanson. (2015).*Consensus-as-a-Service: a brief report on the emergence*

Of permissioned, distributed ledger system.http://www.ofnumbers.com/wp-content/uploads/2015/04/Permissioned-distributed-ledgers.pdf.

20. sK. Croman, C. Decker, I. Eyal, A. E. Gencer, A. Juels, A. Kosba, A. Miller, P. Saxena, E. Shi, E. G¨un Sirer, D. Song, and R. Wattenhofer (2016). *On Scaling Decentralized Blockchains*. Springer Berlin Heidelberg, pp. 106–125.

21. Nakamoto S. Bitcoin (2012). A peer-to-peer electronic cash system. Consulted. 2007, pp 27.
22. Valluri, P. (2012). Role of alternate channels in banking and wealth management
23. Xiwei Xu, Ingo Weber (2007), Mark Staples: Architecture for Blockchain Applications, pp 75
24. Z. Zheng, S. Xie, H.-N. Dai, H. Wang (2016). **Blockchain challenges and opportunities: a survey** Work Pap.

APPENDICES

Appendix I: List of Commercial Banks in Kenya

1. African Banking Corporation Ltd

2. Bank of Africa Kenya Ltd

3. Bank of Baroda (K) Ltd

4. Bank of India

5. Barclays Bank of Kenya Ltd

6. CFC Stanbic Bank Ltd

7. Charterhouse Bank Ltd

7. Chase Bank (K) Ltd.

9. Citibank N.A Kenya

10. Commercial Bank of Africa Ltd

11. Consolidated Bank of Kenya Ltd

12. Co-operative Bank of Kenya Ltd

13. Credit Bank Ltd.

14. Development Bank of Kenya Ltd

15. Diamond Trust Bank Kenya Ltd

16. Dubai Bank Kenya Ltd

17. Ecobank Kenya Ltd

17. Equatorial Commercial Bank Ltd

19. Equity Bank Ltd

20. Family Bank Limited

21. Fidelity Commercial Bank Ltd

22. Fina Bank Ltd

23. First community Bank Limited

24. Giro Commercial Bank Ltd

25. Guardian Bank Ltd

26. Gulf African Bank Limited

27. Habib Bank A.G Zurich

27. Habib Bank Ltd

29. I & M Bank Ltd

30. Imperial Bank Ltd

31. Jamii Bora Bank Limited

32. Kenya Commercial Bank Ltd

33. K-Rep Bank Ltd

34. Middle East Bank (K) Ltd

35. National Bank of Kenya Ltd

36. NIC Bank Ltd

37. Oriental Commercial Bank Ltd

37. Paramount Universal Bank Ltd

39. Prime Bank Ltd

40. Standard Chartered Bank Kenya Ltd

41. Trans-National Bank Ltd

42. UBA Kenya Bank Limited

43. Victoria Commercial Bank Ltd

Appendix II: Agency Banking Questionnaire for agency banking users

We are carrying out a research of agency banking services, to see if we can develop systems and make them safer. Thank you for taking the time to complete this questionnaire, it should take approximately 15 minutes to complete. Please return the filled out questionnaire to the researcher, or send it via the email. Your answers will be handled confidentially and will be fully anonymous unless you chose to include an e-mail address. If you have any questions regarding this questionnaire, please contact [John Kibathi].

Section A

1. On average how much do you use the agency banking services,: (please tick one)

once a month	☐
Less than once a month	☐
once every two weeks	☐
once a week	☐
two or three times a week	☐
Daily	☐

2. Which agency banking services do normally you use? (please tick all that apply)

Deposits	☐
withdrawals	☐
Balance Enquiry	☐
Money Transfer	☐
Loan Application	☐
Accounts opening	☐
Utility Payment (KPLC, ZUKU, DSTV)	☐
other (please specify)	☐

_____

3. What is your primary use of the Agency Banking Platform?

   _____

4. Do you feel that Agency banking security is important?

   Yes ☐
   No ☐
   Maybe ☐

5. On a scale of 1 - 5 do you think that you are vulnerable to from Agency banking threats such as:

	1 Not at risk	2	3	5	6 Very at risk
Malware					
Data leakages i.e. confidential information being compromised					
Phishing					
Doxing					

Definitions

Malware – this is a computer program which is specifically designed to disrupt or damage a computer system. Including Trojans, adware, viruses, etc.

Phishing - the practice of sending spam emails purporting to be from reputable companies fraudulently so as to coerce individuals to reveal personal information, such as passwords and credit card numbers, online.

Doxing - is the practice of researching and distributing private information about an individual or organization without their consent.

b. On a scale of 1 - 5 how concerned are you regarding the following while using agency banking services?

	1 Not at risk	2	3	5	6 Very at risk
My personal information being stolen and used by third parties					
My personal information being collected by agents and being sold to other people					
My bank details being stolen through an illegitimate agency banking transaction					
My Agent's Point Of Sale is infected with spyware which I collecting information about me without my consent					

I am worried about adware					

6. How often do you use the other financial facilities? (select one)

   Daily ☐
   once every two weeks ☐
   Once or twice a week ☐
   once a month ☐
   less than once a month ☐

7. Is your town your only access to agency banking facilities?

   Yes ☐
   No ☐

   if yes, proceed to question 9.
   If no, continue with question 8.

8. Do you have access to agency banking facilities elsewhere, please say where: (please select all that apply)

   home ☐

school/college/university ☐

cybercafé ☐

work ☐

Other (please say where) ☐

9. In regards to Agency banking do you consider yourself:

a beginner ☐

an intermediate user ☐

a fairly experienced user ☐

a very experienced user ☐

10. How would the withdrawal of agency banking facilities from the banking industry affect you?

11. Do you have an e-mail address?

Yes ☐

No ☐

if you are okay with us contacting you in the future, please write your e-mail address here.

_____

Now please proceed to question 14.

Section B. (For non-users of agency banking facilities only)

12. If you do not use the banking facilities in the agent, could you please say why: (please tick one)

didn't know they were there	☐
no interest/use	☐
don't know how to	☐
have access elsewhere	☐
no-one to help/reluctant to ask for help	☐
other (please say what)	☐

_____

Please now continue with sections C. and D.

Section C. (All respondents)

13. Would you be interested in training on how to use the agency banking facilities?

Yes	☐
No	☐

14. How important is it for banks to provide agency banking facilities?

very important	☐
quite important	☐
not very important	☐
not at all important	☐

15. Which of these statements most reflects your view of the agency banking facilities?

a vital service ☐
an add-on service, secondary to other banking services ☐
an unnecessary expense ☐

Please give a reason for your view:

16. Are there any ways the bank could improve your access to the agency banking services on offer?

Section D. (All respondents)

17. Are you a resident of Nairobi?

Yes ☐
no

_____

No ☐
If no, are you visiting from:
within the Kenya ☐
outside the Kenya ☐

18. Do you have bank account with any local banks?

Yes ☐
No ☐

19. Are you:

male ☐
female ☐

20. Are you:

employed full-time ☐
employed part-time ☐
self-employed ☐
unemployed ☐
student ☐
student and working ☐
retired ☐
other (please specify) ☐

21. Are you:

under 18 ☐
18-25 ☐
26-35 ☐
36-45 ☐
46-55 ☐

56-65 ☐

over 65 ☐

22. How would you describe your ethnic background?

White ☐

Black African ☐

Black Caribbean ☐

Black Other ☐

Pakistani ☐

Indian ☐

Bangladeshi ☐

Chinese ☐

Other, please say what ☐

23. Do you have a disability?

No ☐

Yes ☐

(please specify)

Thank you very much for taking the time to complete this questionnaire.
Please hand it back researcher.

If you have any other comments, please add them below:

Appendix III: Questionnaire for Agency Banking Non-Users

Instructions:

We are carrying out a research of agency banking services, to see if we can develop systems and make them safer. Thank you for taking the time to complete this questionnaire, it should take approximately 15 minutes to complete. Please return the filled out questionnaire to the researcher, or send it via the email. Your answers will be handled confidentially and will be fully anonymous unless you chose to include an e-mail address. If you have any questions regarding this questionnaire, please contact [John Kibathi].

1. Do you currently have a bank account?

Yes ☐

No ☐

if no, proceed to question 7

2. What do you use a bank account for? (Select all that apply).

work ☐

savings ☐

paying bills ☐

other (please specify) ☐

_____

3. What banking services do you use? (Please tick all that apply).

Deposits	☐
withdrawals	☐
Balance Enquiry	☐
Money Transfer	☐
Loan Application	☐
Accounts opening	☐
Utility Payment (KPLC, ZUKU, DSTV)	☐
other (Specify what)	☐

_____

4. What else would you like to use a bank account for?

5. When do you use your bank account? (Please tick all that apply).

at work	☐
at home	☐
at school/college	☐

during free time ☐

at the community centre ☐

other (please say when) ☐

6. Where would you go if you wanted to learn more about using agency banking?

7. Are you aware that some agents have account opening services available?

Yes ☐

No ☐

8. Would you use banking services in the banking agent?

Yes ☐

No ☐

Why? / Why not?

_____

what banking services would you like to be made available in your local banking agent?

Deposits ☐

withdrawals ☐

Balance Enquiry ☐

Money Transfer ☐

Loan Application ☐

Accounts opening ☐

Utility Payment (KPLC, ZUKU, DSTV) ☐

other (please specify) ☐

_____

The following questions aim to give us a profile of the respondents. Getting the following details would be very helpful, all answers will be entirely confidential and anonymous.

10. Are you:

male ☐

female ☐

11. Are you:

under 18 ☐

18-25 ☐

26-35 ☐

36-45 ☐

46-55 ☐

56-65 ☐

over 65 ☐

12. Are you:

full-time employed ☐

part-time employed ☐

self-employed ☐

unemployed ☐

student ☐

student and working ☐

retired ☐

other (please say what) ☐

_____

13. How would you describe your ethnic background?

White ☐

Black African ☐

Black Caribbean ☐

Black Other ☐

Indian ☐

Pakistani ☐

Bangladeshi ☐

Chinese ☐

Other (please specify) ☐

_____

14. Do you consider yourself to have a disability?

Yes ☐

No ☐

15. Are you a resident of [insert local authority area]?

Yes ☐

If yes, please ask for their postcode. ☐

No

If no, are you visiting from: ☐

within the Kenya

outside the Kenya ☐

Thank you for taking the time to answer the questionnaire.

Model For Securing Agency Banking Transactions using Block Chain Technology budget

below budget breakdown to justify the project costs. Showing line by line information, inluding rows , for each cost that is specific to the project.

BUDGET SUMMARY

The budget summary will autopopulate based on the figures provided in the budget breakdown.

Proposal title:	*Model For Securing Agency Banking Transactions using Block Chain Technology*
Duration of project:	*3months*

Fees	**840,000.00**
Expenses	**699,600.00**
Data collection	537,000.00
Other direct project cost	71,500.00
Travel for project team	91,100.00
Total budget	**Ksh1,539,600.00**

BUDGET BREAKDOWN

Fees for project personnel

	Role	Number of days	Quantity	Daily rate (Ksh)	Total cost (Ksh)	Justification
Principal and co-Investigators	project manager	60.00	1.00	4,000.00	240,000.00	Function as lead researcher as well as project team leader
					-	
					-	
	Role	**Number of days**		**Daily rate (Ksh)**	**Total cost (Ksh)**	**Justification**
Other project staff	project cordinator	60.00	1.00	2,000.00	120,000.00	Perform data analysis and produce data reports
	project officer	60.00	2.00	1,000.00	120,000.00	document filing, maintain project plan
	Software developer	40.00	3.00	3,000.00	360,000.00	configuration of virtual environment, build of prototype
					-	
				Subtotal	**840,000.00**	

SUBTOTAL FEES	**Ksh840,000.00**

Data collection

	Description of item	Number of days	Quantity	Rate (Ksh)	Total cost (Ksh)	Justification
Field/survey staff salaries	Field surveyor	20.00	5.00	10,000.00	200,000.00	Will be used to interview agents
	Description of item	**Number of days**	**Quantity**	**Cost per Unit (Ksh)**	**Total cost (KSh)**	**Justification**
Field/survey staff travel	Daily Transport	20.00	5.00	100.00	10,000.00	Travel to and fro home
	Site transport	20.00	5.00	300.00	30,000.00	Site visit to visit agents
					-	
					-	
	Description of item	**Number of days**	**Quantity**	**Cost per Unit (KSh)**	**Total cost (KSh)**	**Justification**
Materials	Rental Of Tablets	20.00	5.00	500.00	50,000.00	tablet rental to conduct primary data collection
	Purchase of laptops	1.00	4.00	35,000.00	140,000.00	For use in Projects office
	Rental Of Space for Project Management office	90.00	1.00	400.00	36,000.00	Rental Of Space for Project Management office
					-	
	Description of item	**Number of days**	**Quantity**	**Cost per Unit (KSh)**	**Total cost (KSh)**	**Justification**
Training	Payment for trainer for 1 day training workshop for 5 field staff	1.00	5.00	7,000.00	35,000.00	to provide data analysis training for back checkers and enumerators
					-	
					-	
					-	
	Description of item	**Number of days**	**Quantity**	**Cost per Unit (KSh)**	**Total cost (KSh)**	**Justification**
Other data collection costs	Mcafee Antivirus	90.00	1.00	400.00	36,000.00	Purchase of anti virus for host machine
					-	
					-	
					-	
				Subtotal	**537,000.00**	

Other direct project cost

	Description of item	Number of days	Quantity	Cost per Unit (KSh)	Total cost (KSh)	Justification
Dissemination costs	food for 5 participants attending workshop	1.00	5.00	300.00	1,500.00	Breakfast, Lunch during training
					-	
					-	
	Description of item	**Number of days**	**Quantity**	**Cost per Unit (KSh)**	**Total cost (KSh)**	**Justification**
Capacity building costs	Research methodology training for 1 project coordinator	7.00	1.00	10,000.00	70,000.00	Attending research methodology
					-	
					-	
	Description of item	**Number of days**	**Quantity**	**Cost per Unit (KSh)**	**Total cost (KSh)**	**Justification**
Other direct project cost					-	
					-	
					-	
				Subtotal	**71,500.00**	

Travel expenses for project team

This relates to travel for Principal and Co-Investigators, Research Assistants, Project Managers, etc. Travel expenses for field and survey staff are included in the data collection section of the budget.

	Description of item	Number of flights		Airfare (KSh)	Total cost (KSh)	Justification *(e.g. trip to visit policymakers in Lusaka)*
International flights	Return flight for PI travel to Mombasa	2.00		13,000.00	26,000.00	Project coordinator to attend research methodologytraining
					-	
					-	
					-	
	Description of item	**Number of Days**	**Quantity**	**Cost per Unit (KSh)**	**Total cost (KSh)**	**Justification** *(e.g. RA to conduct field visits)*
In-country travel	Fuel for project managers car for 60 days at KSh5/day	60.00	1.00	300.00	18,000.00	To and fro and home
	Transport Charges for project cordinator to training center and back to	7.00	1.00	500.00	3,500.00	
					-	
					-	
	Description of item	**Number of nights**		**Daily rate (KSh)**	**Total cost (KSh)**	**Justification** *(e.g. trip to meet with field staff in Lahore)*
Accommodation	Accommodation for 1 Project Coordinator during training	8.00		3,500.00	28,000.00	Accomodation during training
					-	
					-	
					-	
	Description of item	**Number of days**		**Daily rate (KSh)**	**Total cost (KSh)**	**Justification** *(e.g. trip to meet with field staff in Lahore)*
Subsistence	subsistence for 1 Project coordinator	7.00		800.00	5,600.00	Per diem costs
					-	
					-	
					-	
	Description of item	**Quantity**		**Cost per Unit (KSh)**	**Total cost (KSh)**	**Justification** *(e.g. trip to visit policymakers in Lusaka)*
Other travel costs	Transport to and for JKIA	2.00		2,500.00	5,000.00	Taxi charges
	Transport to and for Mombasa airport to hotel	2.00		2,500.00	5,000.00	Taxi charges
					-	
					-	
				Subtotal	**91,100.00**	

SUBTOTAL EXPENSES	**Ksh699,600.00**
TOTAL BUDGET	**Ksh1,539,600.00**

Appendix IV: Budget

Document Viewer

Turnitin Originality Report

Processed on: 17-Apr-2020 7:10 PM EAT
ID: 1281603152
Word Count: 15734
Submitted: 12

Model for Secure Storage of Agency Banking Tr... By John Kamau Kibathi

Similarity Index	Similarity by Source	
26%	Internet Sources:	17%
	Publications:	4%
	Student Papers:	20%

Appendix V: Turn-it-in Originality Report

Strathmore UNIVERSITY

30th January 2020

Mr Kibathi, John
john.kibathi@strathmore.edu

Dear Mr Kibathi,

RE: Model for Securing Agency Banking Transactions using Block Chain Technology

This is to inform you that SU-IERC has reviewed and approved your above research proposal. Your application approval number is **SU-IERC0607/19.** The approval period is **30th January, 2020 to 29th January, 2021.**

This approval is subject to compliance with the following requirements:

i. Only approved documents including (informed consents, study instruments, MTA) will be used
ii. All changes including (amendments, deviations, and violations) are submitted for review and approval by SU-IERC.
iii. Death and life threatening problems and serious adverse events or unexpected adverse events whether related or unrelated to the study must be reported to SU-IERC within 72 hours of notification
iv. Any changes, anticipated or otherwise that may increase the risks or affected safety or welfare of study participants and others or affect the integrity of the research must be reported to SU-IERC within 72 hours
v. Clearance for export of biological specimens must be obtained from relevant institutions.
vi. Submission of a request for renewal of approval at least 60 days prior to expiry of the approval period. Attach a comprehensive progress report to support the renewal.
vii. Submission of an executive summary report within 90 days upon completion of the study to SU-IERC.

Prior to commencing your study, you will be expected to obtain a research license from National Commission for Science, Technology and Innovation (NACOSTI) https://oris.nacosti.go.ke and also obtain other clearances needed.

Yours sincerely,

for: Dr Virginia Gichuru,
Secretary; SU-IERC

Cc: Prof Fred Were,
Chairperson; SU-IERC

STRATHMORE UNIVERSITY INSTITUTIONAL ETHICS REVIEW COMMITTEE SU-IERC
30 JAN 2020
TEL: +254 (0)703 034 000
P. O. Box 59857 - 00200
NAIROBI - KENYA

Ole Sangale Rd, Madaraka Estate. PO Box 59857-00200, Nairobi, Kenya. Tel +254 (0)703 034000
Email info@strathmore.edu www.strathmore.edu

Appendix I: Ethical Approval Letter