A CONCEPTUAL SECURE BLOCKCHAIN BASED SETTLEMENT AND CLEARING HOUSE FOR MOBILE FINANCIAL SERVICES IN ZAMBIA

BY

FICKSON MVULA

A Dissertation submitted to the University of Zambia in partial fulfilment of the requirements for the award of the degree in Masters of Engineering in Information and Communications Technology Security

THE UNIVERSITY OF ZAMBIA

LUSAKA

2020

COPYRIGHT DECLARATION

DECLARATION

I, the undersigned, declare that this has not previously been submitted in candidature for any degree. The dissertation is the result of my own work and investigations, except where otherwise stated. Other sources are acknowledged by given explicit references. A complete list of references is appended.

Student Name: ………………………………………………………………….

Signature: ………………………………………………………………….

Date: ………………………………………………………………….

Supervisor Name: ………………………………………………………………….

Signature: ………………………………………………………………….

Date: ………………………………………………………………….

CERTIFICATE OF APPROVAL

This document by ………………..……………………… is approved as fulfilling the requirements for the award of the degree of Maters of Engineering in ……………………………………………………… of the University of Zambia

Examiner 1:

Name:……………………………….Signature:………………………Date:..………

Examiner 2:

Name:……………………………….Signature:………………………Date:..………

Examiner 3:

Name:……………………………….Signature:………………………Date:..………

Supervisor:

Name:……………………………….Signature:………………………Date:..………

Chairperson:

Name:……………………………….Signature:………………………Date:..………

ACKNOWLEDGEMENT

Firstly, I give praise and thanks to our Jehovah for the opportunity to undertake this study as well as for the many blessings that have enabled this to be a success. I am extremely grateful to Dr. Jackson Phiri, Dr. Simon Tembo and Dr. Lighton Phiri who helped enormously and guided me with their knowledge and experience throughout my research to completion.

DEDICATION

I dedicate this research work to my wife Kasapo Musonda Mvula our kids who have been my source of strength and motivation as I pursued this research study.

To my friends and colleagues for the unwavering support and encouragement. To my parents for the never ending moral support, understanding and perseverance during the period of the study.

ABSTRACT

Developing Countries in Africa in general and Zambia in particular, have seen a rapid rise in the use of mobile payment platforms. This has not only revolutionized access to financial services for the poor but also allowed them access to other financial products such as savings or insurance. With a growing number of mobile money providers in Zambia, the need for a solution that provides for end-to-end account-to-account interoperability has become ever more apparent. In this study, we first reviewed the technical landscape and features of mobile payment systems in Zambia and then assessed the feasibility of using blockchain technology in proposing a settlement and clearing system that would facilitate mobile money interoperability. A prototype system was then designed in which amounts being interchanged between providers are managed as assets on a permissioned blockchain. In the end, the study concluded that mobile money interoperability settlement is a valid use case for a permissioned blockchain technology and that it was an ideal solution approach rather than the traditional central processing database systems because of the desirable security features that it provides. The study also brought about key lessons in the practical implementation of blockchain technology other than the much-publicised cryptocurrency.

Keywords: Blockchain, Blockchain Security, Mobile Money Interoperability, Payments, Clearing and Settlement Systems

TABLE OF CONTENTS

Table of Contents

LIST OF TABLES

LIST OF FIGURES

LIST OF ABBREVIATIONS

A2A - Account to Account

ACH - Automated Clearing House

ATM - Automated Teller Machine

B2M - Bank to Mobile

CA - Certificate Authority

DBMS - Database Management System

DFS - Digital Financial Service

DLT - Distributed Ledger Technologies

GSMA - Global System for Mobile Communications Association

MNO - Mobile Network Operator

OMT - Object Modelling Techniques

OOAD - Object Oriented Analysis and Design

POS - Point Of Sale

PoW - Proof Of Work

RTGS - Real Time Gross Settlement

SDK - Software Develpment Kit

SWIFT - Society for Worldwide Interbank Financial Telecommunication

TTP - Trusted Third Party

US - United States

ZECHL - Zambia Electronic Clearing House Limited

CHAPTER ONE:

INTRODUCTION TO THE RESEARCH

1.1 Introduction

This study looks at the design and development of a secure and trusted clearing and settlement system [1] for mobile money services in Zambia. This is in an effort to enable interoperability [2] of the many mobile money service providers which currently are not able to efficiently interoperate. A study of the Zambian Mobile Money ecosystem is conducted and a technical solution is proposed and designed as an appropriate interoperability scheme based on blockchain technology [3] to ensure security and trust among the different service providers.

1.2 Motivation and Significance of the Study

Zambia like most countries in the developing world, has seen tremendous growth in the number of peer to peer mobile money wallet services aside from the traditional mobile money services provided by mobile network operators (MNOs). This has led to a creation different autonomous financial ecosystems with little to no interoperability between them.

The Global System for Mobile Communications Association (GSMA) [4] defines mobile money interoperability to mean that mobile money operators (MNOs) provide the ability for their customers to undertake money services with customers at different mobile money operators as if they were on the same network. They further narrow down interoperability to account-to-account (A2A) interoperability which includes person-to-person (P2P) interoperability, i.e. the possibility for customers to make transfers between their mobile money accounts, as well as bank account to mobile money account (B2M) and mobile money account to bank account (M2B) transfers.

For the purpose of this study, focus is drawn to A2A interoperability and is restricted to transfers that happen between a customer from one network operator (e.g. Airtel Zambia) to another subscriber on a different network (e.g. Zamtel). Integration of wallet providers' systems through a central clearing house for purposes of clearing and settlements is thus necessary to achieve mobile wallet interoperability.

Several benefits have been given for interoperability including the fact that it aims to increase the value of mobile money for providers and customers alike, including a larger addressable market and enhanced customer experience due to its potential for strong network effects. Most importantly, it has been seen as a vital driver for financial inclusion of the poor and unbanked rural populations of most developing countries [5].

A common clearing and settlement infrastructure is thus necessary to provide this interoperability.

1.3 Background

A number of functional requirements for A2A interoperability are necessary and these include:

a) Ability to transact between wallet accounts at different Mobile Network Operators (MNOs),
b) Ability to settle funds for transactions across schemes and between schemes and their respective banks where value is stored,
c) Implementation of common risk management practices that preserve the integrity of the individual mobile money schemes and thus ensure trust of the overall network system.

There is however, greater need for this clearing infrastructure to be trusted and secure because of the financial implications of the transactions processed [6]. Some desirable features for this clearing and settlement facility would include:

a) A means of ensuring trust among participants that the data exchanged is verified and verifiable and that it is tamper proofed

b) Security of communication among participants and that the data exchanged should meet the basic security requirements of confidentiality, integrity, availability, authenticity and accountability,

c) Ease of integration between different participants to lessen the integration headaches because every participant would have to integrate with every other participant.

Clearing and settlement of a financial transaction, regardless of the asset type, requires a network of participants, an asset or set of assets that are transferred among those participants, and a transfer process that defines the procedures and obligations associated with the transaction [12]. Typically, the set of direct participants are financial institutions such as banks or brokers and indeed mobile wallet providers in the case of mobile financial services. Indirect participants include end users such as subscribers in this case. An asset can be any financial instrument, such as a monetary instrument, security, commodity, or derivative. Again in a mobile financial services ecosystem, the asset type of interest is virtual money (or e-money) being transferred from one wallet to another across a network of participants. Communications among the participants in a network involve sending electronic messages, acknowledgements, statements, and other information between computer systems typically maintained by a network operator and its participants [5].

It is worth noting at this stage that the current implementation of such networks is such that each participant maintains and is responsible for their own financial ledger, which acts as their single source of truth on the status of their data. To achieve interoperability, a common central authority may be necessary which would be entrusted by their participants with updating and preserving the integrity of a central ledger and, in some cases, managing certain risks on behalf of participants.

Currently, no live implemented system allows interoperability between the different mobile financial services wallet providers in Zambia. The proposed Zambia National Switch project [7] being undertaken by the Zambia Electronic Clearing House Limited (ZECHL) will among others enable participants in the mobile financial ecosystem to interchange money by providing a clearing and settlement platform. The system implementation will be phased and the first phase expected to cater for interoperability of commercial banks and expected to be launched at the end of 2018. The second phase will cater for integration of other financial services such as mobile money and telegraphic money transfers [8].

The National Financial Switch system however, being a traditional database based central system will have a number of shortfalls in as far of effective provision of the desired features identified for clearing and settlement of A2A interoperability transactions. Firstly, there will be integration complexity, as every participant will be required to connect to a central node. This central node of processing will hinder efficiencies in end-to-end processing speed and thus availability of funds may be hampered. Further, there will be no network resilience offered by distributed data management system such as one provided by a distributed ledger system. And furthermore, there may be operational and financial risks as a result of a single central node rather than a distributed system [9].

Blockchains have emerged with Bitcoin [10] and are widely regarded as a promising technology to run trusted exchanges in the digital world [10]. In brief, blockchain technology can be defined as a linked list of data blocks that allows the creation of transaction records (financial, contractual, etc.) based on a distributed consensus protocol managed by the participants (i.e., the nodes of the network) without the need for a central authority. By construction, the linked list or chain of records becomes immutable; that is, no single node can modify the content of the blocks that have been previously agreed. In other words, only insertions or aggregations of new transactions are allowed, as it is not possible to eliminate or modify existing ones.

The immutability property is complemented with additional characteristics. Firstly, it must be possible to obtain a summary of the status of the entire chain at any given time, so that, if any block of the chain were manipulated, it must be possible to detect such manipulation. Secondly, it would be desirable to have access to a simple way for verifying whether a transaction has been incorporated to the blockchain or not. Finally, the parties involved in a transaction to be included in any of the blocks should be allowed to do so in a pseudo-anonymous manner.

Possibly, one of the best-known implementations of this technology is bitcoin, the cryptocurrency named that way for the use that it makes of several cryptographic primitives to achieve pseudo-anonymity of the participants, immutability of stored records, and distributed consensus without resorting to a central authority [10].

Two main categories of blockchains are used and these are public and private blockchains [11]. In a public or permission-less blockchain, anyone can participate without a specific identity and these typically involve a native cryptocurrency and often use consensus based on proof of work (PoW) and economic incentives. Permissioned blockchains, on the other hand, run a blockchain among a set of known, identified participants. A permissioned blockchain provides a way to secure the interactions among a group of entities that have a common goal but which do not fully trust each other, such as businesses that exchange funds, goods, or information [12].

The proposed solution is directed primarily permissioned blockchains, reflecting the main types of arrangement currently being developed in the financial sector, such as one required for a mobile money account to account interoperability among a number of disparate network providers.

The case for Distributed Ledger Technology (DLT) as a potential technology to disrupt payment, clearing and settlement implementations is because of the technology's ability to introduce a set of synchronized ledgers managed by one or more entities rather than individual non communicating ledgers [13]. This would lead to a reduction in the reliance on traditional central ledger managed by a trusted entity for holding and transferring funds and other financial assets.

DLT may radically change how assets are maintained and stored, obligations are discharged, contracts are enforced, and risks are managed. Proponents of the technology highlight its ability to transform financial services and markets by [13][14]:

a) Reducing complexity;

b) Improving end-to-end processing speed and thus availability of assets and funds;

c) Decreasing the need for reconciliation across multiple record-keeping infrastructures;

d) Increasing transparency and immutability in transaction record keeping;

e) Improving network resilience through distributed data management; and

f) Reducing operational and financial risks.

DLT may also enhance market transparency if information contained on the ledger is shared broadly with participants, authorities and other stakeholders.

1.4 Problem Statement

Subscribers of mobile moneys services keep finding it increasingly difficult to share or transfer value from the mobile money wallets to other subscribers who use different mobile money providers from their own. The problem is further compounded by the increasing number of mobile financial services providers operating without any form of interoperability between them.

1.5 Aim

The study aims to propose the design a framework for a secure and trusted Blockchain based clearing and settlement house for mobile financial services in Zambia.

1.6 Objectives

The main aim of this research is to propose the design of a secure and trusted Blockchain based clearing and settlement system for mobile financial services in Zambia. The following specific objectives have been set:

a) To conduct a baseline study on how mobile financial service are currently implemented in Zambia and the challenges to interoperability associated with the implementation.

b) To design a conceptual model for inter operator mobile financial transactions that enables payments, clearing and settlement in a secure, transparent and trusted manner.

c) To develop a prototype based the model in (b) that demonstrates Blockchain security services in a permissioned and regulated environment.

1.7 Research Questions

This research will be guided by the following research questions;

a) What are the main challenges of the mobile service providers based on the current implementation in Zambia?

b) To what extent could Blockchain technology be employed to enable recording and tracking of inter operator mobile financial transactions to enable payments, clearing and settlement?

c) What is the feasibility of implementing a blockchain based solution in a permissioned and regulated environment?

1.8 Organization of the Thesis

The work done in this study is organised into five chapters. Chapter 'One' is the Introduction to the research. In this chapter, we give a brief overview of the work in this study. We also give the problem statement, aims and motivation of this study. This chapter concludes by the giving an outline of the study.

Chapter 'Two' looks at the background theory and related works. In this chapter, we begin by providing some examples of similar problems and solution approaches in other areas. Next we look at some background information to the technology that we propose as well as some use cases that make this technology applicable to this problem space. Finally, we review works around coming up with a decision framework that is going to assist us build a basis for our choice of the technology.

The general study methodology and methods are given in Chapter 'Three' while an outline of the corresponding study findings is given in Chapter 'Four'.

Finally, Chapter 'Five' will give a general study summary, discussion of the findings and some recommendations arising from the study.

1.9 Summary

In this chapter, we looked at the basic introduction of the work in this study. We begin by looking at the background to the problem and defined the study problem. The motivation, significance and scope of the work in this study were then outlined. Finally we gave the problem statement, outlined the aims, the research contributions and we close this chapter with the outline of the thesis.

CHAPTER TWO

LITERATURE REVIEW

2.1 Introduction

This section presents different literature reviewed from various sources as part of the literature study. These included sources from journals, conference paper proceedings, reports, textbooks, and documents as well as selected items from the internet. The literature study looked at three major themes. These included a study of similar interoperability schemes in markets similar to Zambia, a study of some blockchain use cases and one on a theoretical model on the use of blockchain technologies to solve technological problems.

The section first looks at some background information on payments and settlement in general and mobile money as a particular type of payment option.

2.2 Payments, Clearing and Settlement Processes

2.2.1 Introduction

Payments are the financial instruments used globally to transfer value in the form of money. A payment system is a set of processes and technologies that transfer monetary value from one entity or person to another [16]. Payments are typically made in exchange for the provision of goods, services or to satisfy a legal obligation. They can be made in a variety of currencies using several methods such as cash, cheques, electronic payments and cards. The essence of a payment system is that it uses cash-substitutes, such as cheques or electronic messages, to create the debits and credits that transfer value.

The value that is being transferred is typically stored in depository accounts at banks or other types of financial institutions. The banks, in turn, are connected to a set of payment systems that they use to process payments on behalf of their customers or depositors.

2.2.2 Payment Process

In the simplest case involving the traditional banking system, payments involve four participants:

a) The payer: Makes the payment and has its bank account debited for the value of the transaction.

b) The payer’s financial institution: Processes the transaction on the payer’s behalf.

c) The payee’s financial institution: Processes the transaction on behalf of the payee and generally holds the value in an account.

d) The payee: Receives value of the payment by credit to its accounts.

An illustration of the payment process is given in Figure 2-1 of the two banks who may choose to transfer payment instructions and funds directly with each other. It is also possible for the banks to use various intermediaries to help facilitate the transaction. The figure refers to these intermediaries as “network”. In the real world the network includes central banks along with clearinghouses and also information transmission mechanisms such as the Society for Worldwide Interbank Financial Telecommunications (SWIFT) [17] and other payment systems.

Non-traditional payment systems such as Bitcoin [18] bypass the banking system almost entirely by fulfilling the roles of financial institution, currency and network themselves.

The payment process typically involves four basic steps as follows:

a) Payment instructions are the information contained in a wire transfer or check. These instructions are from the payer and tell the paying bank to transfer value to the beneficiary through the network and receiving bank.

b) Payment generation is when the instructions are entered into the system—e.g. printed on a check or transmitted via ACH or wire.

c) Clearing is the process where the banks use the payment information to transfer money between themselves on behalf of the payer and the beneficiary (payee).

d) Settlement is the final step in the basic process and occurs when the beneficiary's (payee's) bank account is credited and the payer's bank account is debited. Final settlement occurs when the banks irrevocably pass value among themselves, a distinction that has important treasury implications.

The actual payment process will depend on the type of payment instrument that the payer and payee choose to use—or have chosen for them by their financial institutions.

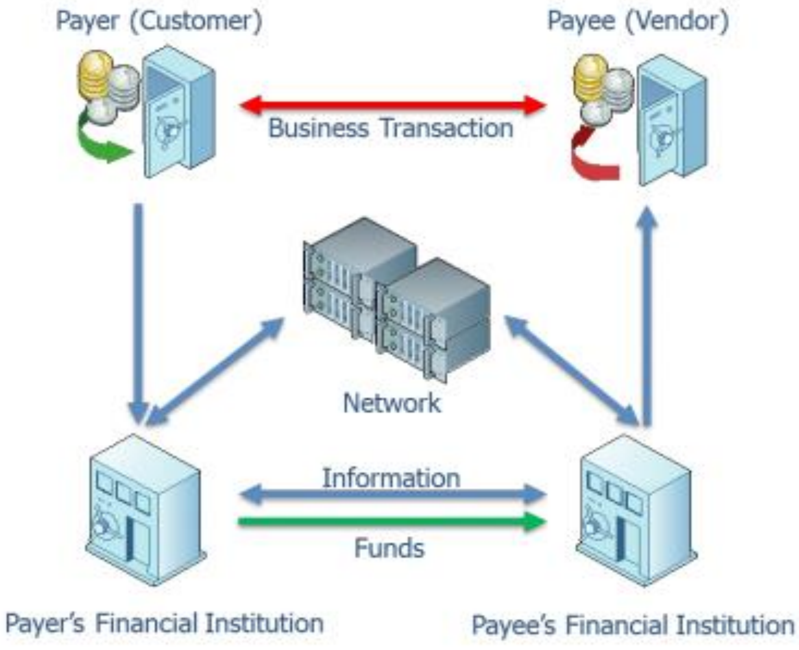


Fig. 2-1 Four Corners Payment Model[1]

[1] Source: Fundamentals of payment Systems. https://www.treasuryalliance.com/

2.2.3 Settlement Process

Settlement, sometimes called availability, refers to the actual movement of funds from the payer’s account to the payee’s account. It is different from finality which is the point in time when the payee knows that the money involved cannot be taken back by the payer or the payer’s bank. Settlement becomes final when a payment is unconditional and irrevocable.

Finality varies depending on the payment system and the parties involved in the transaction. For example, payment systems that offer immediate and irrevocable value are called Real Time Gross Settlement (RTGS) systems [19]. Others, such as cheques-based systems, provide immediate information with value following shortly. But the value is sometimes contingent on the payer or the payer’s bank not attempting to retract the payment, a right which can exist for sixty days or more depending upon the payment system. This can be a major issue for global companies using many different low value payment systems that feed into some sort of cash pooling or concentration system.

While the amount of a rescinded payment may not be large, accounting for the rescission can prove challenging, particularly when it involves two currencies. From the bank perspective the actual transfer of funds, or settlement, can be handled in several different ways. In a domestic transfer, one in which all parties are in the same country, settlement is often handled between the banks using common accounts held at their central bank.

In a cross-border payment involving more than one country, banks typically use depository accounts with each other, called correspondent accounts, to settle their customers’ funds transfers with the correspondent banks using their reserve accounts on behalf of their clients. Settlement through correspondent banks is illustrated in Figure 2-2.

In the figure, the sender based in the United Kingdom has an obligation in US dollars to a beneficiary in Singapore. Because currencies are always settled in the country of currency the sender’s bank and the beneficiary’s bank are required to use correspondent banks located in the US that have accounts with the Federal Reserve. This makes the transaction similar to the high-value example shown earlier with the addition of two intermediary banks. This addition adds a level of complexity—and cost—to a very basic transaction. It also impacts the quality of the information that travels with the payment which can often be truncated, removed or replaced with an intermediary bank's reference number.

Banks operating in multiple countries connect to payment systems in each of the countries where they operate either directly or through a correspondent bank. Significantly for the settlement process and for the discussion of less conventional payment systems, banks in many countries typically maintain accounts with a country's central bank and participate in the central bank's payment systems.

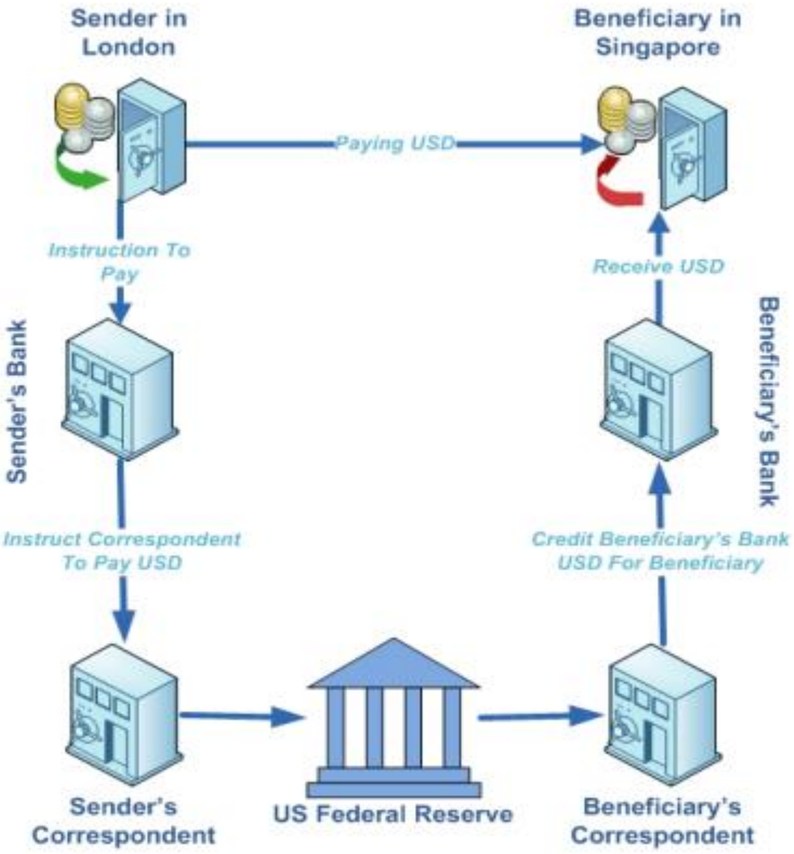


Fig. 2-2 Settlement Process[2]

[2] Source: Fundamentals of payment Systems. https://www.treasuryalliance.com/

2.3 Mobile Money Services

2.3.1 Introduction

Mobile currency or payments made using mobile phones or electronic wallets and other technology devices are becoming increasingly common especially as traditional e-commerce becomes more mobile. Mobile payments are often considered alternative payments in that they use are initiated via phones or smart cards and do not appear to use traditional banking systems. On closer examination, however, most of the current mobile payments programs depend upon traditional payment channels as traditionally provided by banks.

The Zambia financial ecosystem is one such third world country that has seen the rapid rise of the use of mobile much like most of sub-Saharan Africa and this rise is as a result of several factors including easy access to mobile phones and lack of formal banking infrastructure [19].

This section looks at mobile money as a payment option in Zambia with particular focus on the implementation model and regulatory challenges.

2.3.2 Mobile Money as a Payment System

Mobile Money service is a type of Digital Financial Service (DFS) that makes the use of an electronic device or mobile phone application system to access financial services [20]. This is contrasted from a DFS as provided by regular Commercial Banks known as Mobile Banking in that the users of Mobile Money services are not necessarily account holders at the Banks. Mobile Money users instead, make use of their already existing mobile phone numbers as a virtual wallet, storing 'cash' which they can either spend with retailers, pay service providers, transfer to peers, or exchange for physical cash with a participating agent. Corporates also use the service to disburse bulk payments and salaries or receive payments from consumers. As such Mobile money service has become a viable way for the unbanked to access formal financial services for the financially excluded.

Most compelling evidence indicates that increasing access to formal financial services does not only reduce financial exclusion but it has also become an important development goal for stimulating economic growth, increasing welfare and reducing poverty [21]. As such, the recent growth of mobile money has allowed millions of people who were financially excluded from the formal financial system to carry out financial transactions relatively cheaply, securely and reliably [22]. Subsequently, Sub-Saharan Africa has achieved the broadest success in mobile money due to mobile money services that has integrated many adults [22].

2.3.3 Mobile Money Adoption

The highest adoption levels of Mobile money have been observed in East Africa where best example of mobile money in the region is M-Pesa in Kenya, which was launched in 2007 by Safaricom [23]. Mobile money has helped bring 194,000 Kenyans out of poverty [24]. In 2008, Vodacom launched M-Pesa while Zantel launched Z-Pesa in Tanzania [25].

MTN mobile money in Uganda was launched in 2009 with at least 1000 users. Since its launch, several other players like Airtel money, M-cash, Ezee-money, M-Sente and Orange money have also joined the Ugandan market [25].

Micropay is the latest entrant to the Ugandan mobile money market, bringing the number of service providers to seven [26]. This has increased the number of registered mobile money users to at least 21.6 million [26].

Zambia has had its fair share of this rapid growth of mobile money services over the last few years. The major service providers of the service in Zambia include, the major three Mobile Network Operators, Airtel, MTN and Zamtel who operate the Airtel Money, MTN Money and Zamtel Kwacha services respectively [27].

Other providers of mobile money wallet services have emerged in Zambia aside from the Mobile Telecommunications Operators and some of these include Zoona, Broadpay and Kazang [28].

2.3.4 The Zambian Mobile Money Ecosystem

The Mobile money account is linked to the mobile number of the customer. Through an agent of the mobile operator funds may be deposited into or withdrawn from the account. Agents are often referred to in the literature as cash–in and cash-out points of service.

Agents are typically, although not exclusively, general shop owners, distributors, airtime or money change outlets due to their high liquidity. Agents are paid on a commission basis for conducting the transactions. Once funds are in the account a customer is able send money to another person, purchase airtime or other products, pay bills or check their balance directly from the phone using a given application. In some countries, these payment systems have been linked to ATM and POS networks for withdrawals or payments, as well as to banks, so that funds can be transferred between accounts.

The mobile network operator is required by the regulatory authority to hold all of the money in a collective trust account within a selected regulated bank [29]. The accounts are not interest bearing accounts in Zambia, but the funds are protected within the formal banking system. Fees for using the mobile money services are based on the transaction type and vary according to providers. The cost of trying the services is basically free (zero), as there is no cost to open an account or deposit funds.

The figure 2-3 summarizes the main players in a typical mobile money ecosystem [30] as operated in a country like Zambia.

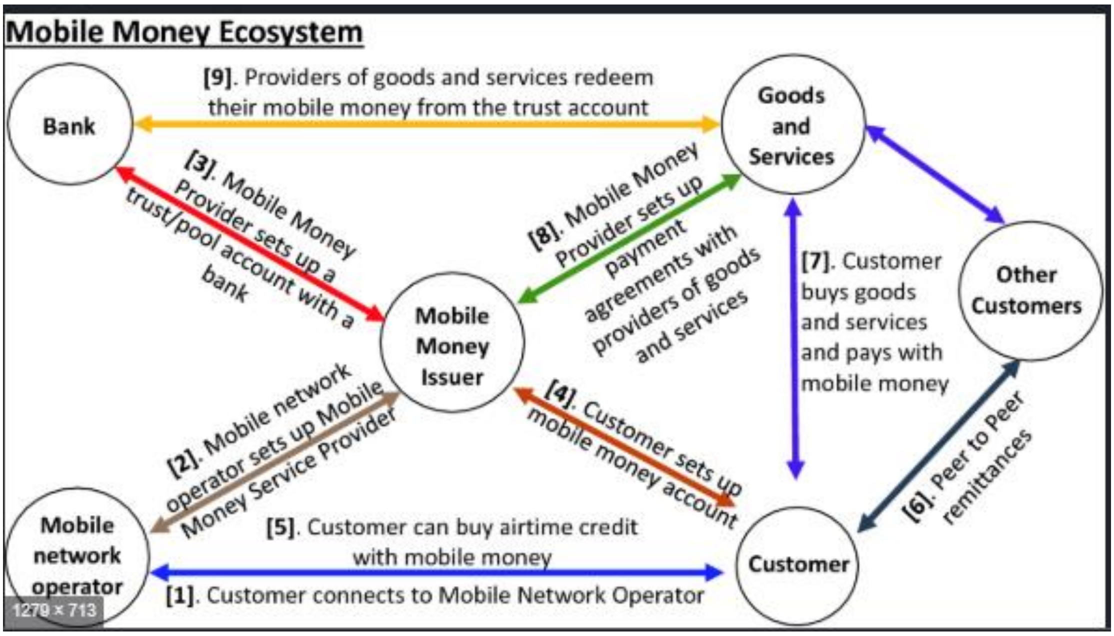

Mobile Money Ecosystem
Bank
[9]. Providers of goods and services redeem their mobile money from the trust account
Goods and Services
[3]. Mobile Money Provider sets up a trust/pool account with a bank
[8]. Mobile Money Provider sets up payment agreements with providers of goods and services
[7]. Customer buys goods and services and pays with mobile money
Other Customers
Mobile Money Issuer
[2]. Mobile network operator sets up Mobile Money Service Provider
[4]. Customer sets up mobile money account
[6]. Peer to Peer remittances
Mobile network operator
[5]. Customer can buy airtime credit with mobile money
[1]. Customer connects to Mobile Network Operator
Customer
1279 × 713

Fig. 2-3 A Typical Mobile Money Ecosystem[3]

2.3.5 Regulatory Issues and Challenges

Regulation of mobile money is very important because mobile money transactions present regulatory challenges that could negatively impact on maximum development benefits [31]. In fact, mobile money blurs the traditionally distinct and independent sectors of regulation (i.e. telecommunications and financial banking sectors) by involving an overlap of multiple ministries and Government agencies which enhances the complexity of oversight needed [31]. Regulators have a duty of articulating a clear policy position on mobile money in particular and digital financial services regulation in general [32]. As such, the regulatory frameworks coupled with the necessary supervisory resources that should accompany any new regulations are supposed to be consistent with regulatory capacity [32].

According to the 2015 study, based on an empirical examination of why mobile money schemes ignite in some developing countries but flounder in other countries found that regulation plays a key role in the success of mobile money service [33]. The findings of the study revealed that most countries where the sector ignited and grew explosively

[3] Source: M. Sunduzwayo. Developments in Mobile Technology and the Emergence of Mobile Money.

did not require a bank to be involved for anything other than to hold funds [33]. While countries that were by far failed to ignite had relatively bank-led model of regulation as opposed to non-bank model regulation in their leading role [33].

2.4 Blockchain Use Cases in Different Industries

A number of blockchain based solutions have been proposed by various researchers across multiple industries over the last few years that the technology has matured. This section highlights some of these solutions.

2.4.1 Distributed Ledger Technology in Payments, Clearing, and Settlement

Firstly, [4] examined the use of Distributed Ledger Technologies (DLT) in general in the area of payments, clearing and settlement and identified both a number of opportunities and challenges facing its long-term implementation and adoption. It was concluded that, DLT has the potential to provide new ways to transfer and record the ownership of digital assets; immutably and securely store information; provide for identity management; and other evolving operations through peer-to-peer networking, access to a distributed but common ledger among participants, and cryptography. Thus potential use cases in payments, clearing, and settlement including clearing and settlement of mobile money transfers between different mobile network operators are possible.

Notwithstanding the fact that since the industry's understanding and application of this technology is still in its infancy, a number of challenges to development and adoption are expected and remain, including in how issues around business cases, technological hurdles, legal considerations, and risk management considerations are addressed.

2.4.2 Bitcoin: A Peer-to-Peer Electronic Cash System

In [10] is proposed a new type of distributed public database (ledger) that maintains a list of transactions in a secure way, preventing alteration of past data. Each transaction is signed by an issuer and submitted to the ledger network. Transactions are collected into blocks that are validated by third party (miners) and stored in the ledger. Once a block is validated it is broadcasted to all network participants, each of the participants maintaining a copy of the ledger. One common application for distributed ledger as envisioned in [10] was creation and management of custom currencies and financial instruments. Bitcoin is one such example which is the first digital currency issued and managed using blockchain technology.

2.4.3 Blockchain in Clinical Records Management

Further calls for the need for tamper-resistant data stores solutions are made in [34] by proposing the use of a write once and read multiple times data storage solution. Similar calls are echoed in the use case that attempts to solve problems in today's methods of recording and sharing of patient data in the management of clinical records [35]. Here it is argued that a blockchain technology has the potential to solve the records management problems by providing a single, secure, decentralized storehouse of clinical data for all patients.

2.4.4 Air Traffic Management

Yet another solution is proposed in this use case [36] for an Air Traffic management solution. A blockchain based infrastructure is proposed aimed at providing security, authentication and privacy of data in the management of air traffic.

2.4.5 Open Parking Slot Management

A solution for parking slot management in a trust-less network is proposed here [37] through the use of blockchain technology which seeks to provide a parking slot management platform capable of being used without a third trusted party.

2.4.6 Blockchain in Pharmaceutical Industry

In [38] and [39] blockchain technology is analysed and use case scenarios are identified in many financial and non-financial sectors. One of the identified sectors is the pharmaceutical sector where blockchain can introduce transparency and trust to the supply chain. As concluded, the technology offers data security and cost-effective transmission of transactions in peer-to-peer networks with no central system.

2.4.7 Food Storage Tracking

In [40] a decentralized traceability system based on IoT and blockchain is proposed for the food industry. The system relies on IoT devices (RFID, WSN, and GPS) devices to collect and transmit data to a BigchainDB ledger database. All actors participating in the process are required to be registered and receive unique private keys to sign the transactions.

2.4.8 Blockchain in Supply Chain

In [41] proposes a hybrid architecture for supply chain management based on a set of private distributed ledgers for storing sensitive customer information and a public ledger where a hash of each private event is stored along with the monitoring events.

In [42] is briefly presented a system called LifeCrypter, which is a blockchain solution aimed at increasing supply chain security for the pharmaceutical industry. In this system, each item is attached an identity tag which allows for virtual ownership of the product to be transferred while it moves in the supply chain. Transactions are verified and validated by means of smart contracts.

Yet another use case is proposed for use of blockchain technology in supply chain finance system [43]. Like many such similar use cases proposed, the goal to implement a secure and trusted system that takes advantage of the blockchain properties of transparency, immutability and shared consensus [44].

2.4.9 Data Centre Management

In [45] a The largest costs associated with e-government projects are the infrastructure costs which this paper argues could be reduced to fractions of what they are today or completely eliminated if existing Blockchain are leveraged. With advancements made in cryptography, cloud computing, data access and storage techniques, governments world over can evolve seamlessly towards true cloud governments by taking advantage of the models implemented in current and future Blockchain technologies. The inherent nature of governments is to keep information in an unaltered state for reference by future generations. The internet and its latest application, Blockchain technologies provide the best solution for the continuation of government.

2.4.10 Summary of Blockchain Use Cases

Blockchain technologies present opportunities that could be utilized to solve a number of technological challenges because of a number of desirable features [46]. These include the distributed ledger which is shared among a private group of users connected through the local area network, or with thousands across the internet. A message is relayed on creation of every new block, to ensure that all users have a latest version of the ledger. Since the ledger is stored on multiple storage devices, possibly in different locations, it also protects the system from data loss in case any devices or servers face downtime [47]. Other users can continue accessing and adding information on the blockchain, as long as there is at least one online device that has the latest version of the blockchain.

Secondly data stored in the blockchain is made secure and immutable using cryptography meaning that there may be no tampering of the data once it is written to the ledger and can only be read back [48].

A number of technological solutions have thus been proposed or implemented across many industries that make the use of these blockchain features [49]. Literature reviewed investigated blockchain features that make it usable in a use case of mobile money account to account interoperability clearing and settlement. An enterprise blockchain platform such as Hyperledger fabric [50] possess practical features that make it ideal as a solution platform for implementation of this use case as it supports non cryptocurrency based blockchain implementations.

2.5 Blockchain Decision Framework

In this study we envisage the use of blockchain technology to design and implement a clearing and settlement system that is going to enable interoperability among the mobile money service providers in Zambia. A review of literature around characteristics of blockchain technologies was done. The rationale was to learn features of the technology that make it usable and in which particular situations. This was to establish a decision framework to be used to test our proposed solution since as pointed by [51], despite the enthusiasm for blockchain technology, it should not be considered as a "magic bullet" for all use cases.

A number of decision models have been proposed that act as a guideline for the choice of a blockchain technology depending on the use case [52] [51]. We present some of these in this section.

2.5.1 The B. Scriber Model

This was a study conducted to gain insights on how application architectures might or might not benefit from blockchains. The study considered literature review and interviews with companies using blockchains for production of products or services, and evaluations of 23 blockchain implementation projects [53]. These studies findings were used to identify questions which were codified to create a framework for the evaluation of an architecture's level of fit for blockchain technology. This framework uses an evaluation form (shown in Table 2-1) to estimate a total percentage of fit from assigned weights of ten different characteristics. The score is then used to determine whether a given implementation's core might be low or high.

The first problem with this approach is that it works using weighted scores which are largely subjective of affirmation for questions related to the characteristics set. As has been pointed out in the study, the tool therefore, can only be used primarily to help its users perform a relativistic comparison of projects and carefully evaluate whether a blockchain is appropriate for the ecosystem under consideration [53]. Secondly, the

Table 2-1. A Form for Evaluating a Blockchain's level of Fit[4]

Architecture or blockchain characteristic	**Example subjective suggested weighting**	**Weight (this column must add up to 100)**	**Subjective percentage of affirmation**	**Weight * affirmation**
Immutability: Will the architecture never need the ability to execute a command with update or delete semantics?	12			
Transparency: Does the architecture require transparency between actors?	12			
Trust: Does the ecosystem currently lack trust between participants?	16			
Identity: Must participants and actors be mapped to their transactions, or do those transactions have a value to be claimed by a participant?	5			
Distribution: Can the implementation manage and afford distribution of nodes and participants? Does the system have multiple writers?	10			
Workflow: Would the addition of a distributed ledger simplify workflow?	5			
Transactions: Does the system follow a transactional model, or is the data transactional?	12			
Historical record: Is the project ready to assume the fiscal, legal, distributive, and cryptographic responsibilities of running this chain for an indeterminate time period?	8			
Ecosystem: Does the architecture support an ecosystem as opposed to a single company?	15			
Inefficiency: Will the architecture support a Blockchain's security overhead, search limitations, and transactional verification model?	5			

study is based on evaluations of the 23 implementations and lessons from other blockchain experiments and might therefore, not necessarily be representative of all use

[4] Source: B. Scriber, IEEE Software Architecture, 2018

cases and might not apply to all environments [54]. Another problem with this tool is that it is rather complex and it uses too many questions covering concepts which may well have been combined rather than split as has been done in alternative approaches [55]. The tool also is not detailed enough and does not provide for determination of what type of blockchain technology may be fit as others do [56].

2.5.2 Cathy Mulligan Model

In their paper [57], Mulligan et al proposed a practical framework that is designed to assist executives in understanding whether blockchain is an appropriate and helpful tool for their business needs. This is a flow chart based model (Figure 2- 3) that helps one to make an assessment of whether or not they need a blockchain for their use. The model uses eleven (11) key questions to assess blockchain suitability to a given problem. It starts from the premise that blockchain is merely a technology (much like many others that are already used in society) and like other technologies it is as much about change management and careful attention to the economics and business models of industries and companies involved as it is about technology evangelism.

Aside from being long as opposed to alternatives [58], this model is rather too restrictive and may not be usable in some cases. The first two questions for example, are looking at removal of brokers and digital assets rather than a more general case such as need for storing state [59].

Another potential shortfall of this model is that it is rather inconclusive in some cases leading options like “Blockchain can’t do this efficiently yet” and “Blockchain may work”.

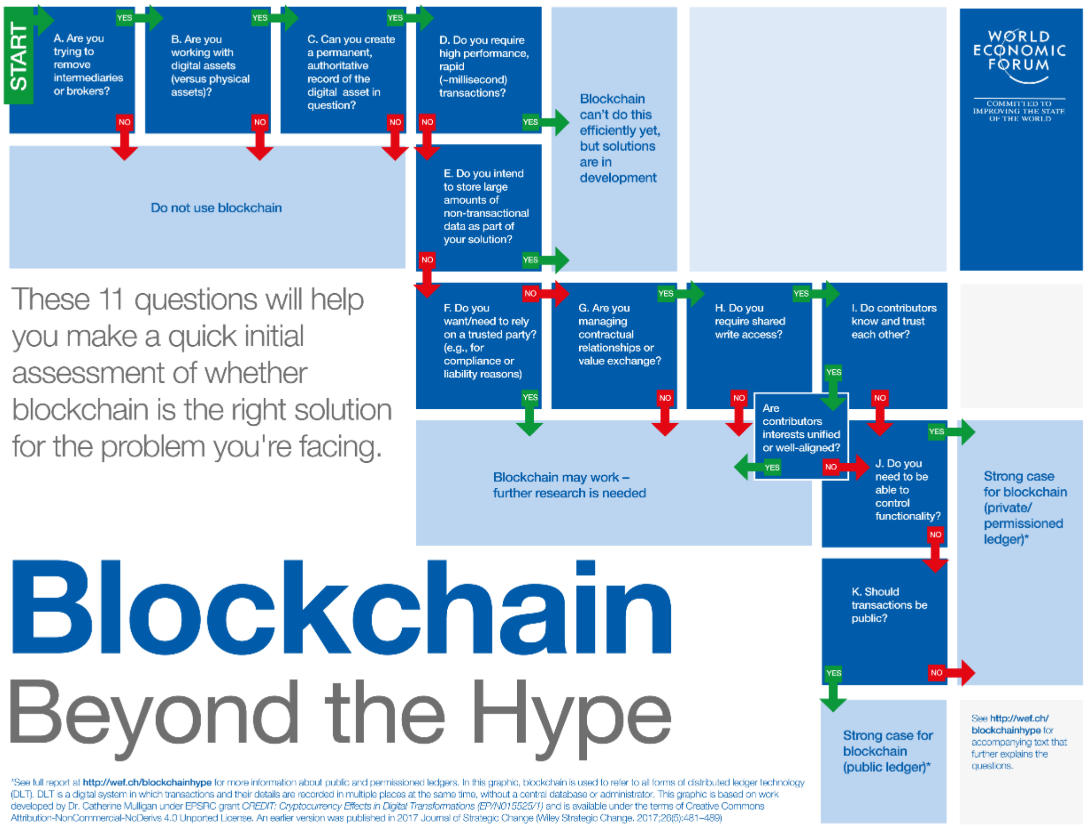

START
A. Are you trying to remove intermediaries or brokers?
YES
NO
B. Are you working with digital assets (versus physical assets)?
YES
NO
C. Can you create a permanent, authoritative record of the digital asset in question?
YES
NO
D. Do you require high performance, rapid (~millisecond) transactions?
YES
NO
Blockchain can't do this efficiently yet, but solutions are in development
WORLD ECONOMIC FORUM
COMMITTED TO IMPROVING THE STATE OF THE WORLD
Do not use blockchain
E. Do you intend to store large amounts of non-transactional data as part of your solution?
YES
NO
These 11 questions will help you make a quick initial assessment of whether blockchain is the right solution for the problem you're facing.
F. Do you want/need to rely on a trusted party? (e.g., for compliance or liability reasons)
NO
YES
G. Are you managing contractual relationships or value exchange?
YES
NO
H. Do you require shared write access?
YES
NO
I. Do contributors know and trust each other?
YES
NO
Are contributors interests unified or well-aligned?
YES
NO
J. Do you need to be able to control functionality?
YES
NO
Blockchain may work – further research is needed
Strong case for blockchain (private/ permissioned ledger)*
Blockchain
Beyond the Hype
K. Should transactions be public?
YES
NO
Strong case for blockchain (public ledger)*
See http://wef.ch/blockchainhype for accompanying text that further explains the questions.
*See full report at http://wef.ch/blockchainhype for more information about public and permissioned ledgers. In this graphic, blockchain is used to refer to all forms of distributed ledger technology (DLT). DLT is a digital system in which transactions and their details are recorded in multiple places at the same time, without a central database or administrator. This graphic is based on work developed by Dr. Catherine Mulligan under EPSRC grant CREDIT: Cryptocurrency Effects in Digital Transformations (EP/N015525/1) and is available under the terms of Creative Commons Attribution-NonCommercial-NoDerivs 4.0 Unported License. An earlier version was published in 2017 Journal of Strategic Change (Wiley Strategic Change. 2017;26(5):481–489)

Fig. 2-4 A blockchain decision tree by Mulligan[5]

2.5.3 Claus Pahl and Sven Helmer Model

Another decision framework is proposed by Pahl and Helmer [60] which focuses on blockchain technology for Internet of Things (IoT) [61] and edge computing [61]. The proposed model does a good job of separating the decision tree into parts with the goal of the first part being to answer the question when to use blockchains and what platforms to use while the second part investigates a set of properties that can be used to compare existing systems. The model also clearly identifies the different kinds of blockchain outcomes in great detail, i.e. permissioned [62] and permission-less [63] blockchains.

The problem with this model however, is that it is not clear on the decision regarding the existence of a trusted authority. It may be ideal to define the role of the third party as far as transaction processing is concerned. Some use cases exist where despite there

[5] Source: www.wef.ch/blockchainhype

being a trusted authority, which trusted authority may not necessarily be always online in transaction processing and would therefore, not be an ideal central data host. The model is also specific to IoT and no demonstration of its applicability was made in other use cases and we may therefore, not be able to accurately generalise from it. An illustration of this model is given in Figure 2-4.

2.5.4 Karl Wüst and Arthur Gervais Model

A much simpler but yet detailed enough model is presented here [64] by Wüst and Gervais. This is also a flow chart model that only uses six questions to arrive at four different possible outcomes and so is much simpler compared to alternatives [52]. This model was found more suitable as it provides a detailed description of the decisions leaving less room for misinterpretation. The model also fits the basic criteria of the major questions that need to considered when assessing a blockchain use case as pointed out by [65] and [51].

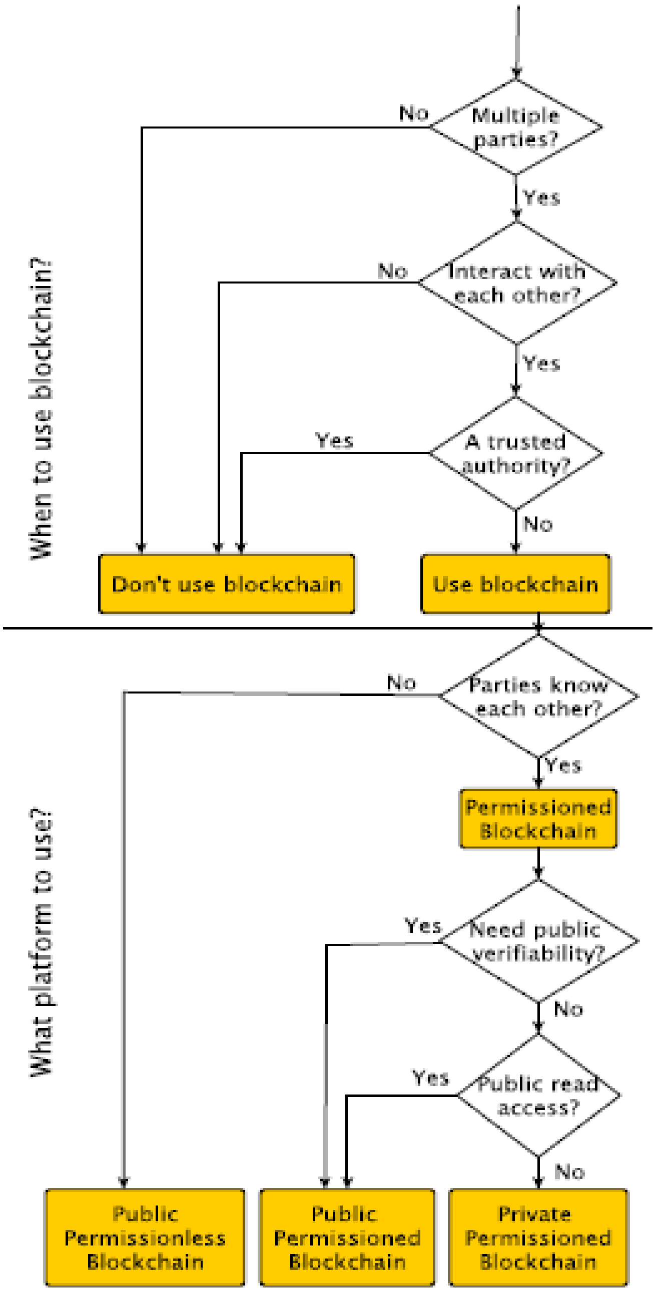


Fig. 2-5 A blockchain decision tree by Pahl[6]

[6] Source: Claus Pahl and Sven Helmer, 2018

2.6 Related Works

2.6.1 Introduction

In their basic sense Mobile payments platforms allow their users to pay and transfer funds in mobile money, but also offer access to other financial products, such as savings and bill payments. A study in [66] reviewed the economic features of mobile payment systems in developing countries, and studied the cooperation models that can emerge between the different firms potentially involved in a mobile payment transaction. Focus was drawn on the main competition concerns that public authorities should be concerned about, and which regulatory tools could be considered as a remedy.

Key among some of the key challenges in mobile money schemes was the issue of interoperability. Different concepts of interoperability are relevant and need to be distinguished according to their implications for regulation and business models.

Different approaches have been undertaken by different countries in an attempt to implement interoperability for their mobile money financial systems. This section reviews a number of such proposed architectures for mobile payments that support mobile money interoperability in a number of Countries. These have been drawn from well-developed mobile money markets and they include India, Kenya, Rwanda, and Tanzania.

2.6.2 Mobile Money Interoperability in India

In 2008 the Reserve Bank of India (RBI) issued guidelines for interoperability among prepaid payment instruments providers specifying among others, requirements for achieving interoperability [67]. These guidelines were aimed at, among other things, facilitating money transfer between different digital wallets. This was to be done through the regulator provided Unified Payments Interface (UPI), the Indian government’s instant payment interface. The UPI model is however, a central integrating node to which all the different mobile wallet providers will need to integrate which may lead to integration complexities. Further, only bank backed mobile wallets that have valid know you customer details captured by the participating banks are eligible to transact in this model leaving out other unbanked customers. Support of new features by the providers is also a challenge in such a model as changes always need to be made the integrating node to accommodate those features.

Alternative architecture approaches for mobile payments that support interoperability, universality and simplicity in the context of highly regulated markets where the customer's mobile phone number is linked to a bank account number such as India have proposed in this study [68]. The study propose three possible options for customer details lookup during processing and these include a central database, a peer-to-peer query and a hierarchical lookup. The paper concludes that initially, among the options considered, the most suitable design for the Indian markets is the peer-to-peer design. This option involves the least complexity and setup time in the current situation where only a small number of subscribers use mobile payments. As the system size increases, the central database option should become the preferred solution.

Other options in the Indian landscape include, the Mobile Payment Foundation of India [69] which is also developing a model for interoperability. Further, Kumar et al. have proposed architectural choices for interoperability [69]. However, their model is specific to highly regulated financial environment in India, where every transaction is processed by a bank.

2.6.3 Mobile Money Interoperability in Kenya

Kenya has one of the most well established mobile money markets in the African region. Common services being the provision of person–to-person money transfer on the mobile money platforms, targeting the low end unbanked customers. These have over the years been expanded to incorporate other transactions including person-to-business (payment of bills, shopping), business-to-business, and credit and savings services, buying and transferring of airtime among others.

Like most developing countries, Kenya's mobile money market landscape is made up of multiple providers and thus suffers the same problems of lack of interoperability as identified [70]. Among MNO-led mobile money initiatives in this region, Mpesa, pioneered by the leading Mobile Network Operator (MNO), Safaricom Ltd is the most well-known and a dominant player in the market. Others include Airtel Kenya and Telkon Kenya [71].

Interoperability has not been mandated under the Kenyan National Payments System (NPS) regulations. The regulator has however, allowed payment service providers are to enter into interoperable arrangements on their own for purposes of providing account to account interoperability [72]. The NPS regulations define interoperability as "commercial interconnectivity between providers of different payment systems or payment instruments including the capability of electronic systems to exchange messages and 'interoperable' shall be construed accordingly" [73]. Under this definition, the Central Bank of Kenya (CBK) has left it to the market to determine how providers interoperate.

The CBK has not taken a prescriptive approach to interoperability, but it has gone to great lengths to propose a framework within which interoperability may be conducted. The NPS regulations permit the Central Bank to recognise a Payment Service Provider Management Body (PSPMB), whose intent is to facilitate interoperability amongst payment service providers. To this effect interoperability in Kenya has thus far been through bilateral arrangements between mobile money providers [74] rather than through a common central switch system.

But as has been observed by [75] a common switch, with its own set of rules for participation, technical and operational issues, improves coordination and customer experience, and allows for a much faster implementation of interoperability, as compared to private switches or bilateral agreements.

2.6.4 Mobile Money Interoperability in Rwanda

Like Kenya and the other East African countries, Rwanda has an equally mature and highly competitive mobile money landscape [76]. Again similar product offerings are on offer by the different mobile money providers and these include balance maintenance, deposits, withdrawals and transfer of funds with convenience that is not currently being met by the commercial banks to the poor unbanked. Despite mobile money services having been operational for a long time now, Rwanda equally does not have a formalized central clearing and settlement system that offers interoperability for the mobile money providers. This study [76] reviewed the regulation of mobile money aspects in Rwanda and considered among others, interoperability for the country with the aim of fostering a conducive financially inclusive society. The study proposes a light handed regulatory approach owing to the highly technical and capital intensive nature of the mobile money industry.

While countries like Kenya have bilateral based interoperability models in place of a central integrator mode, Rwanda has yet been to establish one. New regulation in Rwanda requires interoperability of all payment systems before integration could be realised. What has rather been observed in this market however, is the fact that subscribers transacting across networks through the use of agents. For example, an MTN user can always send money to a Tigo user, but the receiver will have to visit an MTN agent to withdraw the cash and the charges are slightly higher. In addition, if the subscriber then wants to use that cash on the Tigo system, he will have to visit a Tigo agent to make the deposit – so getting cash from a deposit in one system to a deposit in another requires visiting two agents. Interoperability between the Rwanda banking system and mobile money services is similarly available in a weak form – it requires a physical visit to a bank branch. The next step in interoperability would allow the remote payment from an account on one provider directly into the account of another via a command from a mobile phone or bank branch.

2.6.5 Mobile Money Interoperability in Tanzania

There are four different mobile network operators all providing mobile money services to their subscribers in Tanzania [77]. Tanzania is one of the most successful mobile money markets in the world with more than 25 percent of the population being active mobile money users (with almost eleven (11) million in December 2013) and transacting an estimated Two billion United States Dollars in transactions per month in 2014 [77]. According to a study [4] by the Global System for Mobile Communications (GSMA) on account to account (A2A) interoperability models in Tanzania and Pakistan, A2A interoperability was launched in Tanzania in 2014, and in Pakistan in 2015. The study found that in both Pakistan and Tanzania, the regulatory environments were enabling for A2A interoperability and that providers freely choose the technical model that best suited their commercial interests rather than being restricted to a pre-determined or preferred model defined by regulation. This has led to Tanzanian mobile money providers opting for bilateral point to point integrations as a preferred model for interoperability [78].

As been pointed out by [2], bilateral models may seem easy to deploy where there are limited parties involved but later suffer several disadvantages including the increase in complexity with number of parties, duplication of efforts and an increases in complexity of maintenance over time.

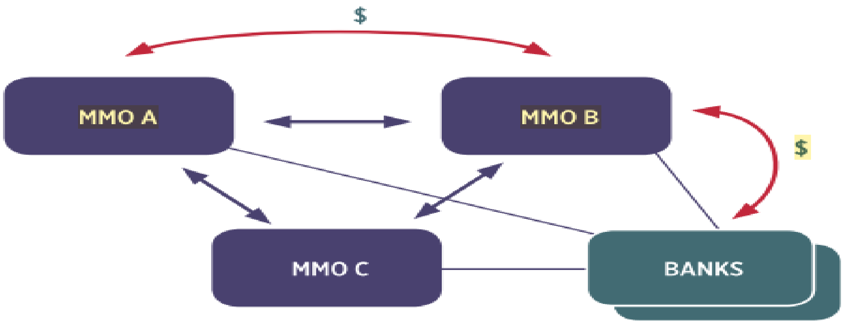


Fig. 2-6 Bilateral Arrangement[7]

[7] Source: GSMA, 2014 A2A Interoperability. Making Mobile Money Schemes Interoperate

2.7 Summary

In this chapter we gave a comprehensive overview of the background theory and some examples of the related works to attempts at solving the interoperability problem as far as mobile money is concerned.

Literature studied showed a number of different approaches to interoperability employed in different countries. One such an approach is the use of a Central Bank led national switching system for clearing and settlement. Mobile Money services in Zambia are regulated by the Central bank and therefore, this makes the use of a central switch an ideal and suitable enough approach to interoperability. So far, the technological setup used in such an approach has been with a central database system. A number of problems with this approach have been pointed out including, complexity of integration, introduction of a single point of failure and lack of trust.

This paper therefore proposed a blockchain based solution approach to address these shortfalls. A number of blockchain use cases were presented to highlight some of the properties of blockchain that make it a suitable technology to address these problems. A review of the decision models to test blockchain suitability was also done.

CHAPTER THREE:

METHODOLOGY

3.1 Introduction

Chapter two of this report presented a literature review of available research works related to the current study. It presented an analysis of studies of markets similar to that of the one under this study. It also looked at studies around similar use cases of the technology that is proposed so as to place the present study into context with the existing body of knowledge. Chapter three of this report focuses on the description of the methods that were applied in carrying out the research.

The chapter is structured around two major areas covering the main areas of the study and these are the baseline study which includes: mixed methods research methodology, descriptive research design, target group, sample size, data collection tools, data analysis, ethical considerations, limitation of the study and presentation of findings and the system design methodology that was followed as a structured approach to software development.

3.2 Study Methods Overview

A study was conducted to propose a secure and trusted settlement and clearing system that will enable account to account interoperability among the mobile money providers in Zambia. The study was guided by three (3) objectives. Firstly, a targeted survey and interviews were conducted to establish how mobile financial services are currently implemented in Zambia. Further, literature and documentation on mobile money system and service implementation was consulted to understand how they are setup. The goal was to try to establish and highlight short falls and inefficiencies in implementation that prevent interoperability and thereby identify opportunities for improvements.

Secondly, an analysis as to whether a conceptual model for inter operator mobile financial transactions payments, clearing and settlement in a secure, transparent and trusted manner could be proposed and designed. The goal was to establish if blockchain [79] technology would be an ideal technology to achieve the proposed design.

Finally, we carried out an implementation of a prototype that demonstrates Blockchain security services in a permissioned and regulated environment [80]. The designed system was a prototype system in which amounts being interchanged between mobile money providers are managed as assets on a permissioned blockchain [62]. The system runs a distributed shared ledger [81] which prevents amount theft as well as fraud such as transferring invalid amounts, or transferring multiple copies of an amount, by leveraging the data consistency features of the blockchain [82].

3.3 Baseline Study

This section describes the process used to establish the mobile money technological landscape. A list of interview questions were designed into a survey and administered to a targeted audience of respondents, deliberately selected according to set criteria. Further, walk in interviews were conducted with subject matter experts to validate and verify researched literature and documentation on mobile money systems and service implementation. The goal was to try to establish and highlight short falls and inefficiencies in implementation that prevent interoperability and thereby identify opportunities for improvements in the solution design.

3.3.1 Target Group

The research participants were purposively selected basing on their expertise, experience and skills relating to the subject under study in order to get rich and relevant information. Survey participation was drawn from employees of Zambia's mobile money operators and employees from Zambia’s mobile money regulatory and supervisory authority, Bank of Zambia (see Table 3-1). The operators included the major Mobile Network Operators (MNOs), Airtel (who run the Airtel Money service), MTN (who run the MTN Mobile Money service) and Zamtel (who run the Zamtel Kwacha service).

Participation was further extended to non-MNO providers who have been running money transfer services on mobile and have since extended their product offerings to include the mobile wallet features on their services. These providers equally allow customers to hold money and transact off those accounts. These included Zoona (who run the Zoona Plus wallet), Broadpay (who run the Broadpay wallet) and cGrate (who run the Konse Konse wallet).

Table 3-1. Survey Participants

Category	**Targeted Participants**	**Completed Responses**
Mobile Money Service Providers	31	16
Regulatory Authority	9	6
Total	40	22

3.3.2 Sampling Rationale

Due to the specialized nature of the data that the research required, survey respondents had to be conveniently sampled.

The Bank of Zambia, for example, is the regulatory authority that supervises and regulatory financial services providers in Zambia. They do this through among others registration and designation of payment systems and institutions as well as oversight of both systemic and non-systemic payment systems [83]. The central bank is also responsible for the clearing and settlement infrastructure and processes in the country. It was felt strongly therefore, that they would be well positioned to provide information on payment system interoperability from regulatory and standards perspectives. Participation therefore, was also drawn from a number of Bank of Zambia staff with varying specializations. These included Payments Systems specialists, Financial

Institutions Supervision specialists, Information Systems specialists and Information Systems Security specialists. Table 3-2 summarizes the participants drawn from the regulatory authority.

Table 3-2. Regulatory Authority Participants

Role	Participants
Payment Systems Analyst	2
Payment Systems Management	2
Financial Systems Examiner	3
ICT Security Specialist	1
Application Development Management	2

The MNO participants targeted were those involved in the development and management of mobile money system operations and therefore, were well-informed and provided relevant information that guided the investigation. Different specializes among these was also considered to obtain a fair representation of all areas being investigated.

Participation was drawn from mobile money development specialists who are charged with the design of mobile money products and services on behalf of the enterprise. Information Technology systems administrators and managers responsible for the technical operations of the mobile money systems and infrastructure were also considered as credible sources of data for the study.

Employees in IT leadership and security and compliance roles were also considered to provide further insight into the study from a strategic and governance perspective. Table 3-3 summarizes the selected targeted participants from Mobile Network Operators and the other mobile wallet service provider organizations.

Aside the survey, data about mobile money operations such as the customers' terms of operation, agents' recruitment forms, mobile money operation training manuals, mobile money regulation guidelines and system documentation were reviewed and critically analyzed to further inform the study.

3.3.3 Other Sources of Data

Further in this research, analysis of existing data sources was another method that was used to gather data. Secondary sources of data were reviewed through internet search. Secondary data is data that were collected from other studies. Secondary data analysis was found more ideal for this study as proved to be faster and less costly method owing to the time constraint of the study. Key terms, including 'mobile money', 'mobile money interoperability', 'payment, settlement and clearing' were used to aid the search for data relating to the research study. The secondary data was analyzed to arrive at a more complete understanding of mobile money technologies and the security mechanisms employed in them.

Mobile money system integration documentation from network operators was also studied to understand how integrations are done between the network operators and the financial institutions and third party vendors.

To ensure that our study list is comprehensive, we used relevant keywords to search in multiple computer science research paper repositories, including journals and digital libraries. We also explored the citations and references of all the papers to and any previous or leading work that is within our scope.

Table 3-3. Participant Areas of Specialization

Role	Participants
Mobile Money Product Specialist	6
IT Administrator	10
IT Systems Manager	8
CTO	2
Security and Compliance	4

3.3.4 Research Survey Approach

This section describes the process and rationalization that was used to come up with an instrument to be used to collect data having sampled the population.

These questions were then formatted into a survey questionnaire and administered to the respondents as an online survey. Follow ups were done where necessary with one to one interviews with the respondents. The following section describes the breakdown of the survey questionnaire sections and the significance of each.

The questionnaire was divided into four (4) different sections as shown in the Table 3-4. The different parts of the questionnaire were used to capture different aspects of the data as described in the following sections.

PART I – Demographic Data

This section was used to capture data about the respondents organization types, the names of the organization and what level of hierarchy the respondents were in their respective organizations.

PART II – Organization Size

The second section was aimed at organization size in terms of a number of different parameters. These included numbers of employees in the respondent's organization, their mobile subscriber base and the distribution of this subscriber base according to segments of high value, medium and low value. The organizations were also looked at in terms of the volume of transactions they generate in a given period as well as their service coverage areas to estimate the size and complexity of the organization.

PART III – Mobile Money Systems

This section looked at the state of the Mobile Money systems implementations in the participating organizations. Areas covered here included whether the participating organizations used technological solutions for their mobile money platforms, ownership of those technological systems and the types or vendors of the systems. Particular consideration was put on the availability of interfaces for outside integrations to these systems. The goal was to understand how these technological landscapes work and identify shortfalls that make interoperability fail or complicated.

PART IV– Mobile Money Systems Integration

Finally this section looked at integration aspects in terms of whether there was desire for interoperability from the stakeholders both from the service operators and the service regulators. Of particular interest was the security requirements desired in this interoperability and a determination of whether a blockchain based solution would be an ideal fit to address these security requirements. Specific questions on blockchain security features of trust, transaction immutability and provenance were thus included to bring out these aspects.

Table 3-4. Survey Breakdown

Group Order	Group Name	Description
1	PART I	Demographic data of respondents
2	PART II	Respondent organization size
3	PART III	Mobile Money platforms in Zambia
4	PART IV	Mobile Money Systems Integrations and desired security requirements

3.3.5 Data Collections and Analysis Tools

The survey questionnaire was created on an online open source platform called LimeSurvey [84] and distributed electronically to respondents for ease of administration. Tracking and follow up of responses was done online to ease the management of the survey.

Data analysis for the study was done by computer based software known as Microsoft Excel [85]. Microsoft Excel is a proprietary computer program that is developed and maintained by the Microsoft Corporation.

3.3.6 Ethical Considerations

Ethical clearance through authorization was awarded to the researchers by the institutions where the research was conducted from, by means of introductory letters which were given to authorities and respondents. Similarly, all questionnaires administered, did not allow respondents to disclose their names or any information that would review their status and ultimately compromise on confidentiality.

3.4 Decision Model

For the second part of the study, we looked at how or whether a blockchain based solution would be ideal for this use case. This was necessary because unlike in Bitcoin's permission-less blockchain, where any writer and reader can join at any time, permissioned blockchains have restricted read and write access thus share close similarities with a centralized database systems. This thus naturally brings up the question whether a blockchain is better suited than a centralized database.

A flow chart based decision model was therefore, adopted and used to determine the suitability of the technology to be adopted as proposed by Wüst and Gervais [64] . The model used here is shown in Figure 3-1. Other such similar models have been proposed [54], [51], [56], [59], [86]. This model was found more suitable as it provides a detailed description of the decisions leaving less room for misinterpretation. The model consist of a decision tree based on a number of properties highlighted in the following section.

3.4.1 Decision Model Tree Properties

A) **Storing of State**. This property refers to the need of storing data that may change both in volume and in content over time. If no data needs to be stored, no database is required at all and consequently, a blockchain, as a form of database, is of no use.

B) **Existence of Writers.** These entities that have write access to the stored state and as such, are able to accumulate transactions within a block and append this block to the blockchain. They represent entities that have a common interest in agreeing on the validity of the stored state.

C) **Trusted Third Party**. A Trusted Third Party (TTP) is a centralized entity that could manage changes and updates the state. A TTP, if present, may also control who can read the state stored.

D) **Status of Writers**. This refers to knowing the identity of all writers.

E) **Writers Trust**. When writers are trusted, they are expected not to behave maliciously. When writers are not trusted, they may behave maliciously.

F) **Public verifiability of state**. This property determines who may read the state stored on the blockchain, and verify the integrity of the ledger.

Based on these six properties, the model determines one of four possible solutions as the best solution for the scenario. The following are the possible outcomes as summarised in Figure 3-1.

a) Permission-less blockchain. Anyone may join the network and read from the state stored, and write to the blockchain.

b) Public permissioned blockchain. A limited set of participants may write to the blockchain. Anyone may join the network and read the state.

c) Private permissioned blockchain. A limited set of participants may join the network, and write a new state. Only this set can read the state.

d) Don't use blockchain. This end state is reached when one of the properties (A), (B), (C) or (E) in the tree is not met.

The model also recommends consideration of other properties that are highlighted in the following section.

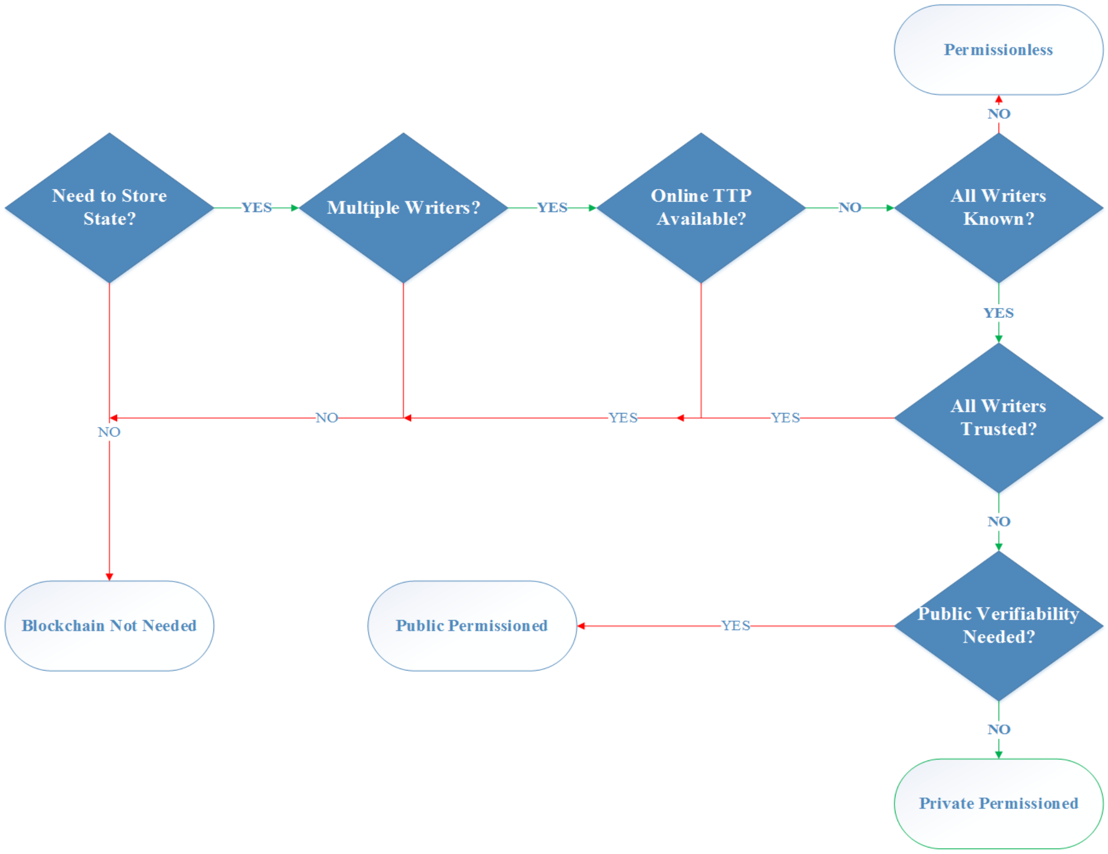


Fig. 3-1 Flow Chart to Determine Blockchain Suitability [8]

3.4.2 Other Properties Considered

The table 3-5 highlights the differences between permissionless, permissioned blockchains and a centralized database as other properties that also key to the decision process.

Table 3-5. Other Properties to Consider

	Permissionless	**Permissioned**	**Central DB**
Throughput	Low	High	Very High
Latency	Slow	Medium	Fast
Number of readers	High	High	High
Number of writers	High	Low	High
Number of untrusted writers	High	Low	0
Consensus mechanism	Mainly PoW	BFT protocol (PBFT)[9]	None
Centrally managed	No	Yes	Yes

[8] Adapted from: Wust and Gervais, 2017

[9] Practical Byzantine Fault Tolerance [115].

3.5 System Automation

The following outlines the prototype design and development processes that were followed in the study. It presents the formal software development methodology followed as well as the various architectural layouts of the proposed system and their associated practical implementation details.

3.5.1 Development Methodology

A formal software development methodology was followed during the design and implementation of the solution prototype proposed. The system development process followed an Object Oriented Analysis and Design methodology (Figure 3-2) [87]. In particular the Object Modelling Techniques (OMT) phases [88] were used to model the different aspects of the prototype as shown in Figure 3-3. The OMT has was used as it proved an easy to understand and use methodology which has proved very successful in many application domains.

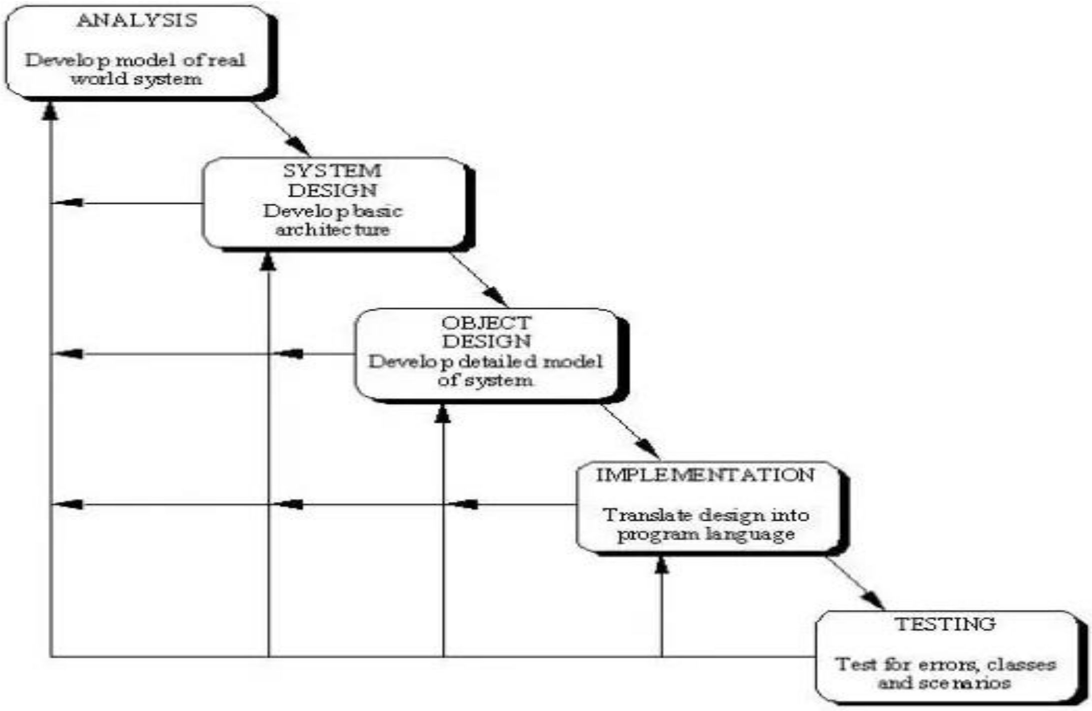

ANALYSIS
Develop model of real world system
SYSTEM DESIGN
Develop basic architecture
OBJECT DESIGN
Develop detailed model of system
IMPLEMENTATION
Translate design into program language
TESTING
Test for errors, classes and scenarios

Fig. 3-2 Iterative OOAD Process[10]

[10] Source: Hunt, Object-Oriented Analysis and Design , 2016

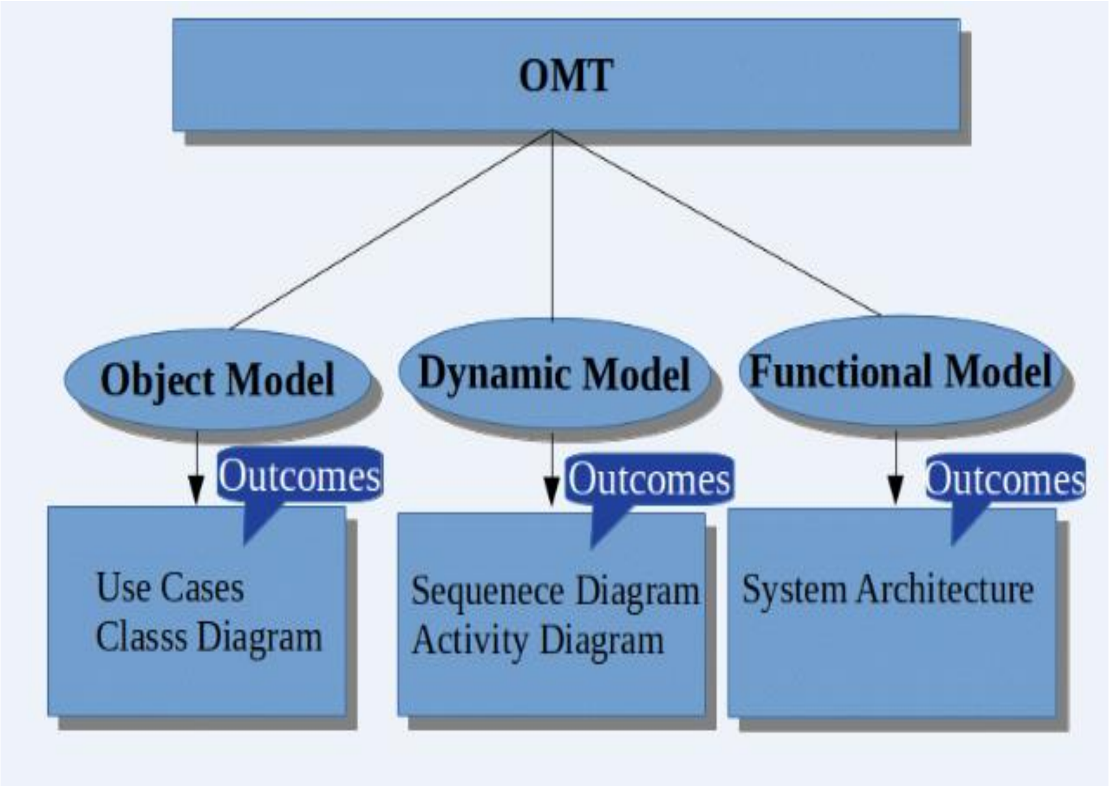


Fig. 3-3 OMT Adaptation[11]

The object modelling techniques is a methodology of object oriented analysis, design and implementation that focuses on creating a model of objects from the real world and then use this model to develop object–oriented software. Now-a-days, OMT is one of the most popular object oriented development techniques. It is primarily used by system and software developers to support full life cycle development while targeting object oriented implementations.

OMT has proven itself easy to understand, to draw and to use. The object-oriented paradigm using the OMT spans the entire development cycle, so there is no need to transform one type of model to another.

The following section presents the deliverables on the OOAD phases followed. A summary of these models are depicted in Figure 3-3.

[11] Source: Hunt, Object-Oriented Analysis and Design , 2016

A) Object Model

The Object Models capture and represents the static structure of the application. Operations in an object model corresponds to events in dynamic model and functions in functional model. The following object model types were used in this study.

(i) Use Cases

(ii) Class Diagrams

B) Dynamic Model

The Dynamic Model is a state change model that represents the essential behaviour of the application. It specifies when particular functionality happens in the system. It also describes the control structure of the objects. It defines decisions which are dependents of object values and which can cause action to change object values and invoke their functions. The following are the dynamic types that were used in this study.

(i) Sequence Diagrams

(ii) State Activity Diagram

C) Functional Model

The Functional Model captures and is used to represent what the application does and not necessarily how it does. It specifies what happens. It describes functions to be invoked by operations in object model and actions in dynamic models. For this study, because this model represents functional structure, it was adapted to capture functional architectures of the system. The following were thus outputs of this model.

(i) System Architecture

(ii) Blockchain Network Architecture

3.5.2 Proposed Network Architecture

This section highlights the proposed network architectural layout of the solution. It show the major nodes that at a high level that are participating in the solution. A detailed node layout is also presented later in the section.

A) Network Design Overview

The proposed framework consists of a common replicated ledger in which transferred amounts are managed as assets on a permissioned blockchain based on Hyperledger Fabric [50]. A summary of the network layout is presented in Figure 3-4. Hyperledger Fabric is an open source permissioned distributed ledger technology (DLT) platform, designed for use in enterprise contexts. Fabric was chosen because of its highly modular and configurable architecture that makes it adaptable to a number of use cases. Fabric also supports the use of general purpose programming languages such as Java [89] in the development of smart contracts [90] and therefore, was an ideal choice for this prototype. Blockchain approach was used to provide key security requirements of confidentiality, origin authentication, non-repudiation and availability [91].

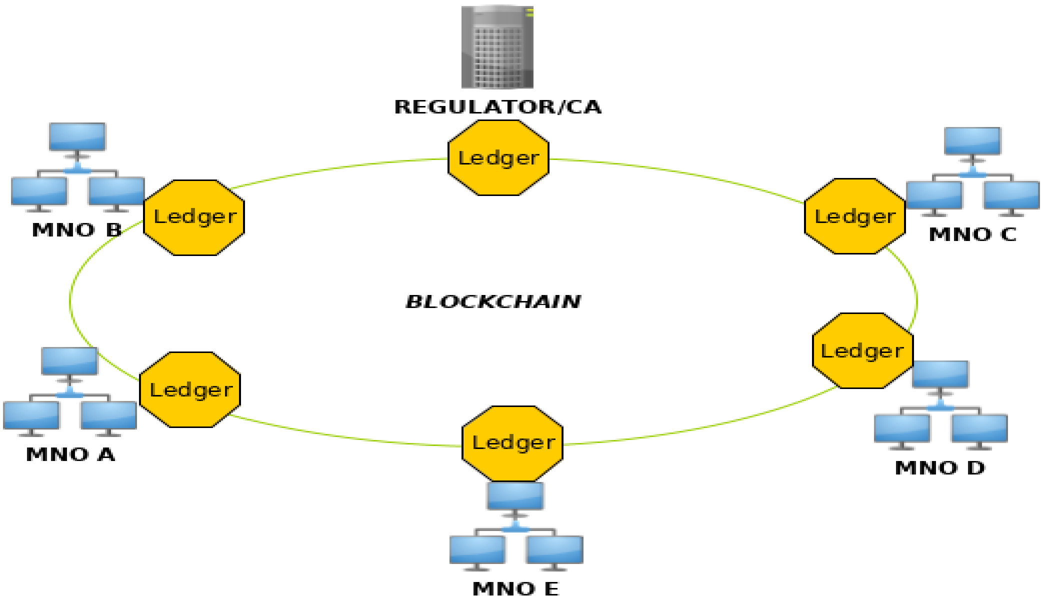


Fig. 3-4 Blockchain High-level Network Architecture[12]

[12] Source: hyperledger-fabric.readthedocs.io

The network layout is depicted in Fig 3-4 as a shared, replicated, permissioned distributed ledger where all participants have a copy of the ledger alongside their systems and data. The blockchain architecture gives participants the ability to share a ledger that is updated every time a transaction occurs through peer-to-peer replication [92]. The solution is a shared, replicated, permissioned distributed ledger where all participants have a copy of the ledger alongside their data. The novel blockchain architecture gives participants the ability to share a ledger that is updated every time a transaction occurs through peer-to-peer replication. Cryptography [93] is used to ensure that network participants see only the parts of the ledger that are relevant to them, and that transactions are secure, authenticated, and verifiable.

Blockchain also allows the contract for asset transfer to be embedded in the transaction database determining the conditions under which the transaction can occur. Network participants agree on how transactions are verified through consensus [3] or similar mechanisms. Oversight, compliance, and audit can be part of the same network.

Blockchain technology consists of the following components to permit the effective collaboration of the players in a business network [94]:

Shared Ledger – An append-only distributed system of records shared across the business network so that all participants have visibility on what is happening.

Smart contract – Business terms embedded in the transaction database and executed with transactions so that the appropriate contracts are executed when a transaction occurs.

Privacy – Ensure that transactions are secure, authenticated, and verifiable.

Trust – Transactions are endorsed by relevant participants.

Transparency – All participants in the network are aware of all transactions that impact them.

Key blockchain characteristics include consensus, provenance, immutability, and finality around the transfer of assets within business networks, hence reducing costs, time and risks, ensuring data quality, and increasing trust [95]:

Consensus – All participants agree that a transaction is valid.

Provenance – Participants know where the asset came from and how its ownership has changed over time.

Immutability – No participant can tamper with a transaction once it's agreed upon. If a transaction was in error, then a new transaction must be used to reverse the error, with both visible.

Finality – There is one place to determine the ownership of an asset or completion of a transaction. This is the role of the shared ledger.

B) Detailed Fabric Network Architecture

The Figure 3-5 shows the main nodes and components that make the proposed solution. Nodes are the communication entities of the blockchain. A node is only a logical function in the sense that multiple nodes of different types can run on the same physical server and may not necessarily be a single server as a whole [96].

Depicted in the Figure 3-5 is an example involving three participants in the network labelled as Org1, Org2 and Org3. Each of participants maintains their own mobile money systems. As part of the Hyperledger fabric network, each participant also runs nodes called peers which allows them to connect to the rest of the blockchain network. These peers receive transaction requests from participant systems though an Application Programming Interfaces (APIs) provided by the Software Development Kit (SDK). Each pair of participants (org1 and org2 for example) connect through a separate channel interface that allows them to maintain data privacy between the two. The Orderer node is responsible for ordering and writing transaction requests to the ledger before replication.

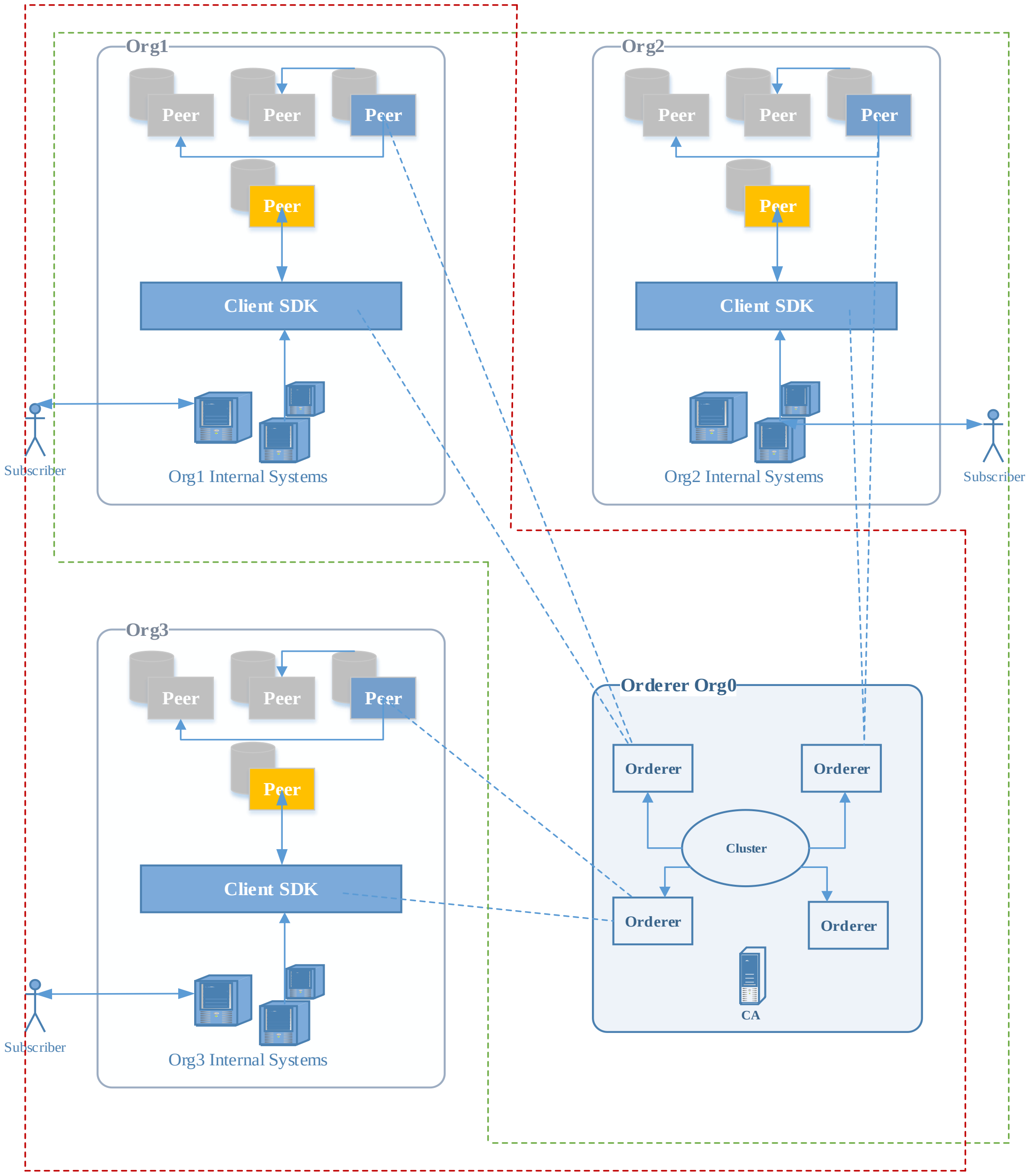


Fig. 3-5 Fabric Detailed Network Architecture[13]

Presented below is an overview [97] of the main components depicted in the network architecture.

C) Network Nodes

Nodes are the communication entities of the blockchain. A "node" is only a logical function in the sense that multiple nodes of different types can run on the same physical server.

[13] Source: hyperledger-fabric.readthedocs.io

There are three types of nodes:

(i) Client or submitting-client: a client that submits an actual transaction-invocation to the endorsers, and broadcasts transaction-proposals to the ordering service. The client represents the entity that acts on behalf of an end-user. It must connect to a peer for communicating with the blockchain. The client may connect to any peer of its choice. Clients create and thereby invoke transactions

(ii) Peer: This is a node that commits transactions and maintains the state and a copy. Peers can also have a special endorser role whose only function will be to endorse transaction-proposals. A peer receives ordered state updates in the form of blocks from the ordering service and maintain the state and the ledger.

(iii) Ordering service nodes (Orderers): The orderers form the ordering service, i.e., a communication fabric that provides delivery guarantees. The ordering service can be implemented in different ways: ranging from a centralized service (used e.g., in development and testing) to distributed protocols that target different network and node fault models. Ordering service provides a shared communication channel to clients and peers, offering a broadcast service for messages containing transactions. Clients connect to the channel and may broadcast messages on the channel which are then delivered to all peers. The channel supports atomic delivery of all messages, that is, message communication with total-order delivery and reliability. In other words, the channel outputs the same messages to all connected peers and outputs them to all peers in the same logical order. This atomic communication guarantee is also called total-order broadcast, atomic broadcast, or consensus in the context of distributed systems. The communicated messages are the candidate transactions for inclusion in the blockchain state.

D) Channel

A fabric network can have multiple channels. Channels allow organizations to utilize the same network while maintaining separation between multiple blockchains. Only members (peers) of the channels are allowed to see the transaction created by any member in a channel. In other words, channels partition the network in order to allow transaction visibility for stakeholders only. Only the members of the channel are involved in consensus, while other members of the network do not see the transactions on the channel. The peer can maintain multiple ledgers. And peer can be connected to multiple channels.

E) Ledger

It is a current state of the business as a journal of transaction. A ledger consists of two different parts, a world state, and a blockchain. A ledger is kept at all peers and, optionally, at a subset of orderers. In the context of an orderer, we refer to the Ledger as the OrdererLedger, whereas in the context of a peer we refer to the ledger as to PeerLedger. PeerLedger differs from the OrdererLedger in that peers locally maintain a bitmask that tells apart valid transactions from invalid ones.

F) Blockchain

A transaction log that records all the changes that have resulted in the current world state. Its data structure is different as once written cannot be removed. It is immutable. It is a historical record of facts about how the objects arrived at the current state. It is structured as a sequential log of interlinked blocks, where each block contains a sequence of transactions, each transaction representing a query or update to the world state.

Each block header includes a hash of blocks transactions, as well as a copy of a hash of the previous block's header. The first block in the chain is the genesis block.

G) Certificate Authority

The Certificate Authority (CA) is used for user management and certificate issuance tasks.

H) Fabric Transaction Flow

The Figure 3-6 describes the step-by-step workflow of Fabric transaction invocation. Firstly, at step 1, **Client** node makes a transaction proposal, signs the proposal with the user’s certificate, and sends the transaction proposal to a set of pre-determined **Endorsing Peers** on a specific channel.

Then each **Endorsing Peer** verifies the user’s identity and authorization from the proposal payload. If the verification check passes, Endorsing Peer simulates the transaction, generates a response together with a read-write set, and endorses the generated response using its certificate.

Then the **Client** node accumulates and checks the endorsed proposal responses from Endorsing Peers.

In step 4, the Client node sends the transaction attached with the endorsed proposal responses out to Orderer.

Step 5, the **Orderer** orders the received transactions, generates a new block of ordered transactions, and signs the generated block with its certificate.

In step 6 the Orderer then broadcasts the generated block to all Peers (to both Endorsing Peers and Committing Peers) on the relevant channel. Then, each Peer ensures that each transaction in the received block was signed by the appropriate Endorsing Peers (i.e., determining from the invoked chaincode’s endorsement policy) and enough endorsements are present. If the verification check passes, the transaction is marked as valid and each Peer’s world state is updated. Otherwise, the transaction is marked as invalid without updating the world state. Finally, the received block is appended into each Peer’s local blockchain regardless of whether or not the block contains any invalid transactions.

Finally the Client receives any subscribed events from EventHub service which is this system, the participant’s organisation systems will use perform further processing such as updating the subscribers account.

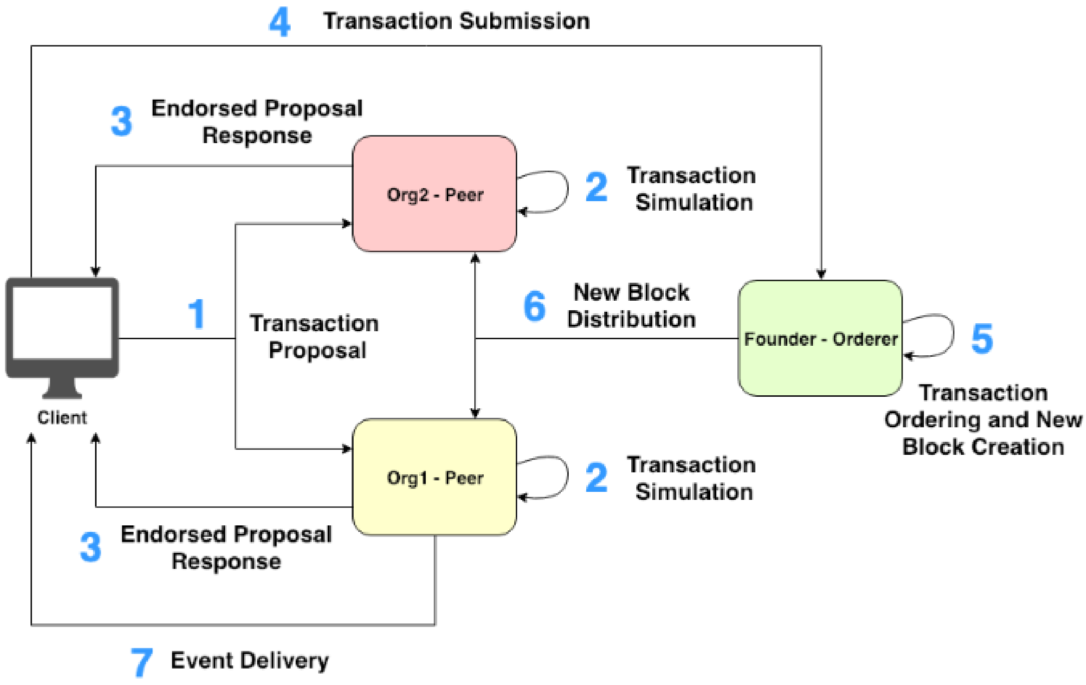


Fig. 3-6 Fabric Transaction Flow[14]

I) Hyperledger Fabric Compared with Traditional Application

Finally in this section we look at a comparison of the full stack fabric layout and that of a traditional database based application system [98]. The Figure 3-7 summarises this comparison. The main different at the top layer is that fabric is decentralised which the traditional application need not necessarily be. In both cases the layer is concerned with the visual aspects of the application.

The connection interface to the business logic in fabric is through client SDK while traditional applications rely on connector libraries such JDBC or ODBC [99].

The data manipulation logic in traditional applications is through query languages while Hyperledger fabric relies on smart contract implementations called chaincode [95] which controls the business logic. The underlying layer that is responsible for data persistence is usually the DBMS in traditional applications while fabric uses the fabric Network of nodes.

[14] Source: hyperledger-fabric.readthedocs.io

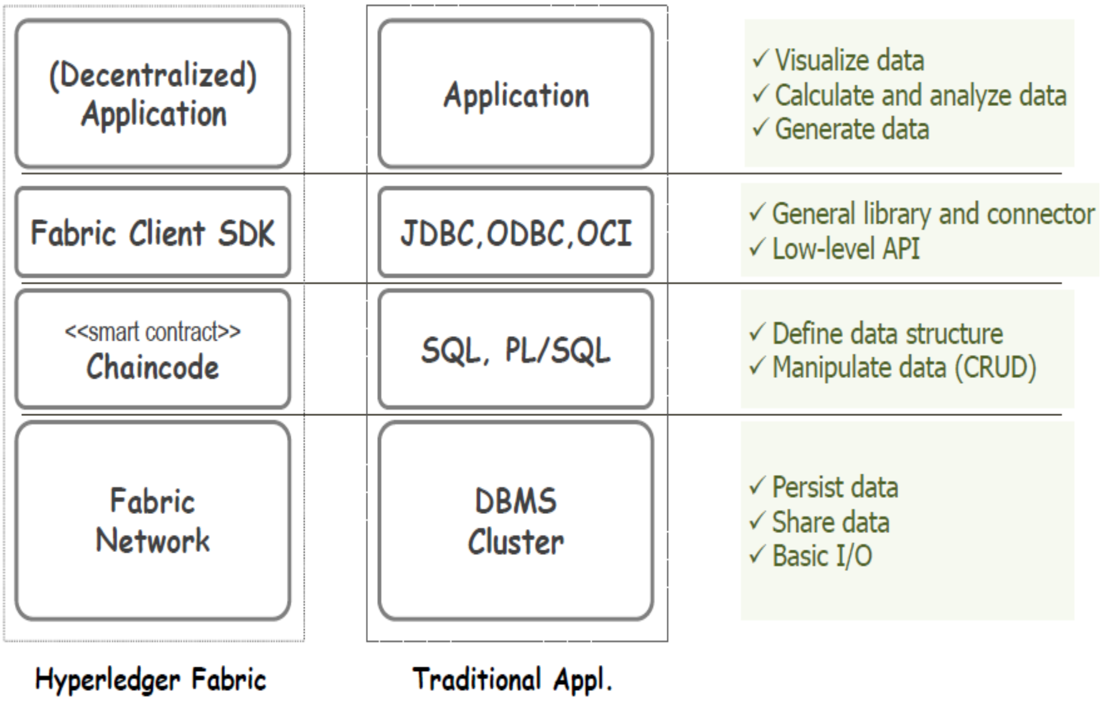


Fig. 3-7 Fabric Full Stack Compared with Traditional Application[15]

3.5.3 Smart Contract Design

This section highlights the application logic design of the proposed solution. At the heart of a blockchain network is a smart contract. A smart contract defines the different states of a business object and governs the processes that move the object between these different states [98]. The object oriented analysis and design methodologies presented earlier were used to design and implement the smart contracts for the system.

A) Smart Contract (Chaincode)

Smart contracts are important because they allow developers to define the key business processes and data that are shared across the different organizations collaborating in a blockchain network.

Chaincode is a program, written in Go, node.js, or Java that implements a prescribed interface [100]. Chaincode runs in a secured Docker container [101] isolated from the

[15] Source: Sangmoon Oh

endorsing peer process. Chaincode initializes and manages the ledger state through transactions submitted by applications.

A chaincode typically handles business logic agreed to by members of the network, so it similar to a “smart contract” [100]. A chaincode can be invoked to update or query the ledger in a proposal transaction. Given the appropriate permission, a chaincode may invoke another chaincode, either in the same channel or in different channels, to access its state. Note that, if the called chaincode is on a different channel from the calling chaincode, only read query is allowed. That is, the called chaincode on a different channel is only a Query, which does not participate in state validation checks in subsequent commit phase.

Hyperledger Fabric offers a number of SDKs to support developing smart contracts (chaincode) in various programming languages. There are three smart contract SDKs available for Go, Node.js, and Java [94]:

- Go SDK documentation.
- Node.js SDK and Node.js SDK documentation.
- Java SDK and Java SDK documentation.

Currently, Node.js and Java support the new smart contract programming model delivered in Hyperledger Fabric v1.4.

In this study, we used the Java SDK and developed the smart contract using the Java development language.

B) Data and Process Design

In this study we propose the design of a system that will enable interoperability among the mobile money providers who will be the participants in the network. These participants will together form a network that will allow them to exchange data on whatever transfers that will take place.

We thus identify the major components of this ecosystem as the participants, the network on which they transact and the asset or assets of value that they transact in.

The main asset that is transacted on the proposed network is a transfer and this represents a request made by one subscriber through a participant to transfer an amount to another subscriber on a different participant's network. We summarise these components in the Figure 3-8.

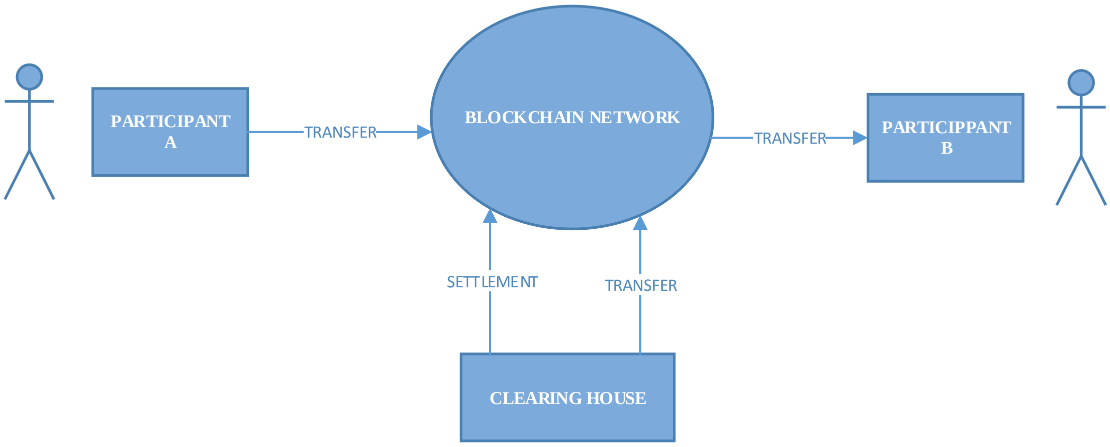


Fig. 3-8 Participants of the proposed system

Next we identify the assets of value being exchanged in the network firstly as a '*Transfer'*. Here a *Transfer* represents the conceptual object of value and is modelled as states, whose lifecycle transitions are described by transactions. The transfer also has properties which sets it as an object in our object oriented model. Table 3-1 shows the transfer as an asset in our network together with its associated key properties.

Table 3-6. A Transfer Asset

Transfer ID	Uniquely identifies a transfer
Sender Mobile Number	Initiator of transfer (and the participant it belongs to)
Receiver Mobile Number	Receiver of transfer (and the participant it belongs to)
Transfer Amount	Amount transferred
Transfer Date	Date of transfer
Current Status	State of the Transfer

The second key asset in the network is the '*BatchTransfer'* which represents a collection of all the transfers that took part in a settlement between any two participants. Like the Transfer, the *BatchTransfer* also represents the conceptual object of value and is modelled as states, whose lifecycle transitions are described by transactions. It also has properties which sets it as an object in our object oriented model. Table 3-2 shows the transfer as an asset in our network together with its associated key properties.

Table 3-7. A BatchTransfer Asset

Batch ID	Uniquely identifies a transfer
Payer	Participant paying the amount in settlement
Payee	Participant receiving the amount in settlement
Net Amount	Settlement Amount transferred
Batch Date	Date of settlement
Current Status	State of the BatchTransfer

C) Use Case Model

Having identified the participants and assets, we looked at the activities or actions that govern the changes to the states of the assets on the network. These are the transactions that govern the asset lifecycle and they have been summarised in a state transition diagram in Figure 3-9. The transfer transitions between requested, fulfilled and settled states by means of the request, fulfil and settle transactions.

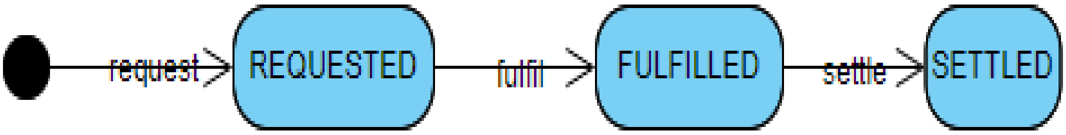


Fig. 3-9 A State Transition Diagram for Transfer Asset

Similarly, the BatchTransfer asset states are shown in Figure 3-10 and they move from PENDING state to SETTLED state through the *createbatch* method and settle transactions.

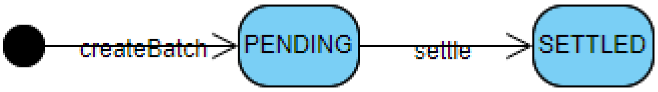


Fig. 3-10 A State Transition Diagram for BatchTransfer asset

The transfer asset is the main asset on the proposed network and this represents a request made by one subscriber through a participant to transfer an amount to another subscriber on a different participant's network. Figure 3-11 shows the main use cases in the system.

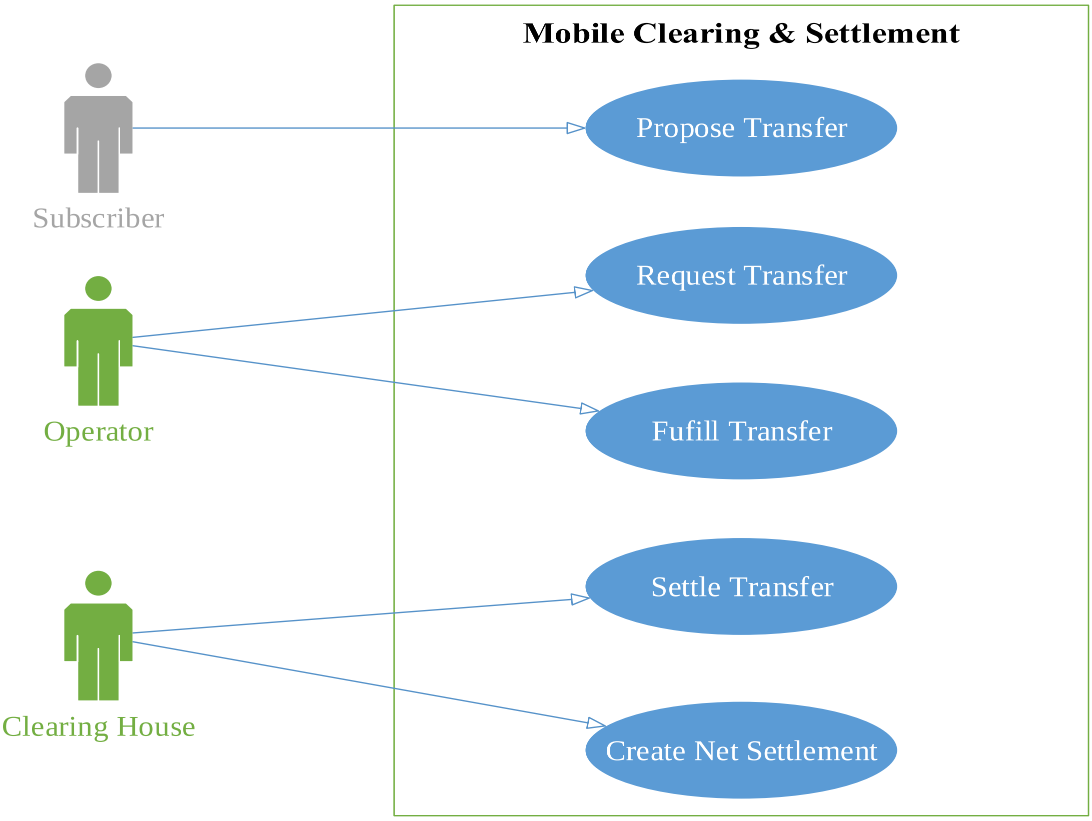


Fig. 3-11 Use Case Diagram

Two main classes of actors are identified in the ecosystem and these are the direct participants and non-direct participants. The direct participants are the mobile money providers that directly take part on the blockchain and the clearing house which is a special institution (the "settler") responsible for netting and settlement. The non-direct actor is the subscriber who participate through the Operator and represents the mobile money subscribers.

D) Object Class Models

On the Blockchain, the Transfer represents the conceptual object of value and is modelled as states, whose lifecycle transitions are described by transactions. A special program called a smart contracts was implemented that models this transaction logic that transitions the transfer between their different states. Smart contracts allowed us to define the key business processes and data that are shared across the different organizations collaborating in the network. Figure 3-12 shows the class model that captures the smart contract and depicts the main objects that make up the smart contract.

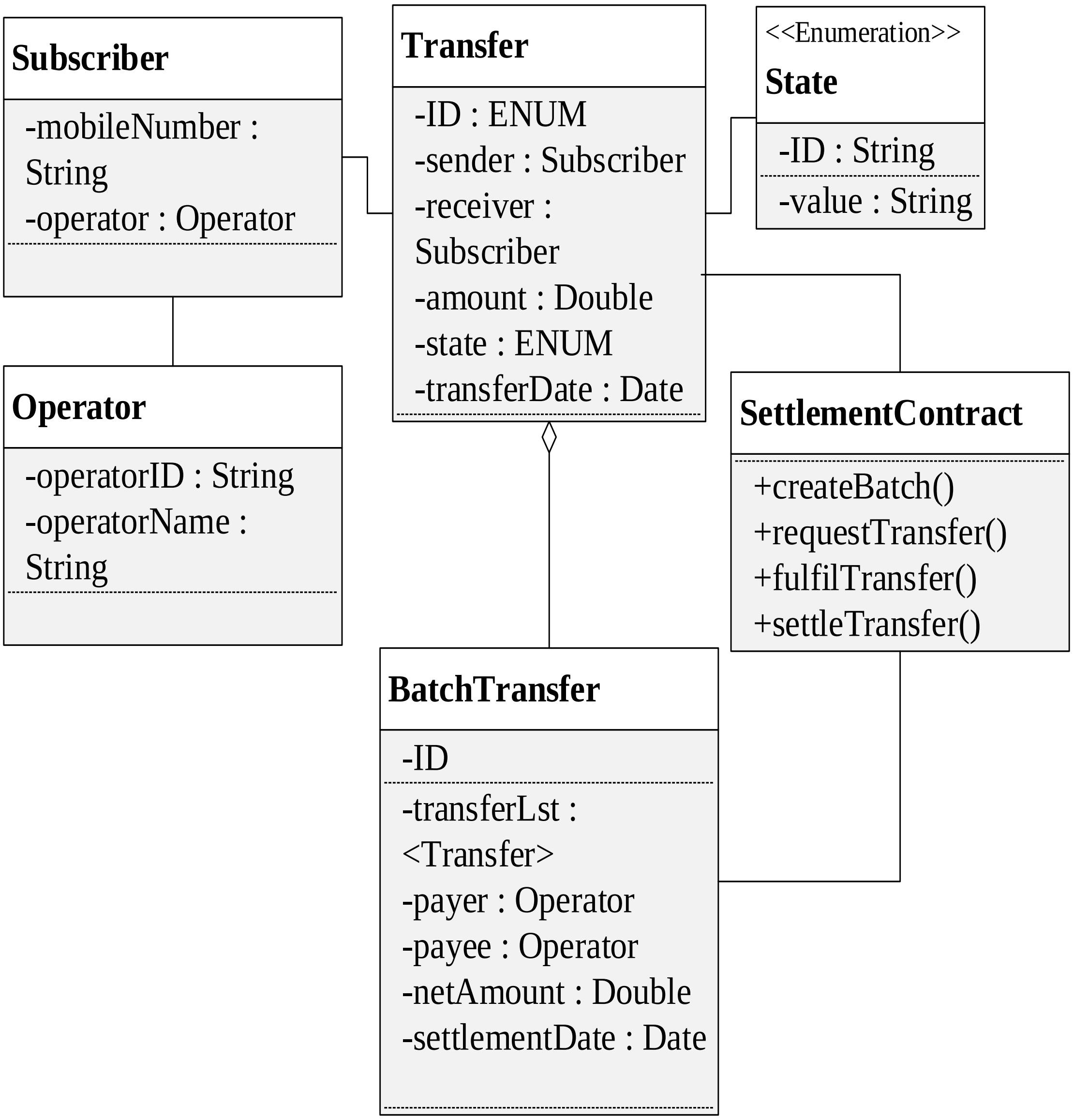


Fig. 3-12 Class Diagram

E) Sequence Models

The following details interactions that take place in the proposed system and is presented as sequence diagrams [102]. Sequence diagrams are not only used to model the interactions between the actors and the objects in a system but also show interactions between the objects themselves [103].

The diagram in Figure 3-13 shows the general sequence of events during the request for a transfer process. The transfer is initiated a subscriber on one network through a participant's client system. The client system then initiate a request to the blockchain to write a new record which is processed until a new block is added to the ledger. Upon completion, an event is generated and sent to the client of the receiving participant as confirmation of the write request. This event then triggers a request to fulfil the transfer by that client which is also processed in a similar until committed to the ledger.

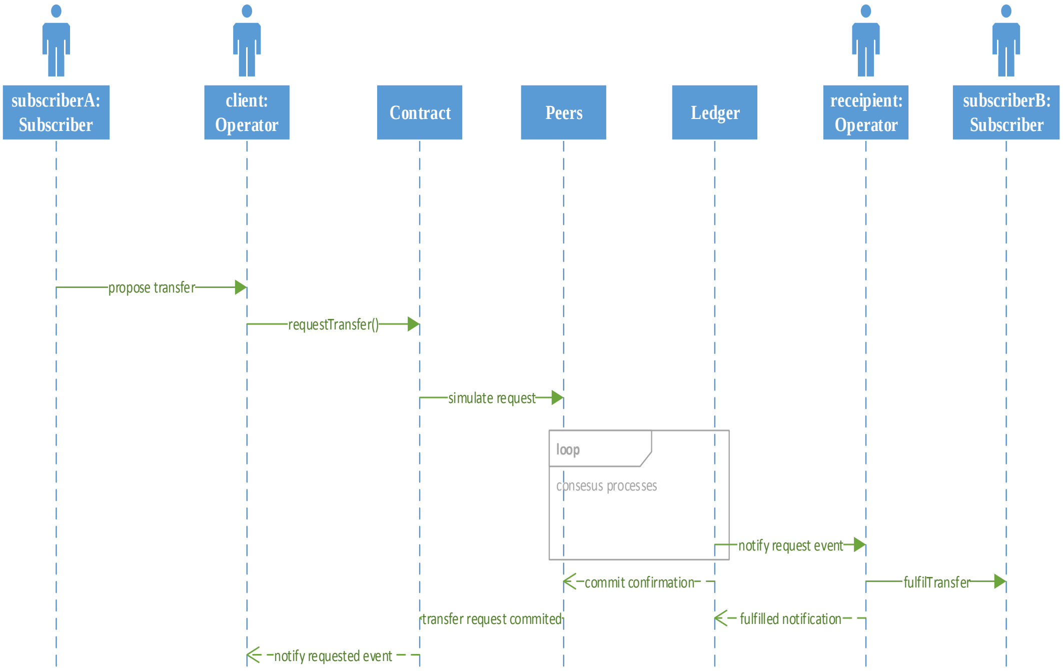


Fig. 3-13 Transfer Request Sequence Diagram

A more detailed sequence of events capturing the consensus processes for a transfer request at the fabric network is shown in the diagram in Figure 3-14. The focus here is on the processing on the peers during consensus validation rather the overall business flow.

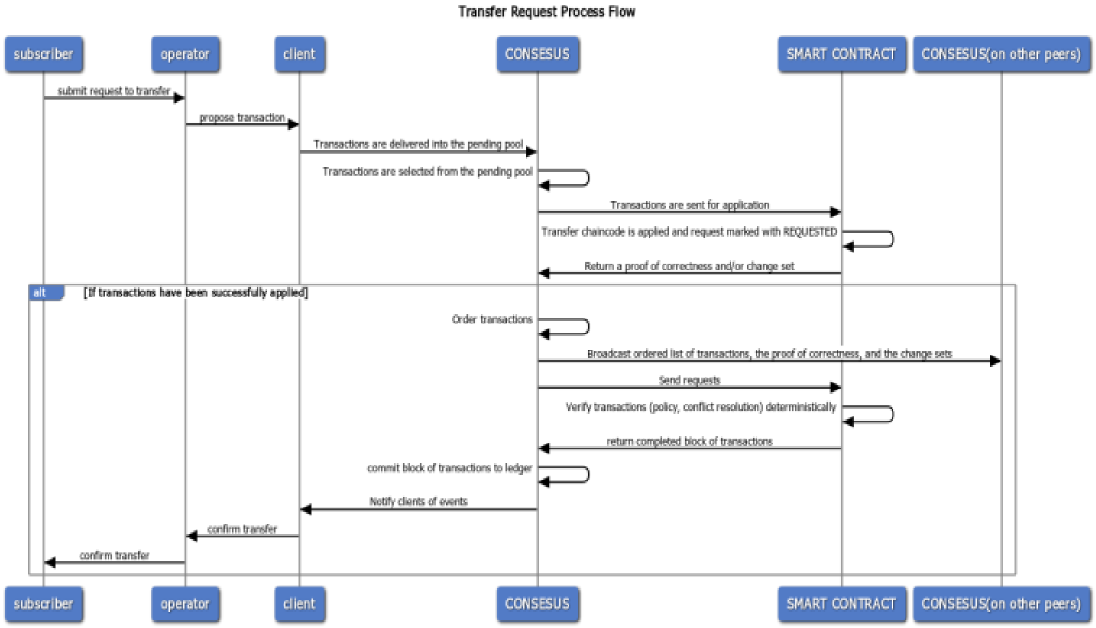

Transfer Request Process Flow
subscriber
operator
client
CONSESUS
SMART CONTRACT
CONSESUS(on other peers)
submit request to transfer
propose transaction
Transactions are delivered into the pending pool
Transactions are selected from the pending pool
Transactions are sent for application
Transfer chaincode is applied and request marked with REQUESTED
Return a proof of correctness and/or change set
alt
[If transactions have been successfully applied]
Order transactions
Broadcast ordered list of transactions, the proof of correctness, and the change sets
Send requests
Verify transactions (policy, conflict resolution) deterministically
return completed block of transactions
commit block of transactions to ledger
Notify clients of events
confirm transfer
confirm transfer
subscriber
operator
client
CONSESUS
SMART CONTRACT
CONSESUS(on other peers)

Fig. 3-14 Transfer Request Detailed Sequence Diagram

The diagram in Figure 3-15 shows that sequence of events during the settlement process and the subsequent creation of the BatchTransfer. A settlement request is made at end of day to summarize all transfers between any pair of participants to come up with the net settlement between them. It considers all transfers in the FULFILLED state and moves them to the SETTLED state as well as creating a new BatchTransfer asset in the PENDING state.

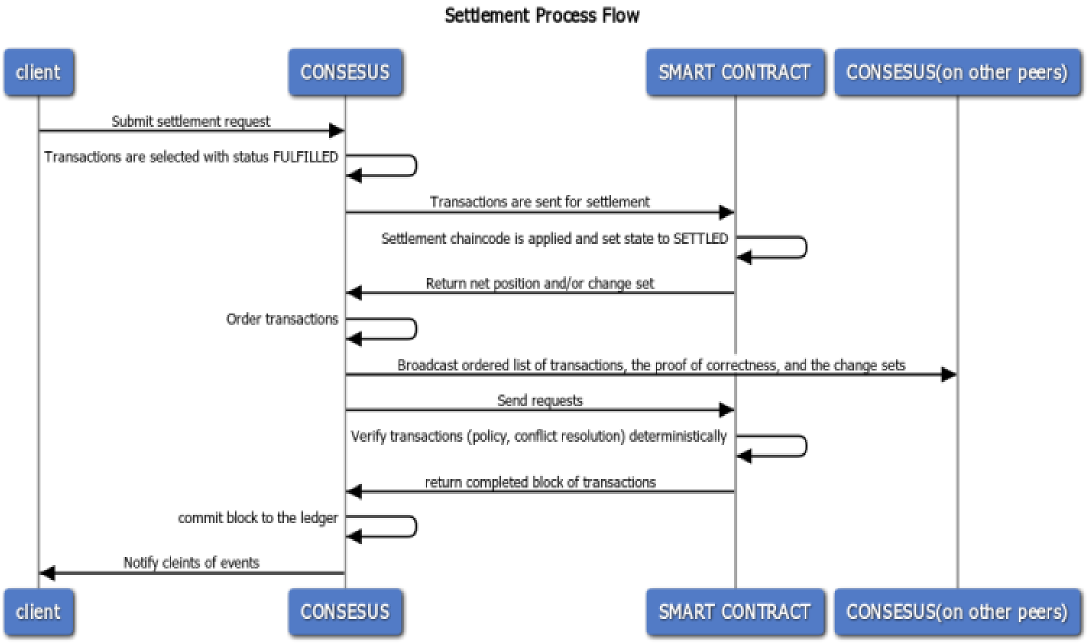

Settlement Process Flow
client
CONSESUS
SMART CONTRACT
CONSESUS(on other peers)
Submit settlement request
Transactions are selected with status FULFILLED
Transactions are sent for settlement
Settlement chaincode is applied and set state to SETTLED
Return net position and/or change set
Order transactions
Broadcast ordered list of transactions, the proof of correctness, and the change sets
Send requests
Verify transactions (policy, conflict resolution) deterministically
return completed block of transactions
commit block to the ledger
Notify cleints of events
client
CONSESUS
SMART CONTRACT
CONSESUS(on other peers)

Fig. 3-15 Settlement Sequence Diagram

3.5.4 System Implementation

Hyperledger Fabric offers a number of SDKs to support developing smart contracts (chaincode) in various programming languages. There are three smart contract SDKs available for Go, Node.js, and Java [94]:

- Go SDK documentation.
- Node.js SDK and Node.js SDK documentation.
- Java SDK and Java SDK documentation.

Currently, Node.js and Java support the new smart contract programming model delivered in Hyperledger Fabric v1.4.

In this study, we used the Java SDK and developed the smart contract using the Java development language. The prototype was built in Netbeans IDE [104] using the Maven [105] development framework to take advantage of the Hyperledger Fabric development model and sources [100].

3.5.5 Deployment and Test Evaluation Criteria

The prototype was deployed on Ubuntu Linux platform using Docker [106] containers to simulate a network of the various components (Peers, Channels, Certificate Authority and Orderer).

3.6 Summary

In this chapter, we gave an account of the methodology and methods that we followed. In this study. A baseline study was used to confirm the problem specification and solution was proposed and technology checked for suitability. A formal method of development was also selected and artefacts presented that were used during the implementation of the prototype.

CHAPTER FOUR

RESULTS

4.1 Introduction

In this chapter, we present the results of the study. Key findings of the baseline are presented and their subsequent application to the study. Highlights of the prototype system designed are also given in terms of code artefacts as well as screenshots of the experimental Fabric network that was setup.

4.2 Baseline Study

This section describes the process that was used to establish the mobile money technological landscape. A list of interview questions were designed into a survey and administered to a target audience of respondents who were deliberately selected according to set criteria.

Further, walk in interviews were conducted with subject matter experts to validate and verify researched literature and documentation on mobile money systems and service implementation. The goal was to try to establish and highlight short falls and inefficiencies in implementation that prevent interoperability and thereby identify opportunities for improvements in the solution design of the use case.

4.2.1 Participant Demographics

A total of 23 participants out of the 46 survey respondents completed the questionnaire. All incomplete responses were excluded from the analysis. Table 4-1 shows the demographics of the participants. The survey respondents included participants from mobile money service providers and regulatory authorities. In addition, the participants included individuals with varying professions and levels of responsibilities in their respective organizations.

Table 4-1. Participants Demographics

Respondents	**Counts**
Mobile Money Service Operator/Provider	**16**
Executive Management	2
Intermediate Non-management	3
Middle/Junior Management	6
Senior Management	5
Regulatory Authority	**7**
Middle/Junior Management	7
Grand Total	**23**

4.2.2 Operator Characteristics

The size of mobile operators and corresponding subscriber base varied in size. Figure 4-1 show the relative size of the mobile money operators and subscriber base, respectively.

Participants were required to specify the distribution of their subscriber base, in terms of the transaction volumes handled, based on three customer segments: low value, medium value and high value. The Low Value segment represents subscribers that perform transactions that generally involve low; the Medium Value segment represents subscribers that perform on average transactions and the High Value segment represents subscribers that perform above average transactions.

Figure 4-2 shows the customer segmentation for the various mobile operators. The Low Value segment was found to be dominant among most of the operators which would suggest a high frequency of transactions by their respective subscribers.

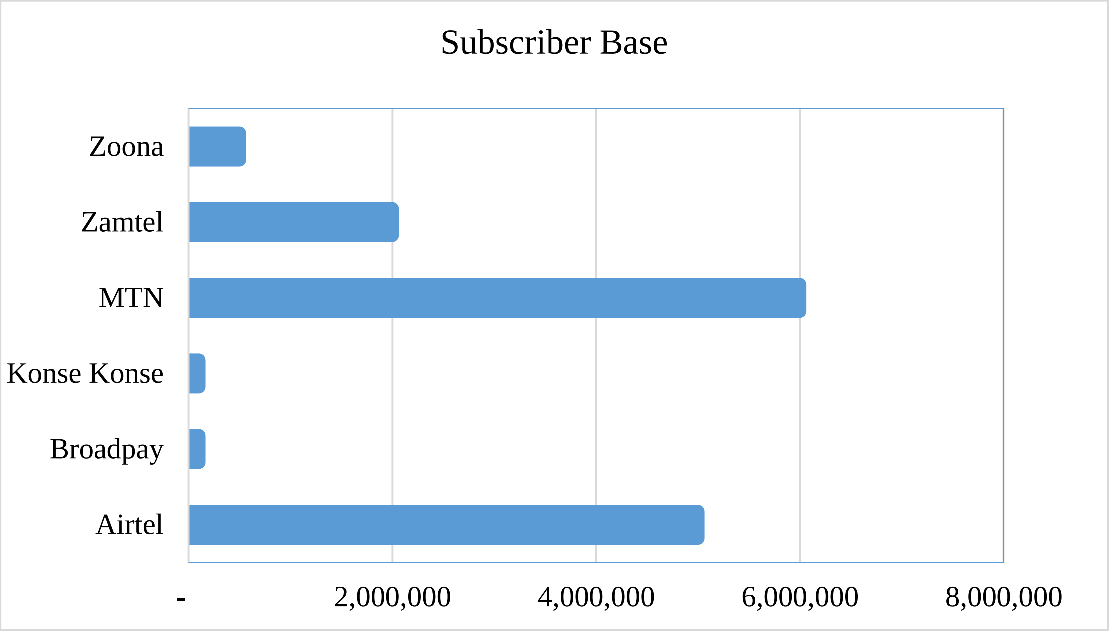


Fig. 4-1 Participant Network Subscriber Base

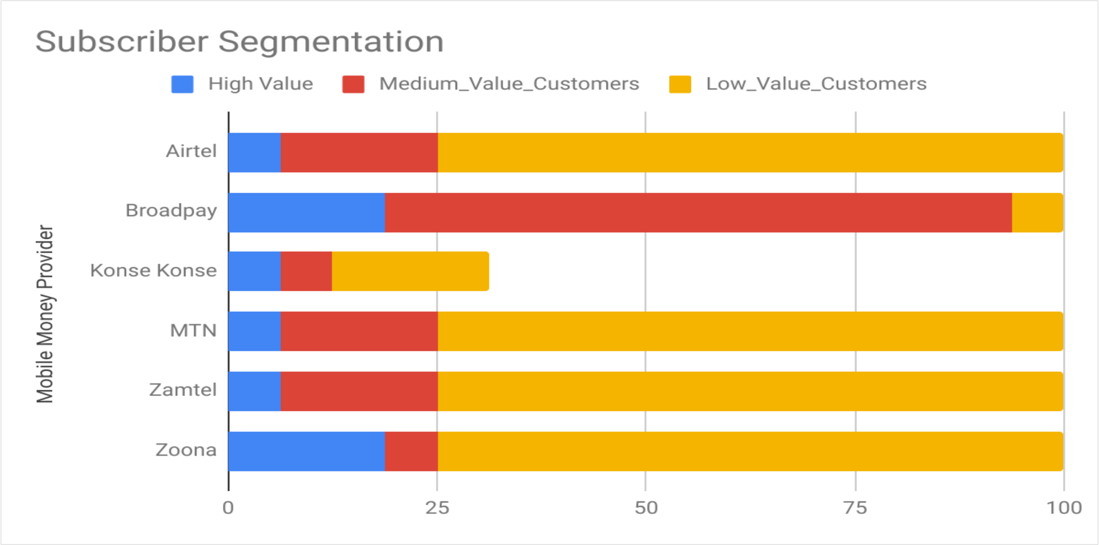


Fig. 4-2 Participant Network Subscriber Segmentation

All participant respondents reported that their respective providers covered all the major provinces of Zambia with a few not having presence in one or two provinces.

4.2.3 Mobile Money Platforms

According to the survey participants, the majority of the mobile money systems used by the mobile money providers in Zambia are sourced from external vendors as a supported contract scheme or as a managed service. Figure 4-3 shows the distribution of the platform sources used by mobile money operators.

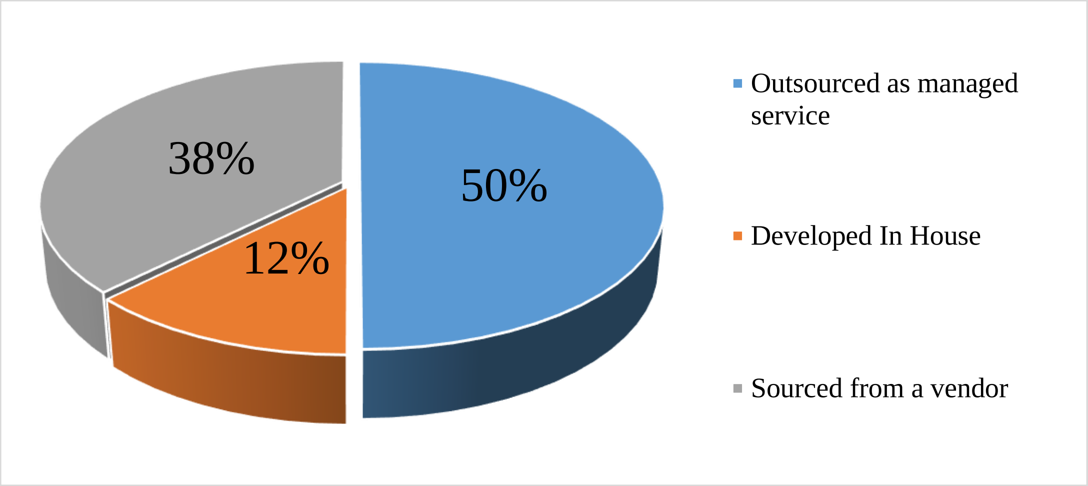


Fig. 4-3 Platform Sources

The survey also showed that the systems are hosted internally at the mobile operator's data centres. It was further established that different platform vendors provide these platforms to the different mobile money providers. Prominent among these vendors in the country include Comviva, Craft Silicon and Ericsson Systems.

No two operators use the same vendor platforms indicating a possibility of variations in setups and therefore differing challenges and approaches to configurations and functionality. One such functionality is the availability and readiness of Application Programming Interfaces (APIs), which are a set of functions and procedures allowing the creation of applications that access the features or data of a system or other service. APIs are generally used to extend a platform's functionality to third party systems. Some respondents reported availability of Application Programming Interfaces (APIs) on their platforms while others said they had no available APIs for integration.

4.2.4 Mobile Money Systems Integration Challenges

Four aspects were used to gauge how much of a challenge it would be for the different operators to implement integration with other operators. These measures included

‘Technological complexity’ – which looked at to what extent that the operator’s technological platform setup would pose a challenge. This was both in terms of availability of ready functionality as well as flexibility to change the existing platform configurations to accommodate the integration efforts.

Integration challenges were also looked at in terms of human resources complexity which looked at how easily an operator would find the required human resources capabilities to undertake an integration project.

Other aspects used were the financing complexity and business case justification which considered the operator’s ability to justify and finance an integration undertaking. Results of the survey regarding these aspects are summarized in Figure 4-4.

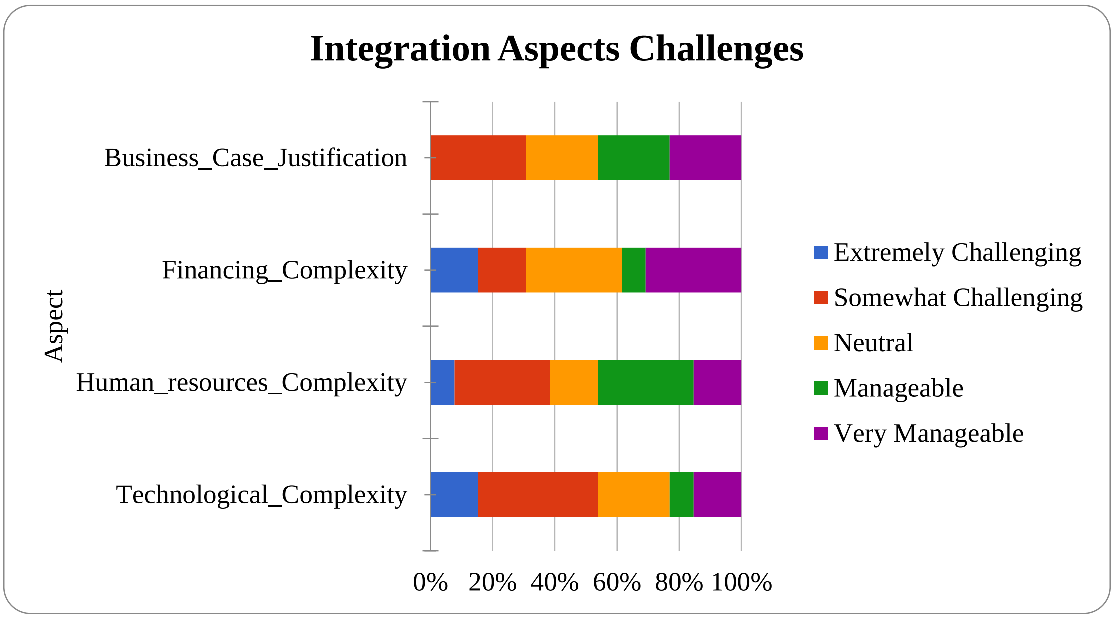


Fig. 4-4 Integration Challenges

From a financing perspective, majority of the respondents felt that is was quite manageable (19 percent) to very manageable (25 percent) to justify funding for mobile money systems integration effort. This is in comparison to the ones who felt it was somewhat challenging (19 percent) to extremely challenging (13 percent). Human resourcing complexity was another measure used and according to the survey responses, it was strongly felt that it was manageable to extremely manageable to find the necessary human resources for such projects by the mobile money providers. Mixed reactions were observed regarding the business case justification for an interoperability integration among the different operator respondents. While none of the respondents felt that it was extremely challenging to provide business justification for integration, the 25 percent that felt that it would be somewhat a challenge could be attributed to the fact that the bigger and more dominant players who would easily feel that they would derive least value from interoperability unlike the smaller ones. This could be concluded from the survey results which showed that the respondents from operators with higher subscriber bases and therefore larger and more complex networks responded with a negative sentiment regarding this measure.

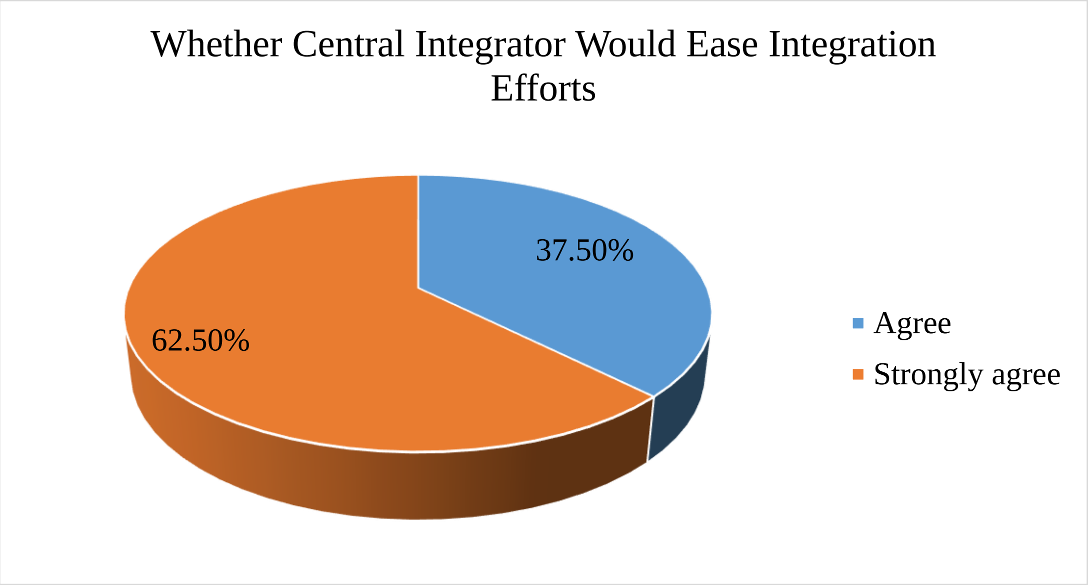


Fig. 4-5 Integration Efforts

Overall, as far as inter operator integration was concerned, the general feeling of the survey was that it was manageable and could further be eased with the use of a central integrator rather than having every operator to integrate individually with every other operator (Figure 4-5).

4.2.5 Mobile Money Systems Interoperability

The final section of the survey considered whether interoperability was a desirable feature among the mobile money players in the Country and what sort of form it would take.

Survey results shows that all the respondents agreed that interoperability would be a desirable feature in the Mobile Money market. Various reasons were given for this response and these ranged from enabling efficiency to market growth and expansion.

For example one respondent stated that "This would be convenient and also increase financial inclusion and it would also make trading easier", while yet others felt that it would quicken roll out of services and would ease the cost of business for the operators.

The survey responses also showed a strong feeling that interoperability would promote and enhance financial inclusion as it would lead to more uptake of mobile money services by more customers. The following are some of the comments that seem to suggest that feeling. "It would enhance customer experience with mobile money service. It would enhance financial inclusion as it would encourage usage of mobile money services" from respondent 40, "Interoperability will enhance the growth of the sector and boost financial inclusion" from respondent 15 and "Interoperability is the key to increase financial inclusion as it avoids the inconvenience of one individual having multiple wallets. With interoperability one wallet is as good as connected to all inter operable wallets. It also helps to dematerialize the use of cash because wallet owners may not need to cash in so that they pay another person with a different wallet but can just send funds to that particular wallet despite the service provider " from respondent 8.

4.2.6 Desired Security Services

The core data security services were used to devise parameters to be used to determine desired security services for interoperability from respondents. A security service is a specific security goal that we may wish to achieve. These security services included the following:

- Confidentiality - which is the assurance that data cannot be viewed by an unauthorized user. It is sometimes referred to as secrecy.
- Data integrity - which is the assurance that data has not been altered in an unauthorized (which includes accidental) manner. This assurance applies from the time that the data was last created, transmitted or stored by an authorized user. Data integrity is not concerned with the prevention of alteration of data, but provides a means for detecting whether data has been manipulated in an unauthorized way.
- Data origin authentication - which is the assurance that a given entity was the original source of received data.
- Non-repudiation - which is the assurance that an entity cannot deny a previous commitment or action.
- Entity authentication - which is the assurance that a given entity is involved and currently active in a communication session.

For ease of administering into a survey, these security services were coded into the following equivalents:

- Trust – which is the assurance that the transactions shared on the network are accessible only for the intended recipients and that they that it is free of tampering. This covered the confidentiality and integrity requirements
- Transparency of transactions was meant to cover the entity authentication requirement as well as the data origin authentication.
- Consensus on the hand, covered the non-repudiation requirement and provides the assurance that there shall be no disputes when settling interchange transactions.

- Verifiability of transactions also covered the data integrity aspect by ensuring that the data is kept in the original state and could be validated at any given time.

The Figure 4-6 shows the findings as far the desired security services is concerned. With an average score of 3.84 on a scale of 0 to 4 where 0 is “Not Important” and 4 is “Very Important”, the results suggests that all the set security services were desired by the respondents.

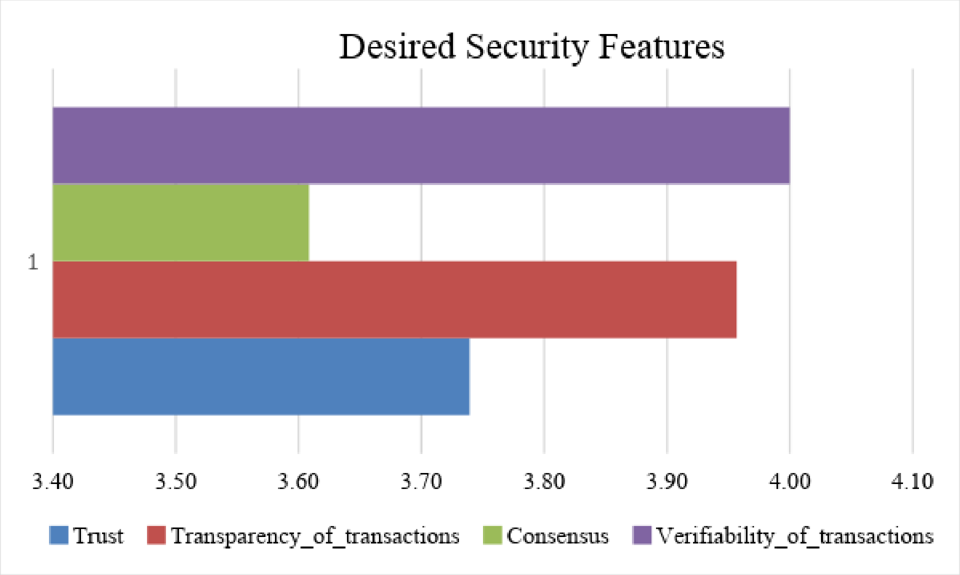


Fig. 4-6 Security Services From Integration

Some security requirements were more apparent and scored highly than others thus could be considered to have been perceived as being more important and more critical to the operation of the systems.

4.2.7 Record Keeping Requirements

Record keeping systems generally must contend with trust issues and methods of organizing historical information. In a case where such information or records are shared among a number of different players in a network, a number of difficulties are encountered such as monitoring of data ownership and transfers of that data. Settlement of interchange data among players will need data to be shared. A number of requirements may be necessary for that shared data to be reasonably acceptable and trusted by participants in the network. The following are the main attributes selected to meet the requirement of trust in a distributed and shared environment.

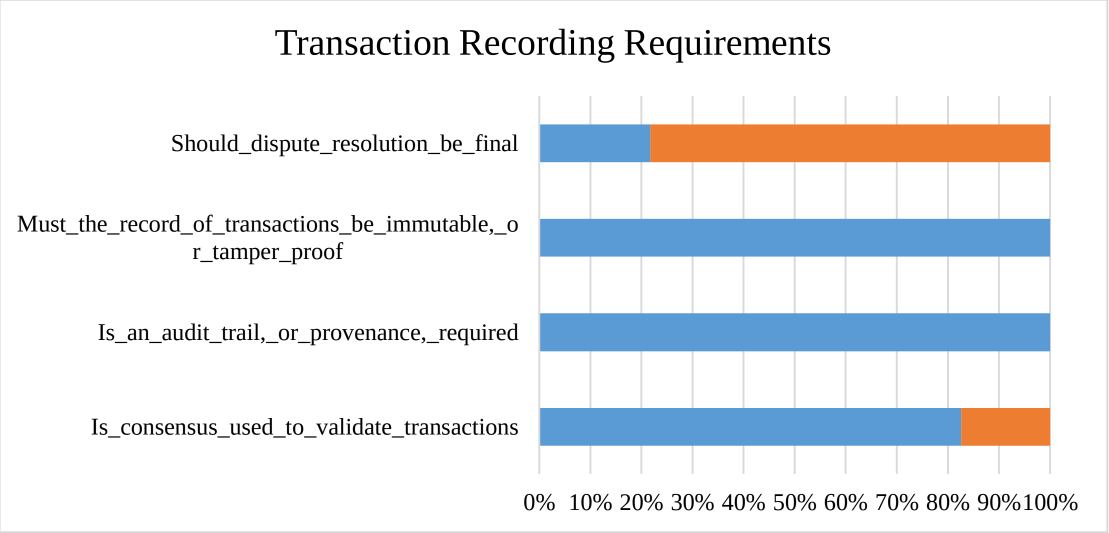


Fig. 4-7 Data Recording Requirements

Firstly, all or at least the key participants must a way of determining and agreeing that a transaction is valid before it can be accepted for settlement in an interchange with other parties.

In addition, the participants in the network must know where a particular transaction data element was originated from and how its ownership has changed over time. Furthermore, no participant should be able to tamper with a transaction once it is processed.

Finally, perhaps a single source of truth would need to be put in place to determine the ownership of an asset or completion of a transaction. These attributes are summarized as consensus, provenance, immutability and finality respectively and are regarded as required attributes for data in a shared and distributed environment [107].

To gauge to what extent, the survey respondents thought these requirements were essential in a networked interoperability system, a number of responses were collected and results summarized in Figure 4-7. While it was clear that the majority of the respondents felt that immutability, provenance and consensus where important aspects, very few felt that finality of transactions was important. This could have emerged from the fact that the current settlement mechanisms employed in similar interchange schemes (such settlement of network transit calls) requires that there is a lot of back and forth exchange of transaction records between parties to settle disputes. The expectation is thus that reversals of transactions settled should be possible where new information emerges even after final settlement. A solution would therefore be necessary that reduces the need for such problems by providing transparency and trust of records of assets interchanged.

4.2.8 Interoperability Rules

The final question looked at some of the major rules that would need to be put in place to govern compliance of the different participants in the network. A number of comments and suggestions were provided by the respondents and common and more prominent themes were extracted from these comments and suggestions.

- Rules and guidelines for participation in the network
- Central Authority or regulator to manage access to the network
- Daily Settlement and Clearing of participant positions
- Transparency and Security of transactions
- Robust systems

4.2.9 Baseline Study Summary

The baseline study to learn the state of mobile money system landscape in Zambia revealed a number of key findings. Key among these findings was the fact there is a network of different participants that run different mobile money platforms in the Country with no interoperability among them. Each of the provider's platforms use different technologies with varying levels of complexities and challenges with integration to other provider platforms.

Further, the mobile money providers find account to account interoperability of their services desirable for various reasons despite them operating and maintaining different subscriber ledgers. This was seen to be true regardless of provider size.

4.3 Decision Model Analysis

A Decision model was adopted and used to assess blockchain suitability to this use case [64]. Key findings from the baseline study were used in the flow chart decision tree as prescribed in this model and it was established that for this particular use case, we could make use of a permissioned blockchain as a technology. The Table 4-5 summarizes these findings.

A number of important aspects such as the need to store state, existence of multiple writers were used to arrive at the decision of the solution. Other aspects like the need for central management and the relatively low number of writers were also considered to arrive at the decision.

Table 4-2. Decision Model Analysis with Key Survey Findings

Decision Model Analysis		
Decision State	**Finding Description**	**Result**
Storing state	Existence of different independent mobile money operators	YES
Existence of writers	Existence of technological platforms or systems on which these operators run their services	YES
Trusted Online Third Party	Controlled access to the network with permissioning.	NO
Are all writers known	The need for integration among these systems to provide interoperability	YES
Are all writers trusted	Security and privacy of transactions	NO
Public verifiability of state	Security and privacy of transactions	NO

4.4 Blockchain Technology and Its Security Features

The great motivation behind the use of blockchain technology lies in the fact that it allows untrusting entities to share valuable data in a secure and tamperproof way. This is possible because blockchains store data using sophisticated mathematical and innovative software rules that are extremely difficult for attackers to manipulate.

Typically, financial transactions have always relied and operated on the principle of a trusted third party to guarantee them. Blockchain ensures trust (as an emergent property) from the inter-node interactions within the network.

Despite being initially linked to Bitcoin, blockchain technology can be used independently in a variety of different use-cases and markets, ranging from insurance to the health industry. A blockchain can be applied in virtually any industry in which assets are managed and transactions occur. It can provide a secure chain of custody for both digital and physical assets through its functional characteristics that facilitate transactions through trust, consensus, security, and smart contracts. A number of aspects of blockchains are presented in the following section as a basis in how they were employed in the development of a prototype system for mobile money interoperability.

4.4.1 Security Principles

As a secure ledger, the blockchain is organised as a growing list of transaction records into a hierarchically expanding chain of blocks [108] with each block guarded by cryptography techniques to enforce strong integrity of its transaction records. New blocks can only be committed into the global blockchain upon their successful completion of the decentralized consensus procedure. Concretely, in addition to information about transaction records, a block also maintains the hash value of the entire block itself, which can be seen as its cryptographic image, plus the hash value of its preceding block, which serves as a cryptographic linkage to the previous block in the blockchain. Figure 4-8 summarizes a typical structure of a blockchain.

A decentralized consensus procedure is enforced by the network, which controls (i) the admission of new blocks into the block chain, (ii) the read protocol for secure verification of the blockchain, and (iii) the consistency of the data content of transaction records included in each copy of the blockchain maintained on each node. As a result, the blockchain ensures that once a transaction record is added into a block and the block has been successfully created and committed into the blockchain, the transaction record cannot be altered or compromised retrospectively, the integrity of the data content in each block of the chain is guaranteed, and the blocks, once committed into the blockchain, cannot be tampered by any means. Thus, a blockchain serves as a secure and distributed ledger, which archives all transactions between any two parties of an open networked system effectively, persistently, and in a verifiable manner.

In the context of Bitcoin systems, the blockchain is employed as its secure, private and trusted public archive for all transactions that trade bitcoins on the Bitcoin network. This ensures that all bitcoin transactions are recorded, organized and stored in cryptographically secured blocks, which are chained in a verifiable and persistent manner. Blockchain is the pivotal guard in securing bitcoin transactions from many known and hard security, privacy and trust problems, such as double spending, unauthorized disclosure of private transactions, reliance of a trusted central authority, and the untrustworthiness of decentralized computing.

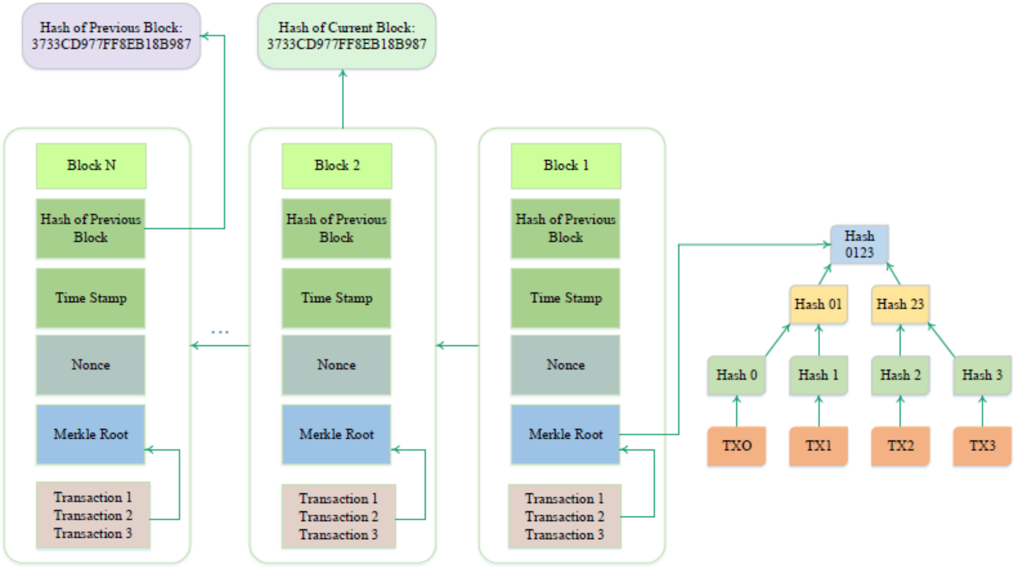


Fig. 4-8 A Basic Block Structure [16]

[16] Source: Muhammed Javed

4.4.2 Implementation of Security Features

In this subsection, implementation of the security features of our proposed model are presented.

Data Integrity

When using online transactions for assets are managed by different intermediaries. It not only increases the transaction costs, but also brings the risk of deliberately falsifying or forging the certificates. Thus, the system must guarantee integrity of transactions and prevent transactions from being tampered with.

In this proposed system, data generated by participant nodes is encrypted using symmetric key encryption. Data is stored in a distributed file system, which returns the hash of the data stored in it. This hash is stored in blockchain, which ensures data integrity because it is not possible to tamper with the data in the blockchain.

Privacy Preservation

The difficulty of efficient and secure sharing of user data among various financial institutions may result in a high cost of repeated user authentication. It also indirectly brings the disclosure risk of users' identity by some intermediaries. In addition, one or both parties to the transaction may be reluctant to let the other party know their real identity in some cases.

In the proposed system, encryption and the concept of channels are used for communication between the participating nodes. The real identification number of the participant is not used as its identity, because it leads to a privacy leakage problem. Hence, the privacy of the proposed system is preserved using the channels. All the transactions are in encrypted form, which ensures data privacy. Therefore, our proposed system preserves the privacy of both data and user's identity.

Data Confidentiality

All the communications between participants are encrypted using symmetric key encryption, which makes it difficult for the malicious node to tamper the communication data. Only an authorized user has access to the encrypted data. By using an encryption mechanism, malicious activities are prevented.

Single Point of Failure

Data on a blockchain network is replicated across all nodes and therefore, distributed. This thus overcomes the problem of single point of failure. Hence, the proposed system is robust and achieves high throughput.

Availability

The proposed solution will make use of the Hyperledger Fabric blockchain network which allows for deployment of redundant set of nodes across each participant on the network. Each of these nodes will maintain an up to date distributed hash table against the data stored in the ledger. Whenever data are required, a request of data are sent to a specific node at which data are placed. Due to the distributed storage, the availability of data is achieved while ensuring high throughput of the system.

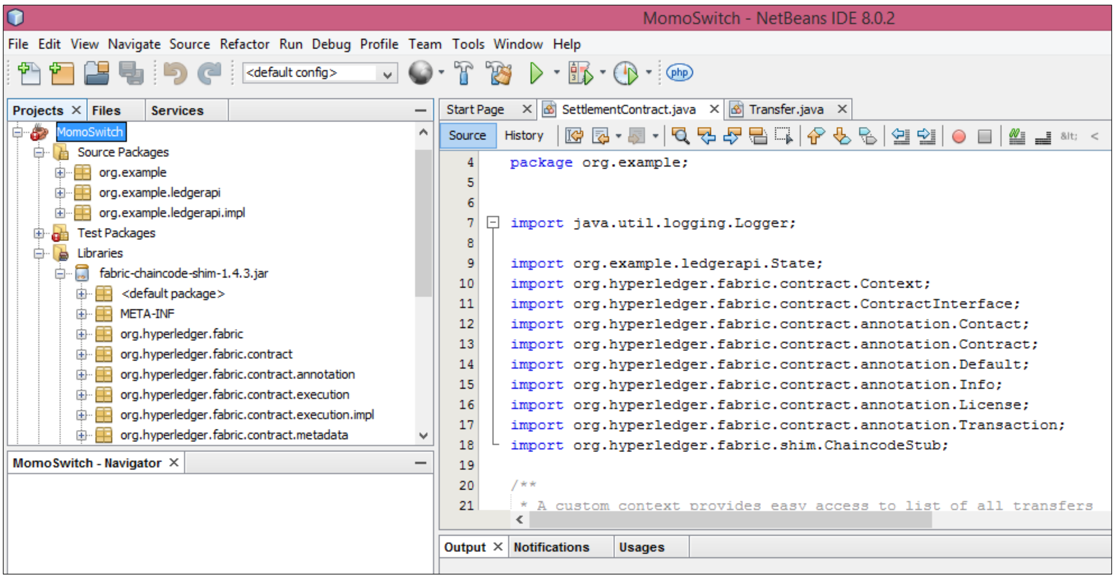
4.5 System Implementation

In this section, we look at the prototype system implementation details and result artefacts. We begin with the development tools and environment and present resulting code snippets of the major parts of the chaincode. The results presented here are limited in scope as they represent only the smart contract implementation and does not cover other areas such as the network deployment, certificate authority, channel and all other such configurations associated with Hyperledger Fabric setup [109].

4.5.1 Build Tools and Environment

The smart contact was developed from the design using java thanks for high level language support on the Hyperledger Fabric version 1.4. The prototype build process made use of the already supported Java based contract SDK and Java SDK documentation to develop the chaincode in the Java programing language.

The prototype was built in Netbeans IDE [104] using the Maven [105] development framework to take advantage of the Hyperledger Fabric development model and sources [100]. The figure 4-8 shows the build environment and sources.



MomoSwitch - NetBeans IDE 8.0.2
File Edit View Navigate Source Refactor Run Debug Profile Team Tools Window Help
<default config>
Projects Files Services
MomoSwitch
Source Packages
org.example
org.example.ledgerapi
org.example.ledgerapi.impl
Test Packages
Libraries
fabric-chaincode-shim-1.4.3.jar
<default package>
META-INF
org.hyperledger.fabric
org.hyperledger.fabric.contract
org.hyperledger.fabric.contract.annotation
org.hyperledger.fabric.contract.execution
org.hyperledger.fabric.contract.execution.impl
org.hyperledger.fabric.contract.metadata
MomoSwitch - Navigator
Start Page SettlementContract.java Transfer.java
Source History
Output Notifications Usages

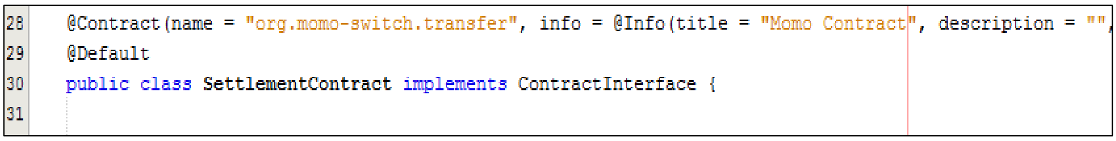
```java
package org.example;


import java.util.logging.Logger;

import org.example.ledgerapi.State;
import org.hyperledger.fabric.contract.Context;
import org.hyperledger.fabric.contract.ContractInterface;
import org.hyperledger.fabric.contract.annotation.Contact;
import org.hyperledger.fabric.contract.annotation.Contract;
import org.hyperledger.fabric.contract.annotation.Default;
import org.hyperledger.fabric.contract.annotation.Info;
import org.hyperledger.fabric.contract.annotation.License;
import org.hyperledger.fabric.contract.annotation.Transaction;
import org.hyperledger.fabric.shim.ChaincodeStub;

/**
 * A custom context provides easy access to list of all transfers
```

Fig. 4-9 Build Environment and Fabric Sources

4.5.2 Main Contract Classes

The main smart contract classes are the SettlementContract class and this contains the transaction definitions for the system. These are the **request**, **fulfil**, **settle** and **batch** transactions that have been defined and which move the assets through the application life cycle (Figure 3-9 and Figure 3-10).

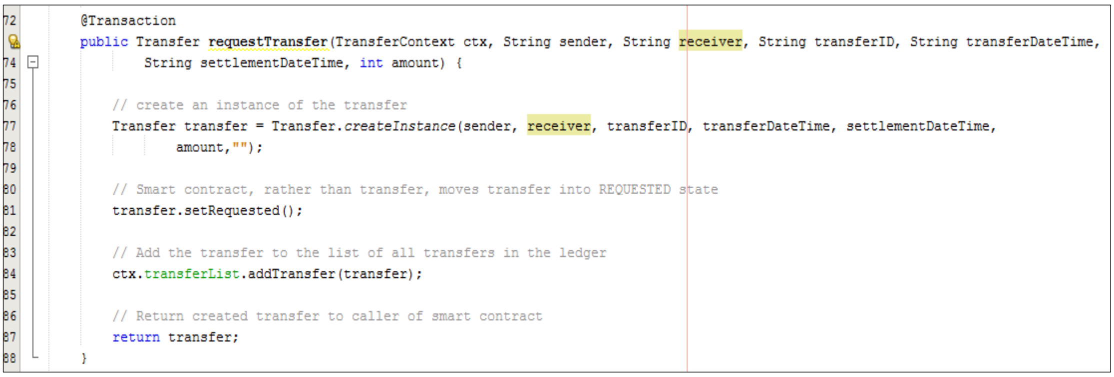
The SettlementContract class implements the ContractInterface and so the Settlement contract uses built-in features of these classes, such as automatic method invocation, a per-transaction context, transaction handlers, and class-shared state. Figure 4-9 shows code snippet of this implementation detail.



```java
@Contract(name = "org.momo-switch.transfer", info = @Info(title = "Momo Contract", description = "",
@Default
public class SettlementContract implements ContractInterface {

```

Fig. 4-10 Main Contract Class

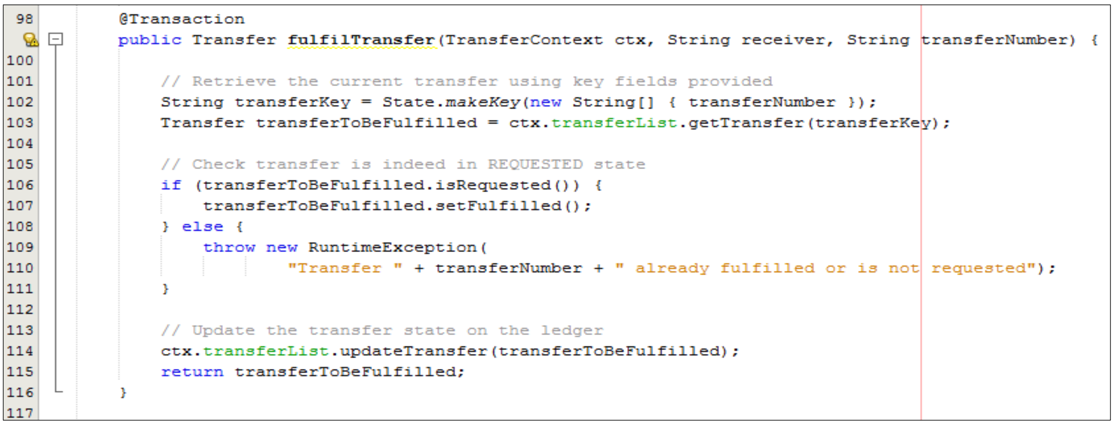
This class contains implementation of a number of methods that control application lifecycle. Firstly, the **requestTransfer** (Figure 4-10) method creates a new transfer context object between two participants (sender and receiver) which is saved on the ledger as an asset.



```
@Transaction
public Transfer requestTransfer(TransferContext ctx, String sender, String receiver, String transferID, String transferDateTime,
        String settlementDateTime, int amount) {

    // create an instance of the transfer
    Transfer transfer = Transfer.createInstance(sender, receiver, transferID, transferDateTime, settlementDateTime,
            amount,"");

    // Smart contract, rather than transfer, moves transfer into REQUESTED state
    transfer.setRequested();

    // Add the transfer to the list of all transfers in the ledger
    ctx.transferList.addTransfer(transfer);

    // Return created transfer to caller of smart contract
    return transfer;
}
```

Fig. 4-11 Request Transfer Method

The **fulfilTransfer** (Figure 4-11) method is another transaction method and it transitions a transfer object in *REQUESTED* state and sets it to the *FULFILLED* state (after the receiver has fulfilled the transaction as confirmation that funds have been moved that participant’s account).

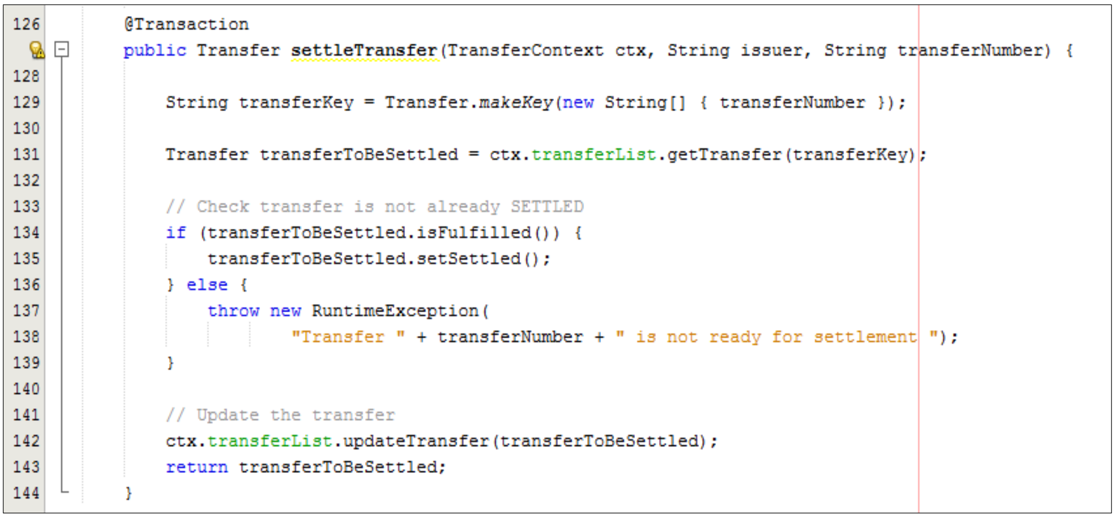


```
@Transaction
public Transfer fulfilTransfer(TransferContext ctx, String receiver, String transferNumber) {

    // Retrieve the current transfer using key fields provided
    String transferKey = State.makeKey(new String[] { transferNumber });
    Transfer transferToBeFulfilled = ctx.transferList.getTransfer(transferKey);

    // Check transfer is indeed in REQUESTED state
    if (transferToBeFulfilled.isRequested()) {
        transferToBeFulfilled.setFulfilled();
    } else {
        throw new RuntimeException(
                "Transfer " + transferNumber + " already fulfilled or is not requested");
    }

    // Update the transfer state on the ledger
    ctx.transferList.updateTransfer(transferToBeFulfilled);
    return transferToBeFulfilled;
}
```

Fig. 4-12 Fulfil Transfer Method

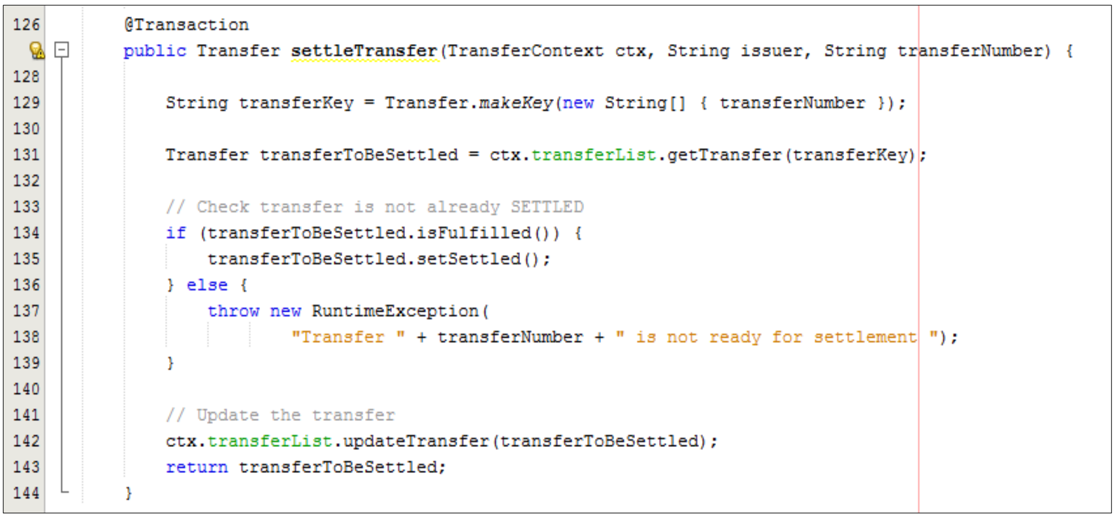
The **settleTransfer** (Figure 4-12) method is also another transaction method and it transitions a transfer object in *FULFILLED* state and sets it to the *SETTLED* state. This method is called by the **createBatch** method during the net settlement process at the end of business day.

Finally, the **createBatch** (Figure 4-13) method is a settlement process method that is called to collate all transfers between any pair of participants and create a BatchTransfer asset which is stored on the ledger.



```
@Transaction
public Transfer settleTransfer(TransferContext ctx, String issuer, String transferNumber) {

    String transferKey = Transfer.makeKey(new String[] { transferNumber });

    Transfer transferToBeSettled = ctx.transferList.getTransfer(transferKey);

    // Check transfer is not already SETTLED
    if (transferToBeSettled.isFulfilled()) {
        transferToBeSettled.setSettled();
    } else {
        throw new RuntimeException(
                "Transfer " + transferNumber + " is not ready for settlement ");
    }

    // Update the transfer
    ctx.transferList.updateTransfer(transferToBeSettled);
    return transferToBeSettled;
}
```

Fig. 4-13 Settle Transfer Method



```
@Transaction
public Transfer settleTransfer(TransferContext ctx, String issuer, String transferNumber) {

    String transferKey = Transfer.makeKey(new String[] { transferNumber });

    Transfer transferToBeSettled = ctx.transferList.getTransfer(transferKey);

    // Check transfer is not already SETTLED
    if (transferToBeSettled.isFulfilled()) {
        transferToBeSettled.setSettled();
    } else {
        throw new RuntimeException(
                "Transfer " + transferNumber + " is not ready for settlement ");
    }

    // Update the transfer
    ctx.transferList.updateTransfer(transferToBeSettled);
    return transferToBeSettled;
}
```

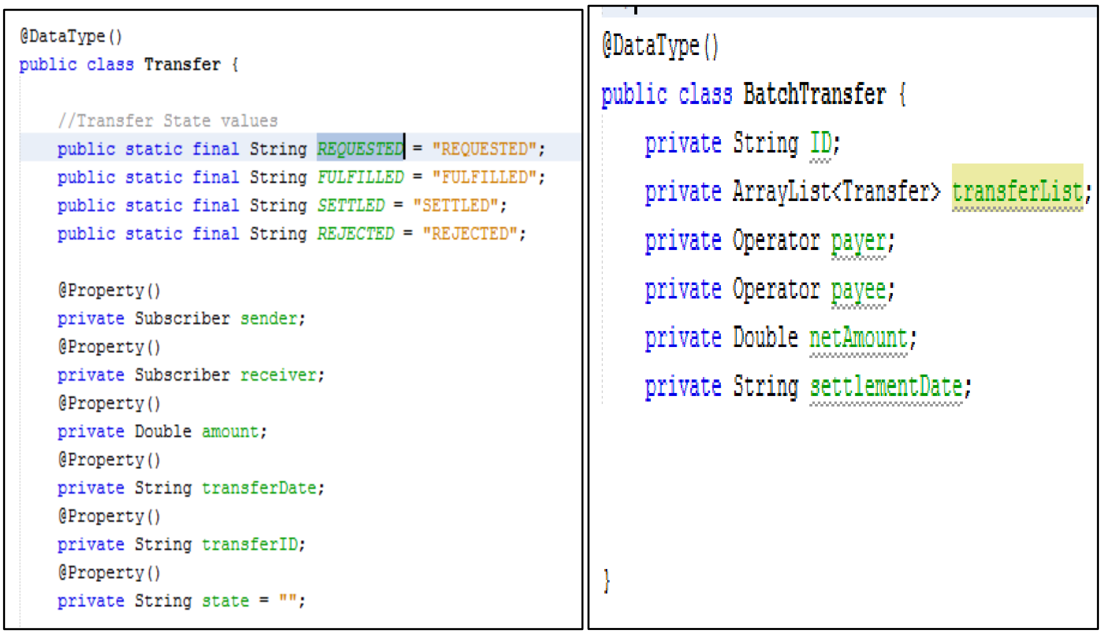
Fig. 4-14 Create Batch Method

This class and methods make up the transaction logic part of the system and represent the control flow logic of processing. Next we highlight the object implementation which represent the main assets.

4.5.3 The Main Object Classes

The main object classes that represent assets on the ledger are the Transfer and the BatchTransfer classes. These classes have member valuables that represent the properties of the assets and have respective **createInstance** methods which are used to initialize their respective objects so as ensure instantiation of these objects is through a transaction rather than through the classes.

These classes also extend the State class which is used to control lifecycle states of the assets and represents the ledger level Fabric state database. Figure 4-14 shows the main parts of these classes.



```
@DataType()
public class Transfer {

    //Transfer State values
    public static final String REQUESTED = "REQUESTED";
    public static final String FULFILLED = "FULFILLED";
    public static final String SETTLED = "SETTLED";
    public static final String REJECTED = "REJECTED";

    @Property()
    private Subscriber sender;
    @Property()
    private Subscriber receiver;
    @Property()
    private Double amount;
    @Property()
    private String transferDate;
    @Property()
    private String transferID;
    @Property()
    private String state = "";
```

```
@DataType()
public class BatchTransfer {
    private String ID;
    private ArrayList<Transfer> transferList;
    private Operator payer;
    private Operator payee;
    private Double netAmount;
    private String settlementDate;



}
```

Fig. 4-15 Transfer and BatchTransfer Object Class Members

The other object classes include the Operator and the Subscriber and these used to represent logical member variables for the respective objects for easier management. Code snippets showing implementation are presented in the appendix for those.

4.6 Summary

In this chapter, we presented findings of a baseline study conducted as part of this study and provided an analysis of how it was used as a basis in the implementation of a prototype system for mobile money interoperability. We successfully implemented a smart contract based on a proposed design using the Java programming language to run on a Hyperledger Fabric network.

CHAPTER FIVE

DISCUSSION AND CONCLUSIONS

5.1 Introduction

Zambia like most of the developing countries that have a high proliferation of mobile money services [110] is still faced with the problem of interoperability among the providers of these services [111]. Challenges range from regulatory to financial incentives to lack of attractive enough technological schemes to foster this interoperability. This study looked at how blockchain technology could be used to close this interoperability problem through the provision of a central clearing and settlement system that offers ease of integration as well as high level of trust through transaction transparency.

5.2 Discussion

In this section, we give a discussion of the study findings and the prototype implementation. We then compare our method with other similar implementations. Finally, we give the possible application and recommendations of this study.

5.2.1 State of Mobile Money Services

The first objective set out to study how mobile financial service are currently implemented in Zambia and the challenges to interoperability associated with the implementation. To formalise our study, we used a standard questionnaire with a combination of interviews and documentation to establish findings in this objective. Key among these findings was the fact there is a network of different participants that run different mobile money platforms in the Country with no interoperability among them. Each of the provider's platforms use different technologies with varying levels of complexities and challenges with integration to other provider platforms.

Further, the mobile money providers find account to account interoperability of their services desirable for various reasons despite them operating and maintaining different subscriber ledgers. This was seen to be true regardless of provider size.

Literature review of other markets showed existence of a similar gap as our study case and different approaches to address the gap with the common approach being bilateral arrangements between different mobile money providers. This we concluded did not offer real account to account interoperability and presented interconnection challenges.

5.2.2 Conceptual Model Proposal and Design

The second objective was to design a conceptual model for inter operator mobile financial transactions that enables payments, clearing and settlement in a secure, transparent and trusted manner. Having surveyed literature, we learnt of some mobile money interoperability schemes being proposed and in some cases implemented.

A blockchain based approach was found to be more ideal as it offered a solution to the key requirements of transaction transparency, trust and security [112]. These were key because it was envisaged that exchange of data especially of financial data among a number of untrusting parties is traditionally delegated to a trusted intermediary who guarantees that trust.

A suitability check however, was deemed necessary as it was learnt that blockchain was not a silver bullet solution to all problems but was more ideal in particular services.

In the end sufficient justification was established for proposing a technical solution to the problem identified and preliminary solution approach as achieved.

5.2.3 Prototype Implementation

Finally, we set out to develop a prototype system based the proposed solution approach that demonstrates Blockchain security services in a permissioned and regulated environment.

Hyperledger Fabric was found to possess the requisite features for the development of this prototype. Firstly, it is modular, which makes it easy to change aspects of it depending on our particular needs making it ideal for prototype development.

Secondly, Fabric uses smart contracts which can be written in popular programming languages, such as Java and does not depend on native blockchain languages and so there was no learning curve for quick prototype build.

The Fabric blockchain is permissioned, meaning that only invited people can participate on the blockchain which is crucial in a regulated environment such as the one for our use case.

Unlike in cryptocurrency where blocks on the blockchain have to be mined [113], Fabric uses other less expensive consensus mechanisms [114].

We thus adopted a formal software development methodology to design and implement a prototype smart contract that could run on the designed network. The prototype was only experimental and could only be deployed on a development network and not in a live network with integration with mobile network operators for a more real world demonstration.

5.2.4 Recommendations

The work in this study is an attempt to propose a different approach to centrally managed data management systems using mobile money interoperability in Zambia. The study was able to show that this is indeed a valid use case for blockchain technology and that it is recommended that it is adopted and further experiments conducted in and end to end network setup.

5.3 Conclusions

The blockchain is highly appraised for its decentralized infrastructure and point to point nature. However, much of previous research on blockchain has focused on cryptocurrencies only. However, blockchain could be applied to many fields beyond only cryptocurrency. Blockchain realizes trust and security by using software programs to verify and validate consensus in new infrastructure. The study proposed the use of blockchain technology to solve the problem of mobile money interoperability in Zambia. A structured approach was used to confirm the gap and then decide a technological solution through the use of a structured decision model for careful determination. We further designed a prototype system on the Hyperledger Fabric network which could developed in an Object Oriented language such as Java for deployment. We conclude that mobile money interoperability settlement is a valid use case for a permissioned blockchain technology and would be an ideal solution approach rather than the traditional central processing database systems.

5.4 Future Works

This study focused on a gap verification of the interoperability problem as well as a technical implementation of a prototype solution. The prototype also only considered the funds transfer between participating entities and their subsequent settlement and did not look at other technical aspects such as the regulatory aspects and the financial and business sides of the ecosystem.

5.5 Summary

The study was able to meet the set objectives with limitations noted and recommended as future works and areas of improvement. The study brought about key lessons in the problem of mobile money interoperability in Zambia, particularly from a technological standpoint and provided insights into how an unexplored technological direction could be utilised to close this gap.

REFERENCES

[1] M. Tompkins, A. Olivares, and M. Tompkins, “Clearing and Settlement Systems from Around the World : A Qualitative Analysis Clearing and Settlement Systems from Around the World : A Qualitative Analysis by,” 2016.

[2] D. Clark and G. Camner, “A2A Interoperability: Making mobile money schemes interoperate,” no. February, 2014.

[3] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, “An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends,” *Proc. - 2017 IEEE 6th Int. Congr. Big Data, BigData Congr. 2017*, no. June, pp. 557–564, 2017.

[4] GSMA, “Choosing a Technical Model for A2A Interoperability: Lessons from Tanzania and Pakistan,” no. December, 2015.

[5] E. H. Diniz, J. Porto de Albuquerque, and A. K. Cernev, “Mobile Money and Payment: A Literature Review Based on Academic and Practitioner - Oriented Publications (2001 - 2011),” *SSRN Electron. J.*, 2017.

[6] W. T. Tsai, R. Blower, Y. Zhu, and L. Yu, “A system view of financial blockchains,” *Proc. - 2016 IEEE Symp. Serv. Syst. Eng. SOSE 2016*, pp. 450–457, 2016.

[7] Bank of Zambia, “Payment Systems Vision and Strategy 2018-2022,” Bank of Zambia, Lusaka.

[8] T. TEMBO, “National financial switch to start this year,” *Daily Mail*, 2017. [Online]. Available: http://www.daily-mail.co.zm/national-financial-switch-to-start-this-year/. [Accessed: 21-Jan-2018].

[9] M. Rauchs *et al.*, “Distributed Ledger Technology Systems: A Conceptual Framework,” *SSRN Electron. J.*, no. August, 2018.

[10] S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System,” pp. 1–9, 2013.

[11] M. K. Shrivas, “The Disruptive Blockchain: Types, Platforms and Applications,” *Texila Int. J. Acad. Res.*, no. December 2018, pp. 17–39, 2019.

[12] G. W. Peters and E. Panayi, “Understanding Modern Banking Ledgers Through Blockchain Technologies: Future of Transaction Processing and Smart Contracts on the Internet of Money,” in *Banking Beyond Banks and Money*, Springer International Publishing Switzerland, 2016, pp. 239–278.

[13] D. C. Mills *et al.*, “Distributed Ledger Technology in Payments, Clearing, and

Settlement," 2016.

[14] N. Szabo, "Smart Contracts: Building Blocks for Digital Markets," *Extropy*, 1996. [Online]. Available: http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart_contracts_2.html. [Accessed: 20-May-2017].

[15] F. Mvula, J. Phiri, and S. Tembo, "A Conceptual Secure Blockchain Based Settlement and Clearinghouse for Mobile Financial Services in Zambia," in *PROCEEDINGS OF THE INTERNATIONAL CONFERENCE IN ICT (ICICT2019) - LUSAKA, ZAMBIA*, 2019, no. December.

[16] Treasury Alliance Group, "Fundamentals of Global Payment Systems and Practices," 2018.

[17] W. Raymaekers, "SWIFT gpi: How industry co-creation transformed global payments," *J. Payments Strateg. Syst.*, vol. 12, no. 3, pp. 207–212, Sep. 2018.

[18] T. Saito, "Bitcoin," *Int. J. Innov. Digit. Econ.*, 2015.

[19] C. M. Kahn and W. Roberds, "Real-time gross settlement and the costs of immediacy," *J. Monet. Econ.*, 2001.

[20] I. Mas and O. Morawczynski, "Designing Mobile Money Services Lessons from M-PESA," *Innov. Technol. Governance, Glob.*, 2009.

[21] R. Martin and V. Mauree, "Commonly identified Consumer Protection themes for Digital Financial Services," 2019.

[22] M. A. Nandhi, "Effects of mobile banking on the savings practices of low-income users: The Indian experience," *Money Margins Glob. Perspect. Technol. Financ. Incl. Des.*, pp. 266–286, 2018.

[23] O. Morawczynski, "Exploring the usage and impact of 'transformational' mobile financial services: the case of M-PESA in Kenya," *J. East. African Stud.*, vol. 3, no. 3, pp. 509–525, Nov. 2009.

[24] GSMA, "The Mobile Economy 2017," 2017.

[25] D. Nampewo, G. A. Tinyinondi, D. R. Kawooya, and G. W. Ssonko, "Determinants of private sector credit in Uganda: the role of mobile money," *Financ. Innov.*, vol. 2, no. 1, 2016.

[26] B. of Uganda, "Bank of Uganda Annual Supervision Report," Kampala, 2016.

[27] L. I. Frederick, "Impact of Mobile Money Usage on Microenterprise Evidence from Zambia," *Master's Theses*, p. 92, 2014.

[28] J. Bazley, C. S. Rayner, and A. P. Power, “Zoona mobile money: investing for impact (cases A and B),” *Emerald Emerg. Mark. Case Stud.*, 2017.

[29] Bank of Zambia, “Payment System Designation.” [Online]. Available: https://www.boz.zm/designation-of-payment-systems.htm. [Accessed: 26-Jan-2017].

[30] S. Madise, “Developments in Mobile Technology and the Emergence of Mobile Money BT - The Regulation of Mobile Money: Law and Practice in Sub-Saharan Africa,” S. Madise, Ed. Cham: Springer International Publishing, 2019, pp. 63–110.

[31] B. Andiva, “Mobile Financial Services and Regulation in Kenya,” *1st Annu. Compet. Econ. Regul. Conf.*, 2015.

[32] N. Yoshino and P. Morgan, “Overview of Financial Inclusion, Regulation, and Education,” *SSRN Electron. J.*, 2016.

[33] D. S. Evans and A. Pirchio, “An Empirical Examination of Why Mobile Money Schemes Ignite in Some Developing Countries but Flounder in Most,” *Review of Network Economics*. 2014.

[34] B. Smith and K. Christidis, “IBM Blockchain: An Enterprise Deployment of a Distributed Consensus-based Transaction Log,” *Proc. Fourth Int. IBM Cloud Acad. Conf.*, pp. 1–4, 2016.

[35] D. Ivan, “Moving Toward a Blockchain-based Method for the Secure Storage of Patient Records,” 2016.

[36] R. J. Reisman, “Air Traffic Management Blockchain Infrastructure for Security , Authentication , and Privacy,” pp. 1–14, 2019.

[37] S. Mitt, L. García-Bañuelos, and F. Milani, “Blockchain Application - Case Study on Hyperledger Fabric,” 2018.

[38] M. Crosby, P. Pattanayak, S. Verma, and V. Kalyanaraman, “Applied Innovation Review,” *Appl. Innov. Rev.*, no. 2, pp. 5–20, 2016.

[39] K. Korpela, J. Hallikas, and T. Dahlberg, “Digital Supply Chain Transformation toward Blockchain Integration,” *Proc. 50th Hawaii Int. Conf. Syst. Sci.*, no. January, 2017.

[40] F. Tian, “A Supply Chain Traceability System for Food Safety Based on HACCP, Blockchain & Internet of Things,” *14th Int. Conf. Serv. Syst. Serv. Manag.*, vol. 323, no. 2, pp. 511–519, 2015.

[41] Z. Li, H. Wu, B. King, Z. Ben Miled, J. Wassick, and J. Tazelaar, “A Hybrid Blockchain Ledger for Supply Chain Visibility,” in *Proceedings - 17th International Symposium on Parallel and Distributed Computing, ISPDC 2018*, 2018.

[42] I. Haq and O. Muselemu, “Blockchain Technology in Pharmaceutical Industry to

Prevent Counterfeit Drugs," *Int. J. Comput. Appl.*, vol. 180, no. 25, pp. 8–12, 2018.

[43] Y. Omran, M. Henke, R. Heines, and E. Hofmann, "Blockchain-driven supply chain finance: Towards a conceptual framework from a buyer perspective," *(Working Pap.*, no. December 2018, p. 15, 2017.

[44] A. Baliga, "The Blockchain Landscape Office of the CTO," *Persistent Syst. Ltd*, p. 21, 2016.

[45] J. Phiri and M. Chibuye, "Blockchain – It ' S Practical Use for," vol. 1, no. 1, pp. 57–62, 2017.

[46] M. Mainelli and M. Smith, "Sharing ledgers for sharing economies: an exploration of mutual distributed ledgers (aka blockchain technology)," *J. Financ. Perspect.*, vol. 3, no. 3 Winter, pp. 38–69, 2015.

[47] A. Deshpande, K. Stewart, L. Lepetit, and S. Gunashekar, "Distributed Ledger Technologies/Blockchain: Challenges, opportunities and the prospects for standards," *Br. Stand. Inst.*, no. May, pp. 1–34, 2017.

[48] G. Zyskind and A. S. Pentland, "Decentralizing Privacy : Using Blockchain to Protect Personal Data," *2015 IEEE Secur. Priv. Work.*, pp. 180–184, 2015.

[49] K. Zīle and S. Renāte, "Blockchain Use Cases and Their Feasibility," *Appl. Comput. Syst.*, vol. 23, no. 1, pp. 12–20, 2018.

[50] E. Androulaki *et al.*, "Hyperledger fabric," pp. 1–15, 2018.

[51] V. Gatteschi, F. Lamberti, C. Demartini, C. Pranteda, and V. Santamaria, "To Blockchain or Not to Blockchain: That Is the Question," *IT Prof.*, vol. 20, no. 2, pp. 62–74, 2018.

[52] T. Koens and E. Poll, "What Blockchain Alternative Do You Need ?"

[53] B. A. Scriber, "A Framework for Determining Blockchain Applicability," *IEEE Softw.*, vol. 35, no. 4, pp. 70–77, 2018.

[54] H. Zubko and T. Bohner, "Lessons Learned from Hyperledger Fabric PoC Projects," 2018. [Online]. Available: https://www.hyperledger.org/blog/2018/04/19/lessons-learned-from-hyperledger-fabric-poc-projects. [Accessed: 30-Sep-2019].

[55] D. Birch, R. Brown, and S. Parulava, "Towards ambient accountability in financial services: Shared ledgers, translucent transactions and the technological legacy of the great financial crisis," *J. Payments Strateg. Syst.*, 2016.

[56] M. Peck, "Do You Need a Blockchain?," *IEEE Spectrum*, 2018. [Online]. Available: https://spectrum.ieee.org/computing/networks/do-you-need-a-blockchain. [Accessed: 12-Dec-2018].

[57] J. Rangaswami, S. Warren, C. Mulligan, and J. Zhu Scott, "Blockchain Beyond the Hype

A Practical Framework for Business Leaders," *White Pap. World Econ. forum 2018*, no. April, 2018.

[58] D. Yaga, P. Mell, N. Roby, and K. Scarfone, "Blockchain Technology Overview - National Institute of Standards and Technology Internal Report 8202," *NIST Interagency/Internal Rep.*, pp. 1–57, 2018.

[59] M. R. Institute, "Survey on Establishing Evaluation Model for Blockchain," no. March, 2017.

[60] C. Pahl, N. El Ioini, and S. Helmer, "A decision framework for blockchain platforms for iot and edge computing," *IoTBDS 2018 - Proc. 3rd Int. Conf. Internet Things, Big Data Secur.*, vol. 2018-March, no. March, pp. 105–113, 2018.

[61] M. Samaniego and R. Deters, "Blockchain as a Service for IoT," in *Proceedings - 2016 IEEE International Conference on Internet of Things; IEEE Green Computing and Communications; IEEE Cyber, Physical, and Social Computing; IEEE Smart Data, iThings-GreenCom-CPSCom-Smart Data 2016*, 2017.

[62] J. Garzik, "Public versus Private Blockchains. Part 1: Permissioned Blockchains," 2015.

[63] J. Garzik, "Public versus Private Blockchains. Part 2: Permissionless Blockchains," 2015.

[64] K. Wüst and A. Gervais, "Do you need a Blockchain?," *IACR Cryptol. ePrint Arch.*, no. i, p. 375, 2017.

[65] G. Greenspan, "Avoiding the pointless blockchain project | MultiChain," 2015.

[66] M. Bourreau and T. Valletti, "Competition and Interoperability in Mobile Money Platform Markets: What Works and What Doesn't? (*)," *Commun. Strateg.*, 2015.

[67] R. B. of I. Department of Payment and Settlement Systems, "Prepaid Payment Instruments (PPIs) – Operational Guidelines for Interoperability," no. 808. Mumbai, India, pp. 2–4, 2018.

[68] D. Kumar, T. A. Gonsalves, A. Jhunjhunwala, and G. Raina, "Mobile payment architectures for India," *Proc. 16th Natl. Conf. Commun. NCC 2010*, no. 1, pp. 4–8, 2010.

[69] K. Kumar and M. Tarazi, "Interoperability in Branchless Banking and Mobile Money. Consultative Group to Assist the Poor (CGAP).," *CGAP*, 2012. [Online]. Available: http://www.cgap.org/blog/interoperability-branchless-banking-and-mobile-money-0.

[70] B. Andiva, "Mobile Financial Services and Regulation in Kenya," in *1st Annual Competition and Economic Regulation (ACER) Conference*, 2015.

[71] B. Muthiora, "Enabling mobile money policies in Kenya - Fostering a digital financial

revolution," *GSM Assoc.*, no. January, p. 30, 2015.

[72] M. Mamabolo, "Kenya's Central Bank gives mobile money interoperability thumbs up," *IT WebAfrica*, 2018. [Online]. Available: http://www.itwebafrica.com/fintech/842-kenya/243988-kenyas-central-bank-gives-mobile-money-interoperability-thumbs-up. [Accessed: 20-Dec-2018].

[73] Central Bank of Kenya, "Mobile Money Interoperability," no. January, p. 2018, 2018.

[74] M. Mamabolo, "Kenya pilots mobile money interoperability," *IT WebAfrica*, 2018. [Online]. Available: http://www.itwebafrica.com/mobilex/309-kenya/242443-kenya-launches-mobile-money-interoperability-pilot-today. [Accessed: 20-Dec-2018].

[75] M. Bourreau and S. Hoernig, "Interoperability of Mobile Money: International Experience and Recommendations for Mozambique," no. December, 2016.

[76] J. Argent and J. A. Hanson, "The Regulation of Mobile Money in Rwanda," *J. ICT*, 2013.

[77] Bank of Tanzania, "National Payment System Directorate Statistics:" [Online]. Available: http://www.bot-tz.org/PaymentSystem/statistics.asp. [Accessed: 18-Dec-2018].

[78] N. Davidson and P. Leishman, "The case for interoperability: Assessing the value that the interconnection of mobile money services would create for customers and operators," 2016.

[79] S. H. Ammous, "Blockchain Technology: What is it Good for?," *SSRN Electron. J.*, 2017.

[80] I. C. Lin and T. C. Liao, "A survey of blockchain security issues and challenges," *Int. J. Netw. Secur.*, 2017.

[81] M. Rauchs *et al.*, "Distributed Ledger Technology Systems: A Conceptual Framework," *SSRN Electron. J.*, 2018.

[82] H. Halpin and M. Piekarska, "Introduction to Security and Privacy on the Blockchain," *2017 IEEE Eur. Symp. Secur. Priv. Work.*, vol. 43, 2017.

[83] Bank of Zambia, "Bank of Zambia - Payment Systems," 2016. [Online]. Available: https://www.boz.zm/payment-systems.htm. [Accessed: 02-Mar-2018].

[84] C. Schmitz, "LimeSurvey: An Open Source survey tool. LimeSurvey Project Hamburg, Germany.," *Limesurvey GmbH*, 2015. [Online]. Available: www.limesurvey.org. [Accessed: 10-Apr-2017].

[85] Microsoft, "Microsoft Excel." [Online]. Available: https://products.office.com/en/excel. [Accessed: 11-Dec-2018].

[86] P. Rosati and T. Cuk, “Blockchain Beyond Cryptocurrencies,” in *Disrupting Finance FinTech and Strategy in the 21st Century*, T. Lynn, Ed. Palgrave Macmillan, 2018, pp. 149–164.

[87] M. Mukherjee, “Object-Oriented Analysis and Design,” *Int. J. Adv. Eng. Manag.*, 2016.

[88] J. Hunt, “The Object Modeling Technique,” in *Java and Object Orientation: An Introduction. Applied Computing*, London: Springer, 1998, pp. 375–399.

[89] A. Gosling, James; Joy, Bill; Steele, Guy; Bracha, Gilad; Buckley, “The Java ® Language Specification. Java SE 8 Edition,” *Addison-Wesley*, 2014.

[90] B. K. Mohanta, S. S. Panda, and D. Jena, “An Overview of Smart Contract and Use Cases in Blockchain Technology,” in *2018 9th International Conference on Computing, Communication and Networking Technologies, ICCCNT 2018*, 2018.

[91] N. Kshetri, “Blockchain’s roles in strengthening cybersecurity and protecting privacy,” *Telecomm. Policy*, 2017.

[92] S. Androutsellis-Theotokis and D. Spinellis, “A survey of peer-to-peer content distribution technologies,” *ACM Computing Surveys*. 2004.

[93] W. J. Buchanan, *Cryptography*. 2017.

[94] A. Lewis, “Blockchain Technology Explained,” *Blockchain Technologies*, 2015. .

[95] The Linux Foundation, *hyperledger-fabricdocs Documentation Release master*. The Linux Foundation, 2019.

[96] E. Androulaki *et al.*, “Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains,” in *Proceedings of the 13th EuroSys Conference, EuroSys 2018*, 2018.

[97] C. Cachin, “Architecture of the Hyperledger Blockchain Fabric,” *Work. Distrib. Cryptocurrencies Consens. Ledgers (DCCL 2016)*, 2016.

[98] Varun Raj, “Hyperledger Fabric Architecture: Explained in detail,” 2018.

[99] S. Mankovskii *et al.*, “ODBC,” in *Encyclopedia of Database Systems*, 2009.

[100] The Linux Foundation, “Hyperledger Reference Manual,” 2017. [Online]. Available: https://hyperledger-fabric.readthedocs.io/en/release-1.4/arch-deep-dive.html. [Accessed: 01-Mar-2017].

[101] D. Merkel, “Docker: lightweight Linux containers for consistent development and deployment,” *Linux Journal*. 2014.

[102] X. Li, Z. Liu, and H. Jifeng, “A formal semantics of UML sequence diagram,” in *Proceedings of the Australian Software Engineering Conference, ASWEC*, 2004.

[103] “Sequence Diagrams,” in *Use Case Driven Object Modeling with UML*, 2008.

[104] B. T. Boudreau, J. Glick, S. Greene, V. Spurlin, and J. J. Woehr, “NetBeans: The Definitive Guide,” *Building*, 2002.

[105] S. Company, “Maven: The Definitive Guide: The Definitive Guide,” *Java*, 2008.

[106] J. Nickoloff, *Docker in Action*. 2016.

[107] D. Andolfatto, “Blockchain: What it is, what it does, and why you probably don’t need one,” *Fed. Reserv. Bank St. Louis Rev.*, 2018.

[108] M. U. Javed, M. Rehman, N. Javaid, A. Aldegheishem, N. Alrajeh, and M. Tahir, “Blockchain-based secure data storage for distributed vehicular networks,” *Appl. Sci.*, vol. 10, no. 6, pp. 1–22, 2020.

[109] S. Dhanalakshmi, B. G. Obula Reddy, and K. Yogitha Lakshmi, “Building a blockchain approach with hyperledger transaction flow and distributed consensus algorithms,” *Int. J. Innov. Technol. Explor. Eng.*, vol. 8, no. 2S, pp. 423–426, 2018.

[110] C. Muya, “Mobile money in Africa,” *The Economist: Intelligence Unit*, 2016.

[111] T. A. Riley and A. Kulathunga, *Bringing E-money to the Poor: Successes and Failures*. 2017.

[112] F. S. Hardwick, R. N. Akram, and K. Markantonakis, “Fair and Transparent Blockchain Based Tendering Framework - A Step Towards Open Governance,” in *Proceedings - 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications and 12th IEEE International Conference on Big Data Science and Engineering, Trustcom/BigDataSE 2018*, 2018.

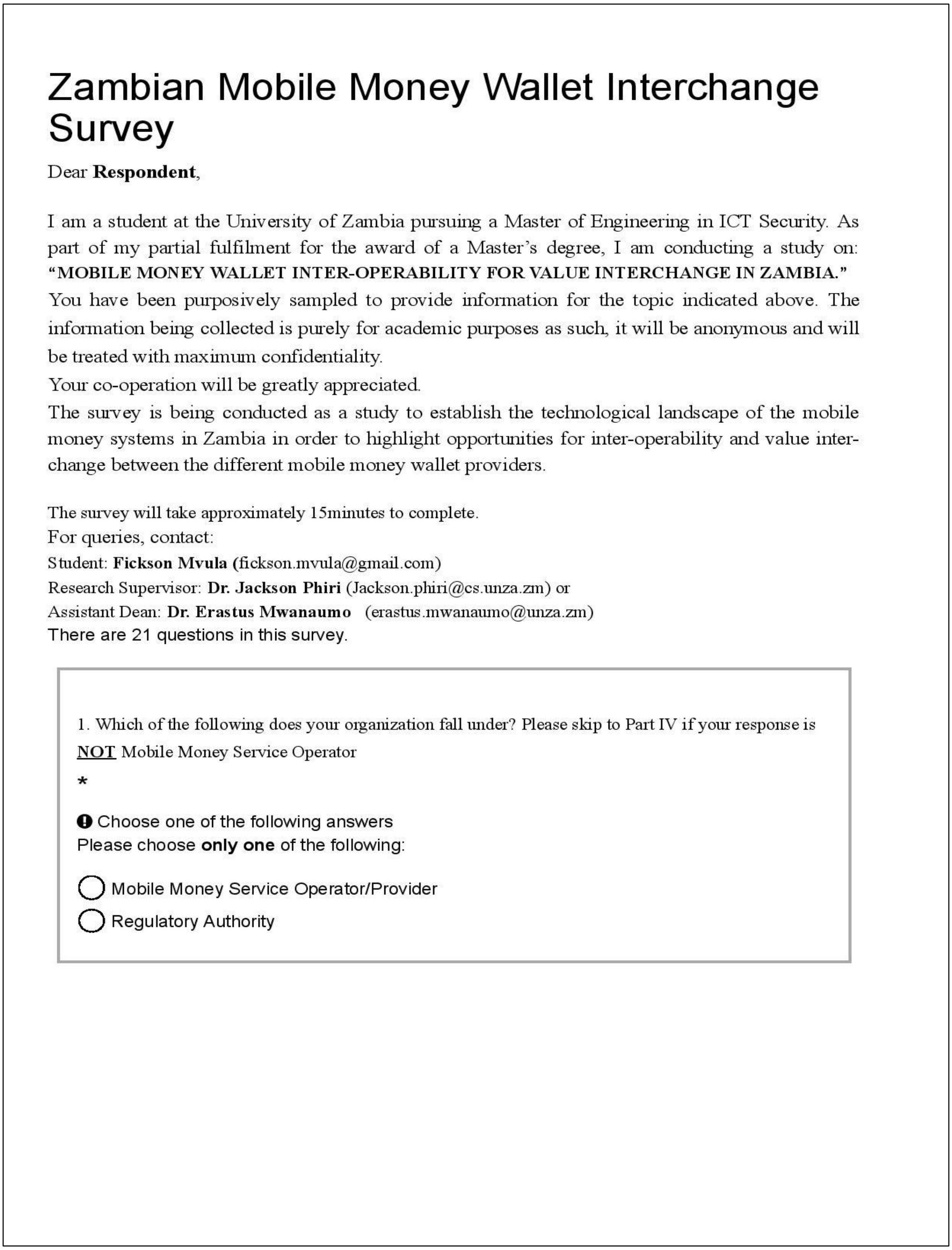
[113] A. Kiayias, E. Koutsoupias, M. Kyropoulou, and Y. Tselekounis, “Blockchain mining games,” in *EC 2016 - Proceedings of the 2016 ACM Conference on Economics and Computation*, 2016.

[114] M. Valenta and P. Sandner, “Comparison of Ethereum, Hyperledger Fabric and Corda,” *Frankfurt Sch. Blockchain Cent.*, 2017.

[115] M. Castro, “Practical Byzantine Fault Tolerance,” 2001.

APPENDIX

A. Appendix: Survey Questionnaire



Zambian Mobile Money Wallet Interchange Survey

Dear **Respondent**,

I am a student at the University of Zambia pursuing a Master of Engineering in ICT Security. As part of my partial fulfilment for the award of a Master's degree, I am conducting a study on: **"MOBILE MONEY WALLET INTER-OPERABILITY FOR VALUE INTERCHANGE IN ZAMBIA."**
You have been purposively sampled to provide information for the topic indicated above. The information being collected is purely for academic purposes as such, it will be anonymous and will be treated with maximum confidentiality.
Your co-operation will be greatly appreciated.
The survey is being conducted as a study to establish the technological landscape of the mobile money systems in Zambia in order to highlight opportunities for inter-operability and value interchange between the different mobile money wallet providers.

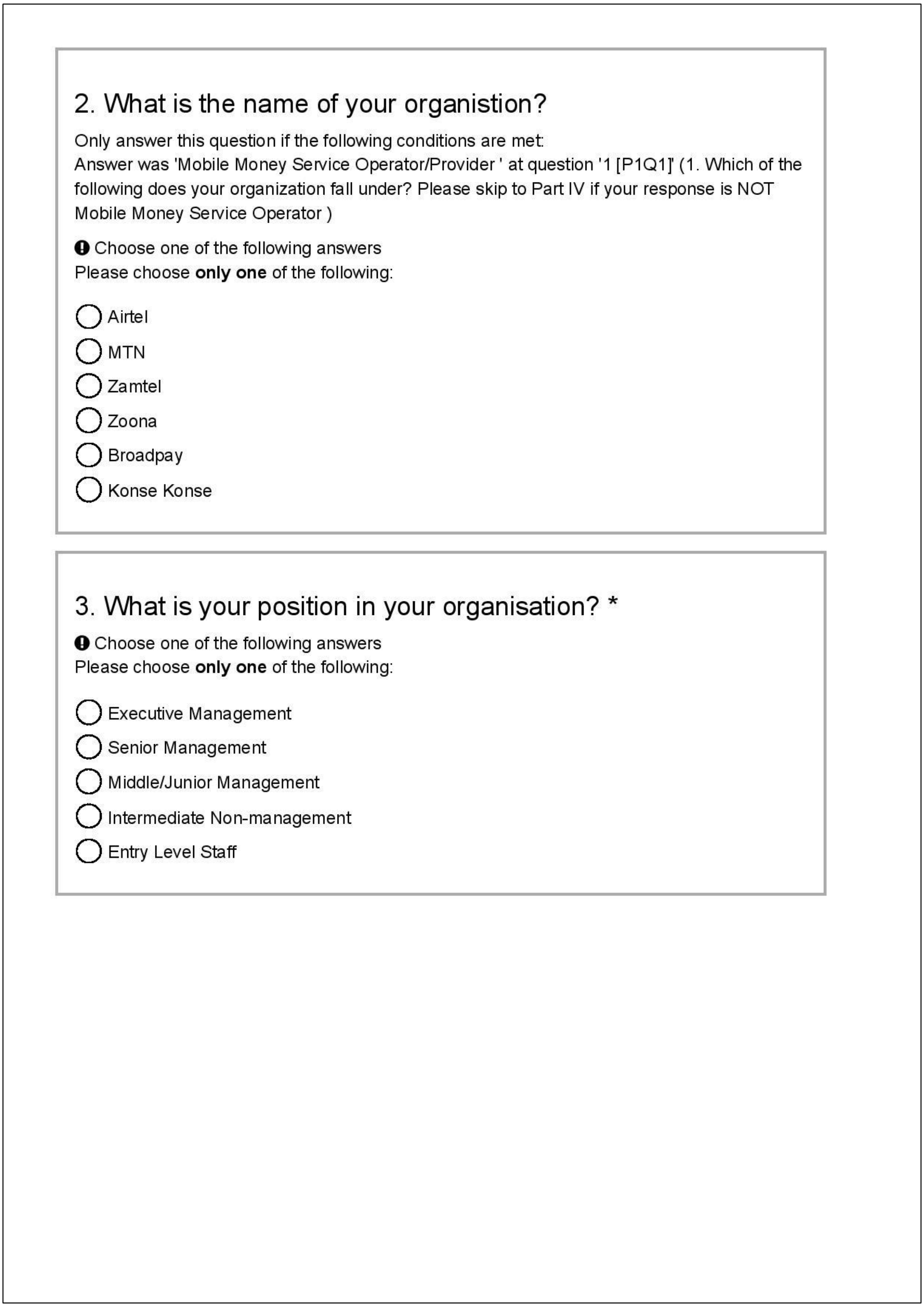
The survey will take approximately 15minutes to complete.
For queries, contact:
Student: **Fickson Mvula (**fickson.mvula@gmail.com)
Research Supervisor: **Dr. Jackson Phiri** (Jackson.phiri@cs.unza.zm) or
Assistant Dean: **Dr. Erastus Mwanaumo** (erastus.mwanaumo@unza.zm)
There are 21 questions in this survey.

1. Which of the following does your organization fall under? Please skip to Part IV if your response is **NOT** Mobile Money Service Operator

*

❗ Choose one of the following answers
Please choose **only one** of the following:

○ Mobile Money Service Operator/Provider
○ Regulatory Authority



2. What is the name of your organistion?

Only answer this question if the following conditions are met:
Answer was 'Mobile Money Service Operator/Provider ' at question '1 [P1Q1]' (1. Which of the following does your organization fall under? Please skip to Part IV if your response is NOT Mobile Money Service Operator)

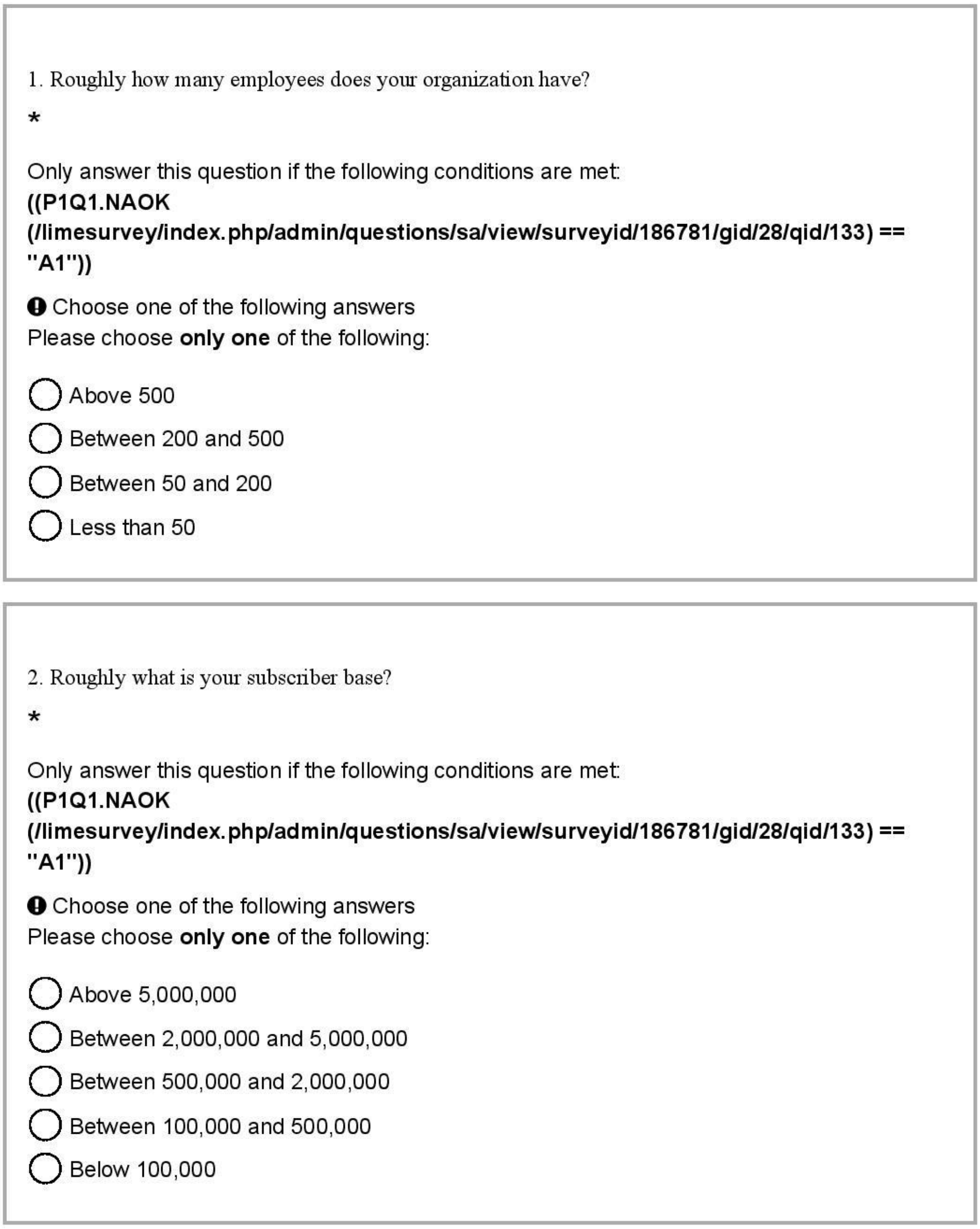
❗ Choose one of the following answers
Please choose **only one** of the following:

○ Airtel
○ MTN
○ Zamtel
○ Zoona
○ Broadpay
○ Konse Konse

3. What is your position in your organisation? *

❗ Choose one of the following answers
Please choose **only one** of the following:

○ Executive Management
○ Senior Management
○ Middle/Junior Management
○ Intermediate Non-management
○ Entry Level Staff



1. Roughly how many employees does your organization have?

*

Only answer this question if the following conditions are met:
((P1Q1.NAOK (/limesurvey/index.php/admin/questions/sa/view/surveyid/186781/gid/28/qid/133) == "A1"))

❗ Choose one of the following answers
Please choose **only one** of the following:

○ Above 500

○ Between 200 and 500

○ Between 50 and 200

○ Less than 50

2. Roughly what is your subscriber base?

*

Only answer this question if the following conditions are met:
((P1Q1.NAOK (/limesurvey/index.php/admin/questions/sa/view/surveyid/186781/gid/28/qid/133) == "A1"))

❗ Choose one of the following answers
Please choose **only one** of the following:

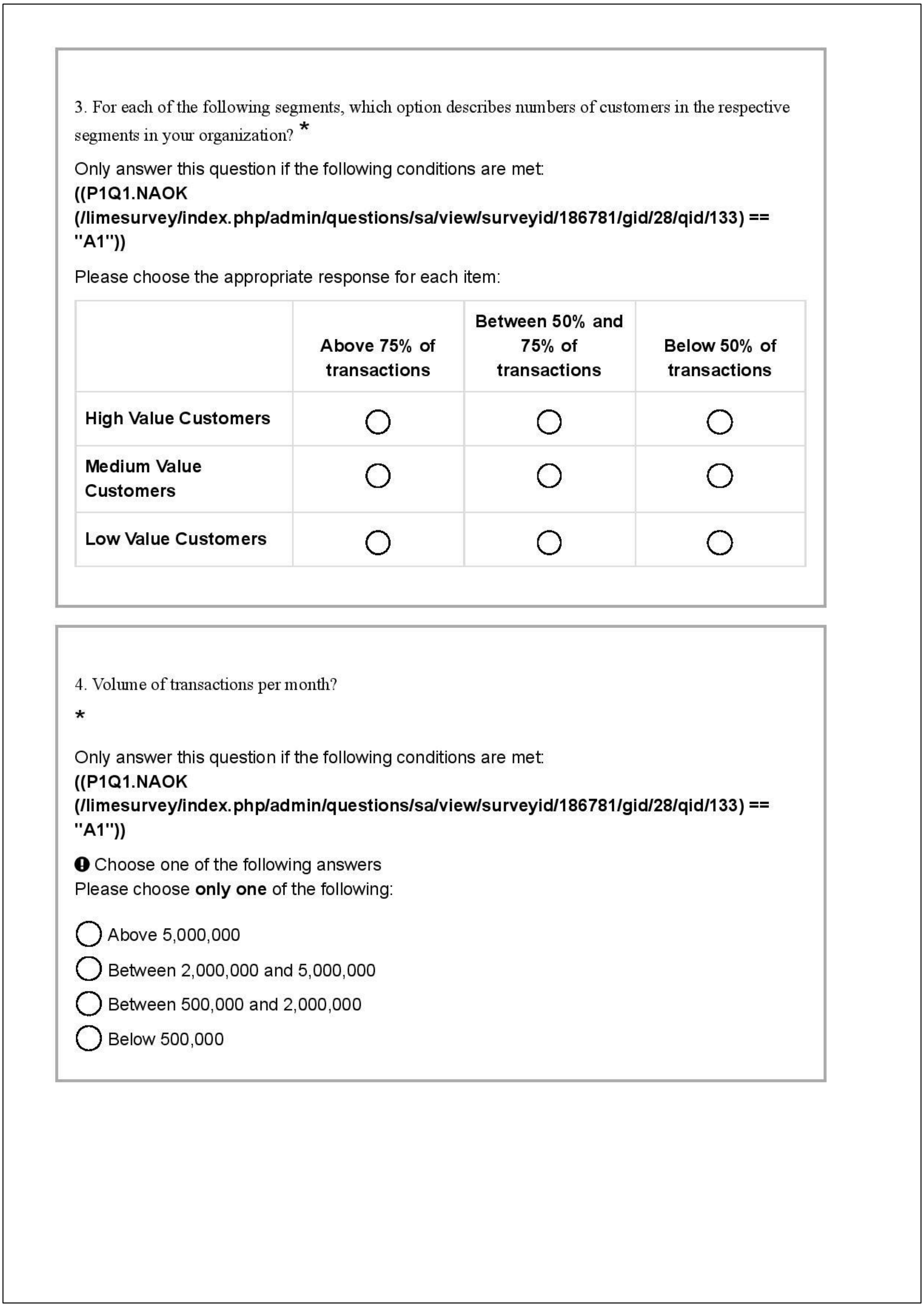
○ Above 5,000,000

○ Between 2,000,000 and 5,000,000

○ Between 500,000 and 2,000,000

○ Between 100,000 and 500,000

○ Below 100,000



3. For each of the following segments, which option describes numbers of customers in the respective segments in your organization? *

Only answer this question if the following conditions are met:
((P1Q1.NAOK (/limesurvey/index.php/admin/questions/sa/view/surveyid/186781/gid/28/qid/133) == "A1"))

Please choose the appropriate response for each item:

	Above 75% of transactions	**Between 50% and 75% of transactions**	**Below 50% of transactions**
High Value Customers	○	○	○
Medium Value Customers	○	○	○
Low Value Customers	○	○	○

4. Volume of transactions per month?

*

Only answer this question if the following conditions are met:
((P1Q1.NAOK (/limesurvey/index.php/admin/questions/sa/view/surveyid/186781/gid/28/qid/133) == "A1"))

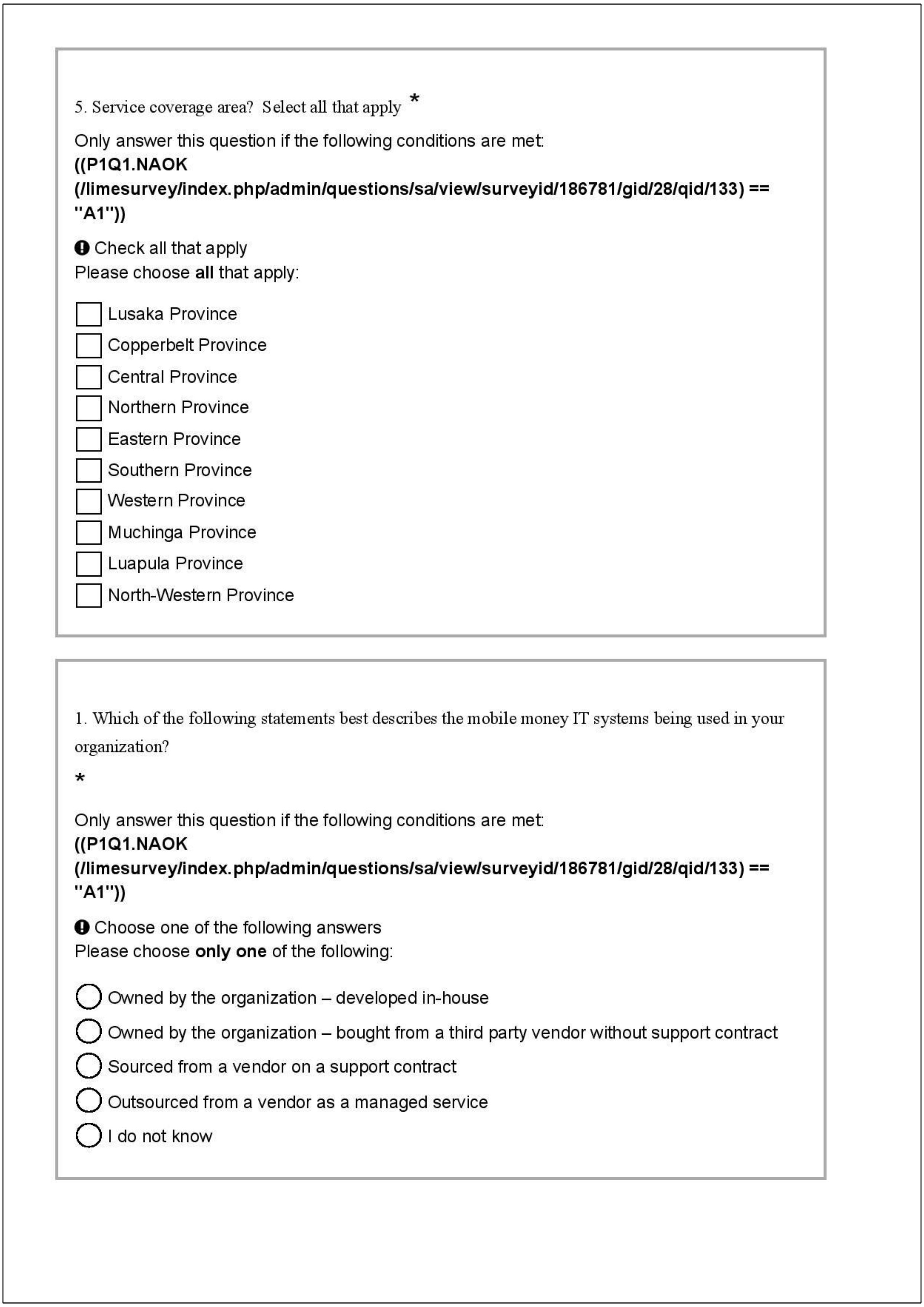
❗ Choose one of the following answers
Please choose **only one** of the following:

○ Above 5,000,000

○ Between 2,000,000 and 5,000,000

○ Between 500,000 and 2,000,000

○ Below 500,000



5. Service coverage area? Select all that apply *

Only answer this question if the following conditions are met:
((P1Q1.NAOK (/limesurvey/index.php/admin/questions/sa/view/surveyid/186781/gid/28/qid/133) == "A1"))

❶ Check all that apply
Please choose **all** that apply:

□ Lusaka Province
□ Copperbelt Province
□ Central Province
□ Northern Province
□ Eastern Province
□ Southern Province
□ Western Province
□ Muchinga Province
□ Luapula Province
□ North-Western Province

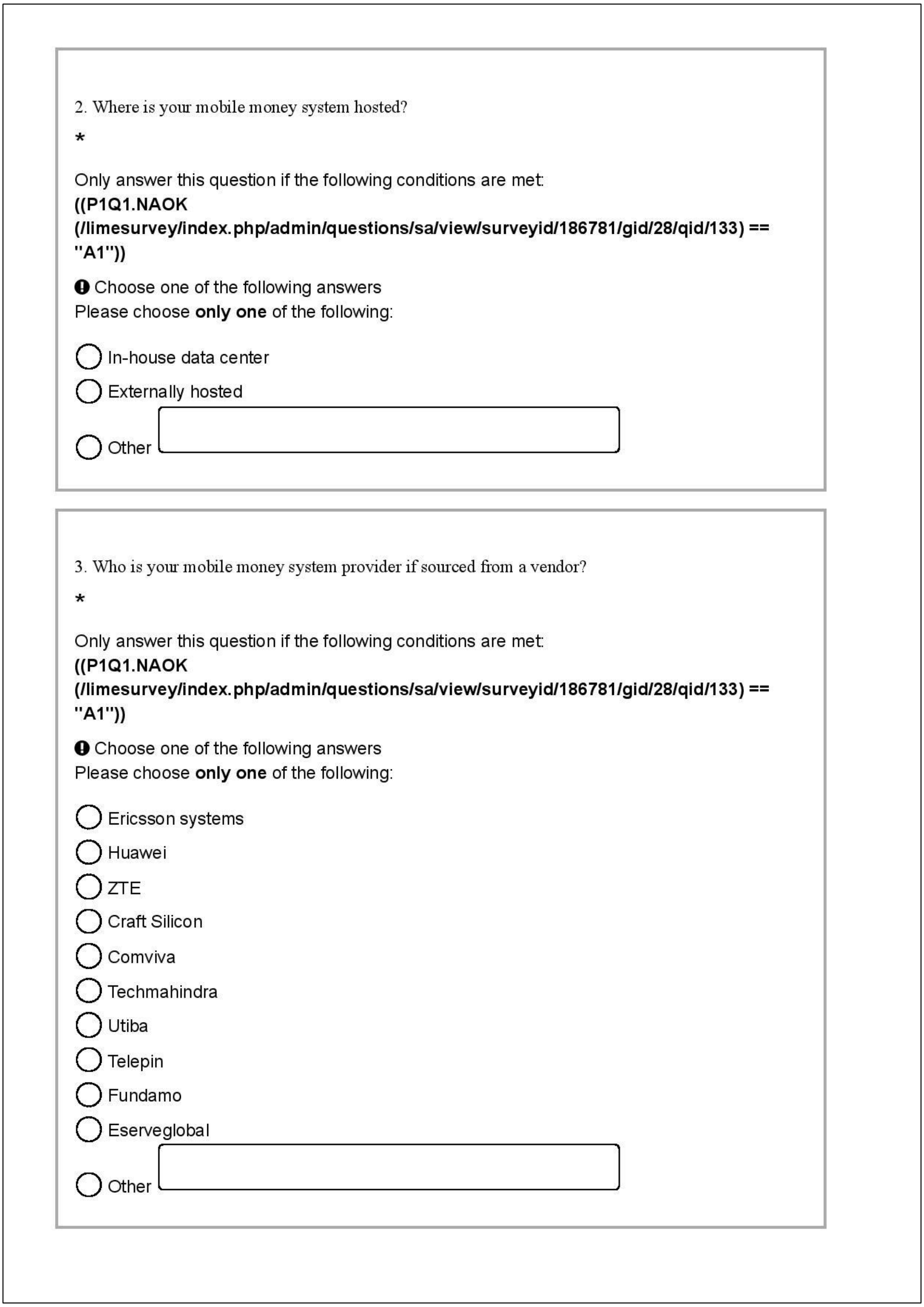
1. Which of the following statements best describes the mobile money IT systems being used in your organization?

*

Only answer this question if the following conditions are met:
((P1Q1.NAOK (/limesurvey/index.php/admin/questions/sa/view/surveyid/186781/gid/28/qid/133) == "A1"))

❶ Choose one of the following answers
Please choose **only one** of the following:

○ Owned by the organization – developed in-house
○ Owned by the organization – bought from a third party vendor without support contract
○ Sourced from a vendor on a support contract
○ Outsourced from a vendor as a managed service
○ I do not know



2. Where is your mobile money system hosted?

*

Only answer this question if the following conditions are met:
((P1Q1.NAOK (/limesurvey/index.php/admin/questions/sa/view/surveyid/186781/gid/28/qid/133) == "A1"))

❶ Choose one of the following answers
Please choose **only one** of the following:

○ In-house data center
○ Externally hosted
○ Other

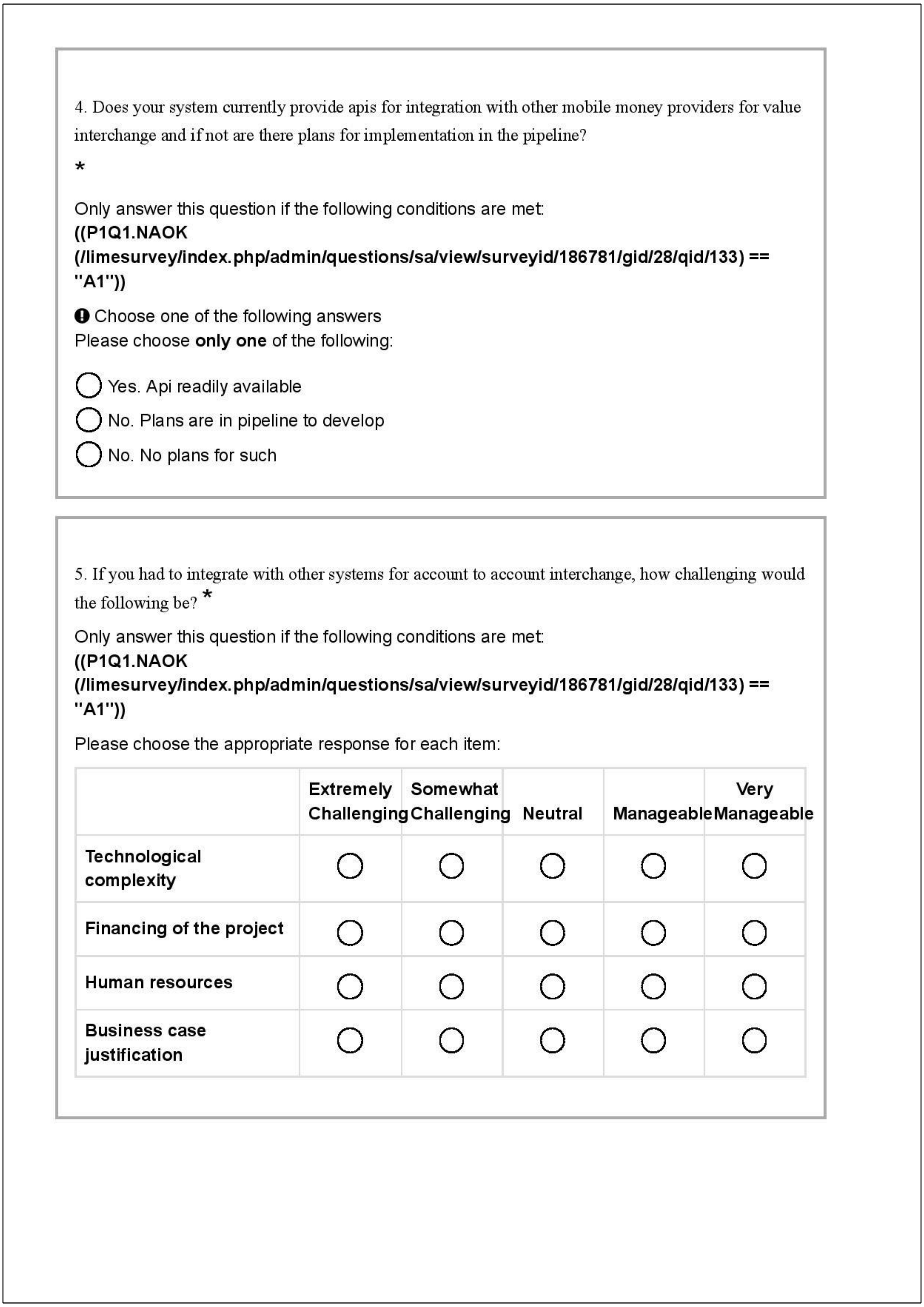
3. Who is your mobile money system provider if sourced from a vendor?

*

Only answer this question if the following conditions are met:
((P1Q1.NAOK (/limesurvey/index.php/admin/questions/sa/view/surveyid/186781/gid/28/qid/133) == "A1"))

❶ Choose one of the following answers
Please choose **only one** of the following:

○ Ericsson systems
○ Huawei
○ ZTE
○ Craft Silicon
○ Comviva
○ Techmahindra
○ Utiba
○ Telepin
○ Fundamo
○ Eserveglobal
○ Other



4. Does your system currently provide apis for integration with other mobile money providers for value interchange and if not are there plans for implementation in the pipeline?

*

Only answer this question if the following conditions are met:
((P1Q1.NAOK (/limesurvey/index.php/admin/questions/sa/view/surveyid/186781/gid/28/qid/133) == "A1"))

❶ Choose one of the following answers
Please choose **only one** of the following:

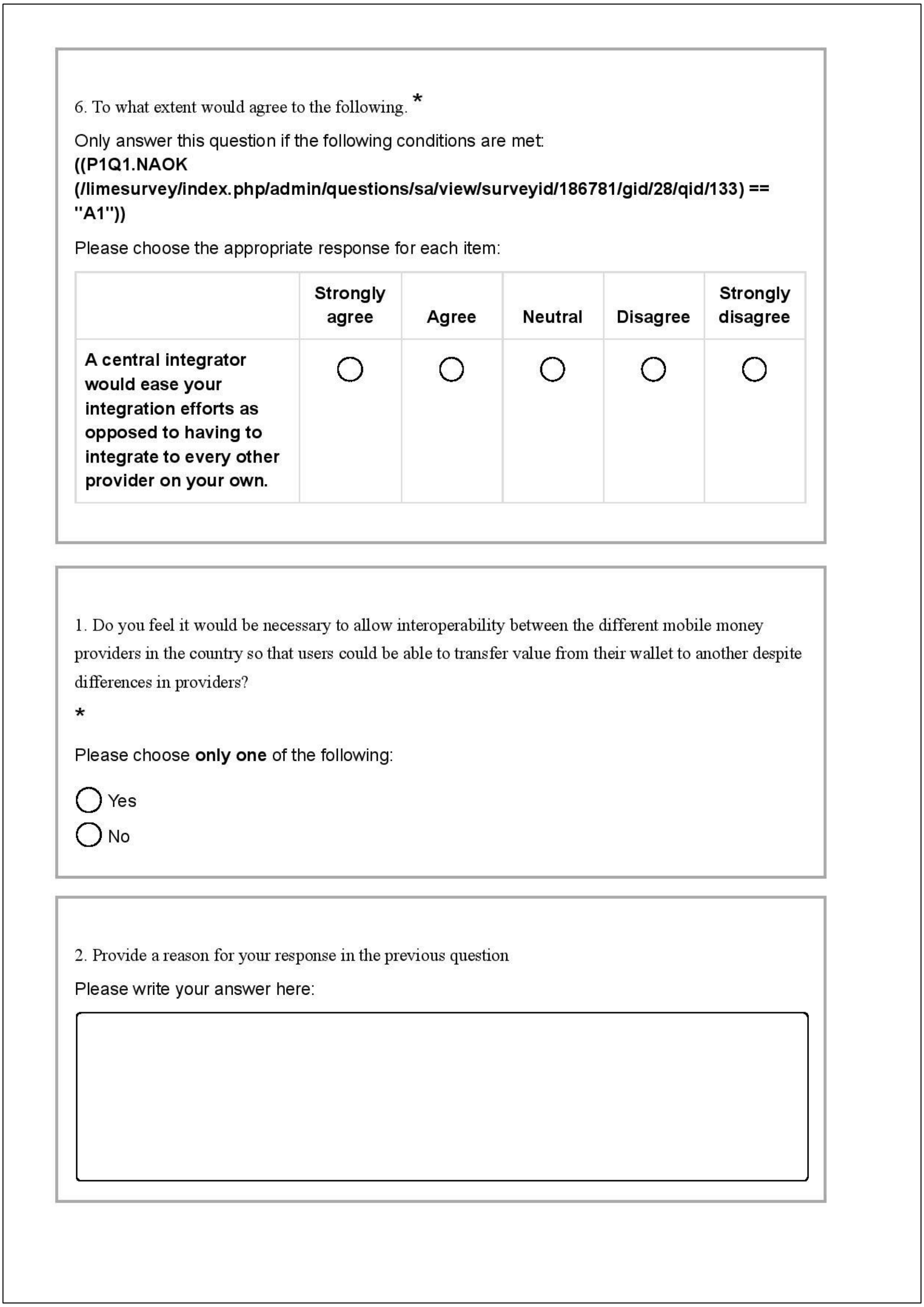
○ Yes. Api readily available
○ No. Plans are in pipeline to develop
○ No. No plans for such

5. If you had to integrate with other systems for account to account interchange, how challenging would the following be? *

Only answer this question if the following conditions are met:
((P1Q1.NAOK (/limesurvey/index.php/admin/questions/sa/view/surveyid/186781/gid/28/qid/133) == "A1"))

Please choose the appropriate response for each item:

	Extremely Challenging	**Somewhat Challenging**	**Neutral**	**Manageable**	**Very Manageable**
Technological complexity	○	○	○	○	○
Financing of the project	○	○	○	○	○
Human resources	○	○	○	○	○
Business case justification	○	○	○	○	○



6. To what extent would agree to the following. *

Only answer this question if the following conditions are met:
((P1Q1.NAOK (/limesurvey/index.php/admin/questions/sa/view/surveyid/186781/gid/28/qid/133) == "A1"))

Please choose the appropriate response for each item:

	Strongly agree	Agree	Neutral	Disagree	Strongly disagree
A central integrator would ease your integration efforts as opposed to having to integrate to every other provider on your own.	○	○	○	○	○

1. Do you feel it would be necessary to allow interoperability between the different mobile money providers in the country so that users could be able to transfer value from their wallet to another despite differences in providers?

*

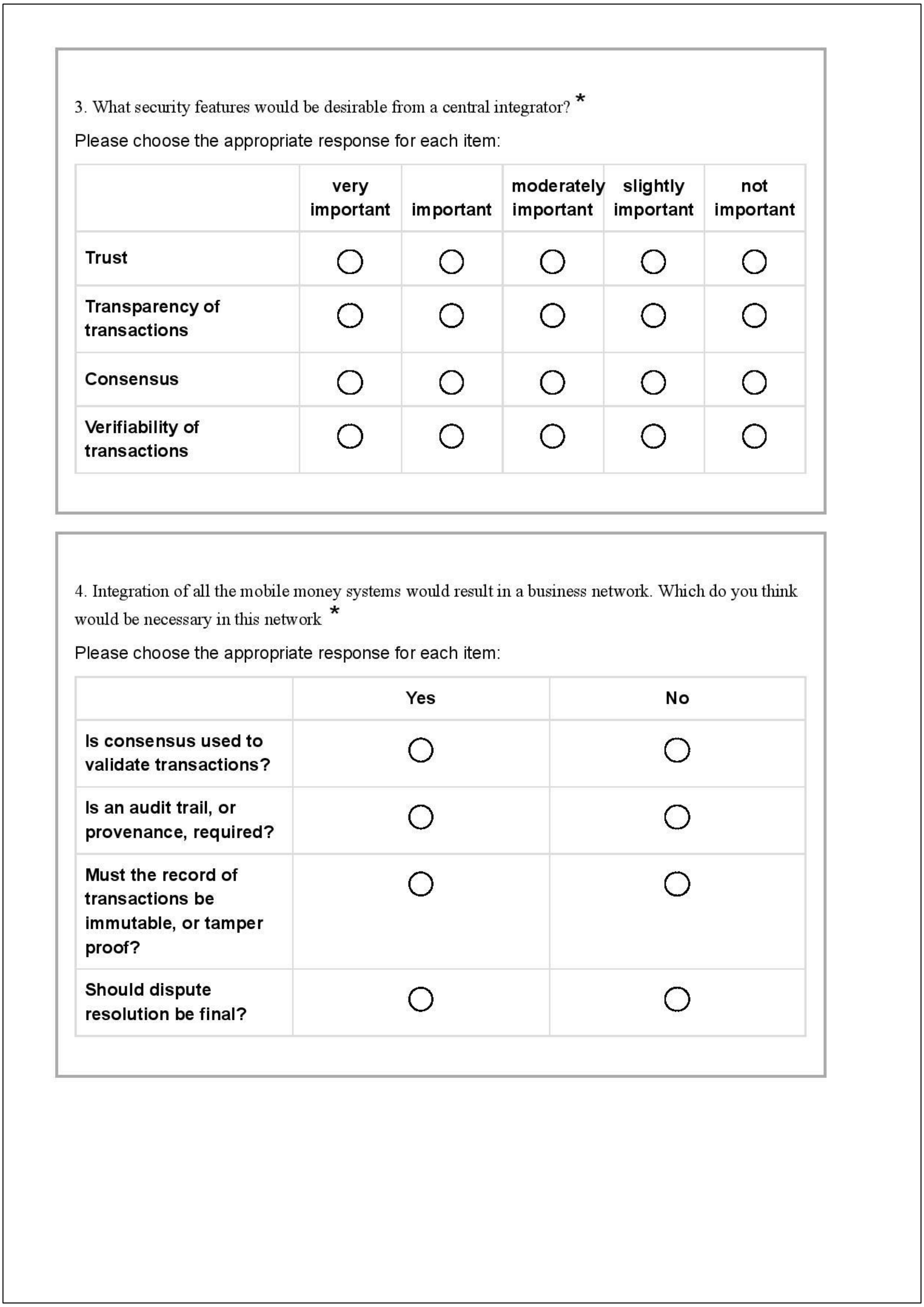
Please choose **only one** of the following:

○ Yes

○ No

2. Provide a reason for your response in the previous question

Please write your answer here:



3. What security features would be desirable from a central integrator? *

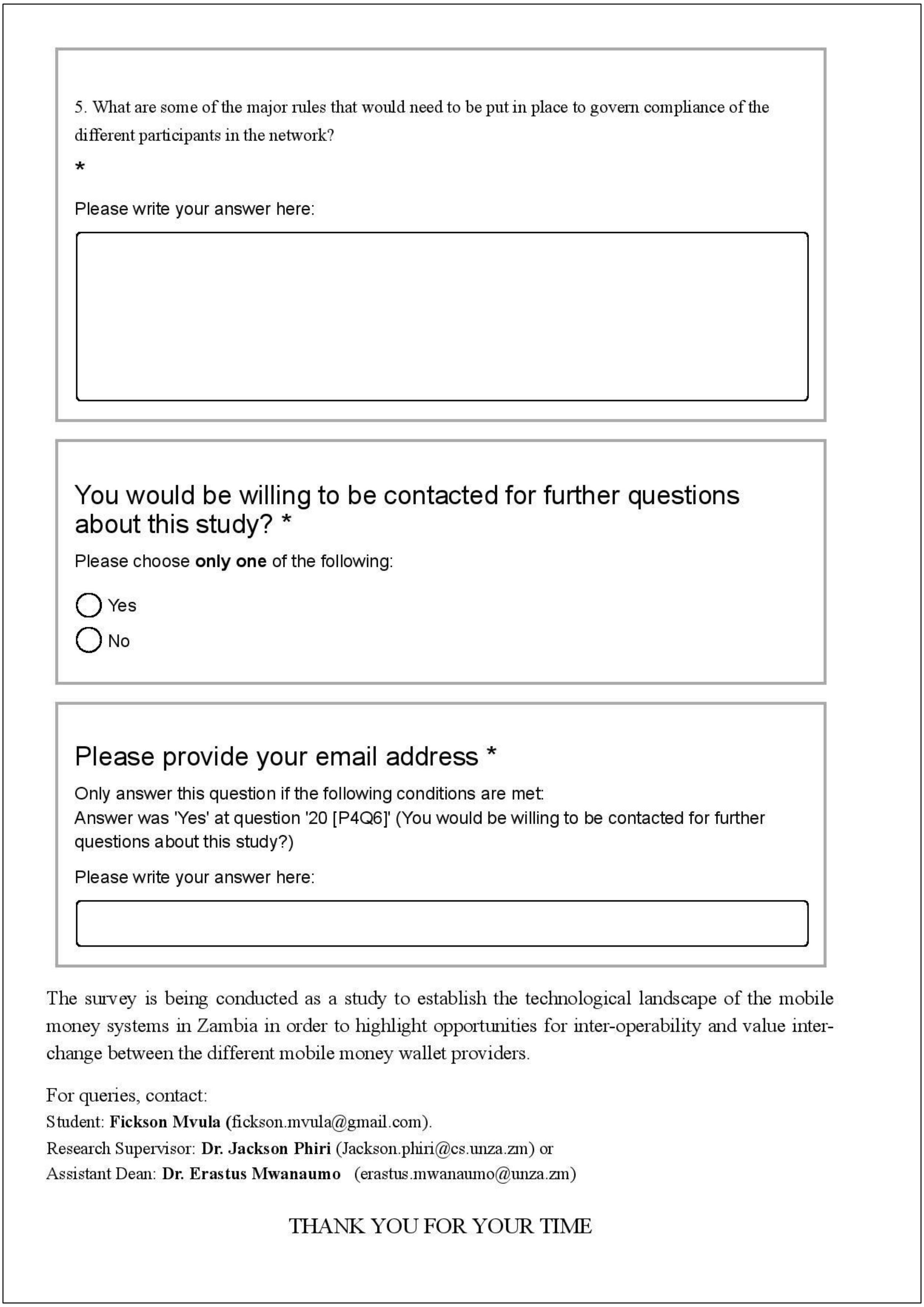
Please choose the appropriate response for each item:

	very important	important	moderately important	slightly important	not important
Trust	○	○	○	○	○
Transparency of transactions	○	○	○	○	○
Consensus	○	○	○	○	○
Verifiability of transactions	○	○	○	○	○

4. Integration of all the mobile money systems would result in a business network. Which do you think would be necessary in this network *

Please choose the appropriate response for each item:

	Yes	No
Is consensus used to validate transactions?	○	○
Is an audit trail, or provenance, required?	○	○
Must the record of transactions be immutable, or tamper proof?	○	○
Should dispute resolution be final?	○	○



5. What are some of the major rules that would need to be put in place to govern compliance of the different participants in the network?

*

Please write your answer here:

You would be willing to be contacted for further questions about this study? *

Please choose **only one** of the following:

○ Yes

○ No

Please provide your email address *

Only answer this question if the following conditions are met:
Answer was 'Yes' at question '20 [P4Q6]' (You would be willing to be contacted for further questions about this study?)

Please write your answer here:

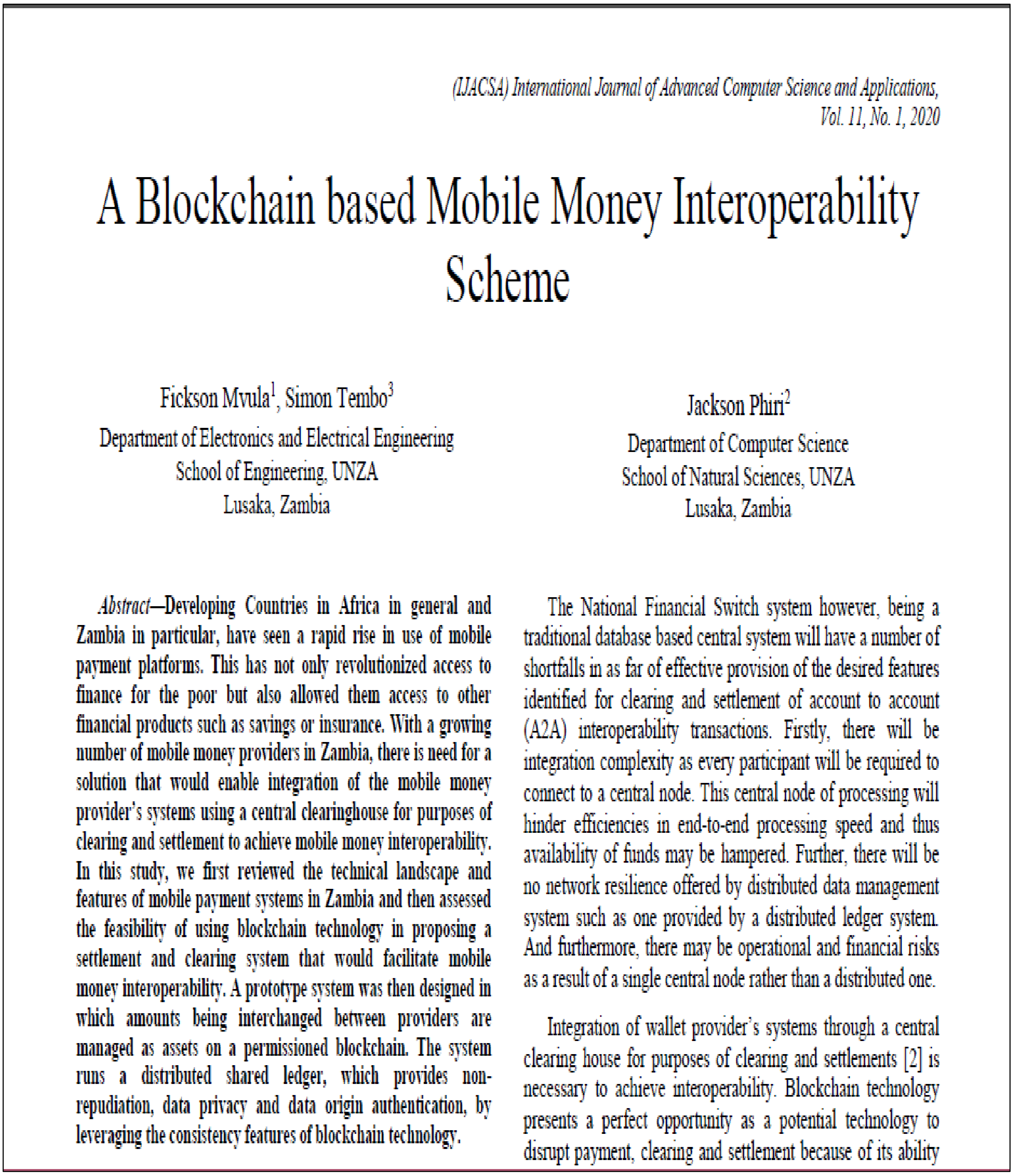
The survey is being conducted as a study to establish the technological landscape of the mobile money systems in Zambia in order to highlight opportunities for inter-operability and value interchange between the different mobile money wallet providers.

For queries, contact:
Student: **Fickson Mvula (**fickson.mvula@gmail.com).
Research Supervisor: **Dr. Jackson Phiri** (Jackson.phiri@cs.unza.zm) or
Assistant Dean: **Dr. Erastus Mwanaumo** (erastus.mwanaumo@unza.zm)

THANK YOU FOR YOUR TIME

Submit your survey.
Thank you for completing this survey.

B. IJACSA Journal Publication



(IJACSA) International Journal of Advanced Computer Science and Applications,
Vol. 11, No. 1, 2020

A Blockchain based Mobile Money Interoperability Scheme

Fickson Mvula[1], Simon Tembo[3]
Department of Electronics and Electrical Engineering
School of Engineering, UNZA
Lusaka, Zambia

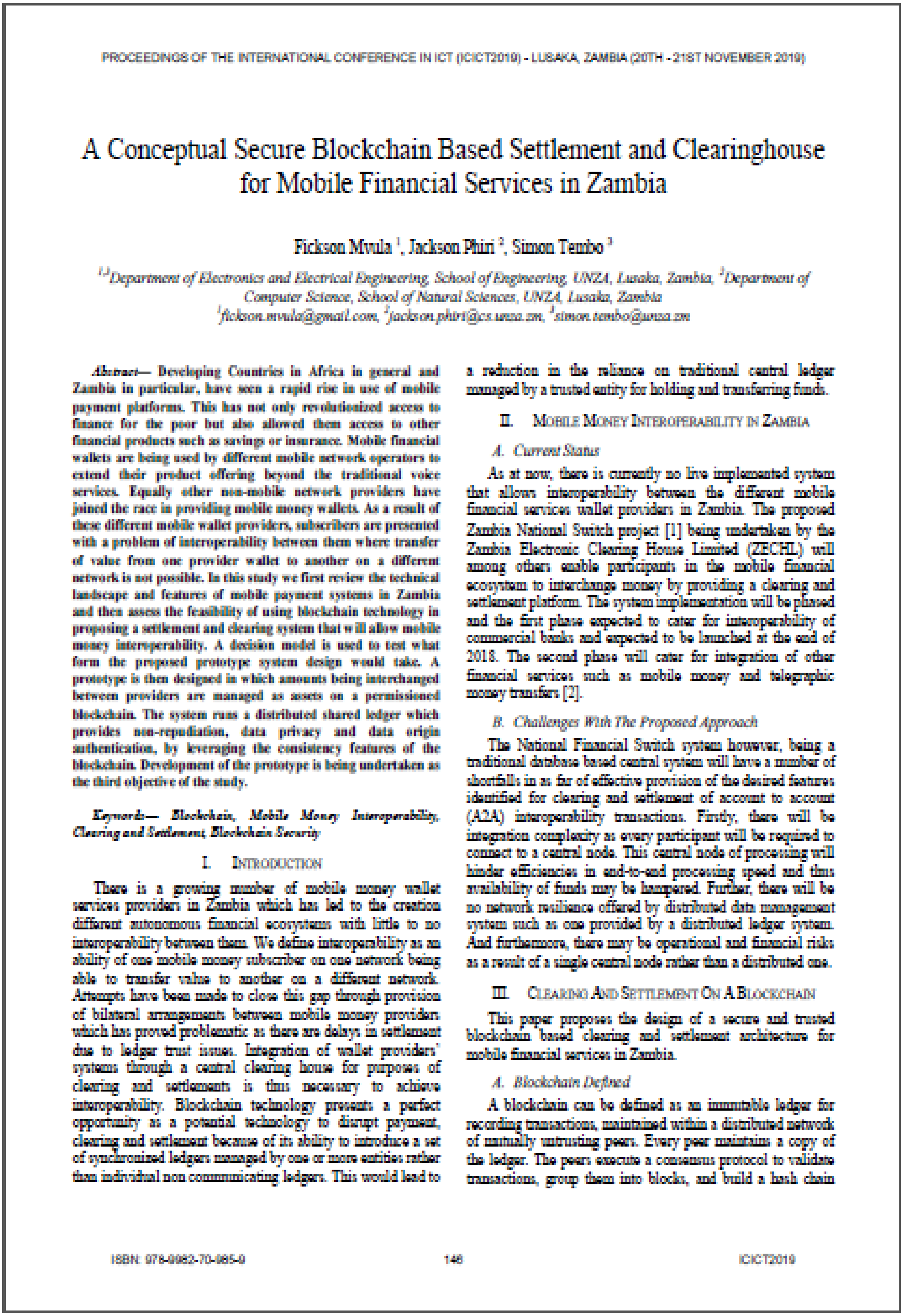
Jackson Phiri[2]
Department of Computer Science
School of Natural Sciences, UNZA
Lusaka, Zambia

Abstract—Developing Countries in Africa in general and Zambia in particular, have seen a rapid rise in use of mobile payment platforms. This has not only revolutionized access to finance for the poor but also allowed them access to other financial products such as savings or insurance. With a growing number of mobile money providers in Zambia, there is need for a solution that would enable integration of the mobile money provider's systems using a central clearinghouse for purposes of clearing and settlement to achieve mobile money interoperability. In this study, we first reviewed the technical landscape and features of mobile payment systems in Zambia and then assessed the feasibility of using blockchain technology in proposing a settlement and clearing system that would facilitate mobile money interoperability. A prototype system was then designed in which amounts being interchanged between providers are managed as assets on a permissioned blockchain. The system runs a distributed shared ledger, which provides non-repudiation, data privacy and data origin authentication, by leveraging the consistency features of blockchain technology.

The National Financial Switch system however, being a traditional database based central system will have a number of shortfalls in as far of effective provision of the desired features identified for clearing and settlement of account to account (A2A) interoperability transactions. Firstly, there will be integration complexity as every participant will be required to connect to a central node. This central node of processing will hinder efficiencies in end-to-end processing speed and thus availability of funds may be hampered. Further, there will be no network resilience offered by distributed data management system such as one provided by a distributed ledger system. And furthermore, there may be operational and financial risks as a result of a single central node rather than a distributed one.

Integration of wallet provider's systems through a central clearing house for purposes of clearing and settlements [2] is necessary to achieve interoperability. Blockchain technology presents a perfect opportunity as a potential technology to disrupt payment, clearing and settlement because of its ability

C. ICICT 2019 Lusaka Publication



A Conceptual Secure Blockchain Based Settlement and Clearinghouse for Mobile Financial Services in Zambia

Fickson Mvula [1], Jackson Phiri [2], Simon Tembo [3]

[1,3]*Department of Electronics and Electrical Engineering, School of Engineering, UNZA, Lusaka, Zambia,* [2]*Department of Computer Science, School of Natural Sciences, UNZA, Lusaka, Zambia*

[1]*fickson.mvula@gmail.com,* [2]*jackson.phiri@cs.unza.zm,* [3]*simon.tembo@unza.zm*

***Abstract*— Developing Countries in Africa in general and Zambia in particular, have seen a rapid rise in use of mobile payment platforms. This has not only revolutionized access to finance for the poor but also allowed them access to other financial products such as savings or insurance. Mobile financial wallets are being used by different mobile network operators to extend their product offering beyond the traditional voice services. Equally other non-mobile network providers have joined the race in providing mobile money wallets. As a result of these different mobile wallet providers, subscribers are presented with a problem of interoperability between them where transfer of value from one provider wallet to another on a different network is not possible. In this study we first review the technical landscape and features of mobile payment systems in Zambia and then assess the feasibility of using blockchain technology in proposing a settlement and clearing system that will allow mobile money interoperability. A decision model is used to test what form the proposed prototype system design would take. A prototype is then designed in which amounts being interchanged between providers are managed as assets on a permissioned blockchain. The system runs a distributed shared ledger which provides non-repudiation, data privacy and data origin authentication, by leveraging the consistency features of the blockchain. Development of the prototype is being undertaken as the third objective of the study.**

Keywords*— *Blockchain, Mobile Money Interoperability, Clearing and Settlement, Blockchain Security

I. Introduction

There is a growing number of mobile money wallet services providers in Zambia which has led to the creation different autonomous financial ecosystems with little to no interoperability between them. We define interoperability as an ability of one mobile money subscriber on one network being able to transfer value to another on a different network. Attempts have been made to close this gap through provision of bilateral arrangements between mobile money providers which has proved problematic as there are delays in settlement due to ledger trust issues. Integration of wallet providers' systems through a central clearing house for purposes of clearing and settlements is thus necessary to achieve interoperability. Blockchain technology presents a perfect opportunity as a potential technology to disrupt payment, clearing and settlement because of its ability to introduce a set of synchronized ledgers managed by one or more entities rather than individual non communicating ledgers. This would lead to a reduction in the reliance on traditional central ledger managed by a trusted entity for holding and transferring funds.

II. Mobile Money Interoperability in Zambia

A. Current Status

As at now, there is currently no live implemented system that allows interoperability between the different mobile financial services wallet providers in Zambia. The proposed Zambia National Switch project [1] being undertaken by the Zambia Electronic Clearing House Limited (ZECHL) will among others enable participants in the mobile financial ecosystem to interchange money by providing a clearing and settlement platform. The system implementation will be phased and the first phase expected to cater for interoperability of commercial banks and expected to be launched at the end of 2018. The second phase will cater for integration of other financial services such as mobile money and telegraphic money transfers [2].

B. Challenges With The Proposed Approach

The National Financial Switch system however, being a traditional database based central system will have a number of shortfalls in as far of effective provision of the desired features identified for clearing and settlement of account to account (A2A) interoperability transactions. Firstly, there will be integration complexity as every participant will be required to connect to a central node. This central node of processing will hinder efficiencies in end-to-end processing speed and thus availability of funds may be hampered. Further, there will be no network resilience offered by distributed data management system such as one provided by a distributed ledger system. And furthermore, there may be operational and financial risks as a result of a single central node rather than a distributed one.

III. Clearing And Settlement On A Blockchain

This paper proposes the design of a secure and trusted blockchain based clearing and settlement architecture for mobile financial services in Zambia.

A. Blockchain Defined

A blockchain can be defined as an immutable ledger for recording transactions, maintained within a distributed network of mutually untrusting peers. Every peer maintains a copy of the ledger. The peers execute a consensus protocol to validate transactions, group them into blocks, and build a hash chain

LIST OF PUBLICATIONS

[1] F. Mvula, J. Phiri, and S. Tembo, “A Conceptual Secure Blockchain Based Settlement and Clearinghouse for Mobile Financial Services in Zambia,” in *PROCEEDINGS OF THE INTERNATIONAL CONFERENCE IN ICT (ICICT2019) - LUSAKA, ZAMBIA*, 2019, no. December.

[2] F. Mvula, J. Phiri, and S. Tembo, “A Blockchain Based Mobile Money Interoperability Scheme In Zambia,” in *(IJACSA) International Journal of Advanced Computer Science and Applications Vol. 11, No. 1, 2020.*