SECURE MOBILE PAYMENT SYSTEM BASED ON BLOCKCHAIN TECHNOLOGY FOR HIGHER LEARNING INSTITUTIONS

BY

CHIMUKA MOONDE

A dissertation submitted to the University of Zambia in partial fulfilment of the requirements of the degree of Master of Science in Computer Science

THE UNIVERSITY OF ZAMBIA

LUSAKA

2023

Declaration

I, **Chimuka Moonde**, do hereby declare that the work in this dissertation has not been previously submitted in candidature for any degree. This 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 reference is given.

Signature: ..... Date: ….....

Copyright

Certificate of Approval

This dissertation of Chimuka Moonde has been approved as fulfilling the requirements or partial fulfilment of the requirements for the award of Master of Science in Computer Science by the University of Zambia;

Examiner 1	Signature	Date
……..	……	……
Examiner 2	Signature	Date
……..	……	……
Examiner 3	Signature	Date
……..	……	……
Chairperson/ Board of Examiners	Signature	Date
……..	……	……
Supervisor	Signature	Date
……..	……	……

Abstract

The present procedures for paying student fees in higher learning institutions are inefficient and complex. In addition, the rise in the number of students studying in higher learning institutions has led to long frustrating queues and overcrowding in most financial institutions and higher learning institutions during payment of student fees. Cash and contact-based payment methods should be avoided, according to the World Health Organization, because they could be a source of infection of Covid-19. This study sought to build and implement a Blockchain-based mobile payment system for higher education institutions in Zambia by first investigating factors influencing the adoption of e-wallets by students. The study used cross-sectional design method as a study design. Stratified random sampling was adopted for selecting the hostels at the higher learning institutions whose occupants were then randomly selected for participation in this study. The study adopted a closed-ended questionnaire administered by the researcher. The primary data from questionnaires was analyzed using Statistical Package for Social Science (SPSS) and Excel. This study considered seven factors as possible predictor variables; perceived ease of use, perceived usefulness, perceived cost, perceived risk, social norm, gender and age. The Likelihood Ratio Test was used in this study, and the results showed that perceived ease of use and gender influenced student adoption of e-wallets at a 5% level of significance. Thus, designers and software developers of e-wallet products should make their products simple to use and must consider the preferences of each gender when designing mobile e-wallets. To develop the model, Unified Modelling Language (UML) diagrams were used to visually describe the proposed system, including its major actors, roles, actions and classes. The prototype was developed using object-oriented software development methodology. The prototype included an e-wallet mobile application and a RESTful API with blockchain technologies as the underlying component. This study adopted blockchain technology because blockchain creatively blends cryptography with a decentralized database in a novel way, allowing a blockchain to be decentralized, immutable and transparent. Additionally, blockchain is a distributed and decentralized ledger that is tamper-proof and preserves the growing array of data such as transactions. The test results demonstrate that the proposed payment system can be used by students to pay various fees remotely. Hence, the proposed system can be used as a safer avenue for paying tuition and other fees in higher learning institutions midst the Covid-19 pandemic.

Key Terms: *e-wallet, perceived ease of use, perceived usefulness, gender, Likelihood Ratio Test, blockchain and cryptography.*

Dedication

I would love to dedicate this work to my loving, understanding and inspiring late father, Givious H. Moonde. I have no doubt that without his support and counsel earlier in my childhood, I could have not had the courage to take up such a great endeavour.

Acknowledgements

I would love to express my gratitude to my supervisor, Dr. Jackson Phiri. His concern towards my progress, reading and commenting on each section of the project thereby offering good guidance. I salute you for the counsel that provoked me to put more effort in my work.

I wish to extend my sincere gratitude to my mother, Cleopatra Moonde and my brother, Pasmo Moonde and my sisters Nandipa Moonde and Ferinah Sakala for the support and encouragement rendered to me. Without you, the desire to pursue a Masters' Degree would have remained a dream without execution.

A special thanks goes out to fiancé Sheena Kabombwe and my secondary school friend Chipego Hachinene for their support and encouragement throughout this work. In addition, I would love to recognise the inspiration I acquired from my senior year classmates, France Chulu and Simon H. Chiwamba.

TABLE OF CONTENTS

List of Figures

List of Tables

List of Abbreviations

API	Application Programming Interface
CBU	Copperbelt University
DFS	Digital financial services
G2P	Government-to-Person
GSM	Groupe Speciale Mobile
ICT	Information and Communication Technologies
KYC	Know Your Customer
MST	Magnetic Secure Transmission
NFC	Near Field Communication
NGO	Non-Governmental Organizations
P2P	Peer-to-Peer
PAN	Primary Account Number
PEOU	Perceived Ease-of-Use
POS	Point-of-Sale
PoW	Proof of Work
PU	Perceived Usefulness
QR	Quick Response
SIM	Subscriber Identity Module

SMS	Short Message Service
SPSS	Statistical Package for Social Sciences
TAM	Technology Acceptance Model
TPB	Planned Behaviour Theory
TRA	Reasoned Action Theory
UML	Unified Modelling Language
UNZA	University of Zambia
USAID	United States Agency for International Development
USSD	Unstructured Supplementary Service Data
UTAUT	Unified Theory of Acceptance and Use of Technology
VTS	Visa Token Service
WHO	World Health Organization
ZANACO	Zambia National Commercial Bank

CHAPTER ONE

INTRODUCTION

1.1 Introduction

This chapter explains why this study is being conducted. It begins by outlining the study's context. The chapter also includes a statement of the problem, as well as the aim, objectives, and relevance, as well as the scope.

1.2 Background to the Study

Mobile phones and other mobile communications devices have had and will continue to have a significant social and economic impact on the world for the foreseeable future [1]. One aspect of mobile operation that has lately gained importance is the use of mobile phones to make payments. Globally, the adoption of mobile payments has taken a course unlike nearly any other technology breakthrough, with rapid growth in some emerging economies and delayed adoption in wealthier economies. This is because various forms of mobile payments have provided significant benefits to developing economies in terms of financial inclusion and payment system performance, whereas the case for implementing such forms of payment has been less compelling in developed economies with ready access to financial services. Different mobile payment models based on newer mobile phone and network technology, which is only now becoming more widely available in developed economies, are anticipated to drive the adoption of mobile payments [1].

Mobile payments refer to a variety of financial transactions that can be completed using a mobile device [1]. This could range from a remittance sent to a distant destination utilizing only the mobile network operator's infrastructure to a credit card transaction completed in a store using a mobile phone [2]. Mobile payments should not be considered a single type of payment; the phrase encompasses a number of different classes and subclasses of payments, each with its own set of advantages.

According to [1] and [3], to fully comprehend the many payment types that fall under the umbrella of mobile payments, it is necessary to analyse a number of factors. The following describes the

wide range of characteristics of mobile payment systems. Combining these characters in various ways results in a diverse set of mobile payment methods. The transaction's purpose, the technology available in mobile handsets, networks, point-of-sale terminals and most significantly, the level of access customers have to traditional financial infrastructure will all influence which model is used.

Firstly, the economic purpose, there are two forms of economic and financial activities which are facilitated by mobile payments. Purchases, that is, payments in exchange for products and/or services. Purchases can be further divided into point-of-sale purchases, in which the payer and payee are in the same area and interact via a payment terminal, and remote purchases, in which the payer and payee are in separate locations. Transfer/remittances, that is, payments that do not create (or erase) an obligation for (or against) another person. Domestic and cross-border remittances, which are frequently sent via a mobile money, are included in this category.

Secondarily, the technological interface, on a mobile device, there are three main ways to initiate a payment. Short Message Service (SMS) or Unstructured Supplementary Service Data (USSD) where the user sends a message via the mobile phone network to initiate a payment, which is known as SMS or USSD. USSD is a mobile messaging service that, unlike SMS, allows users to send and receive messages in real time. Mobile Internet where the mobile device acts as an internet access point. Payments initiated through this interface are comparable to those made on a personal computer, however website services (including Internet Banking) can be adapted to be more mobile-friendlier by providing a separate application (app). Near Field Communication (NFC) is a contactless payment method in which an electronic device with an NFC chip is put near an NFC-enabled terminal and transfers payment information utilizing radio frequencies. The communication between the devices can provide the same basic functionality as a contactless credit or debit card, or it can provide a more complex interaction that allows for the provision of additional services.

Thirdly, funding source, a credit or debit account with a financial institution, a deposit account with a financial institution (including a "prepaid card" account), or funds held in store with another entity ("stored value funds," which are often held by a mobile network operator in Zambia such as Airtel, MTN or Zamtel) are the three most common sources of funds used in a mobile payment.

Fourth, payment network, traditional interbank payment networks can be used when mobile payments are made between accounts owned by financial institutions. Payments from prepaid accounts based on credit, debit, or financial institutions could also be processed through the card scheme networks that handle regular card transactions (for instance MasterCard or Visa). Other systems use a "closed" network, which means that anyone who wants to send or receive money through the system must have an account within the system. This may be the case for a system where prepaid funds are stored by a mobile network provider. Such systems are easier to set up since they do not require the transfer of funds between different companies, and hence do not necessitate the collaboration of third parties. However, there are certain features for instance Stanbic's Instant Money within "closed" network that do not require the recipient to have an account with Stanbic.

E-wallets, also known as digital wallets or electronic wallets, are computer applications that store and transmit payment authorization data for one or more credit or bank accounts. When a customer adds his or her payment account information to a digital wallet, the wallet serves as a payment device for that account by transmitting the funds to a merchant when a customer authorizes the payment. Digital wallets are comparable to traditional wallets in that they store several payment cards and transmit payment authorisation data [3]. Chandra, et al. [4] defines an e-wallet as a consumer device used to keep and handle electronic cash, whereas Sakalauskas, et al. [5] defines an e-wallet as a type of financial technology that allows users to save money, purchase items and services from both individuals and businesses. E-wallets can also be used to send money to other e-wallet users, purchase goods and services online and pay bills. The term "mobile wallet" refers to smartphone apps that bundle many mobile payment methods into one package [1].

The initial generation of mobile payment systems in the world were primarily based on the 'mobile money' paradigm, in which funds were retained with the mobile network carrier and transactions were initiated by SMS or USSD. Given that the carrier was already storing stored value such as air time and data bundles on behalf of users, this was a relatively straightforward extension of existing prepaid mobile services. In economies with well-developed payment systems, mobile payment systems have gotten little traction, but it looks to be more applicable in many developing economies.

According to the GSM Association [6], there are already 163 mobile payment products in use in emerging economies, with another 107 on the way. Around 90 of them are based in Africa, with another 40 in the Asia-Pacific region and 17 in the America. According to a study of 78 service providers in 49 emerging economies, as of June 2012, there were 82 million clients (30 million of whom were active), with six service providers reporting over one million active customers each [6]. Nonetheless, adoption rates vary; in 2011, the majority of recorded mobile transactions were conducted through Kenya's highly successful M-Pesa network [7], where 73% of people use mobile money and 23% use it at least once a day [8]. Smart Money in the Philippines, which has over 10 million customers, and M-Pesa in Tanzania, which has 4.4 million registered subscribers, are two more popular systems in developing nations [2].

The mobile money industry reached a critical milestone in 2019 when the number of registered mobile money accounts crossed one billion [9]. This was a huge accomplishment for an industry that was only a few years old. Today's mobile money industry includes a plethora of seasoned providers with a diverse set of operating capabilities, a comprehensive product portfolio and a global reach [9]. Mobile money, which was formerly only available in a few areas, has grown to become a global phenomenon, with phenomenal growth in emerging nations and a wide spectrum of customers. According to Naghavi [9], customers can now choose from a variety of tailored products thanks to the rapid rise in internet and smartphone adoption, improved interoperability, and new business models. Digital transactions accounted for the bulk of mobile money flows for the first time in 2019. Customers can now pay for school fees, e-commerce, foreign remittances, savings, credit, pay-as-you-go utilities and more with digital payments rather than cash.

As economies become more reliant on digital technology, mobile money plays an increasingly important role in leveraging digital finance for long-term development. Mobile money contributes to the economic empowerment of individuals and communities, including marginalized groups and companies, and accelerates progress toward the Sustainable Development Goals [9].

The digitisation of payments reached new heights: Although there has been a progressive movement from cash to digital payments over the last five years, digital transactions accounted for the majority of mobile money flows for the first time in 2019 [9]. As a higher share of money enters and leaves the system in digital form, the ratio of digital to cash-based transactions has

increased by about 50% since 2017. This indicates that providers have taken significant steps to ensure that digital transactions become ingrained in their customers' daily life [9].

More value circulating in the mobile money system than exiting: In December 2019, the total value in circulation (peer-to-peer (P2P) and merchant payments) surpassed $22 billion, more than doubling over the previous two years and well surpassing the total value of outbound transactions ($18 billion). The industry has clearly identified what keeps funds circulating. For example, by using business management technologies such as customer analytics and inventory management to create more attractive value propositions for small and medium enterprises, and by providing credit lines to agents and merchants [9].

The industry increasingly interoperable and integrated: Interoperability with banks and account-to-account (A2A) interoperability are addressing the needs of previously underserved and cash-dependent customers. As the mobile money industry has become more integrated with international financial system actors, mobile money-enabled international remittances have grown in popularity. API integration is also on the rise with government organizations, utility providers, online businesses and local entrepreneurs [9].

A step towards a digital future for all: In 2019, Sub-Saharan Africa remained the epicentre of mobile money, with over 50 million registered accounts. Strong growth in Western Africa (21 million new accounts) and Central Africa (six new accounts), as well as consistent growth in Eastern Africa, were the driving forces behind 22 million new accounts. The GSMA predicts that account adoption will continue to grow in Sub-Saharan Africa, with the area surpassing the half-billion mark by the end of 2020 [9].

When the COVID-19 outbreak struck in early 2020, it was inevitable that mobile technology, particularly mobile money, would be vital in keeping people connected, providing critical financial aid, and enabling safe, no-contact payment for food, electricity and other necessities. Mobile money became a new daily routine for millions of people all over the world, with daily transactions exceeding $2 billion [10]. According to Andersson-Manjang & Naghavi [10], the year 2020 was unlike any other. COVID-19 triggered a wide range of responses around the world, including school and workplace closures, movement restrictions, and complete lockdown. Handling physical

cash, paying for daily essentials and conducting business in person all became risky, prompting more people than ever to turn to mobile money as a safer alternative.

The pandemic made it more difficult for mobile money providers to operate. Consumer spending was down, and transaction fees were waived, making it difficult for providers to profit on increased mobile money usage and a widespread shift from cash to digital. The industry, on the other hand, proved robust, as mobile money providers did everything they could to keep economies afloat and provide a vital service to those in need [10].

According to the GSM Association [10]**, the following highlights some of the trends in 2020**; Globally, the number of registered accounts increased by 12.7% to 1.21 billion in 2020, more than doubling the expected growth rate. This impressive growth was attributable to authorities creating more flexible Know Your Customer (KYC) processes and reducing on boarding rules to make it easier to open an account, in addition to shifts in consumer behaviour.

Account activity increased even faster. There were over 300 million active mobile money accounts on a monthly basis. Customers were not only using their accounts more frequently, but they are also using them in new and more advanced ways. This shows that a growing number of people were migrating away from the financial system's fringes and into a more digital lifestyle.

As more money flowed and was cashed-in and cashed-out than ever before, transaction values increased across the board. The global value of daily transactions surpassed $2 billion for the first time, and is predicted to top $3 billion by the end of 2022.

National governments provided unprecedented monetary and fiscal support to individuals and businesses in order to reduce the pandemic's human and financial toll as well as keep economies afloat. During the epidemic, the value of government-to-person (G2P) payments quadrupled as the mobile money industry collaborated with governments and non-governmental organizations (NGOs) to send social and humanitarian payments to those in need promptly, safely and efficiently. Collaboration with lenders and insurance providers is projected to grow as remote operations become more crucial [10].

The value of transactions between mobile money platforms and banks quadrupled in the last five years, hitting $68 billion in 2020, up from $15 billion in 2015. During this time, the amount of money flowing between the two systems has stayed relatively constant, illustrating the banks' and mobile money services' complementing relationship [10].

COVID-19 sparked a sweeping shift in the adoption of digital tools, despite the problems and disruptions it brought. Suddenly, a greater number of people were relying on mobile services. Consumers soon turned to digital payments as a safer and more accessible choice because of movement restrictions and the inherent risks of handling cash.

1.3 Problem Statement

With the rise in the number of students enrolled in higher institutions of learning in Zambia, registration and payment of student fees has been characterised by long unbearable queues and overcrowding in most of the financial institutions [11]. This has been further marked with late registration by students owing to long queues. In addition, after depositing the funds, a student is required to submit the stamped deposit slip obtained from the financial institution to the higher institution of learning to confirm that he or she has paid. Similarly, submission of stamped deposit slips is characterised by long intolerable queues and overcrowding in the higher institution of learning. With the advent of Covid-19, an alternative method avenue for paying of student fees has to be proposed. Therefore, this study aimed to design and develop a Blockchain-based mobile payment system for higher learning institutions by first evaluating the willingness of students to use and adopt a mobile payment system by analysing factors affecting the adoption of e-wallets. This study adopted blockchain technology because blockchain creatively blends cryptography with a decentralized database in a novel way, allowing a blockchain to be decentralized, immutable and transparent all at once [12].

1.4 Aim of the Study

To design and develop a secure mobile payment system for higher learning institutions in Zambia based on Blockchain by first examining the factors that influence the adoption of e-wallets by students in higher learning institutions and finally developing a prototype.

1.5 Research Objectives

The objectives were:

i. Identify the key payment systems that students use in higher learning institutions in Zambia and the challenges faced by students when transacting with Higher Education Institutions.
ii. Design a model based on Blockchain for a mobile payment system for higher learning institutions in Zambia.
iii. Develop a prototype based on the model in (ii) that leverages the inherent characteristic of Blockchain.

1.6 Research Questions

Questions that will guide the research are:

i. What are the payment systems used by students in higher learning institutions in Zambia and what are the challenges faced by students when transacting with Higher Education Institutions?
ii. How can a Blockchain-based mobile payment model be created?
iii. What is the feasibility of implementing a prototype based on the model in (ii) to address the identified challenges?

1.7 Significance of the study

The study had two significant contributions. First is the contribution to the body of knowledge. This is in the form of two conference proceedings, one book chapter, one journal publication and a book.

The second contribution is the development of a payment solution based on blockchain technologies for higher learning institutions. This is to address the payment challenges in the midst of Covid-19.

1.8 Scope of the Study

Four higher learning institutions (University of Zambia, Mulungushi University, Evelyn Hone College of Applied Arts and Commerce, and National Institute of Public Administration) were used as study settings. The findings of this study provided vital information for the design and development of a mobile payment system which will used for paying of fees. However, the implementation and evaluation of the prototype was restricted to the University of Zambia.

1.9 Chapter Summary

This chapter provided the background to the study, problem statement, aim of the study, research objectives and research questions. In addition, the chapter provided the significance of the study and scope.

CHAPTER TWO

LITERATURE REVIEW

2.1 Introduction

This section seeks to analyse relevant documentation and findings that are essential to improve the research and its capacity to analyse the concerns it seeks to accomplish, that is, the theoretical literature and the empirical literature. The theoretical literature presents and attempts to explain theories that relate to the subject matter that is adoption of e-wallets amongst users in some selected higher learning institutions. The empirical literature describes what has been practically observed and validated objectively in relation to the subject matter.

2.2 Background to the Study

One of the most significant activities that accounting officers performed manually was receiving tuition funds from students. From 1965 to 2009, the majority of payments in higher education institutions were performed manually. This meant accounting employees had to physically receive cash and check payments by hand, as well as keep track of the transactions in books. However, as the number of students grew, the manual payment system encountered the following issues: accounting staff were unable to handle the volume of payments, there were risks of fraud/theft, challenges with accountability, delays in creating financial reports and students were spending more time queuing to pay fees [17].

Students had to pay fees directly to individual school financial officers at the time, which was a hardship for them because they had to queue up for extended periods of time, registration took a long time and students risked losing funds in the process. The fees collected from students would subsequently be remitted to central administration to pay the university's and bursary system's responsibilities. The administration, on the other hand, had various difficulties, including some schools failing to remit funds collected from students [17].

Universities such as the University of Zambia (UNZA) and Copperbelt University (CBU) adopted a student electronic payment system to improve efficiency, efficacy and accountability while also

lowering the risk of fraud. The university administration opted to use the electronic Bill Muster payment system after signing a contract with Zambia National Commercial Bank (ZANACO). The new payment method was designed to improve traffic flow, efficiency, effectiveness, and accountability. Under this system, UNZA and CBU fees were collected on a commission basis by ZANACO. The Bill Muster electronic payment system's major flaw was that it was inconvenient and time-consuming because the students had to physically visit a ZANACO branch to complete the transaction [17].

Makerere University in Uganda has a significant number of students who pay their institution tuition in cash, electronic funds transfer, or bank drafts to the university's accounts in selected bank branches, according to Lwanga et al [18]. These payment options have not shown to be effective, particularly during test and examination seasons, when the majority of students are required to pay fees in order to meet the requirements to access examination rooms. The process of paying fees is characterized by long queues, excessive waiting by students and congestion at banks where payments are made. As a result, a number of students miss tests and/or examinations while standing in a queue to pay their fees.

2.2.1 Digital Financial Services Ecosystem

Payment systems have become a critical component of contemporary societies' economic existence. The smooth functioning of payment systems is important for the overall effectiveness and reliability of payment systems (Payment system oversight and interoperability). Hence the need to review and understand the digital financial services ecosystem. The digital financial services ecosystem maps the overall ecosystem of digital financial services by identifying all key stakeholders as well as looks at the critical elements necessary to make the ecosystem develop so that it encourages and enables financial inclusion policies [19].

Furthermore, the digital financial services framework defines participants within the ecosystem and their functions. The players consists of users (consumers, businesses, government agencies and non-profit groups) who have needs for digital and interoperable financial products and services; the providers (banks, other licensed financial institutions and non-banks) who supply products and services through digital means; the financial, technical and other infrastructures that

make them possible; and the governmental policies, laws and regulations which enable them to be delivered in an accessible, affordable and safe manner [20]. Figure 2.1 shows the digital financial services ecosystem.

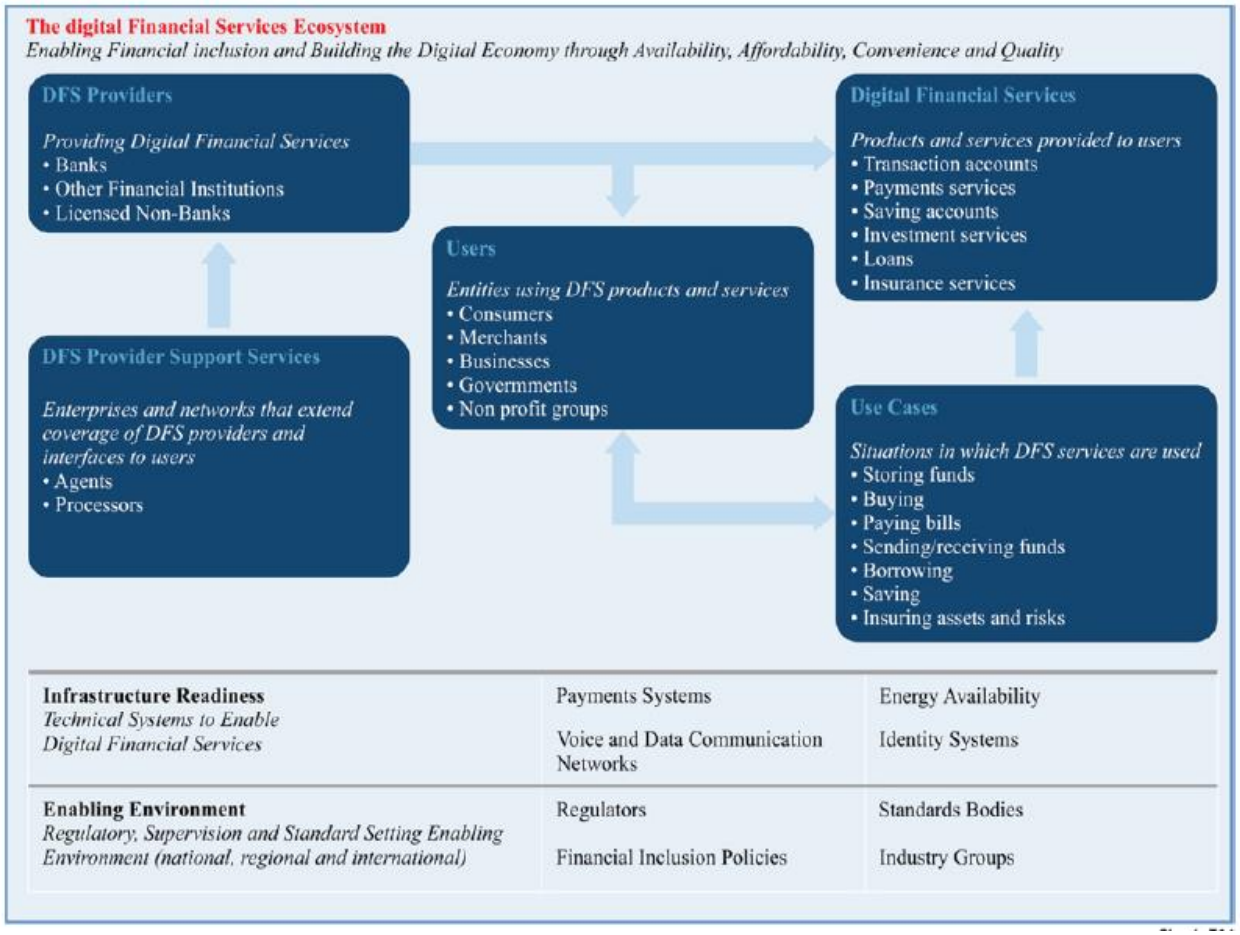


Figure 2.1. The Digital Financial Services Ecosystem [20]

Payment systems available for transaction between and among end users such as consumers, merchants, businesses and governments. These payment systems may be public, semi-public, or private; they may be "closed-loop" or "open-loop". Security of payment systems is an infrastructure readiness requirement. Furthermore, a certain degree of payment system interoperability among participants in payments is a required component of infrastructure readiness.

Identity schemes that can recognise end users and their providers and authentication mechanisms that can accept and verify certain identities. In the Digital Financial Services environment,

identification schemes can be national IDs, sectoral IDs (for instance finance company identities, bank account numbers, cell phone numbers) or private sector IDs (for example WeChat or PayPal IDs) are often essential. Particularly some national IDs are biometrically enabled; this is expected to become an important part of the ecosystem.

2.2.2 Digital Financial Services

Digital financial services (DFS) refers to the use of an electronic device or mobile phone application to access financial services. Digital financial services include automated financial services among which are storing funds, making and receiving payments [21]. DFS have become a viable way for the unbanked to access formal financial services. Where the service is available, users can securely receive funds, pay bills, make bank transactions, transfer funds, and purchase goods and services. 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].

Money transfer and payment applications focused on mobile phones have been accepted as the means for bringing banking facilities to users beyond the traditional finance system. Mobile banking systems provide various advantages for the community, including improved profitability and capital transfers, helping to control cash balance and improving volatile income protection [23].

A sector that can highly benefit from the services provided by digital financial services is the Education sector. Most school systems in Zambia rely significantly on cash transactions. This reliance on cash for financial transactions contributes to inefficiencies, cash leakage and carries security risks. Digital financial services will be able to provide unique opportunities in institutions of learning such as primary and secondary schools as well as universities. These opportunities include replacing cash thus bringing efficiency to institutions of learning by improving management, increasing financial support from donor and non-governmental organizations,

reducing financial costs as well as laying a concrete way to developing more multifaceted systems that otherwise would not have been feasible in a cash environment [24].

Looking at the higher institutions of learning in Zambia, there is no doubt that the existing student fee collection mechanisms are ineffective, inconvenient, and time-consuming. Inefficient collection processes are especially troublesome for students in remote and hard-to- reach locations, and affect the productivity and efficiency of the workforce in accounting departments and administration. Payments via digital financial services will save time and money traveling to nearby cities to locate approved bank branches to deposit money. Digital financial services also eliminate the risk of carrying large sums of money of by students.

2.2.3 Potential Threats and Vulnerabilities

The digital financial services ecosystem is uniquely exposed to a variety of security threats. The vulnerability steams from the interconnectedness of system entities, extended security boundaries due to reliance on numerous parties and mobile ecosystem which includes the devices and mobile operating system of the device [25]. Different threats to the digital financial services environment were defined and evaluated in order to establish control measures or mitigations in the proposed mobile payment system. The Table 2.1 summarizes the identified threats and affected entities.

Table 2.1. DFS Ecosystem Threats and Vulnerabilities [25]

Affected Entity	Identified Threats	Identified Vulnerabilities
User	a) Phishing attacks b) Social engineering c) Unauthorized access to mobile device d) Unintended disclosure of personal information	a) Lack of user's due carefulness of validating content in emails or SMS before selecting URLs or downloading attachments b) Use of public Wi-Fi connections c) Use of fake access point with a familiar name of the network d) Use of fake websites with familiar content e) Missing minimum security hygiene rules f) Installation of untrusted applications
Mobile Device	a) Unauthorized access to mobile device b) Lost or stolen mobile device c) Unintentional installation of rogue and malware applications d) Unauthorized access to DFS data	a) No PIN set or usage of a weak PIN. b) Lack of a mechanism to remotely disable a lost or stolen mobile device c) Not up-to-date Mobile Operating System
Mobile Wallet App	a) Reverse engineering b) Data interception via installation of malware c) Code exploitation attack	a) Weak PIN exposing app to brute force attacks.
DFS provider's Network, Bank's Network and Mobile Network Operator	a) Unauthorized access to DFS data b) Compromises of DFS infrastructure c) Insider attacks d) Denial of service e) Man-in-the Middle attacks f) Unauthorized disclose of personal information g) Account and session hijack	a) Inability to perform transactions due to a service outage b) Transaction failure due to high delays c) Network failure due to insufficient network capacity or maintenance or design
DFS provider	a) Attacks against credentials b) Attacks against systems and platforms	a) Inability to perform transactions due to a service

	c) Code exploitation attack d) Compromise of DFS services e) Data misuse f) Insider attacks g) Denial of service h) Zero-day attacks i) Unintended disclosure of personal information	b) Transaction failure due to high delays outage c) Weaknesses in enforcing strong authentication for access to critical systems and databases where wallet account data is stored for validation and payment authorization. d) Non-effective malware detection and prevention measures. e) Weaknesses and vulnerabilities on digital wallet servers and applications hosted at the mobile wallet application provider.
Third Party (Merchants, Acquirers, Payment Service Providers)	a) Code exploitation attack b) Denial of Service c) Malware d) Unauthorized access to DFS data e) Payment system compromise, network and system infrastructure compromise	1. Unauthorized access to payment processing systems or applications and shortcomings in enforcement of internal security measures and compliance controls 2. Inadequate intrusion detection, data outflow detection/prevention and fraud detection/prevention 3. Gaps in non-repudiation controls for processing authorizations

Under the Security Design section of this report, established control measures or mitigations for the defined threats and vulnerabilities are outlined in the next chapter (Chapter 3).

2.2.4 Blockchain Technologies in Digital Financial Services

Blockchain and digital finance have gotten a lot of attention from academics and practitioners. The blockchain concept, which dates back to 2008, is based on distributed open ledgers and is intended to provide a trust mechanism and intelligent data management for digital business applications. Originally used to create digital currency (such as bitcoin), blockchain applications have recently been broadened to cover digital finance and other commercial fields. Companies and consumers have begun to embrace electronic currency. Digital payments, crowdfunding, digital lending, supply chain financing, and robo-advising, for example, have had significant commercial and societal benefits [26].

Stuart Haber and W.Scott Stornetta were the first to propose the Blockchain concept. They did not coin or introduce the word "Blockchain", as that occurred much later following Satoshi Nakamoto's original paper [27]. Despite this, Stuart Haber and W.Scott Stornetta published "How to time stamp a digital document" in 1991. The principles of what we currently refer to as a Blockchain, as well as all or most of the features and ideas that underpin it, are all included in that paper.

Since Satoshi Nakamoto first proposed blockchain in 2008 as a vital component for supporting transactions of digital currency, it has been known as the public ledger for all transactions and has solved the double-spend problem by merging peer-to-peer technology with public-key cryptography. A blockchain, literally, is a chain of blocks that records digital currency transactions. There are strict rules that regulate how to verify the block's validity and ensure that it will not be altered or disappear. Blockchain technology refers to the techniques and computer infrastructure for creating, inserting and utilising blocks [26].

A Blockchain can be defined as an immutable transaction recording ledger, held within a distributed network of mutually untrusting peers. A consensus protocol is used by the peers to verify transactions, group them into blocks and construct a hash chain over the blocks [28]. A Blockchain can be considered as a data structure, that is, a Blockchain contains a connected list of blocks, each containing a collection of transactions.

Figure 2.2 shows blocks in a Blockchain. Furthermore, a Blockchain can be thought of as a network, as it is a collection of peer-to-peer networks [29]. From a software engineering standpoint, blockchain allows for the creation of a novel distributed and decentralized system software architecture in which sensitive transactions or confidential transaction agreements can be formed with untrustworthy individuals throughout the chain [30]. Furthermore, Blockchain is a distributed system that does not rely on a central authority or third-party intermediaries to function [31].

Public and private Blockchain are the two primary types of Blockchain. In a public or permission-less Blockchain, without a particular identity, any device can participate. Usually, public Blockchain provide a native cryptocurrency, use consensus based on Proof of Work (PoW) and financial rewards. A private or permissioned Blockchain, on the other hand, runs a Blockchain among a collection of known, identified devices. A private Blockchain provides a way for a group of organizations that have a common purpose but do not fully trust each other to secure interactions, such as businesses that share money, products or information [28].

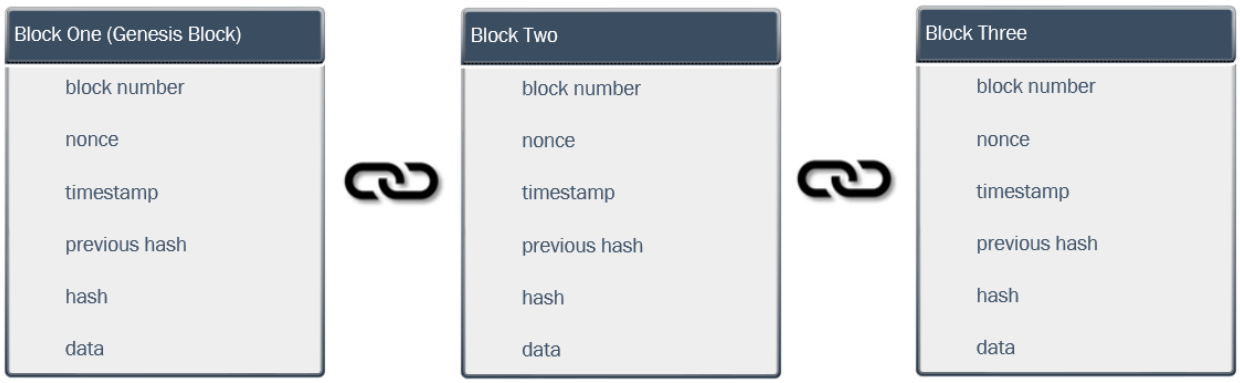


Figure 2.2. Blocks in Blockchain

The Genesis block is the first block in a Blockchain, and it's called that because once the Blockchain is set up, this block will always be number one and will never change. Block one contains the following;

- Meta data: index and timestamp
- Some data

- It doesn't have a previous hash inside and this is the only block in the Blockchain that won't have a previous hash. Conventionally the previous hash for the Genesis is represented with all zeros
- Its own hash

Block two proceeds the Genesis block and contains the following;

- Meta data: index and timestamp
- Data to store
- The previous hash. The previous hash of block number two is identical to the hash for block number one and that is where the link comes. That is why a Blockchain is called a chain or a Blockchain because the blocks are cryptographically linked with each other through the hashes.
- Its own hash

Block three proceeds block number two and contains the following;

- Meta data: index and timestamp
- Data to store
- The previous hash
- Its own hash

On the Blockchain network, blocks are used to store data or transactions. It is irreversible once a block is added to the chain of blocks that came before it. Every block is assigned a distinct value, which appears to be a random string of characters. The hash is a random string of characters formed by a hash function, which generates a unique output for each unique input it gets [32].

The hash is generated using the unique data in the block. This block's data can be anything: a text, an array of numbers, or, more importantly, a list of transactions. The block's unique hash is derived not just from the data it contains, but also from metadata about it, such as when it was formed and where it belongs in the chain. Another highly important data point is the unique hash of the previous block, which is used to generate the hash of a new block. The prior block's unique hash is included in the input used by the current block to generate its hash. This indicates that the hash value of the new block is based on the hash value of the prior block [27].

Due to that each new block refers to the previous block's hash value, links between blocks are formed. This reference to the hash value of the previous block connects it to the current one. As more blocks are formed, a chain of blocks will eventually become the Blockchain. This is how a Blockchain works conceptually: each block has its own fingerprint and refers to the fingerprint of the preceding block. To put it another way, each block is cryptographically connected to the one before it [27] and [32].

With the help of public-key cryptography, which assigns each user a private key while sharing a public key with all other users, blockchain technology overcomes the double-spend problem. The basic concept behind blockchain is that it is a distributed database that contains transaction records that are shared among participants. Fraudulent transactions are unable to pass collective verification since each of these transactions is confirmed by the consensus of a majority of the participating parties. A record cannot be changed once it has been created and acknowledged by the Blockchain [26].

Blockchain as an emerging technology became popular in 2008. It was first used as a peer-to-peer ledger for registering the transactions of Bitcoin cryptocurrency [32]. The aim was to eliminate any third-party intermediary and allow users to make their transactions directly. Thus, Blockchain was designed as a decentralized network of peer nodes. Each node in the network: (1) Holds a replica of the transaction's ledger; (2) writes an entry to its own ledger when it receives consensus from the other nodes in the network; (3) broadcasts any transaction made by its user to the other nodes in the network; (4) checks, on a regular basis, that the ledger it holds is identical to the ones across the network [33]. As Bitcoin continues to grow in popularity, researchers and practitioners have realized the enormous potential of its underlying technology [34].

The unique capabilities of Blockchain, which include immutability, transparency and trustworthiness, were found to be useful not only in cryptocurrencies, but also in many other fields. Therefore, an increasing number of Blockchain-based applications have been developed in various fields [35]. Furthermore, the various features of Blockchain technology, such as decentralization, immutability, robustness, privacy, consensus and cryptographic algorithms have the ability to alleviate reliance on a single centralized authority which is more susceptible to inaccuracy, insecurity, lack of complete trust and single point of failure [36]. This would lead to a reduction in

the reliance on traditional central ledger managed by a trusted entity for holding and transferring funds [28].

To lessen the risk of cyber-attacks, blockchain technology incorporates a number of preventive features such as distributed consensus and cryptography. The primary benefits regarded by early adopters of blockchain in the finance sector are immutability and other capabilities to secure transactions [37].

The following describes the advantages of using Blockchain technology;

Reliability: the decentralized nature of a Blockchain network changes the databases of the entire transaction records from closed and centralized ledgers maintained by only a few accredited institutions to open distributed ledgers maintained by tens of thousands of nodes. The failure of a single node does not affect the operation of the whole net-work. This avoids the single point of failure and ensures the high reliability of the applications which are built on Blockchain technology.

Trust: Blockchain network makes the trust decentralized too. Unlike the centralized trust we take for granted, such as central governments issuing currencies and commercial banks, Blockchain network acts as new trust bearers with decentralized ledgers. These ledgers are shared among a network of tamper-proofed nodes [37].

Security: blockchain network uses the one-way hash function which is a mathematical function that takes a variable-length input string and converts it into a fixed-length binary sequence. The output bears no apparent relationship to the input. The process is hard to reverse because, given just the output, the input is impossible to determine [38]. Furthermore, the newly generated block is strictly following the linear sequence of time.

Efficiency: all data are automatically run through pre-set procedures. Therefore, Blockchain technology can not only significantly reduce the cost of labour but also improve efficiency. For the digital currency of Blockchain 1.0, the automation of distributed ledger is mainly the automation of settlement. Blockchain technology could speed the clearing and settlement of certain

financial transactions by reducing the number of intermediaries involved and making the reconciliation process faster and more efficient [39].

According to Gatteschi et al. [40], Blockchain-based application development can be separated into three stages: Blockchain 1.0, 2.0, and 3.0. For cryptocurrencies, Blockchain 1.0 was utilized, and its goal was to make simple monetary transactions easier. Following that, Blockchain 2.0 for properties and smart contracts was introduced. Before being registered in the Blockchain, these smart contracts impose precise rules and criteria that must be followed. The registration process is completed without the involvement of a third party. Many applications in numerous industries, such as government, education, health, and science, have been developed in Blockchain 3.0. Blockchain's implementation in education is still in its early phases. Blockchain technology is being used by a small number of educational institutions.

The financial services sector is leading the way with blockchain-related business innovations, which must innovate to decrease transaction costs due to fierce competition in today's globalized market. Blockchain has been offered as a novel solution to problems including clearing and settlement of financial assets, payment systems, smart contracts, and financial market operating concerns, among others [41] and [42].

2.2.5 Payment Challenges and Higher Institutions of Learning

Cash has been recognized as a form of payment in exchange for goods and services. However, this method of payment has come with a number of drawbacks. Due to a scarcity of automated teller machines (ATMs) and banks on and around various university campuses, students have been left stranded on multiple occasions. Furthermore, owing to ATMs' incapacity to dispense cash, some students are unable to withdraw funds from ATMs so as to purchase goods or pay their school fees on campus [43].

The biggest issue with the Bill Muster electronic payment system is that it is cumbersome and inconvenient because the student must physically visit the Zambia National Commercial Bank to complete the transaction [17].

Participants in research conducted by Mwewa Mukonde [17] stated that a payment took at least 48 hours to process, that the system was frequently down, and that the system periodically failed to update electronic payments owing to network problems. Participants also mentioned a lack of network support accessories as well as a lack of knowledge about how to use the system. Furthermore, one of the challenges faced by students was a lack of access to a payment platform; for example, those who utilized banks had to travel long distances to obtain banking services. Some participants claimed that electronic payment systems required sophisticated procedures. Furthermore, the majority of participants were sceptical of non-cash transactions and favoured cash transactions.

2.2.6 E-wallets for Higher Institutions of Learning

A digital wallet is software, an electronic device, or an internet service that allows individuals or organizations to conduct electronic transactions. It keeps track of users' payment information for various payment methods on multiple websites, as well as other products like gift cards and driver's licenses. An e-wallet is another term for a digital wallet.

In a study by de Lunaa, Cabanillas, and Fernándezb, the researchers revealed that payment systems have evolved and progressed from simple cash and credit payments to more modern mobile payment methods. The most up-to-date mobile payment technologies are rapidly being used in transactions. The report, on the other hand, attempted to explain the shift by claiming that it was brought about by economic changes, technological advancements on the internet, the expansion of social networks, and increased use of mobile devices. Mobile wallets are still in their infancy in most countries, while some countries are starting to see an uptick in adoption of mobile wallets [44].

The COVID-19 epidemic had a profound impact on nearly every element of human life. To meet the pandemic's constraint, people had to adopt new habits in their regular routines, and these changes in human behaviour may last even after the pandemic is ended [45]. The implementation of safety and preventive measures to minimize the spread of COVID-19 and save people's lives has been aided by the digitization of banking and financial services. In the same vein, the epidemic

shifted customer preferences away from traditional payment methods and toward digital payment methods such as e-wallets [46].

The current coronavirus pandemic has demonstrated the critical importance of digital financial services. Consumers can benefit significantly from advances in electronic wallets, financial technology services and online banking [44]. Consumers should avoid cash and contact-based payments according to the World Health Organization (WHO), because they can be a possible source of infection. Instead, digital payment mechanisms should be used. The suggestions were based on findings from health specialists who confirmed that the SARS-CoV-2 virus could persist for two to four days on surfaces such as cash and banknotes. As a result, use of e-wallets might be seen as a type of pandemic-related protective behaviour. Some even suggested that shifting consumers to digital financial services, such as electronic wallets, could aid limit the virus's spread and severity [47]. Unfortunately, there is little to no documentation or prototype of e-wallets in higher institutions of learning in Zambia. Hence one of the objectives of this study was to design and implement an e-wallet for students.

2.3 Theoretical Frameworks

A number of theories/models have been established with the aim of explaining technology usage behaviour by users. However, for this study, two theories will be considered, these being the Technology Acceptance Model (TAM) and the Unified Theory of Acceptance and Use of Technology (UTAUT).

2.3.1 Technology Acceptance Model

The Technology Acceptance Model serves as the theoretical foundation for this study (TAM). This model is primarily used to predict user acceptance of information systems and to comprehend the users' motivations and potential problems. Through the construction of an extended framework, it is a model that integrates Reasoned Action Theory (TRA) and Planned Behaviour Theory (TPB) [48]. The Technology Acceptance Model was developed by Davis [48] , and it contains both user motivating variables (such as perceived ease of use, perceived usefulness, and attitude toward technology) and outcome variables (namely behavioural intentions, technology use).

A person can act to accept or reject the usage of a new technology or software. The Technology Acceptance Model helps us to understand why a particular information system or software is adopted. TAM, as it is more often known, asserts that if a user believes a technology to be simple to use and beneficial for their purpose, they will be more inclined to use it. This would lead to 'actual' use of the technology. Attitude towards using a system is a function of perceived usefulness and perceived ease of use. Therefore, TAM can be used to predict or find out why a person might use a technology. Figure 2.3 illustrates the Technology Acceptance Model.

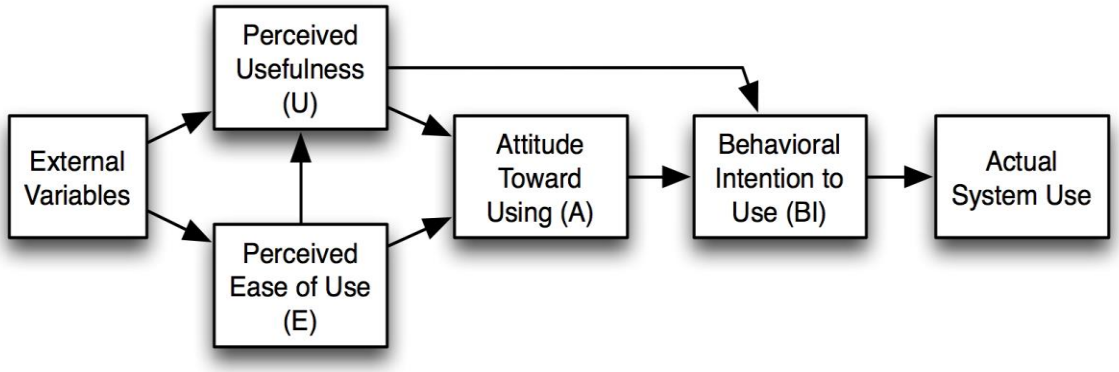


Figure 2.3. Technology Acceptance Model [49]

The Technology Acceptance Model is an information systems theory that describes how consumers accept and use technology or software. The model claims that when consumers are presented with new technology, a multitude of factors impact their decision on how and when to use it [50], notably;

i. Perceived Usefulness (PU). Fred Davis described this as the extent to which a person believes that embracing a specific technology or software system will improve his or her job performance. If potential users believe a new technology or software system will help them do a better job, they are more likely to use it [48].
ii. Perceived Ease-of-Use (PEOU). This is described by Fred Davis as the degree to which a person believes that using a specific technology or software system will be effortless. Potential consumers are more likely to adopt new technology or software if it requires less

physical or mental effort. The utilization of technology is proportionate to the effort required to use it. [48].

Many researchers have used TAM to explore the adoption of various information systems and technologies, including Gefen et al. [51], Moon and Kim [52], and Venkatesh and Davis [49]. Chandra et al contrasted bank-based e-wallets against telecommunication-based e-wallets in their research. TAM was employed as the foundation for the authors' conclusions [4]. Nag and Gilitwala also used TAM constructs in their study to look at the factors that influence people's desire to use e-wallets in Bangkok, Thailand [53].

Masinge [54] conducted an analysis of the factors affecting the adoption of mobile banking services at the bottom of the pyramid (BOP) in South Africa, and added perceived costs, confidence and perceived risk as constructs to TAM. The study findings revealed that perceived usefulness, perceived user-friendliness, perceived expense and customer trust had a significant effect on the adoption of M-bank at the BOP while perceived danger had no significant effect.

Although the TAM has many advantages, such as excellent measuring properties, conciseness, common consumer and methodological soundness [55], [56] points out that the model’s disadvantage is that it provides general user-friendly information and has been chastised for its parsimony by several researchers.

2.3.2 Unified Theory on Acceptance and Use of Technology Model

Unified Theory of Acceptance and Use of Technology (UTAUT) is a technology acceptance model formulated by Venkatesh and others in "User acceptance of information technology: Toward a unified view" [57]. This theory was formulated in an attempt to harmonise various technology adoption models. Figure 2.4 illustrates the Unified Theory of Acceptance and Use of Technology.

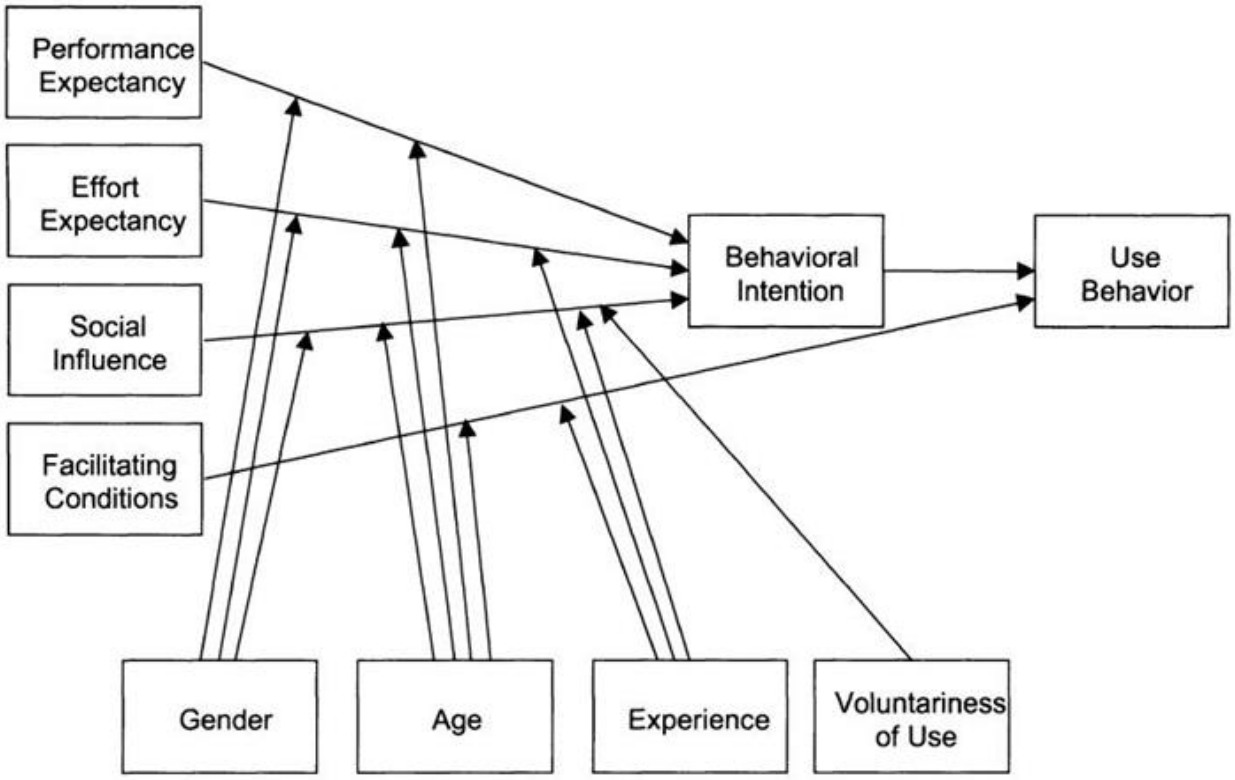


Figure 2.4. Unified Theory on Acceptance and Use of Technology [57]

The UTAUT aims to explain user intentions to use an information system and subsequent usage behaviour.

The theory has four key determinants, notably;

i. Performance Expectancy. The degree to which an individual believes that a technology will assist them in performing job duties. This is influenced by the construct of perceived ease of use [48].
ii. Effort Expectancy. The degree of easy associated with the use of a particular technology [48].
iii. Social influence. The degree to which an individual feels social pressure to use a particular technology. This is based on the construct of subjective norm from the theory of reasoned action [58].
iv. Facilitating conditions. The degree to which an individual believes that organizational and technical infrastructure exists to support the use of a technology.

Furthermore, the theory has four main moderators, namely;

i. Gender (Male, Female)
ii. Age (Age by range)
iii. Experience (Ordinal-low, medium, high)
iv. Voluntariness of use (A categorical variable (high, low))

The model describes some variables, such as performance expectancy, which is an act in which an individual assumes the use of the information system will help one achieve performance gains. Effort expectancy is a level of comfort associated with the use of a system; social impact is the degree to which a person perceives the value of labour-environment influences (in this case the social sphere) in the use of the new system; therefore, it can impact or reassure the person that he or she must also use the new system as well. Facilitating condition refers to the conviction of a person that organizational and technical infrastructure facilities are available to support system utilisation. Usage behaviour is user's severity or frequency in the use of information technology.

In addition, the model consists of four major independent variables-expectation of results, expectation of commitment, social impact and conditions facilitating. As shown in Figure 2.4, behavioural purpose and use actions are viewed as the dependent variables, while gender, age, experience and voluntariness of use are considered as factors that specifically affect the relationship between the dependent variables and the independent ones.

The first three being direct determinants of usage intention and behaviour (or rather they fall under determinants of perceived ease to use under the TAM theory), and the fourth a direct determinant of use behaviour (or rather a determinant of perceived usefulness under the TAM theory). Gender, age, experience, and voluntariness of use are posited to moderate the impact of the four key constructs on usage intention and behaviour which ultimately all these above four determinants are wrapped in under the TAM theory's perceived ease to use and perceived usefulness of a particular technology or software.

The model suggests that performance expectation, expectation of effort and social influence determine behavioural purpose towards technology or software acceptance [59]. It is further suggested by the theory that the facilitation of circumstances and behavioural intent determines the technology or software acceptance [59]. The theory has been validated using different

applications since its inception, and it has become a dè factor model for evaluating user acceptance [60].

According to Wasitarini and Tritawirasta [61], the theory of IT acceptance or UTAUT is based on theories of behaviour in the use of technology and acceptance of technology. This theoretical model is intended to clarify users' preferences in using the information system and user behaviour.

Although this model can be used to forecast perceptions, purpose and attitudes towards technology adoption, it is a bit complicated as it encapsulates eight other theoretical models predicting IT use behaviour and it has also been criticized for providing multiple references without actually using them [62] and [59].

2.4 Review of Predicator Variables

2.4.1 Perceived Usefulness and Perceived Ease of Use

Perceived usefulness was one of the two dimensions of TAM originating from Davis, [48]. Davis and Venkatesh [49] further argue that a technology or software system's effectiveness may be measured by its user acceptance, which is based on three factors: perceived usefulness, perceived ease of use and attitude. If the technology or software system is not user friendly then it should not be deemed useful [63] and [48]. This is in line with the original concept of perceived usefulness and perceived ease of use as the extent to which a person believes that using a specific technology or software system will enhance their job performance and the extent to which the consumer believes that using a particular technology or software would be effort-free, respectively [48]. A technology or software system high in perceived usefulness, in turn, is arguably one for which a user believes in the relationship between positive use and performance [48].

A technology or software perceived to be easier to use than another is more likely to be embraced by users [48]. Many studies found perceived usefulness and perceived ease of use to be major factors in acceptance of technology. [64, 65, 66, 55, 67, 68, 69, 49, 57].

2.4.2 Perceived Cost

Amberg et al. [70] proposed to incorporate perceived cost into TAM, because it appeared to be a major predictor of mobile payment usage. It is described as to what extent a person thinks that using mobile payment system will cost money [71]. Mallat, [72] is of the opinion that, if the expense is passed on to consumers, the expense of a payment process would have a direct impact on market adoption. This belief appearing subjective in the sense that the impact on customers depends on an individual's class. The cost may be higher among the less affluent population while being minimal in well-off communities. According to Dahlberg et al. [73] cost was one of the most important factors in their critical analysis of mobile payment research and ranked as number 10 of 23.

2.4.3 Perceived Risk

According to Gerrard and Cunningham [74], perceived risk is the uncertainty over the consequence of using innovation. Typically, various risks are associated with innovations. According to Suki [75], perceived risk is the consumer's subjective expectation of suffering a loss in pursuit of a desired outcome. This has a negative impact on acceptance. In addition, Lockett and Littler [76] in their early investigations found that perceived risks of an innovation were inversely connected to uptake of telephone-based direct banking services. Perceived risk has been identified as a crucial element impacting the adoption or use of mobile payment services in recent studies.

2.4.4 Social Norm Factor

Social norm, also referred to as subjective norm, is characterized as the perception of a person that most people, perceived as essential to them, believe they should or should not conduct the behaviour at issue [77]. Other research defines social norm as the degree to which an individual perceives that the majority of people who are important to him / her think that the system should or should not be used [49]. Venkatesh and Davis [49] further argues that people may choose to act, even if they are not themselves in favour of the conduct or its effects, if they believe that one or more significant referents think they should and are sufficiently motivated to comply with the references.

For any model of adoption, the development of social forces cannot be ignored [78]. It is not surprising, therefore, that social norms have been widely validated in information and IT systems [79], and the adoption of mobile banking [80] and [81].

2.4.5 Gender

The influence of gender on new technology adoption has received considerable attention. Earlier studies have shown that compared to men, women are less likely to adopt and to use new technology and, in some cases, have less confidence in their ability to use new technology. High masculinity individuals or males tend to believe in their own abilities and less concerned with ease of use, so the perceived ease of use has little to no effect on perceived usefulness and intentions [82] and [83]. However, recent studies have found that gender gaps in adoption of new technology are lessening or disappearing as increasing numbers of men and women are exposed to and are using computers and computer applications in their work and personal life [84] and [83]. Gender based perceptions of the Internet are changing over time, with ICT being seen as essential to business and integral to daily life [84].

2.4.6 Age

Whether a technology is actually useful or actually ease to use is not a matter of the technology but a matter of the individual's perception based on age. The age of the potential adopter can determine whether or not a person will use a new technology [85]. It is not advisable, according to Pedersen [86], to treat young users as though their adoption behaviour is systematically different from that of older age groups. In a comprehensive analysis of the e-Commerce adoption literature, Zhou et al [87] found inconsistent results on the association between age and online buying intention.

2.5 Related Works

Relevant systems and technologies were analyzed to learn how common challenges and pitfalls were handled and to obtain a deeper understanding of the approaches currently in place. Best practices in the existing systems were learnt and shortcomings noted to seek and resolve them in the proposed system. The following are related existing systems and applications that were studied.

2.5.1 M-Pesa

M-Pesa an innovative payment service for the unbanked. “Pesa” is the Swahili word for cash and the “M” is for mobile. Customers turn cash into e-money at Safaricom dealers, and then follow simple instructions on their phones to make payments through their M-Pesa accounts; the system provides money transfers as banks do. The account is very secure, PIN-protected and supported with a 24/7 service provided by Safaricom and Vodafone Group. To implement, Vodafone had to marry the incredibly divergent cultures of global telecommunications companies, banks, and microfinance institutions and cope with their massive and often contradictory regulatory requirements [88].

Using data preloaded on the SIM card, M-Pesa utilizes a SMS based interface to transmit money virtually to other phones. To load money into one’s virtual account, a customer visits one of Safaricom agents and exchanges currency for e-money which is automatically deposited into their account. Customers can transfer money to anyone who owns a mobile phone [89].

2.5.2 Paytm Wallet

Paytm is one of the largest mobile commerce platform and digital wallet company in India. Paytm offers a secure digital wallet where you can store money and use it to make quick recharges, pay bills, shop on Paytm. You can also send money to friends and pay for various services like Uber. Paytm also provides payment gateway solution that can be integrated into web and mobile apps with debit/ credit card, Net Banking and Paytm Wallet payment options.

Paytm short for ‘Pay Through Mobile’ is an Indian electronic payment and e-commerce brand. Paytm (earlier written as PayTM) began its journey as a recharge and bill payment platform which made its way into the e-commerce market. The Paytm wallet facilities ease of payment on almost all possible needs of daily life ranging from daily or monthly essentials, utilities (electricity bill, metro card, gas and water), entertainment, travel, mobile recharge, electronic gadgets, appliances, fashion and many more [90].

A user can pay through scanning Quick Response (QR) codes or entering their registered mobile phone number. Users have the facility to add credit or debit cards, especially bank accounts to

transfer money to Paytm wallets and transfer money from Paytm wallets to bank accounts. Paytm can be used to transact the smallest amount of money but there are rules for transactions between the digital wallet and a bank- there are minimum and maximum capping for money transfers in a day and the total transacted money for a day [91].

2.5.3 PayPal

PayPal is one of the most accepted payment services in the world. PayPal allows any business or individual to securely, conveniently and cost-effectively send and receive payments online, in-store or on mobile. PayPal builds on the existing financial infrastructure of banks and credit card schemes to create a global, real-time payment solution. PayPal allows consumers to send and receive money without sharing financial information. Consumers have the flexibility to pay online or with any connected mobile device. [92].

Lots of physical merchants can also let consumers pay with PayPal, no actual credit card needed. Consumers will just have to enter their mobile number and PIN and there are good to go. PayPal deducts the funds from whatever bank account or credit card consumer has linked. PayPal customers enter their name, email address, phone number, and create a username and password to set up an account. They answer security questions to be used if they forget their login credentials or when additional verification is needed. PayPal customers can also opt to create a PIN as a second factor of authentication for purchases [92].

PayPal uses public key cryptography to encrypt communication between the consumer and merchant. Public key cryptography is a popular technique used to encrypt data which are transmitted over the Internet from one location to another and to ensure that the sender's identity is guaranteed. It operates by using public keys and private keys, which are bits of data mathematically connected to each other by means of an algorithm [93].

2.5.4 Google Wallet

Google Wallet allows users to store their debit cards, credit cards, gift cards and loyalty cards on a smartphone, transforming it into a virtual wallet. A consumer can also make payments online and make contactless payments with their mobile phone. Google Wallet offers tap-to-pay for Near

Field Communication (NFC) enabled devices. If a consumer needs to send money to someone, a consumer can do so without any transaction charges if they're using Google Wallet as well [94].

Google Wallet is a container for payment cards, gift cards, reward cards and special offers. It consists of an Android app with a user interface. The user interface is used to protect the wallet with a PIN code, to manage the payment, gift and reward cards, to select the currently active card, to find specific offers and to view the transaction history. The secure element of the wallet is used to store sensitive information of the payment, gift and reward cards, and to interact with existing POS reader infrastructures [95].

2.5.5 Apple Pay

Apple Pay is a mobile payment system that lets iPhone (iPhone 6 and higher versions) users pay for goods and services using Touch ID. As compared to entering or confirming payment card information (credit or debit card) every time they make a purchase, users can authorize payment for items securely by touching the home button of the iPhone. A payment token stores all the information needed to process the payment all the way from authorization to settlement. During an Apple Pay transaction, payment card information never leaves the user's phone; this information is stored securely in the device [96].

To set up Apple Pay, users simply add a debit or credit card on the wallet app. The card information can be imported from iTunes, entered manually, or added by taking a picture of a card. Users can start using Apple Pay after the card verification process. To tap-and-pay in stores, users need to hold their iPhone close to an NFC reader. A default payment card can be pre-selected on the wallet app. Users then place a finger on Touch ID (fingerprint scanner) to authenticate themselves and complete the payment process. The wallet app immediately notifies users about confirmed transactions [97].

2.5.6 Samsung Pay

Samsung Pay is a method to make purchases over the latest line of Samsung smartphones devices. Samsung Pay enables consumers to make mobile payments simple and secure at most merchant POS terminals. Leveraging a proprietary technology called Magnetic Secure Transmission (MST)

and NFC. Samsung Pay makes mobile payment more accessible to both merchants and customers. Samsung implements a sophisticated alphanumeric algorithm called tokenization. In addition, Samsung partnered with card providers like Visa, MasterCard and embraced the VTS framework (Visa Token Service) to push its ambitious project. When a user adds a card to their Samsung Pay, the system generates a new "virtual random" CC (a new card number with some parameters) implementing the framework which assigns a token to each card. That token is saved in a token vault relating the original Primary Account Number (PAN) information. Therefore, in each transaction instead of using the original CC's data, the mobile device sends a tokenized number: a new card number with some "parameters" [98].

Samsung Pay works with traditional point-of-sale (POS) devices that allow the use of magnetic card swipes. The key technology that gives Samsung Pay such a superior position is called MST. Under this technology, devices using the Samsung Pay app can generate a magnetic signal that contains the same payment information as that generated by swiping a magnetic card in the POS card reader. Thus, the POS device can recognize the Samsung Pay signal if the mobile device is sufficiently close, even though nothing is swiped on the card reader. Unlike Apple Pay, Samsung Pay supports MST alongside NFC, which means it works with any payment terminal that accepts contactless payments or the more traditional method of swiping a card through the reader [99].

2.5.7 Zoona

Zoona founded by Brad and Brett Magrath in July 2008 with funding from United States Agency for International Development (USAID) and Dunavant with the aim of developing a product that would not only digitize payments but also provide communication to rural cotton farmers. Around 2009, Zoona began to develop the software that would process money transfers following an approval by the Bank of Zambia. Zoona's Business to Business (B2B) and Business to Consumer (B2C) model reached the most compelling evidence of success by focusing on meeting the requirements for their clients through the use of proprietary software [100].

Money transfers by Zoona agents are made by supplying the receiver's mobile number which is recorded in the system to receive the transacted funds. An SMS is sent to the recipient and will give the recipient an acknowledgment confirming the recipient can redeem the funds at any or

nearest Zoona agent. Zoona charges a transaction fee that is tiered and depends on the transaction size and type. In addition, the agents also get a commission for their service [100].

2.6 Summary of Gaps in Related Works

Table 2.2 demonstrates the gaps and insight gained from reviewing related works

Table 2.2. Summary of Gaps in Related Works

Research Topic	Authors	Objectives	Summary of Findings(strengths)	Comments/Gap (weakness)
Effectiveness Of The Student's Electronic Payment System: A Case Study Of The University Of Zambia	Mukonde Mwewa	The main objective of this study was to investigate the effectiveness of the student's electronic payment system at the University of Zambia.	• The existing electronic payment system was only moderately functional. This is due to the fact that students must physically visit the university to complete their payment and registration processes.	• The study did not investigate the factors that influence the adoption of payment systems by students.
Pandora's Digital Box: The Promise and Perils of Digital Wallets	Adam J. Levitin	This Article considers the potential legal and business issues digital wallets raise for both consumers and merchants, and proposes a pair of necessary interventions in the digital wallet marketplace	• Highlighted the advantages of digit wallets • Identified risks for both consumers and merchants for adoption of digit wallets	• Puts emphasis on mitigation of the identified risks on regulatory bodies and financial regulations such as the "Honor All Wallets" than the digit wallet's technology
Zerocoin: Anonymous Distributed E-Cash from Bitcoin	Ian Miers, Christina Garman, Matthew Green, Aviel D. Rubin	Propose Zerocoin, a cryptographic extension to Bitcoin that	• Identified significant limitations in Bitcoin regarding privacy	• The need for a double-discrete logarithm proof leads to large proof sizes and verification times

		augments the protocol to allow for fully anonymous currency transactions.		• Derives both its anonymity and security against counterfeiting from strong cryptographic assumptions at the cost of substantially increased computational complexity and size
Blockchain: Bitcoin wallet cryptography security, challenges and countermeasures	Latifa, Er-Rajy, and Achbarou Omar (Journal of Internet Banking and Commerce, 22(3), pp.1-29)	Describe the operating principles of peer-to-peer cryptographic currencies and especially security of bitcoin system	• Described the operating principles of peer-to-peer cryptographic currencies and especially security and we have shown that although the cryptography behind Bitcoin is not currently broken, the system can be attacked with a lot of computer power or cancer nodes • These attacks are very difficult and, in reality, hackers go after Bitcoin customers to steal their wallets with malicious software	• Did not provide mitigation measures and their implementation
Factors Affecting	Lute Sakala, Jackson Phiri	Identify the factors that affect the adoption and	• The results of study were that there is a significant positive	• The study did not consider gender and age as possible

Adoption and Use of Mobile Banking Services in Zambia Based on TAM Model		use of mobile banking services in Zambia based on the Technology Acceptance Model	relationship between perceived ease of use, perceived usefulness, user attitude, external variables, user intention and system use	factors that affect the adoption of technology
An interoperable and secure e-wallet architecture based on digital ledger technology using blockchain.	Singh Karan, Nikita Singh, and Dharmender Singh	An interoperable and secure e-wallet architecture based on digital ledger technology using Blockchain.	• The proposed e-wallet system is implemented using interplanetary file system (IPFS)	• The study did not highlight the design and development of the e-wallet
Bank vs Telecommunication E-Wallet: System Analysis, Purchase, and Payment Method of GOMobile CIMB Niaga and T-Cash Telkomsel	Yakob Utama Chandra and Ernawaty, Suryanto	This research aimed to analyse the system, purchase and payment methods in Go Mobile and T-Cash.	main changes that lead to the creation of those innovations, such as: (1) the change of consumer's behaviour and expectation; (2) rapid development of e-commerce; (3) the development of innovative technologies such as internet,	• The study did not investigate factors the lead to adoption of digital wallets

			cellular applications, big service provider companies; and (4) regulation reformation related to e-commerce and online payments	
A Blockchain based Mobile Money Interoperability Scheme	Fickson Mvula, Jackson Phiri and Simon Tembo	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	• The study proposed the use of Blockchain technology to solve the problem of mobile money interoperability in Zambia • Further designed a prototype system on the Hyperledger Fabric network which could develop in an Object-Oriented language such as Java for deployment.	• This study focused on a gap verification of the interoperability problem as well as a technical implementation of a prototype solution. • 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
A conceptual secure blockchain based settlement and clearing	Fickson Mvula, Jackson Phiri	This study, first reviewed the technical landscape and features of mobile payment systems	• study concluded that mobile money interoperability settlement is a valid use case for a permissioned blockchain technology	• The study did not investigate factors the lead to adoption of digital wallets

house for mobile financial services in Zambia		in Zambia and then assessed the feasibility of using blockchain technology in proposing a settlement and clearing system that would facilitate mobile money interoperability	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	
Evaluation of Blockchain-based Data Sharing Acceptance among Intelligence Community	Wan Nurhidayat Wan Muhamad, Noor Afiza Mat Razali, Muslihah Wook, Khairul Khalil Ishak, Norulzahrah Mohd Zainudin, Nor Asiakin Hasbullah, Suzaimah Ramli	Proposed an evaluation method to study the acceptance of Blockchain technology by integrating a reliable acceptance model for Blockchain technology implementation in the intelligence community	• Job relevance has a positive influence on the perceived usefulness of the Blockchain-based data-sharing system, optimism has a positive influence on the perceived usefulness of Blockchain-based data-sharing system and insecurity has a negative influence on the perceived ease of use of the Blockchain-based data-sharing system.	• This study did not include perceived risk, gender and age possible constructs that influence the adoption of a Blockchain-based product • Sample size was small

Blockchain: Methods, Applications and Technology Progress	Cheryl Ann Alexander and Lidong Wang	The methods, impacts and benefits of Blockchain are introduced. The applications and the technology progress of the Blockchain technology are presented	• The impacts of the Blockchain technology lie in: creating secure and almost immutable records, excellent certainty among contract parties without intermediaries, allowing parties to track and verify the quality and origin of products,	• The study does not look at the design and development of a Blockchain-based product
A Blockchain Technology Evolution between Business Process Management (BPM) and Internet-of-Things (IoT)	Doaa Mohey El-Din M. Hussein, Mohamed Hamed N. Taha, Nour Eldeen M. Khalifa	Study shows a proposed comprehensive study of Blockchain technology. It also examines the research efforts in Blockchain. It presents a proposed Blockchain lifecycle which refers to an evolution and a linked ring between business process management improvement and	This paper presents a comprehensive study of Blockchain technology and its effect in business process management and Internet-of-thing. It presents IoT life cycle and its relation between BPM lifecycle. It also proposes a solution for higher security in Blockchain in a smart-city	• This paper did not investigate the factors that affect the adoption of Blockchain-based technology

		Internet-of-Things concepts		
Blockchain – A Financial Technology For Future Sustainable Development	Quoc Khanh Nguyen	article attempts to synthesize and analyse available information with a focus on the role of Blockchain, a financial tool that can potentially play an important role in the sustainable development of the global economy	• Leading the trend by transforming business model and taking steps to apply Blockchain technology in financial activities would be a tactical preparation for a sustainable development of corporations in general.	• No steps were undertaken to investigate possible factors that might influence the adoption of Blockchain as a financial tool
Study on Factors Affecting Mobile Payment Systems Diffusion in Zambia	Ernest Lesa, Simon Tembo	This study sought to examine consumer's behavioural intention to use or not-use m-payment services through the applicability of the extended Technology Acceptance Model (TAM).	• The proposed, extended TAM, model was empirically validated with survey data whose study's results suggests that service providers can leverage on high mobile penetration to promote M-payments services by enhancing factors that have high significance in Zambia.	• This study focused only on a few respondents from the urban setup of the capital city of Lusaka for collection of empirical evidence. • This is study did not capture age and gender as constructs that would affect the behavioural intention to use m-payment services

A model of technology acceptance and trust that in□luences attitudes and affects the intention to use Samsung pay in Thailand	Pubass Direkwuttanakunchai, Khanchitpol Yousapronpaiboon	The objective of this research was to study a model of technology acceptance and trust that influences attitudes and affects the intention to use Samsung Pay	• This study examines the variables, model of technology acceptance, and trust that influences attitude and affect the intention to use Samsung Pay. • Perceived usefulness was the most significant. Secondly, • Perceived ease of use and the respondents' level of trust were at a high level of agreement.	• This study did not consider age and gender as factors that could affect the intention to use a technology
The Influence of Gender on New Technology Adoption and Use-Mobile Commerce	Suhong Li, Richard Glass, Hal Records	This study empirically investigated the impact of gender differences on the adoption and use of a new technology mobile commerce (m-Commerce)	• It was found that the adoption rate of m-Commerce is the same at about 30% for both male and female respondents. It was also found that respondents' perception of price, ease of use, and usefulness of m-Commerce services had a greater impact than gender, age, or trust for distinguishing between adopters and non-	• The study did not consider perceived risk as a factor that could affect the adoption of new technology and Mobile Commerce

			adopters of m-Commerce services	
Are Gender Perceptions of Computing Changing Over Time?	R. Kelly Rainer, Kittipong Laosethakul, Mary K. Astone	This cross-sectional study compares college students in 1995 and 2002 to examine changes in attitudes toward, and usage of computers	• Results show that gender gaps in usage and attitudes present in 1995 are lessening, or disappearing altogether, in 2002.	• The study primarily focused on gender and age as factors that affect adoption of adoption of technology
Apple - Pay, Towards the Acceptance of German Customers	Martin Fiedler	This article is based on a study that aims to analyse factors influencing the acceptance of contactless payment devices by customers in Germany	• The study reveals that perceived ease of use of the technology has been found as a significant factor in affecting the acceptance of contactless payment processes	• This study primary focused on perceived usefulness and perceived ease as factors that could influence adoption of technology
Factors Affecting Mobile Payment Adoption Intention: An Indian Perspective	Amit Shankar, Biplab Datta	This study aims to identify the factors affecting mobile payment (m-payment) adoption intention in India by proposing a conceptual framework based	• The results exhibit that perceived ease of use (PEOU), • perceived usefulness (PU), trust, and self-efficacy (SE) have a significant positive impact on m-payment	• This study did not consider perceived risk, age and gender as factors that could affect the adoption of mobile payment

		on technology acceptance model (TAM).	adoption intention. However, subjective norms (SN) and personal innovativeness (PI) have no significant impact on m-payment adoption intention	

2.7 Chapter Summary

This chapter presented the detailed background to the study which comprised of brief description of digital financial services ecosystem, potential threats and vulnerabilities to the proposed mobile payment system. Blockchain technologies in digital financial services, payment challenges experienced by students in the current payment systems were reviewed. Furthermore, the chapter presented theoretical and conceptual models used in this study as well as the empirical review. Digital wallets on the market were reviewed.

CHAPTER THREE

RESEARCH METHODOLOGY

3.1 Introduction

This chapter includes the study design, study settings, population, sampling procedure, research instruments, data processing, analysis and interpretation in order to come up with sufficient quality information that will be useful for decision-making. For this reason, any kind of research should be governed by a well-defined methodology based on scientific principles.

3.2 Baseline Study

The cross-sectional design method (quantitative approach) was utilized in this study to identify the factors influencing e-wallet adoption among students at the sampled higher learning institutions. A cross-sectional design, according to Saunders, et al. [101], entails the investigation of a specific phenomenon (or phenomena) in a population at a single point in time. The phenomenon being explored in this instance was the use of e-wallets by students in higher education institutions. A cross-sectional study allowed the researcher to gather a large amount of data in a short period of time.

3.2.1 Variables

The use of e-wallets was the dependent variable, whereas demographics (age and gender), perceived usefulness, perceived ease of use, perceived cost, perceived risk and social norm were the independent variables.

3.2.2 Study Site and Population

Participants in this study were chosen from four higher education institutions offering accommodation to students. The University of Zambia's Great East Campus, NIPA, Evelyn Hone College, and Mulungushi University were among the institutions. The four institutions were chosen for this study because the target population, which consisted of students who used mobile phones to check account balances or bank statements, receive money from family or friends, or

send money to family or friends. The students could easily be sampled from the four campuses' hostels as they were within easy reach of the researcher.

The inclusion criteria were students studying at public higher institutions of learning and were accommodated in the institutions' accommodation facilities while the exclusion criteria were students studying at public higher institution of learning but were not accommodated in the institutions' accommodation facilities.

3.2.3 Sampling

The hostels of the higher learning institutions were chosen using stratified random sampling, and the occupants were subsequently chosen for participation in this study. Stratified random sampling occurs when a population is divided into strata (or subgroups) and a random sample is chosen from each subgroup [102]. A subgroup is a naturally occurring collection of elements. The use of stratified random sampling in this study was justified since subgroups in the form of hostels had been established, which met the criteria for utilizing stratified random sampling.

3.2.4 Sample Size

Using stratified random sampling, certain hostel blocks were chosen at random from the hostel strata of the sampled institutions. When those hostels were chosen at random, it meant that a representative from each room in the hostel was considered for participation in the study. The number of participants was determined using a formula adapted from Taherdoost [102]:

$$n = \frac{Z^2 p(100 - p)}{E^2} \quad (1)$$

Where:

- **n** is number of participants
- **Z** is the value corresponding to level of confidence required at 95%= 1.96 confidence level.
- **P** is the percentage occurrence of a state or condition which is 0.5
- **E** is the percentage maximum error required which is 0.05

As a result, the minimal sample size was 210 participants, with 28 of them being disqualified owing to incomplete questionnaire responses, leaving a total of 182 people who took part in the study.

3.2.5 Data Collection

The quantitative data from the sampled students was collected using a structured questionnaire. The questionnaire was mostly closed-ended, with a few open-ended questions. The researcher personally administered the questionnaire to the participants in order to ensure that their replies were comprehensive and to facilitate the validity and reliability of their responses.

3.2.6 Ethical Considerations

To ensure that this study upheld the accepted research ethics, ethical clearance to conduct the study was obtained from the University of Zambia's School of Natural Sciences Ethics Committee. This committee is responsible for approving research conducted in the School of Natural Science at the University of Zambia. REF No. NASREC: 2021-APR-008 is the approval reference number. The actual ethical clearance approval document can be found in appendix A.

3.3 Conceptual Model

To describe user behaviour in the use of technology, several theories or models have been established. The TAM [48] and the UTAUT [57] were both taken into consideration for this study. As a result, using constructs from both models, this study proposed a conceptual framework as illustrated in Figure 3.1

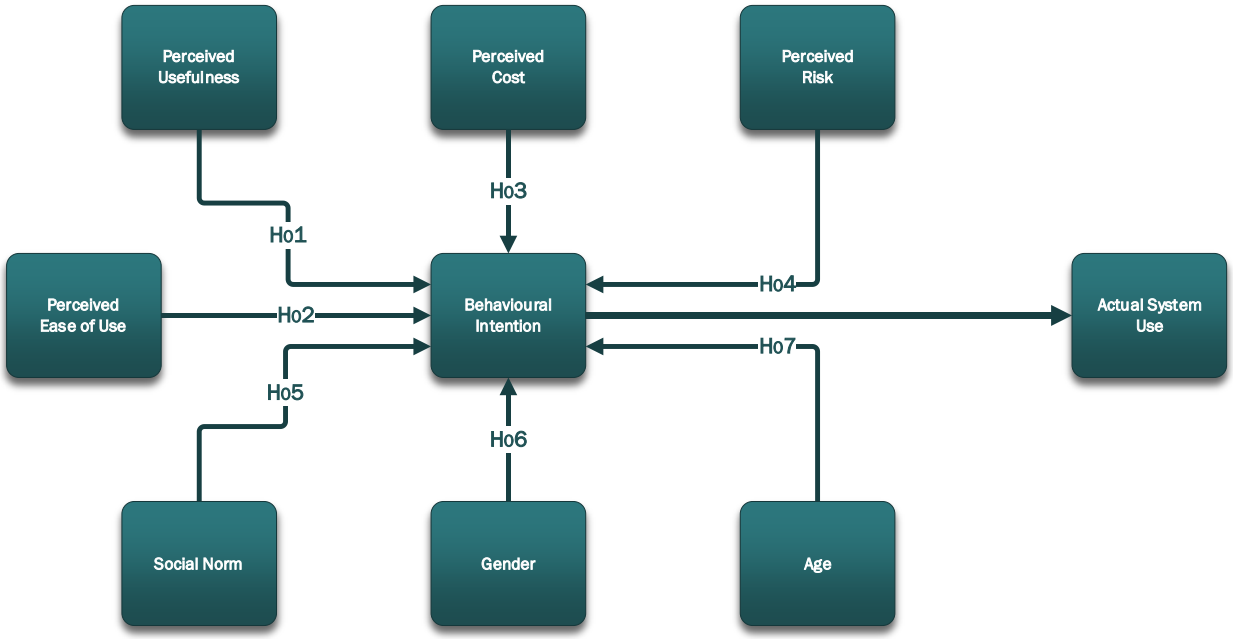


Figure 3.1. Conceptual Framework

In this study, seven factors were considered as possible predictor variables, these variables being perceived ease of use, perceived usefulness, perceived cost, perceived risk, social norm, gender and age. Perceived ease of use, usefulness, cost [70] and risk [76] were derived from variables TAM while social norm, gender and age were derived from UTAUT.

3.3.1 Hypotheses

1. $H_0 1$: Perceived usefulness does not influence the adoption of e-wallets by students in higher learning institutions.
2. $H_0 2$: Perceived ease of use does not influence the adoption of e-wallets by students in higher learning institutions.
3. $H_0 3$: Perceived cost does not influence the adoption of e-wallets by students in higher learning institutions.
4. $H_0 4$: Perceived risk does not influence the adoption of e-wallets by students in higher learning institutions.
5. $H_0 5$: Social Norm does not influence the adoption of e-wallets by students in higher learning institutions.

6. $H_0 6$: Age does not influence the adoption of e-wallets by students in higher learning institutions.
7. $H_0 7$: Gender does not influence the adoption of e-wallets by students in higher learning institutions.

3.4 Data Analysis

3.4.1 Analysis of Descriptive Statistics

The quantitative data was entered into a computer and statistically analyzed using Statistical Package for Social Sciences (SPSS) to generate frequency and association tables. In addition, the SPSS output was exported to Excel, which allowed for the creation of charts and tables.

3.4.2 Analysis of Inferential Statistics

The Multinomial Logistic Regression's Likelihood Ratio Test was used to determine the significance of the associations between the dependent and independent categorical variables at a 5% level of significance, and SPSS aided the analysis of inferential statistics.

3.5 Design and Development of Prototype

In this study, an object-oriented software development methodology was adopted. It is a design strategy where system designers think in terms of "things" or real-life objects instead of operations or functions. The object-oriented software development methodology ensures that the system being developed is refined and transformed through phases of analysis, design, code and testing [103]. Through successive iterations, specifics and modifications are introduced and gradual releases of software modules are given. Object-oriented software development Life Cycle is an iterative process that has five key phases. The following are the phases of the methodology;

3.5.1 Requirements Specification

Requirements specification brings out the functional and non-functional requirements that will be involved in the design of the proposed system leading to its implementation. Requirements specification looks at functional requirements which are defined as "system must do" and non-

functional requirements which are “system shall be”. Functional requirements were captured in a use case while non-functional requirements were captured as a quality attribute. The end result of a functional requirement is a product feature while for a non-functional requirement are product properties. Functional requirements verify the functionality of the software and non-requirements verify the performance of the software system [104].

3.5.1.1 Functional Requirements

Functional requirement are system services which are expected by the user of the software system. Functional requirements “should define the fundamental actions that must take place in software acceptance, processing of inputs and generating the outputs”. Functional requirements may be calculation, technical details, data manipulation and processing, and other functionality that define what is a system is supposed to accomplish.

The following list highlights the functional requirements for students;

1. A user should be able to create a mobile wallet account using his/her registered student number, mobile number and PIN
2. A user should be able to login his/her mobile wallet account using their mobile number and PIN
3. A user should be able to reset his/her forgotten PIN
4. A user should be able to view his/her current mobile wallet balance, private and public keys
5. A user should be able to view his/her profile.
6. A user should be able to load funds into his/her mobile wallet account from either his/her bank account or mobile money account.
7. A user should be able to input necessary information in order to perform a transaction
8. A user should be able to view payment information before committing a transaction
9. A user should be able to receive feedback that relates to the transaction
10. A user should be able to pay for various student fees and other merchant fees
11. A user should be able to send funds from his/her mobile wallet to another registered mobile wallet
12. A user should be able to request transfer of funds from another registered mobile wallet to their mobile wallet.
13. A user should be able to view his/her transaction history

3.5.1.2 Non-Function Requirements

Non-functional requirements set out the quality attribute of a software system as well as impose constraints under which the system must operate. Non-functional requirements specify software system attributes such as responsiveness, usability, security, performance and other non-functional criteria essential to the software system's success. Non-functional requirements describe critical operational qualities required for release of the software system. This is a description of the hardware and software constraints of the proposed software system. These are categorized into hardware and software requirements.

3.5.1.2.1 Hardware Requirements

This section describes the physical components that will support and be used by the proposed system. It also specifies the minimum requirements of the components of the proposed system to run efficiently and effectively.

The designed mobile application must run on an Android or iOS device with the following minimum device hardware requirements:

i. Network Technology: - GSM (3G)/ HSPA(3G+)/ LTE(4G)
   - WLAN Wi-Fi 802.11 a/c/g/n/ac
ii. Display Screen: - Size 3.5 inches
iii. Camera: - 10 Megapixel
iv. Platform: - CPU 1.5 GHz
v. Memory: - RAM 1 GB
vi. Storage: - 500MB

The designed RESTful API must run on server with the following minimum hardware requirements:

i. Memory: - RAM 4 GB
ii. Storage: - 500 GB

3.5.1.2.2 Software Requirements

This section describes the operating system that will run the proposed system.

The designed mobile application must run on the following mobile operating system;

i. Android Version KitKat or higher
ii. iOS 10 or higher

The designed RESTful API must be hosted on server running;

i. Ubuntu 18.04 LTS
ii. Ngnix

3.5.1.2.3 Constraints

The proposed system is to have the following system properties and constraints;

i. Correctness: The system should produce the right user financial information and updated output before and after a transaction has been completed.
ii. Integrity: The system should ensure that no unauthorized user has access to financial or personal information about another user. Only the institution system administrator should have the access to view financial and personal information as well as add or edit user details.
iii. Maintainability: The system should be able to be modified easily in the future should user requirements evolve.
iv. Flexibility: Customization of the system such as change of logo, background images and institution name shall be done with ease. The system should tolerate changes in configuration and functionality to demonstrate new or different business models within the same or different institution.
v. Usability: All functions of the system should be built in such a way as to simplify end-user's tasks. The system should deliver optimal user experience.
vi. Efficiency: The application should be able to run and execute all of its functions effectively on most, if not all, smartphones with various hardware specifications and vendors.
vii. Reliability: The system should be able to fully commit transactions and if an interruption occurs during a transaction, the system should gracefully abort the transaction. Users should be able to depend on the system to be available at all times despite of the factors that may affect the system's availability.
viii. Scalability: The system should be able handle a significant number of transactions without performance degrade. The feature set of the system should be able to be extended

so as meet changing user requirements without negatively affecting the implemented features.

3.5.2 Design Specification

The design specification provides a description of the design that will help to realize the specified or identified requirements of the proposed system. It is a brief description of how the system will meet the user's expectations. It is the bridge between requirements and the implementation that satisfies those requirements.

The design will include the following;

i. Overview Design: this shows an overview of the interacting components of the system.
ii. User Journey Design: shows of the journey of the user in interacting with the system.
iii. System Architecture: shows the conceptual model that defines the structure and behaviour of the system.
iv. Logical Design: pertains to the abstract representation of the system. This is often included via modelling.
v. Data Design: this shows the data tables and how they are related to each other. This will specify the entity relationships, data tables, E-R diagrams as well as relational schemas.
vi. Security Design: the security mechanisms that have been applied in the system.

3.5.2.1 Overview Design

Figure 3.2 shows the components that constitute the proposed system. It describes an overview of the actual set-up of the system being developed.

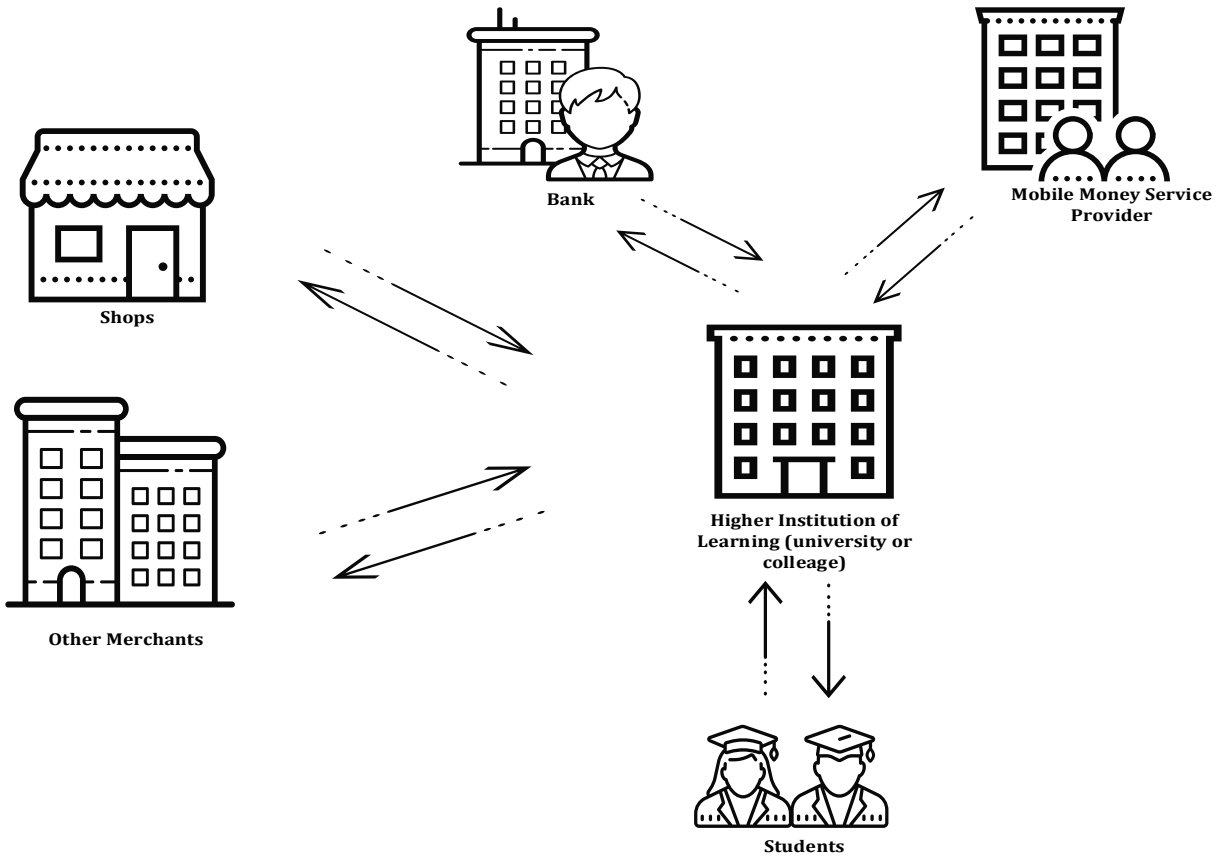


Figure 3.2. Outlines how the overview design supports the system's conceptual design to meet the user requirements

The system will consist of the following interacting components;

i. Bank
ii. Mobile Money Service Providers
iii. Higher Institution of Learning (University or College)
iv. Students
v. Shops
vi. Other Merchants

3.5.2.1.1 Bank

Payment of tuition and other fees is mostly done at an accepted bank chosen by the higher institution of learning. The bank will provide an escrow account and current account to the higher institution of learning. An escrow account is an account that keeps funds in trust while a transaction is yet to be completed by two or more parties. It is an account designed to safely hold

funds temporarily. The funds are disbursed to the current account of the institution after a payment using the mobile e-wallet application is successfully fulfilled. The current account will be the account that will cater as the active account for daily deposits and cheque withdrawals. This is where all payments made to the institution will be stored.

3.5.2.1.2 Mobile Money Service Provider

The mobile money service is a technology that proposes to change how consumers are transferring and exchanging money. Mobile money service meets the needs of unbanked, unconnected, often semi-educated consumers. The customer such as a student does not need to have a bank account, but registers with the service provide for mobile money account. Mobile money allows transfer of funds from one individual to another without need of traditional bank accounts. Therefore, mobile money service providers will serve as alternative to using a bank for students to deposit funds into their mobile e-wallet application.

The higher institution of learning will have a merchant account with the mobile money service providers. The merchant account will allow the institution to receive deposits from the students conducted using mobile money transfer.

3.5.2.1.3 Higher Institution of Learning

This will be in this case the University of Zambia. The University of Zambia will be the custodian of the Blockchain and the mobile e-wallet application.

3.5.2.1.4 Students

Students are the primary users of the mobile e-wallet application. During their studies, students are required to pay for registration, tuition, examination, medical, accommodation, library, recreation, internet, maintenance and student union fees. Students will be able pay school fees using the mobile wallet application.

3.5.2.1.5 Shops

These will be participating shops within the University of Zambia campus and East Park Shopping Mall. Students will be able to make payments for either products or services using the mobile e-wallet application.

3.5.2.1.6 Other Merchants

These are future interested merchants of the higher institution of learning's Blockchain ecosystem. A RESTful API will be provisioned for easier and faster integration with any other already existing merchant to facilitate communication and data exchange.

Current Business Process

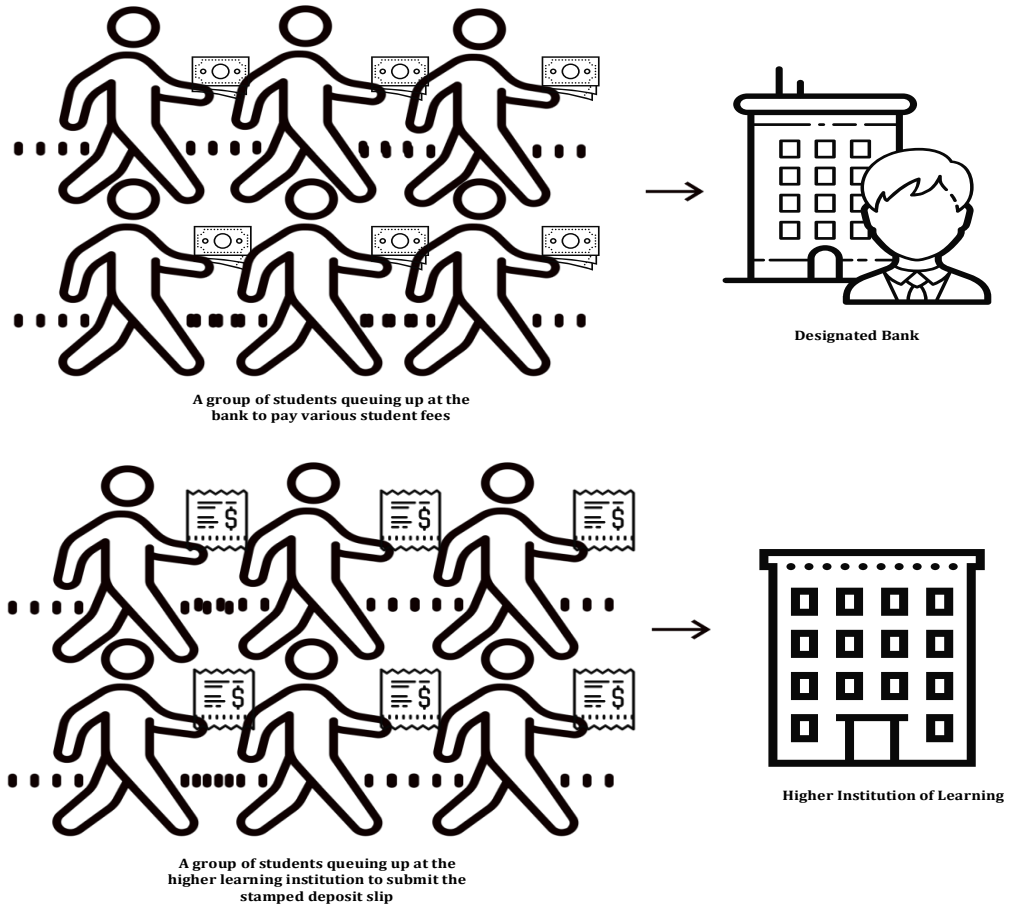


Figure 3.3. Current Student Fee Payment Process

Figure 3.3 illustrates the current student fee payment process. A month before enrolment of students for a particular academic year commences, the higher institution of learning publishes the student fees payable to the institution. After a student views the student fees payable for that academic year, he or she has to go a bank approved by the higher institution of learning to deposit money. Due to the rise in the number of students enrolled in higher institution of learning, payment of student fees is characterised by long unbearable queues and overcrowding in most of the designated banks. Furthermore, after depositing the funds, a student is required to submit the stamped deposit slip to the higher institution of learning to confirm that he or she has paid. Equally, submission of stamped deposit slips is characterised by long intolerable queues and overcrowding in the higher institution of learning.

3.5.2.2 Proposed Business Process

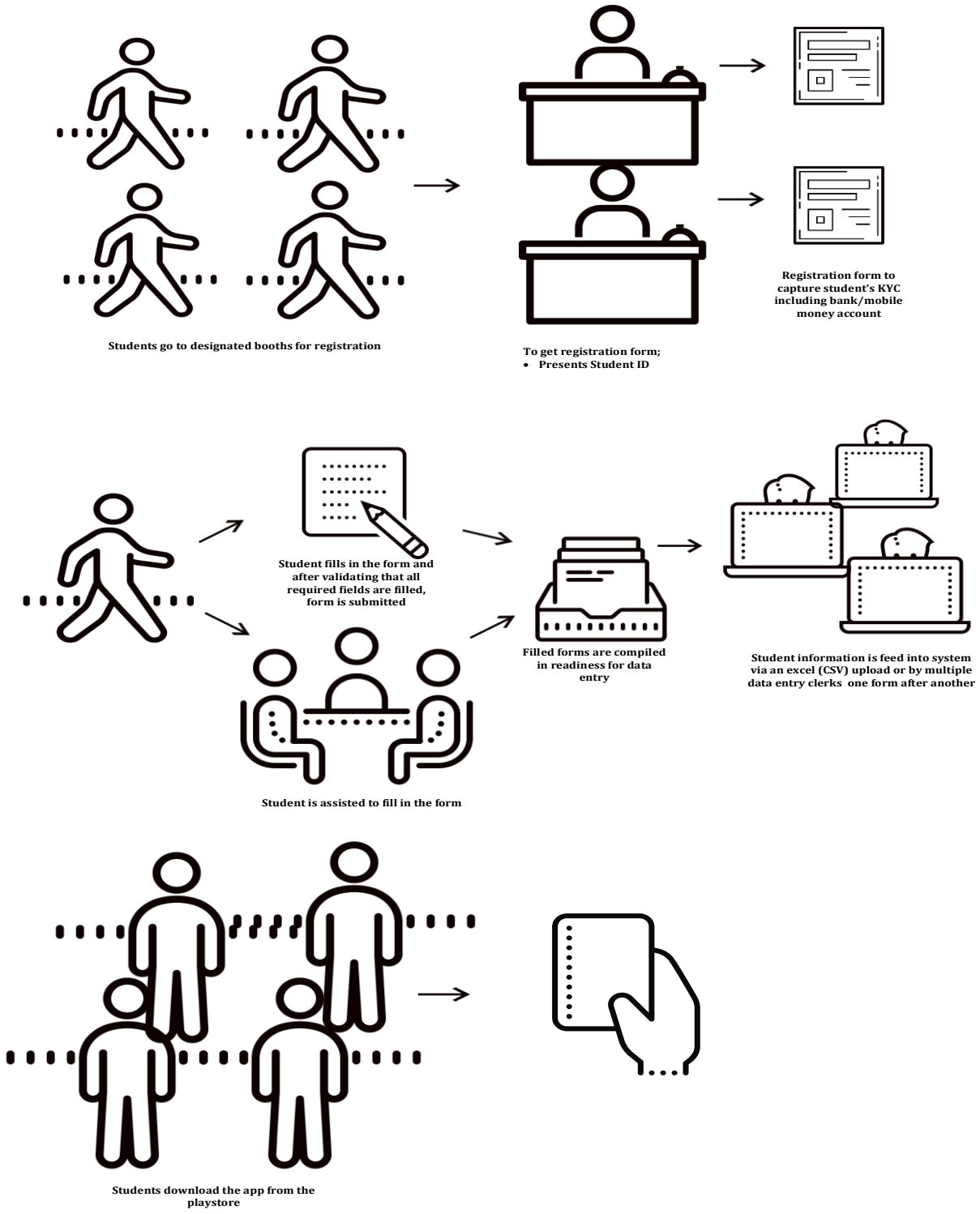


Figure 3.4. Student On-Boarding Process

Figure 3.4 shows the student on-boarding process. During the student registration process, students are prompted to enrol in the Blockchain mobile payment system. The student can fill in the form or can be assisted to be fill in the form. The form is validated to ensure all mandatory fields are filled. Filled forms are compiled in readiness for data entry. Student details are uploaded into the system via an excel or data entry clerks one form after another. Students then proceed to download and install the mobile wallet app from Google Play Store or Apple Store. This is a once-off step that is done at the beginning of the student's academic stay at the institution.

After installing the mobile e-wallet app, the student enters their details including his or her student number, mobile number, PIN and is logged in.

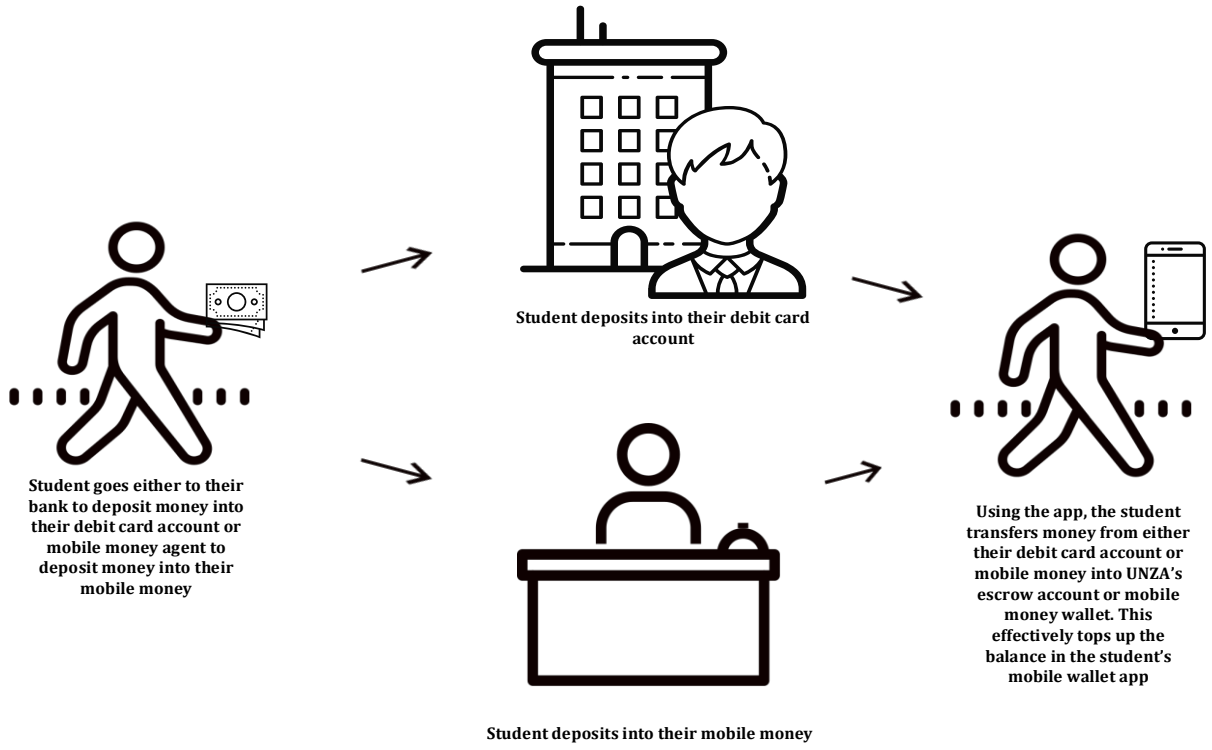


Figure 3.5. Loading of Funds

Figure 3.5 illustrates the loading of funds into the mobile wallet app. Before using the mobile wallet app to make any payment, the student has to load their e-wallet account with funds of which in the wallet are referred to as coins. The student goes to the bank to deposit funds into their debit

card account. Alternatively, the student can go to a mobile money agent to deposit funds into their mobile money account.

Using the mobile wallet app, the student transfers funds from either their debit card account or mobile money into their wallet. This effectively transfers funds to the higher institution of learning's escrow account.

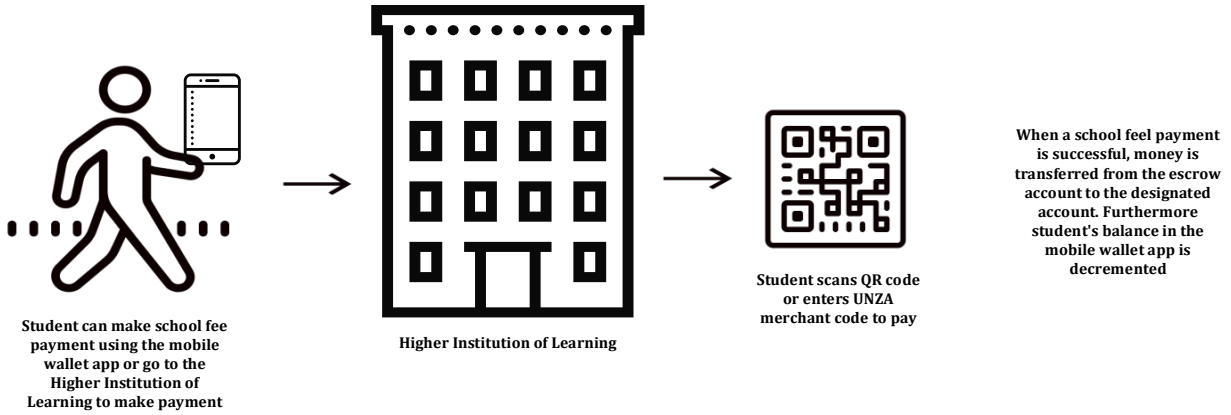


Figure 3.6. Payment of School Fees

To make a payment within the higher institution of learning, using the mobile wallet application, the student scans the QR code tag displayed within the premises of the institution as illustrated in Figure 3.6. In general, there are two types of QR codes available on the market; dynamic and static. For the dynamic QR code, the buyer does not need to enter the purchase amount for QR payment because the account information and payment amount are included within the QR code. The static QR code is the polar opposite of the dynamic QR code. The buyer must enter the purchase amount for QR payment, and the QR code merely contains the account information.

On the other hand, using the mobile wallet application, the student can select the fee that he or she wants pay for and make a payment remotely without sharing financial information. If a payment is successful, funds are transferred from the escrow account to the institution's designated account. Furthermore, the student's balance in the mobile wallet application is decremented.

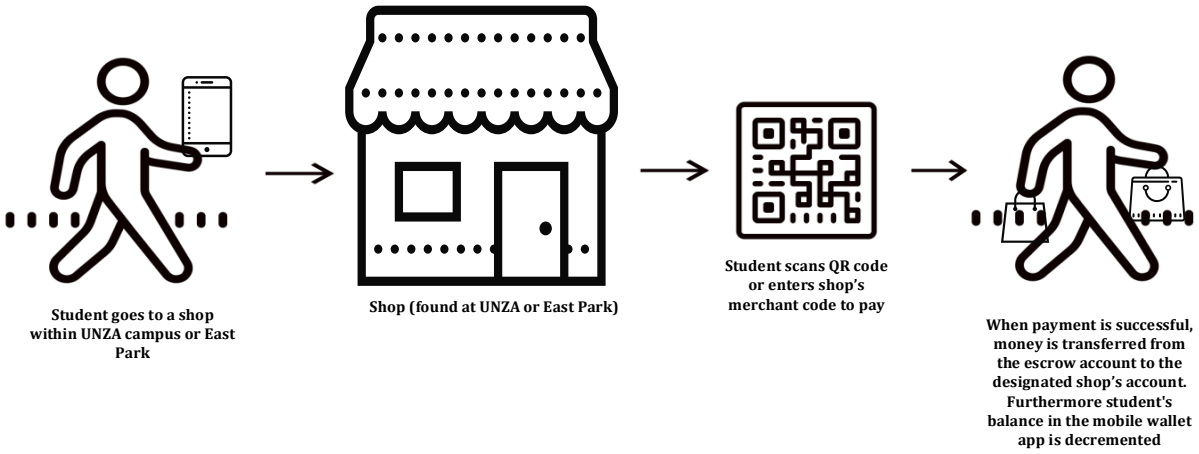


Figure 3.7. Payment for Groceries

To make a payment for groceries or products obtained from shops within the University of Zambia campus or East Park Shopping Mall, using the mobile e-wallet application, the student either scans the QR code tag displayed within the shop or enters the shop's merchant code as demonstrated in Figure 3.7. Students can use the mobile wallet application to purchase goods from designated campus stores and cafeterias without having to exchange cash.

If the payment is successful, funds are transferred from the escrow account to shop's designated account. At the same time the balance in the mobile wallet app is decremented.

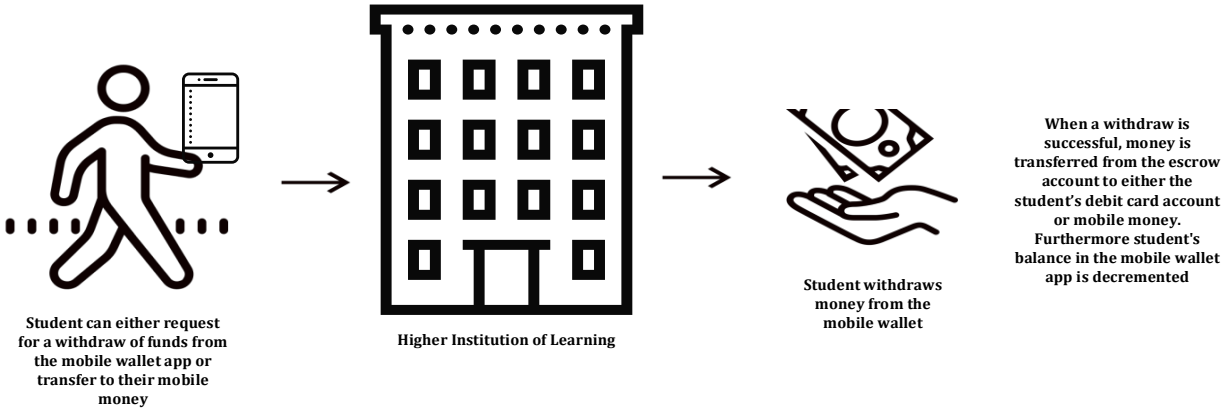


Figure 3.8. Withdrawing Funds from the Wallet Account

As shown in Figure 3.8, in an event the student has completed their studies and would like to withdraw their funds from the mobile e-wallet application account, the student can withdraw their funds by transferring funds to either their debit card account or mobile money. This would effectively decrement funds in the escrow account. Moreover, for this process to be successful, the higher institution of learning would have to approve the transaction. The student can only withdraw an amount equivalent to their mobile wallet balance.

3.5.2.3 System High Level Overview Design

Figure 3.9 shows the proposed system's high-level overview design for this study.

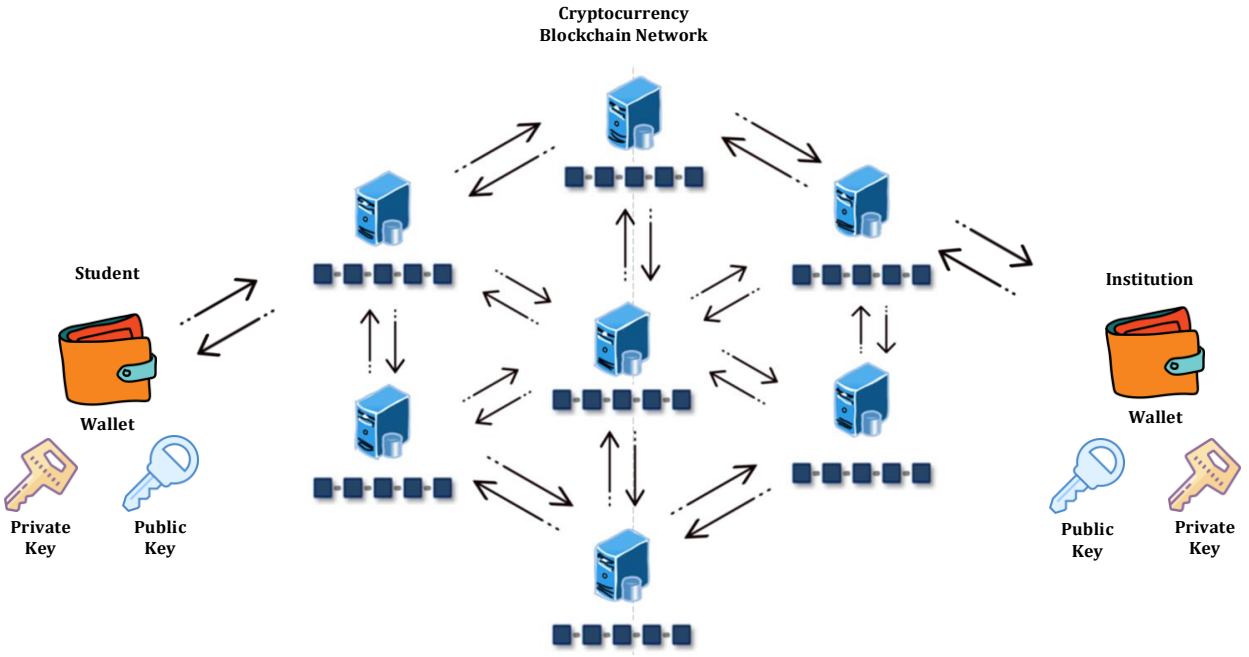


Figure 3.9. Proposed System High Level Design

The proposed system's high-level overview design provides an understanding of system component interconnections and interaction. The overview addresses how the system components will support system functionality.

3.5.3 Logical Design

A model is an abstract, partial representation of a real-world system. An inexpensive way of analysing, communicating, testing and documenting the understanding of the system to be developed. This is a crucial step not only in the development of software but in all engineering fields. Modelling not only helps in the construction of the software system but also in the clarification of system requirements [105].

This study used Non-Analytical/Descriptive Model particularly Unified Modelling Language (UML). Non-analytical/Descriptive is a description of the components within a system and how they are related. In the sense that there are no numbers, they are qualitative in nature but they offer a very good feeling of what to construct. The non-analytical/descriptive models are fairly easy to construct and intuitive to understand, unlike computational and analytical models that require a high degree of knowledge in mathematics and computational sciences [105].

Non-analytical models of software engineering can be loosely divided into two categories. One modelling data, like entity-relationship models, and the other modelling the application that is working on that data. UML models falls under non-analytical/descriptive models, meaning that while UML models refer to data, they also focus on modelling the logic and application structure that uses that data [105]. Unified Modelling Language is a family of graphical notations to describe and design software systems, especially those using an object-oriented approach [105].

3.5.3.1 Use Case Diagrams

Use case diagrams are a precursor to use case specifications capturing the overall functionality of a system at very high-level using notations for actors, use cases and relationships among them. They often serve as a summary of all use cases in a software system.

A use case diagram has four components; use cases, the framework for which use cases have been defined, the actors and relations among all of these components. An actor represents the roles that users of the cases play and it can denote a person (for instance a student, an admin) a device (for instance a server) or rather other systems (for example bank, mobile money service provider). A use case diagram for the mobile application can be observed in Figure 3.10.

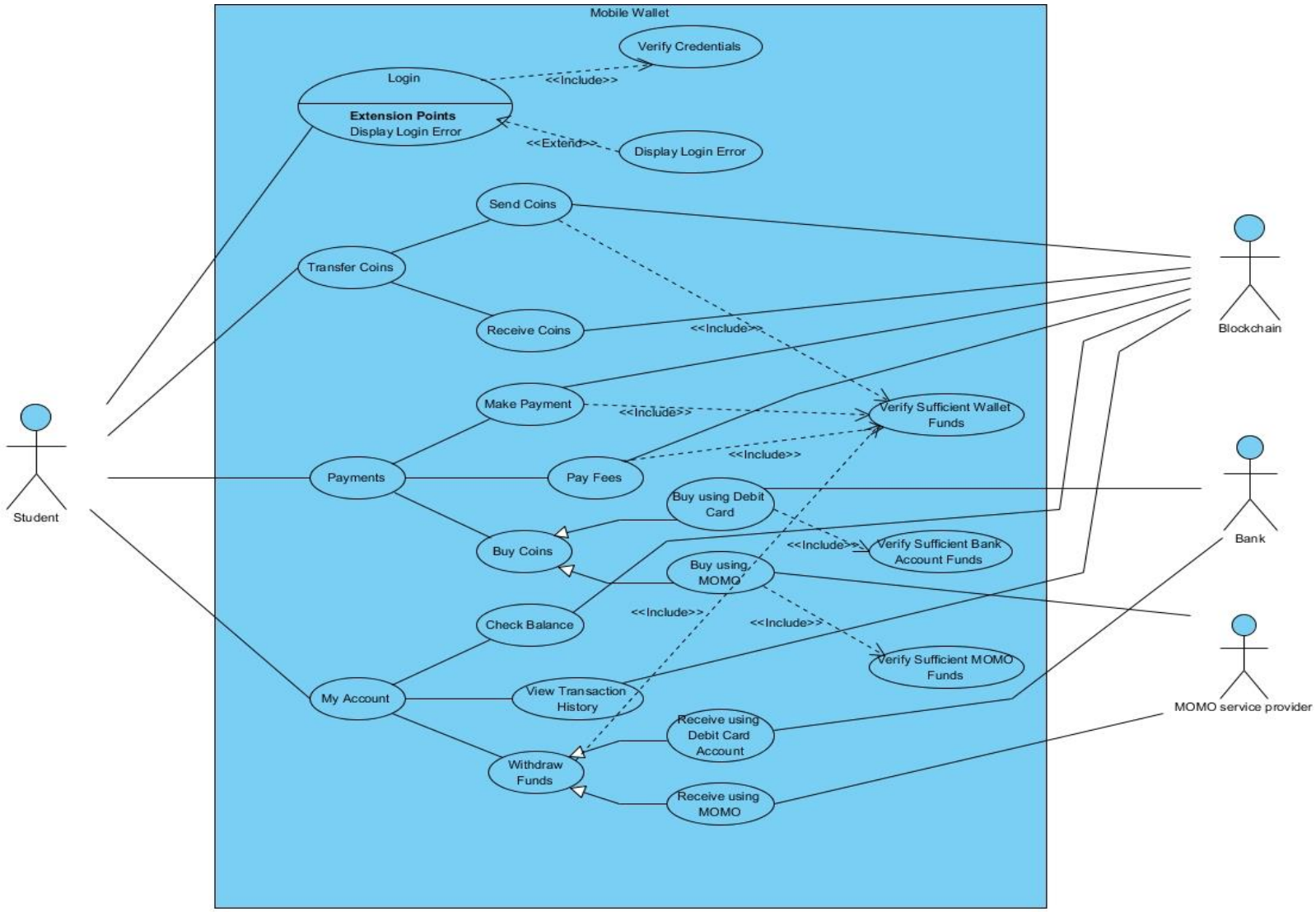


Figure 3.10. Student Use Case Diagram

A summary of the mobile application use case diagram can be seen in Table 3.1.

Table 3.1. Description of the Student Use Case Diagram

Use Case	Description
Login	The student will use a mobile number and PIN to login the e-wallet account
Send Coins	The student will be able to transfer funds from their e-wallet account to another e-wallet account
Receive Coins	The student will be able to receive funds from another e-wallet account to their e-wallet account
Make Payment	The student will be able to make a payment by scanning a QR code or providing merchant code
Pay fees	The student will be able to pay for various fees
Buy coins	The student will be able to transfer funds from their mobile money account or bank account to their e-wallet account
Check balance	The student will be able to view their e-wallet account balance
View Transaction History	The student will be able to view types of transactions that occur by using the wallet
Withdraw Funds	The students will be able to withdraw funds from the wallet

3.5.3.2 Activity Diagrams

An activity diagram is a behavioural diagram that captures the workflow or the process model of a system. An activity diagram is used for workflow and process modelling. It is similar to flow charts but with parallel behaviour and multiple actors. It illustrates a series of actions or flow of control in a system. Activities modelled can be sequential and concurrent. An activity diagram is quite powerful in its ability to capture parallel tracks in a process, as well as multiple actors involved in a process [105]. Figure 3.11 to Figure 3.14 illustrate the activity diagrams used in this study.

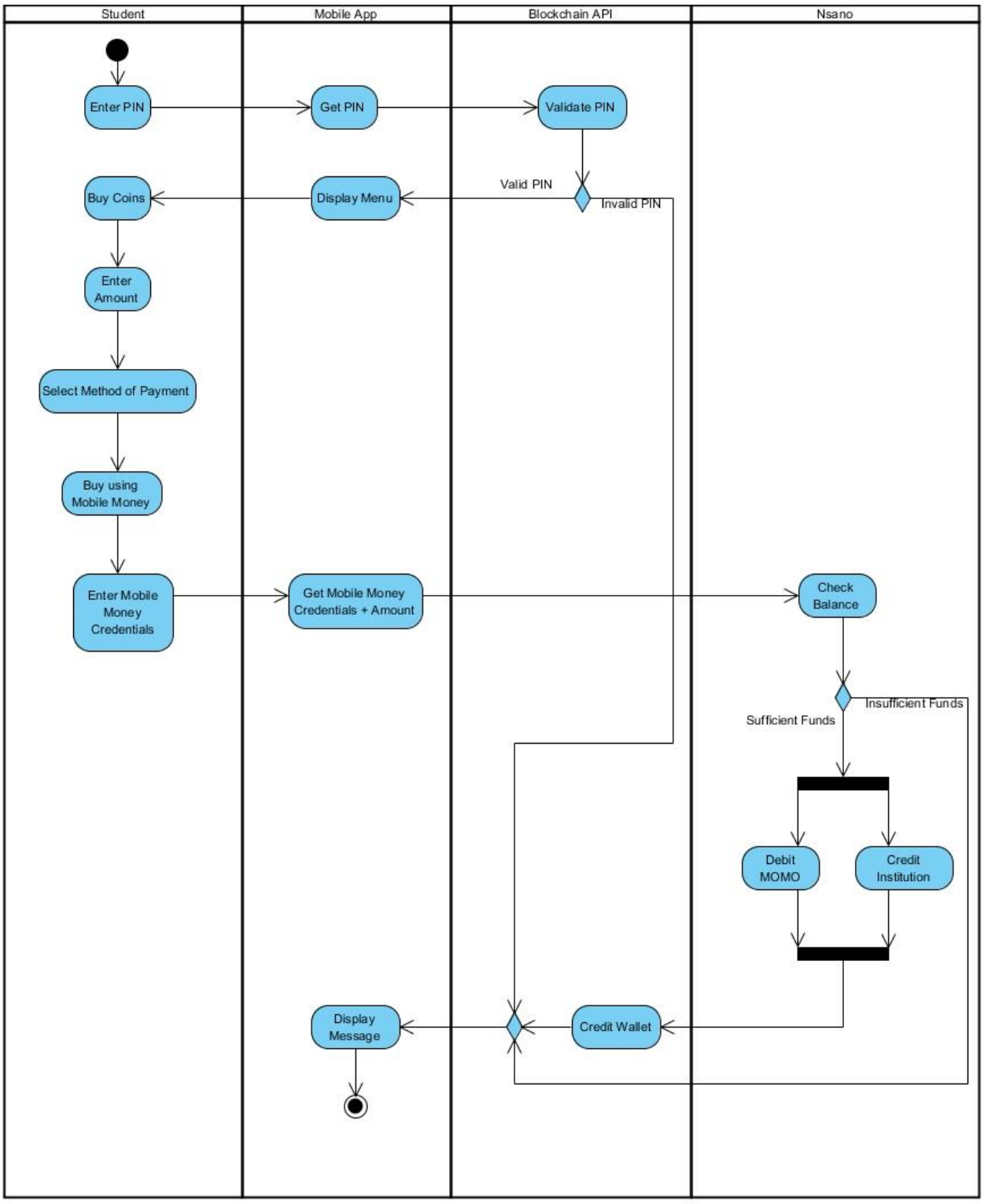


Figure 3.11. Buy Coins Using Mobile Money Activity Diagram

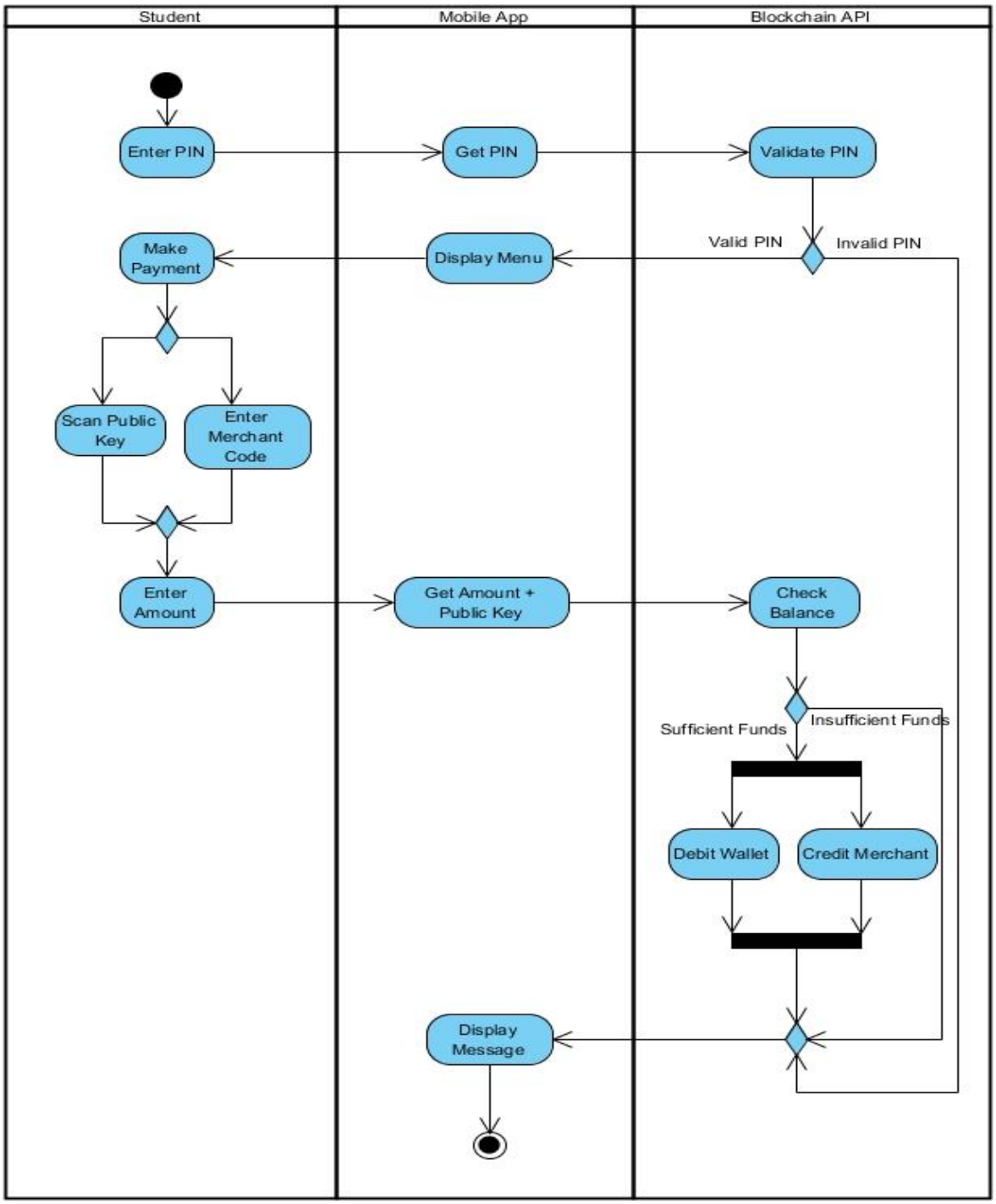


Figure 3.12. Make Payment Activity Diagram

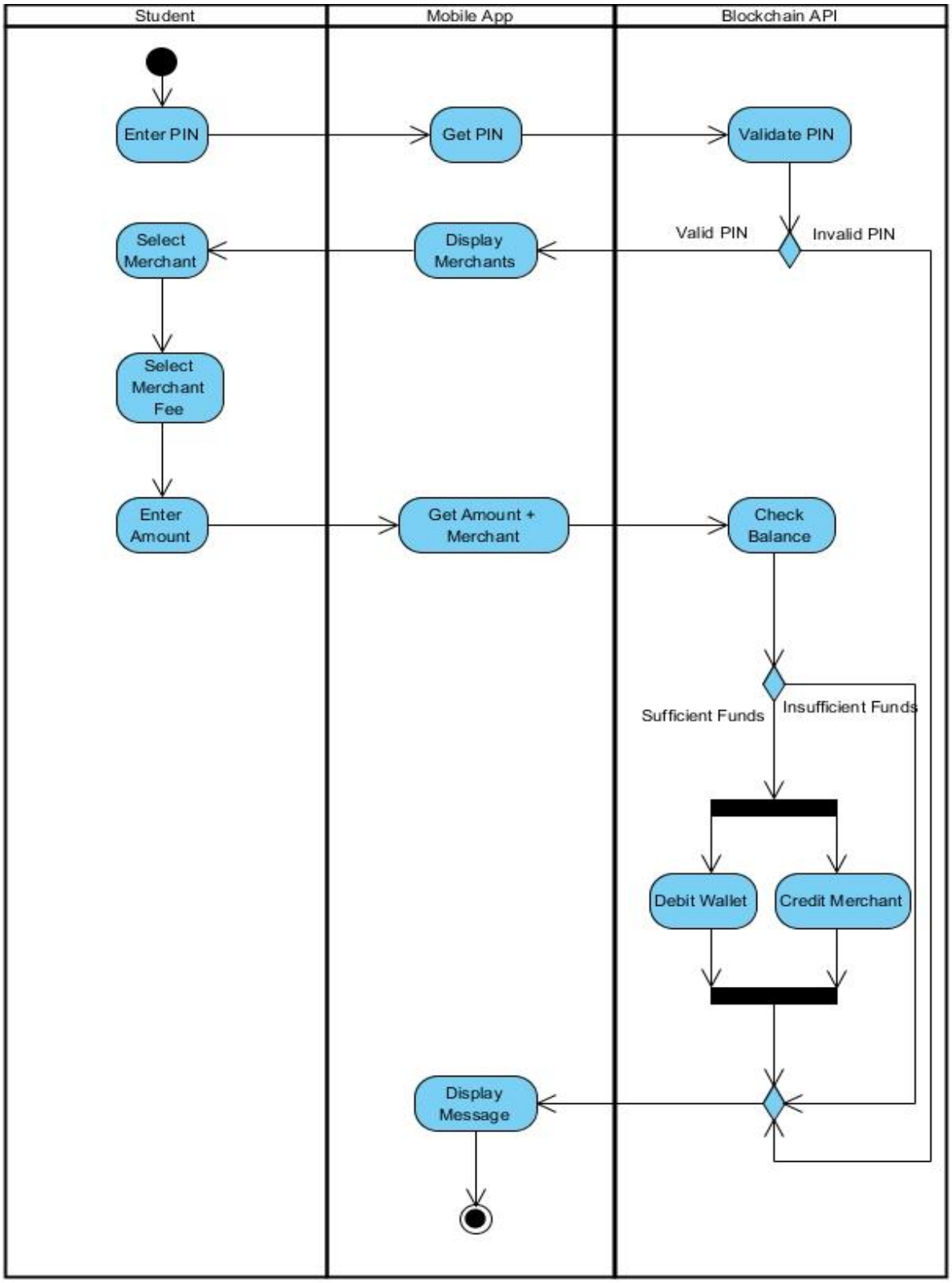


Figure 3.13. Pay Fees Activity Diagram

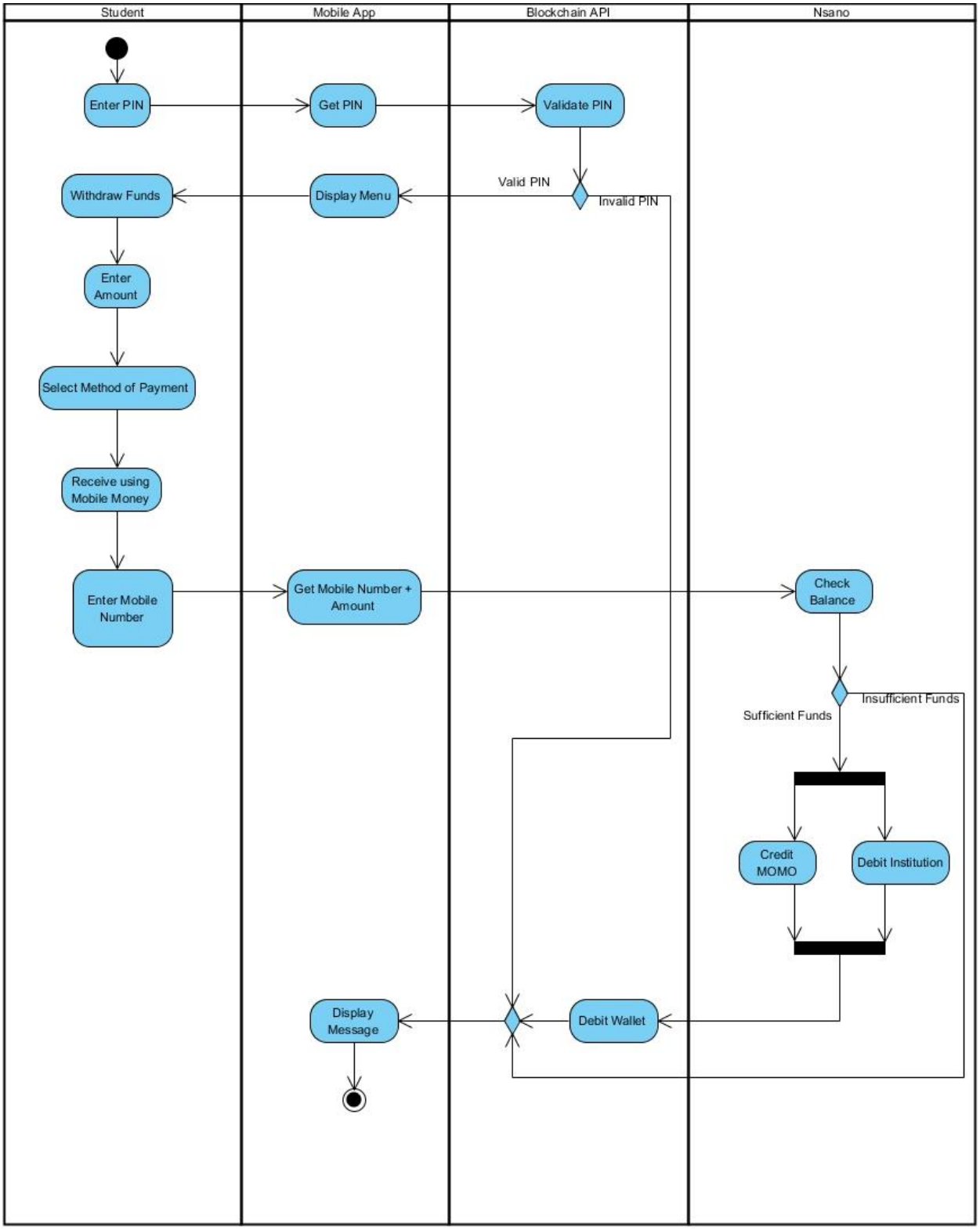


Figure 3.14. Withdraw Funds Activity Diagram

3.5.3.3 Class Diagram

Class diagrams model the type of objects in the system, along with the relationships among them. They are the most widely-used structural models, showing a static view of the system. The key elements in class diagrams can be divided into three groups: classifiers, features, and relationships. Classifiers represent the types of entities in your system, features represent the structural and behavioural characteristics of these entities, and relationships depict how these entities are related to each other. The class diagram depicts the classes in a system, their attributes and operations, as well as the relationships between them. A class diagram can be seen in Figure 3.15

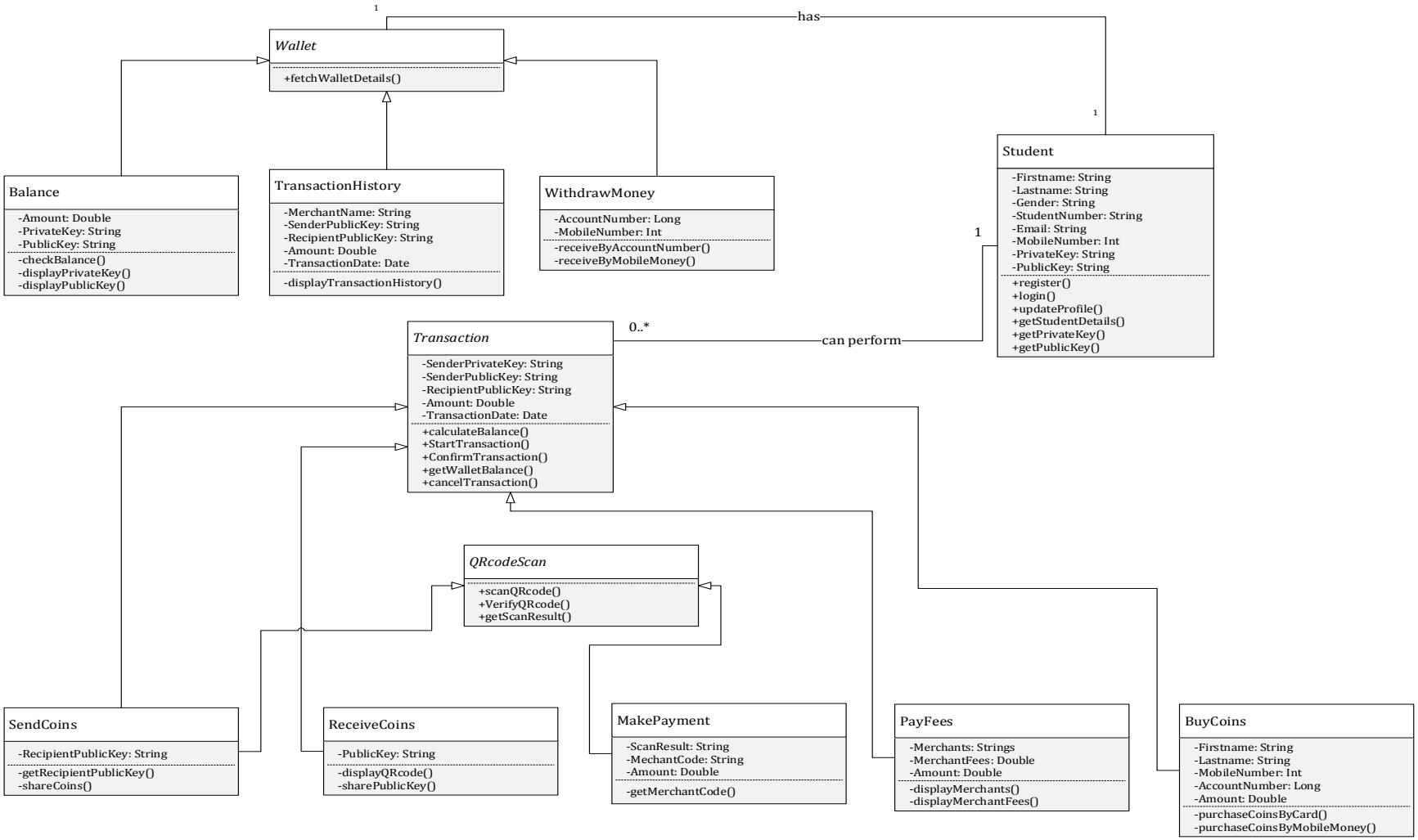


Figure 3.15. Class Diagram

3.5.3.4 Sequence Diagrams

Sequence Diagrams are one of the interaction diagrams that model the dynamic behaviour of a system, focusing on interaction among the entities within a system. Sequence diagrams are not only one of the most widely-used interaction diagrams, but also one of the most popular UML diagrams as well. They capture the dynamic view of the system in terms of the sequence of interaction among its entities. They help capture the communication among classes, and through that, helps identify the behaviour needed to implement in the code. A sequence diagram is read in two directions: from top to bottom, and then horizontally, from left to right or right to left, depending on the direction of the arrows. Figure 3.16 to Figure 3.20 illustrate sequence diagrams used in this study.

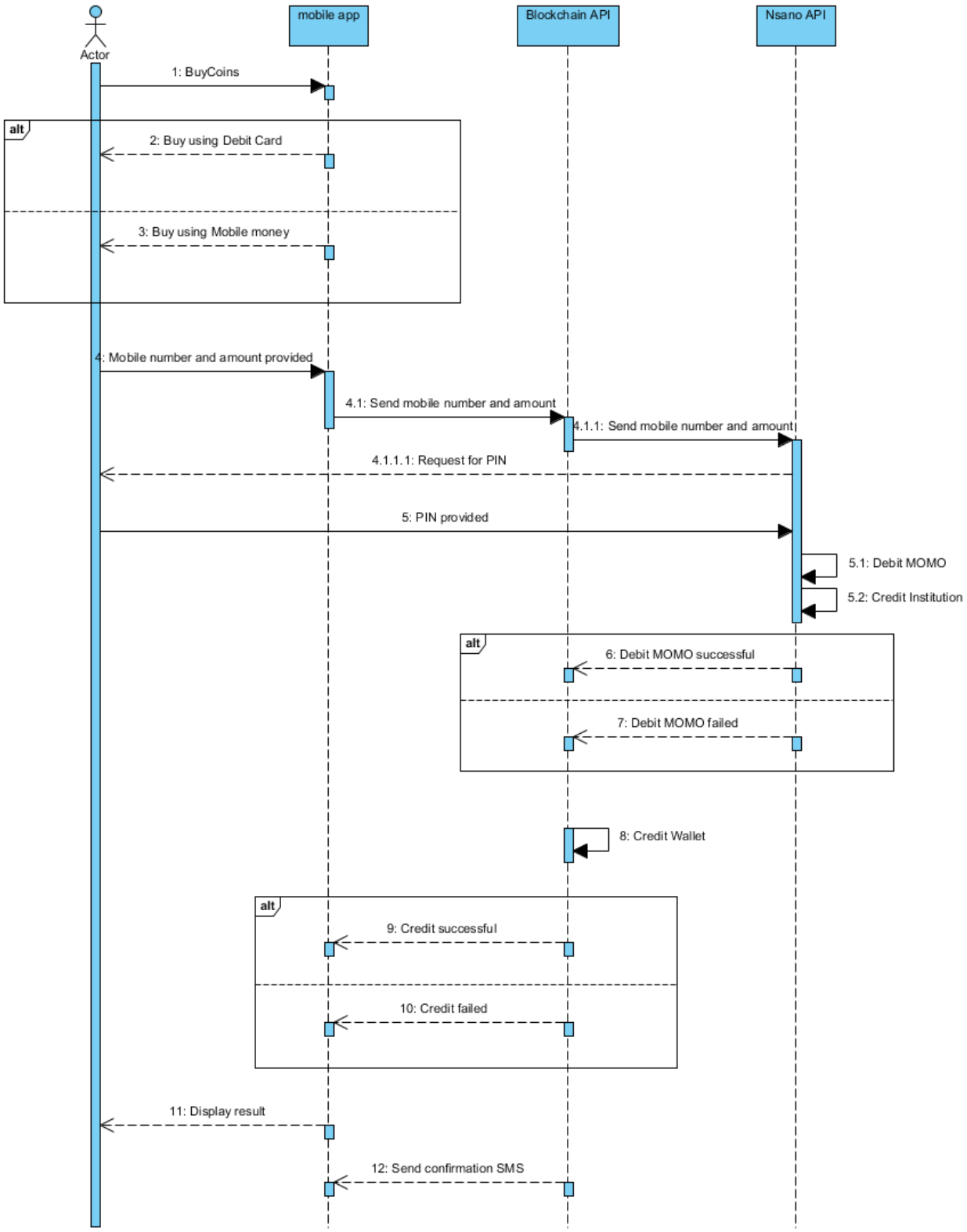


Figure 3.16. Buy Coins Using Mobile Money Sequence Diagram

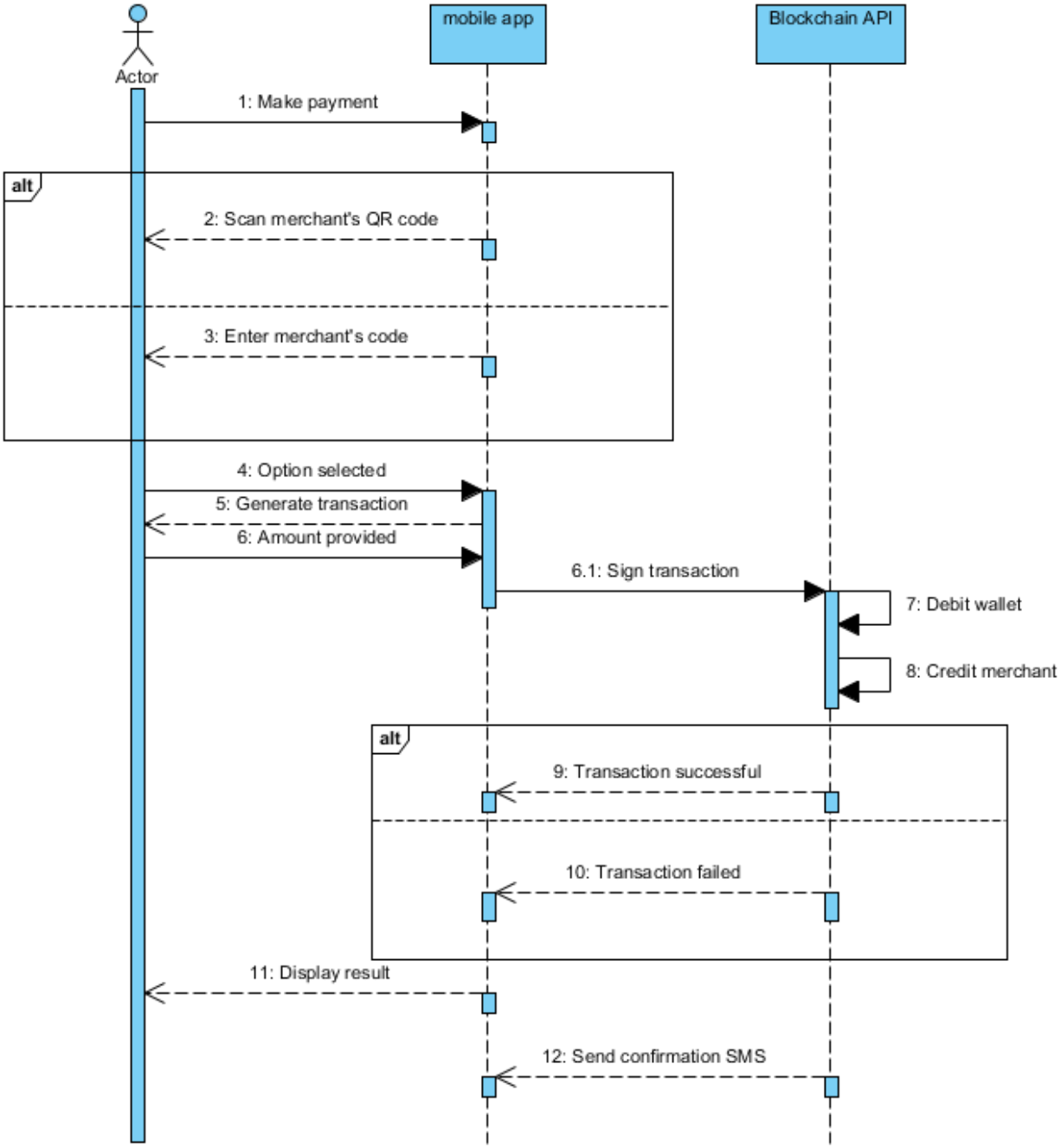


Figure 3.17. Make Payment Sequence Diagram

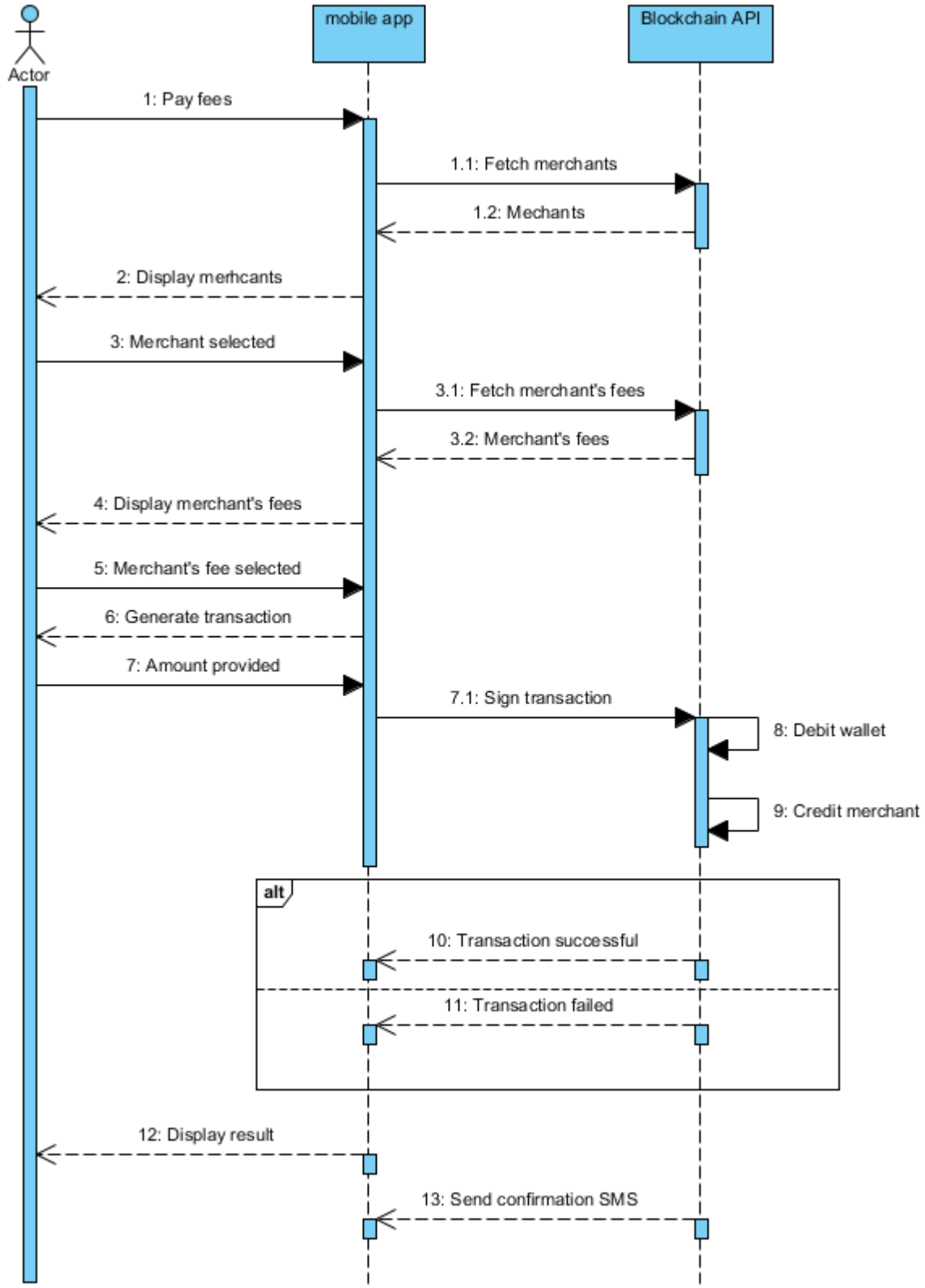


Figure 3.18. Pay Fees Sequence Diagram

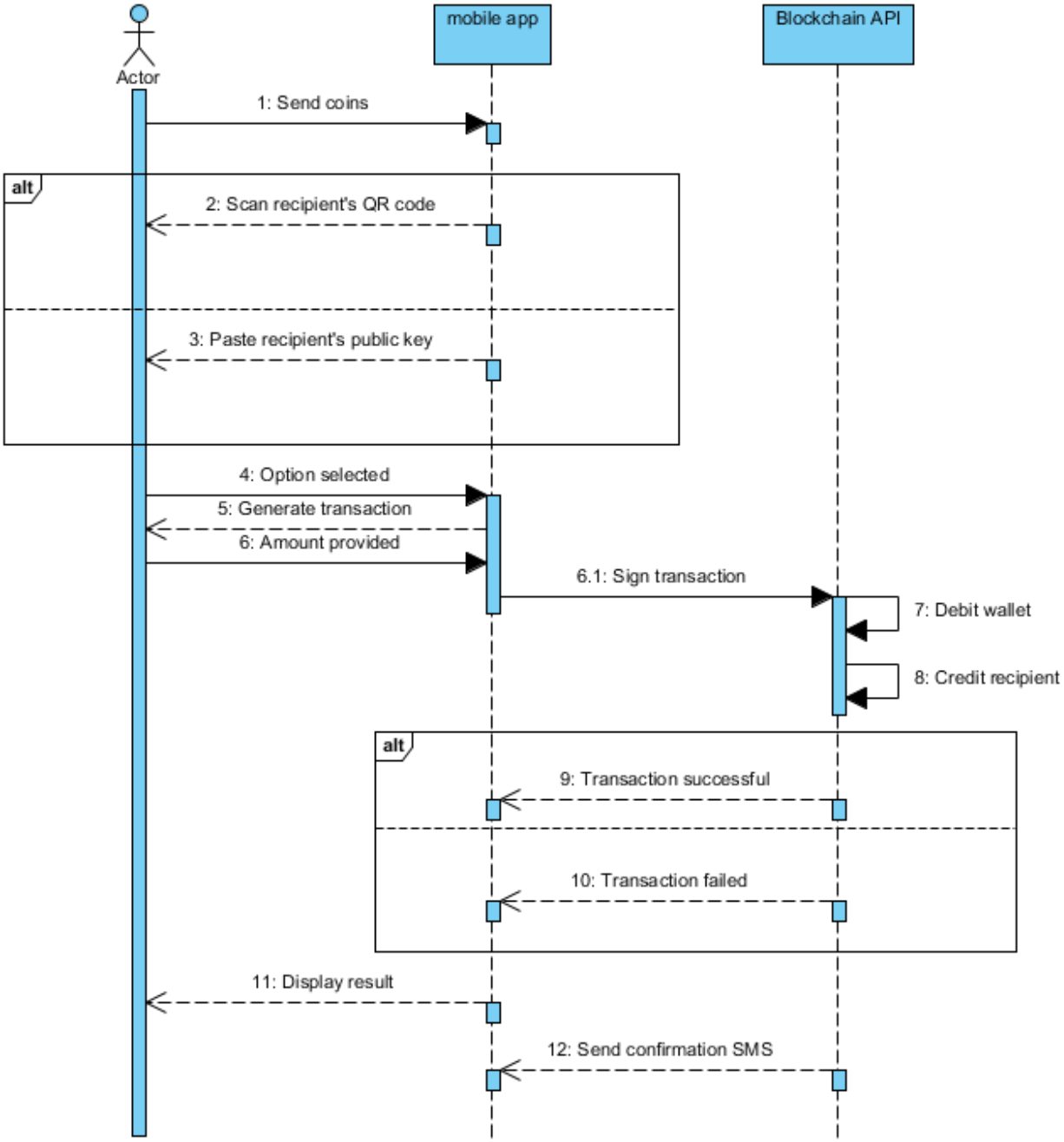


Figure 3.19. Send Coins Sequence Diagram

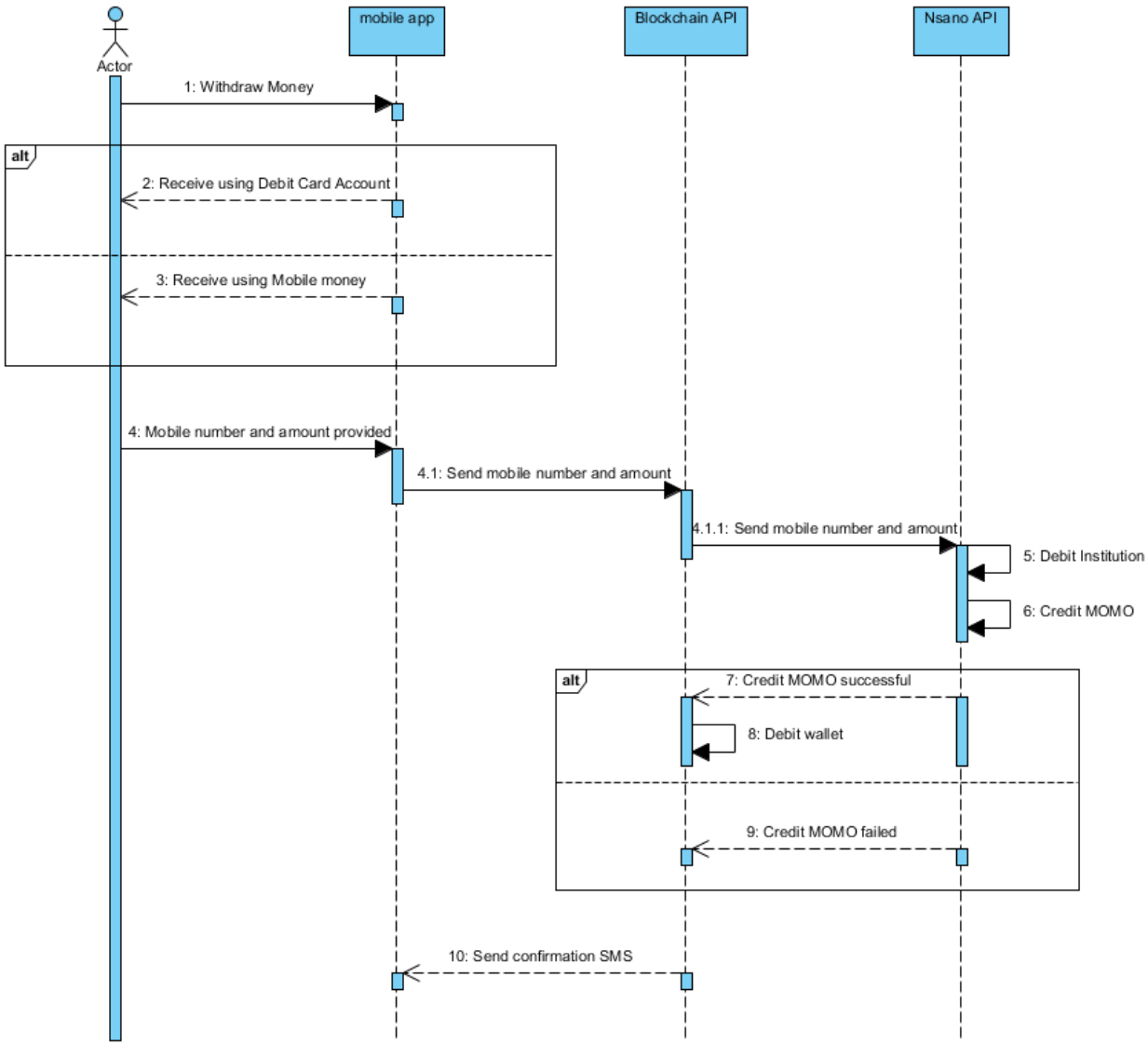


Figure 3.20. Withdraw Funds Sequence Diagram

3.5.4 Database Design

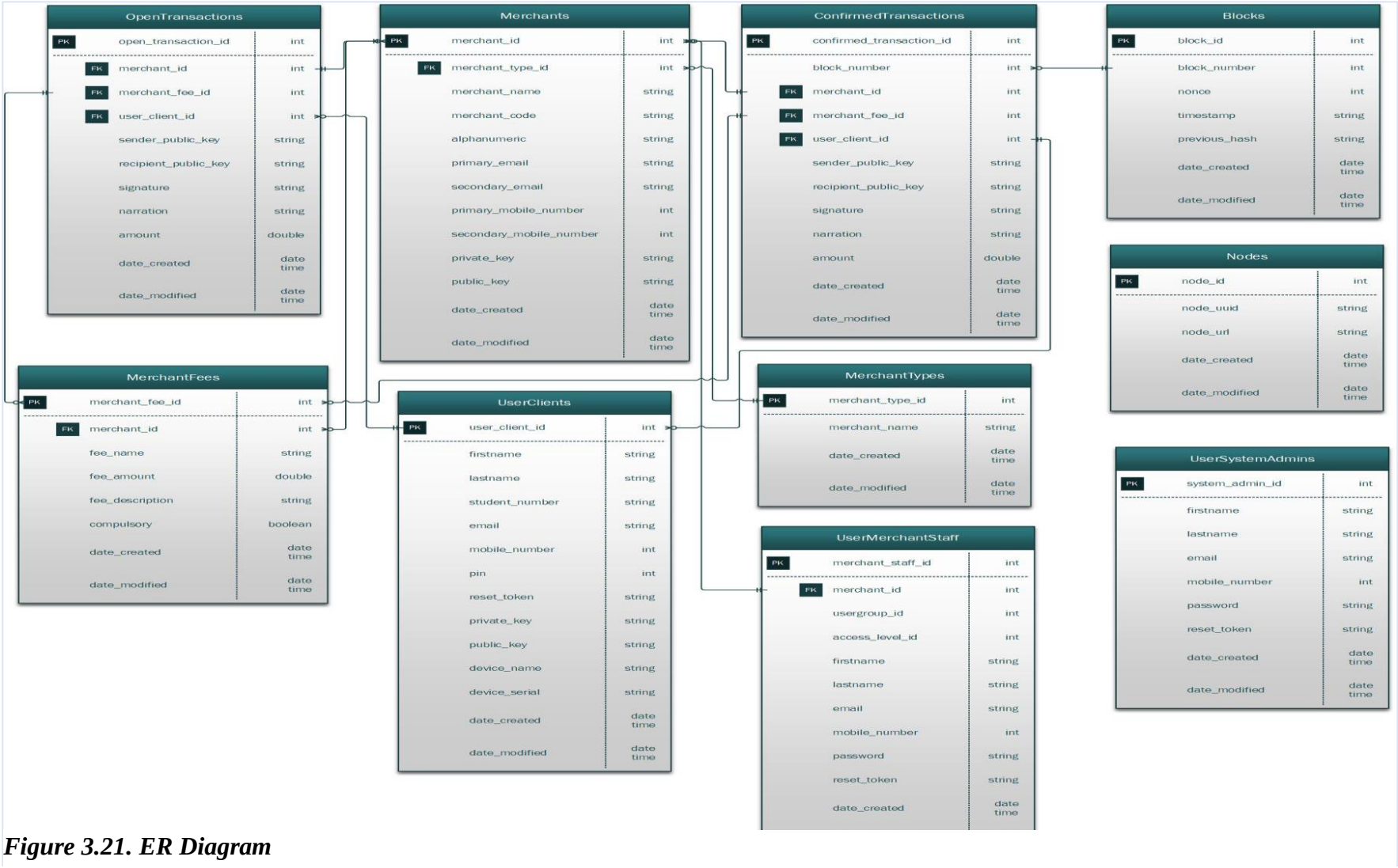


Figure 3.21. ER Diagram

Figure 3.21 shows the Entity Relationship diagram. In addition, Table 3.2 shows a summary of the entities captured in Figure 3.21

Table 3.2. Entity Description

Entity	Description
OpenTransactions	Stores the details of the transactions to be added to the next block
ConfirmedTransactions	Stores the details of transactions on the Blockchain
Blocks	Stores the details of confirmed transactions and other Blockchain meta data
MerchantTypes	Stores the types of merchants. For instance, Bank, MNO, University, Shop
Merchants	Stores the details of the merchants
MerchantFees	Stores the details of the merchant's fees
MerchantStaff	Stores the details of the merchant admin
UserStudents	Stores the details of the students

3.5.5 Security Design

The section addresses the threats identified earlier in Chapter 2. Table 3.3 specifies the best practices and various control measures.

Table 3.3. Control Measures (Adapted from: Mauree and Butler, 2017)

Target Entity	Control Measures
User	a) Security awareness, education and communication. b) Do not use public Wi-Fi hotspots for mobile wallet payments. c) Distinguish real and fake website and access point, only use real one. d) Keep Mobile Operating System up to date
Mobile device	a) Remote device lock and Remote data wipe. b) PIN lock and Strong PINs. c) Keep OS up to date. d) Keep default security controls & measures on device.
Mobile Wallet Application	a) Adopt secure coding practices and secure code reviews manual and automated via tools. b) Source code complication an untrusted code detection. c) Anti-debug and Integrity source code protections. d) White-box cryptography. e) Secure application provisioning through trusted application stores. f) Takedown rogue applications from unauthorized application stores.
DFS provider's Network, Bank's Network and Mobile Network Operator	a) All network operators should take steps to ensure high network availability to allow access to DFS b) All network operators should perform technical capacity tests simulating different transactions based on customer numbers, expected growth, expected number of transactions and expected peak periods to ensure continued system performance c) Secure configuration and hardening of critical servers. d) Secure key storage in hardware encrypted security modules. e) Anti-DOS measures are application and network layer to protect token services.

DFS provider	a) Enforce information security policies and processes requiring identification and remediation of vulnerabilities in servers and applications. b) Deploy malware detection and prevention measures. c) Deploy fraud detection and prevention for high-risk functions such as change of account profile, wallet account enrolment and payment transactions. d) Inbound internet traffic should be limited and continuously monitored e) Set restrictive firewall rules by default, use ports whitelisting, f) Use of packet filters and continuously monitor access to whitelisted/permitted ports and IP's.
Third Party (Merchants, Acquirers, Payment Service Providers)	a) Deploy and configure firewalls. b) Restrict POI and POS access to authorized users. c) Secure by-default design. d) Vulnerability testing e) Enforce high security standard measures for payment processing systems and second factor authentication (2FA) for user authentication/access. f) Require digital signatures to sign and verify payment authorizations.

3.5.6 System Implementation

Fundamental in the implementation of the proposed Blockchain-based payment system was the use of elliptic curve public-key encryption and signature scheme. Cryptography is the transformation of plain message to a different form that secure and immune from intruders. Elliptic Curve Cryptography (ECC) is an independently developed public key cryptography by Victor Miller and Neal Koblitz [106]. This study adopted Equations 2,3,4 and 5 as outlined by D. Hankerson et al [107] as essential components in the algorithms used in the proposed system.

An elliptic curve E is defined by an equation over a field K

$$\boldsymbol{E: y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6} \quad (2)$$

Where a_1, a_2, a_3, a_4, $a_6 \in K$ and $\Delta \neq 0$, where Δ is the discriminant of E and is defined as follows:

$$\Delta = -d\frac{2}{2}d_8 - 8d\frac{3}{4} - 27d\frac{2}{6} + 9d_2d_4d_6$$

$$d_2 = a\frac{2}{1} + 4a_2 \tag{3}$$

$$d_4 = 2a_4 + a_1a_3$$

$$d_6 = a\frac{2}{3} + 4a_6$$

$$d_8 = a\frac{2}{1}a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a\frac{2}{3} - a\frac{2}{4}$$

If L is any extension field of *K*, then the set of *L*-rational points on *E* is

$$E(L) = \{(x, y) \in L\ x\ L : y^2 + a_1xy + a_3y - x^3 - a_2x^2 - a_4x - a_6 = 0\} \cup \{\infty\} \tag{4}$$

Where ∞ is the point at infinity.

For the generation of the key pair, this study utilized equation 5.

$$\langle P \rangle = \{\infty, P, 2P, 3P, \ldots, (n-1)P\} \tag{5}$$

Let *E* define an elliptic curve over a finite field F_p. Let *P* be a point in $E(\mathrm{F}_p)$ and assume *P* has prime order *n*. The cyclic subgroup of $E(\mathrm{F}_p)$ generated by *P* is equation 5.

Where prime *p*, the equation of the elliptic curve *E* and the point *P* and its order *n*, are the public domain parameters. A private key is an integer *d* that is generated randomly from the interval [1, *n*-1] and the respective public key is $Q = dP$

Elliptic curve key pair generation used in the proposed system can be represented as follows;

INPUT: Elliptic curve domain parameters (*p*, *E*, *P*, *n*)

OUTPUT: Public key Q and private key d

1. Select $d \in_R [1, n-1]$
2. Compute $Q = dP$
3. Return (Q, d)

For the encryption scheme in this study, the authors adopted the following algorithm;

INPUT: Plain transactional data denoted as m, public key Q and elliptic curve domain parameters (p, E, P, n).

OUTPUT: Ciphertext (C_1, C_2)

1. Represent the plain transactional data m as a point M in $E(\mathrm{F}_p)$
2. Select $k \in_R [1, n-1]$
3. Compute $C_1 = kP$
4. Compute $C_2 = M + kQ$
5. Return (C_1, C_2)
6. Transmit C_1 and C_2

Plain transactional data denoted m is first represented as point M, then encrypted by adding it to kQ where k is a randomly selected integer and Q is the public key of the intended recipient of the plain transactional data. The sender transmits the points $C_1 = kP$ and $C_2 = M + kQ$ to the recipient.

For the decryption scheme in this study, the authors adopted the following algorithm;

INPUT: Ciphertext (C_1, C_2), private key d, and elliptic curve domain parameters (p, E, P, n).

OUT: Plain transactional data denoted as m

1. Compute $dC_1 = d(kP) = k(dP) = kQ$
2. Compute $M = C_2 - dC_1$
3. Extract m from M
4. Return (m)

The recipient uses his/her private key d to compute $dC_1 = d(kP) = k(dP) = kQ$ and thereafter recovers $M = C_2 - dC_1$

A prototype of the proposed Blockchain-based mobile payment system was implemented. Implementation is the realization of the proposed Blockchain mobile payment system. The implementation stage of software development is the process of converting design specification to an executable software system. The Blockchain mobile payment system was implemented using the following technology stack;

a) Flutter 2.0.0
b) Node.js 12.18.1
c) Express.js 4.17.1
d) HTML
e) Bootstrap 4
f) Angular JS 1.6
g) MySQL

Postman 7.1.2 and GitHub were the development tools used while IntelliJ IDEA 2018.3.2 was the integrated development environment that was utilised in the implementation of the prototype.

3.5.6.1 Blockchain API

A RESTful API using Express.js, which is a web framework for Node.js was implemented. JavaScript was the programming language, was used to implement the API, while IntelliJ IDEA was the integrated development environment tool used to build the API. The API used JSON as the data-interchange format. Postman was used to test the API. Furthermore, postman was used to view the various responses from the endpoints of the API. The completed API was hosted on Ubuntu 18.04 LTS powered virtual server provisioned from Amazon Web Services. At the core of the API, the Blockchain was implemented using JavaScript.

3.5.6.2 Mobile Application

An Android-based and iOS-based e-wallet mobile application was implemented using Flutter which is a tool used to build a native cross-platform (Android and iOS) application with one programming language and codebase. The user interface (UI), business and application logic were implemented using dart as the programming language. Overall, the mobile application was developed using IntelliJ IDEA as the development tool. The mobile wallet application was installed on an Android device running Android Marshmallow for testing purposes.

3.6 Chapter Summary

This chapter presented the baseline study's variables, study site, sample size as well as data collection tools and data collection technique. A conceptual model and corresponding hypotheses were presented. Furthermore, the chapter described the functional and non-functional requirements and various design specifications of the proposed Blockchain-based mobile payment system.

CHAPTER FOUR

RESULTS

4.1 Introduction

This chapter presents the survey results from 182 respondents. The results in this chapter were obtained from the data analysis done in SPSS 25 and Excel (MS Office 2016) statistical packages using descriptive and inferential statistics facilities therein. Furthermore, the results of system implementation and testing are highlighted in this chapter.

4.2 Descriptive Statistics

4.2.1 Demographics

This section displays results on the demographic profile of respondents. This study had a total 182 respondents.

4.2.1.1 Gender Distribution

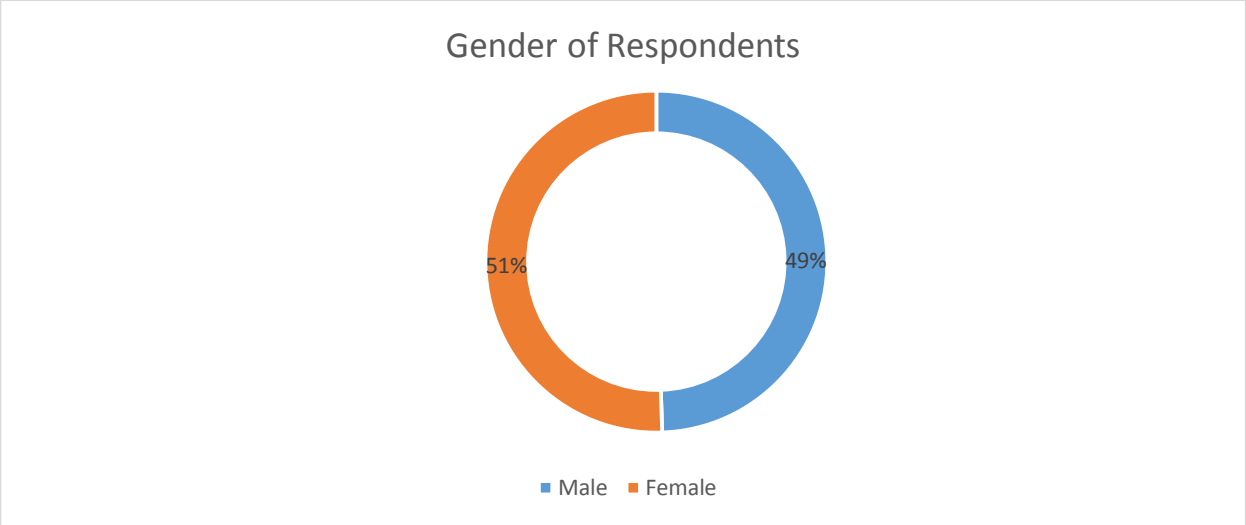


Figure 4.1. Gender of Respondents

Figure 4.1 shows the gender of the respondents sampled for the study. 51% (n=92) of the respondents who made up the majority were females, while 49% (n=90) were males.

4.2.1.2 Age of Respondents

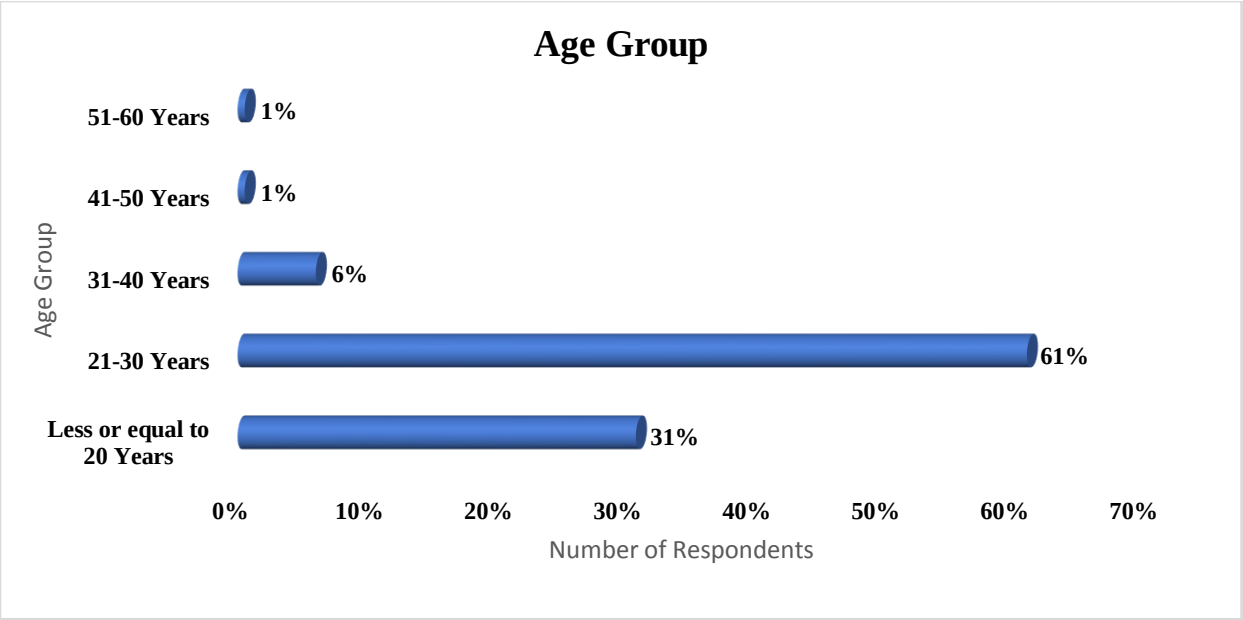


Figure 4.2. Age of Respondents

Figure 4.2 shows the age group distribution of the study's respondents. 31% (n=56) of the respondents were in the age group of less or equal to 20 years, 61% (n=111) who made the majority were in the age group of 21-30 years, 6% (n=11) were in the age group of 31-40 years, 1% (n=2) were in the age group 41-50 years and the other 1% (n=2) belonged to the age group of 51-60 years.

4.2.1.3 Respondents' Marital Status

Table 4.1. Respondent's Marital Status

Marital Status		
	Percent	**Frequency**
Single	91%	165
Married	9%	17
Total	**100%**	**182**

Table 4.1 shows the marital status of the study's respondents. 91% (n=165) of the respondents who made the majority were single, while 9% (n=17) of the respondents were married.

4.2.1.4 Highest Level of Education Attained

Table 4.2. Highest Level of Education Attained

Highest Level of Education Attained		
	Percent	**Frequency**
Certificate	62%	112
Diploma	14%	26
Degree	7%	12
Master's Degree	17%	31
Missing Response	1%	1
Total	**100%**	**182**

Table 4.2 indicates the highest level of education attained by the study's respondents. 62% (n=112) of the respondents who made the majority had attained an education level of up to certificate level, 14% (n=26) attained an education level of up to diploma level, 7% (12) had attained an education level of up to degree level, 17% (n=31) attained an education level of up to master's degree, while 1% (n=1) of the respondents did not indicate the highest level of education they had attained.

4.2.1.5 Current Level of Education Being Attained

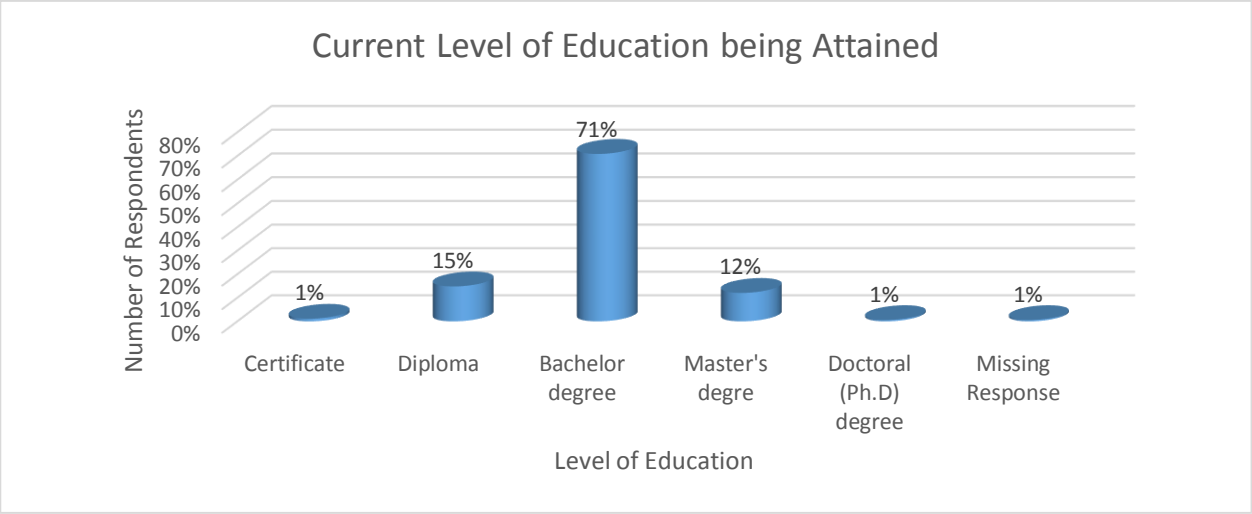


Figure 4.3. Current Level of Education being attained by Respondents

Figure 4.3 indicates the current level of education being attained by the study's respondents. 1% (n=2) of the sampled respondents were pursuing their studies at a Certificate level, 15% (n=27) were pursuing their studies at Diploma level, 71% (n=129) who made the majority were pursuing

their studies at Bachelor's degree level, 12% (n=22) were pursuing their studies at Master's degree level, 1% (n=1) were pursuing their studies at Doctoral (PhD) degree level, while the other 1% (n=1) did not indicate the level of studies they were pursuing.

4.2.1.6 ICT Knowledge and Experience

This section displays results on the respondents' knowledge in ICT, together with their experience in usage of the same.

4.2.1.7 Description of Knowledge or Skill in ICT usage

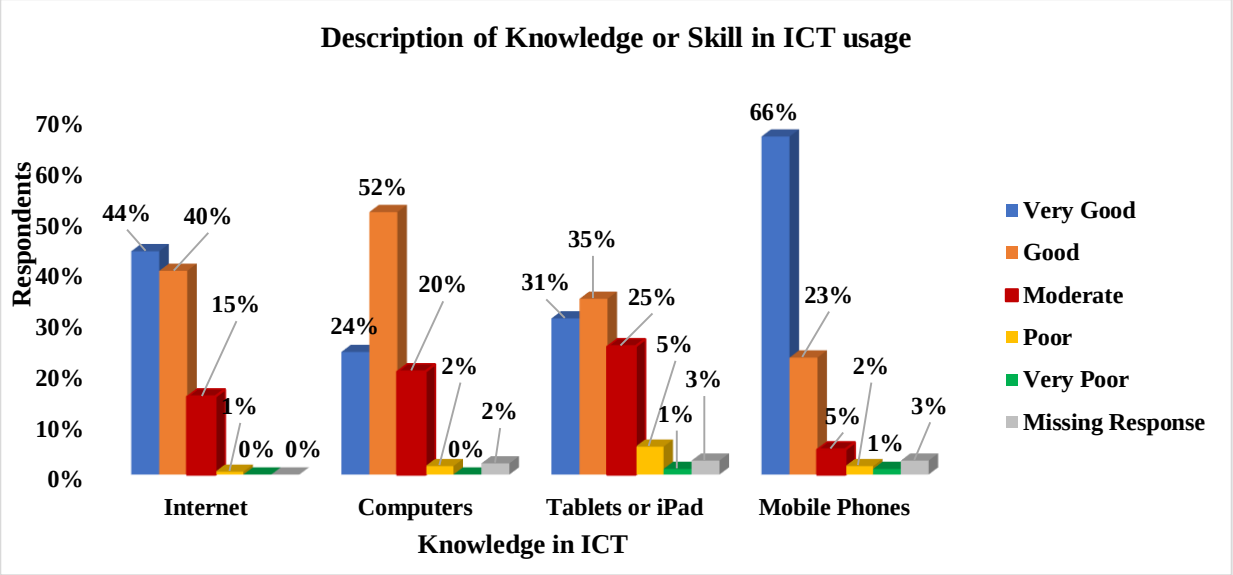


Figure 4.4. Description of Knowledge or Skill in ICT

Figure 4.4 shows the respondents' description of their knowledge in ICT and their skills in utilisation of the same.

Concerning knowledge and skills using the internet, most of the respondents represented by 44% (n=80) stated that their knowledge and skills in internet usage were very good, 40% (n=73) stated that it was good, 15% (n=28) stated that it was moderate, while the other 1% (n=1) stated that it was poor.

Concerning knowledge and skills using computers, 24% (n=44) of the respondents stated that their knowledge and skills in computer usage was very good, with the majority of them represented by 52% (n=94) stating that their knowledge and skills in computer usage was good, 20% (n=37) stated that they had moderate knowledge and skills in computer usage, where 2% (n=3) stated that their knowledge and skills in computer usage was poor and the other 2% (n=4) did not describe how knowledgeable and skilful they were in computer usage.

Concerning knowledge and skills using tablets/iPads, it can be observed from Figure 4.4 that 31% (n=56) stated that their knowledge and skills in the usage of tablets/iPads was very good, 35% (n=63) who made the majority possessed very good knowledge and skills in using tables/iPads, 25% (n=46) possessed moderate knowledge and skills in the same, 5% (n=10) had poor knowledge and skills in tablet/iPad usage, 1% (n=1) had very poor knowledge and skills in utilisation of the same, while the other 3% (n=5) did not state how knowledgeable or skilful they were in utilizing tablets/iPads.

The research as well sought to establish whether the respondents possessed any knowledge and skills on the usage of mobile phones. Figure 4.4 shows that most of the respondents represented by 66% (n=121) stated that their knowledge and skills in utilisation of mobile phones was very good, 23% (n=42) stated that their knowledge and skills in utilisation of the same was good, 5% (n=9) stated that their knowledge and skills in utilisation of the same was moderate, with 2% (n=3) of the respondents stating that their knowledge and skills in using the same was poor, 1% (=2) of the respondents stated that their knowledge and skills in utilisation of a mobile phone was very poor, while 3% (n=5) did not state how knowledgeable or skilful they were in utilisation of the same.

4.2.1.8 Period of Using ICT

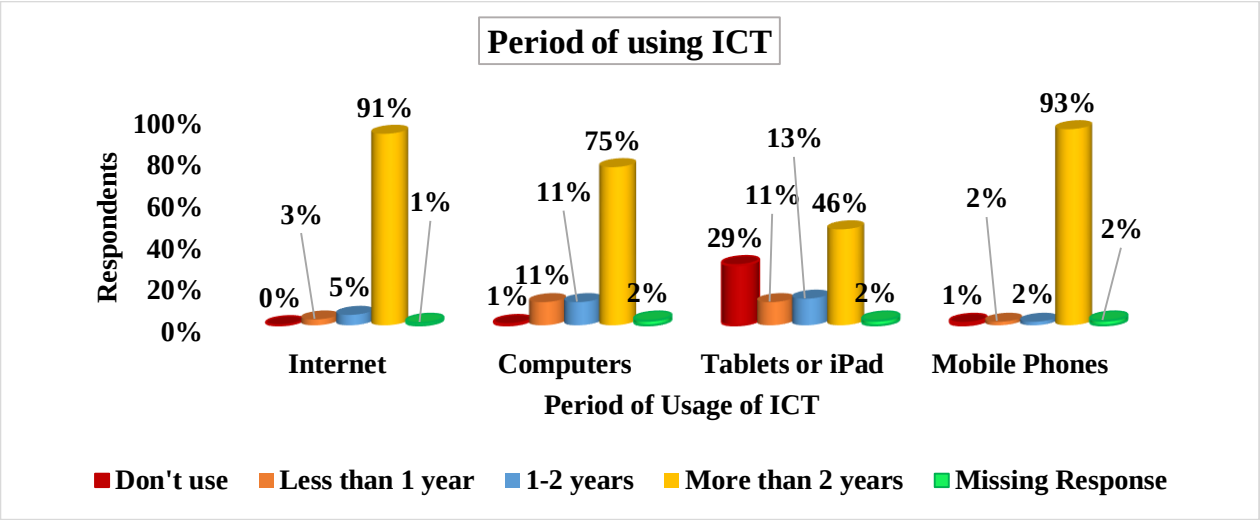


Figure 4.5. Period of Using ICT

Figure 4.5 shows the period of time of which the sampled respondents had been using the stated ICT.

Figure 4.5 shows that 3% (n=5) of the respondents had been using the Internet for a period of less than 1 year, 5% (n=9) had been using the Internet for a period of between 1 to 2 years, most of the respondents represented by 91% (n=166) stated that they had been using the internet for a period of more than 2 years, while only 1% (n=2) of the respondents never stated the period of which they had been using the Internet.

Figure 4.5 illustrates that 1% (n=1) of the sampled respondents do not use computers, 11% (n=20) had been using computers for a period of less than one year, another 11% (n=20) had been using computers for a period of between 1 to 2 years, with the majority of respondents represented by 75% (n=137) had been using computers for more than two years, only 2% (n=4) of the respondents never stated the period of which they had been using computers.

Figure 4.5 shows that 29% (n=52) of the respondents did not use tablets or iPad, 11% (n=20) had used the gadgets for less than 1 year, 13% (n=23) had used the gadgets for a period of 1 to 2 years,

46% (n=83) who were the majority had used the gadgets for more than 2 years, while only 2% (n=4) of the respondents never stated the period of which they had been using the gadgets.

Figure 4.5 illustrates that 1% (n=2) of the respondents do not use mobile phones, 2% (n=3) had been using mobile phones for a period of less than 1 year, another 2% (n=3) of the respondents had been using mobile phones for a period of 1 to 2 years, most of the respondents represented by 93% (n=170) had been using their mobile phone for a period of more than 2 years, while only 2% (n=4) of the respondents never stated the period that they had been using mobile phones.

4.2.1.9 Frequency of Using Mobile Phones for Carrying Out Selected Tasks

Table 4.3. Frequency of using mobile phones for carrying out selected tasks

Frequency of using mobile phones for carrying out tasks								
	Checking Account Balances		**Viewing Bank Statements**		**Receiving Money from family or friends**		**Sending money to family or friends**	
	Percent	**Frequency**	**Percent**	**Frequency**	**Percent**	**Frequency**	**Percent**	**Frequency**
Always	43%	78	17%	31	36%	65	32%	59
Often	26%	47	19%	34	32%	58	24%	43
Sometimes	13%	24	26%	48	24%	43	29%	52
Rarely	13%	23	20%	36	7%	12	10%	18
Never	4%	8	16%	29	1%	2	3%	6
Missing Response	1%	2	2%	4	1%	2	2%	4
Total	**100%**	**182**	**100%**	**182**	**100%**	**182**	**100%**	**182**

Table 4.3 shows the frequency of using mobile phones by respondents when carrying out the specified tasks.

Table 4.3 shows that 43% (n=78) of the respondents who were the majority stated that they always used their mobile phone for checking their bank account balance, 26% (n=47) stated that they often used them for the same, 13% (n=24) stated that they sometimes use their mobile phone when checking for their account balance, another 13% (n=23) stated that they rarely used their mobile phone when doing the same, 4% (n=8) stated that they never used their mobile phone when

checking their account balance, while only 1% (n=2) never stated their frequency of using the phone whenever they wanted to check their account balance.

Table 4.3 shows that 17% (n=31) stated that they always used their mobile phone for viewing their bank statement, 19% (n=34) stated that they often used them for the same, 26% (n=48) of respondents who made the majority stated that they sometimes used their mobile phone when viewing their bank statement, 20% (n=36) stated that they rarely used their mobile phone when doing the same, 16% (n=29) stated that they never used their mobile phone when viewing their bank statements, while only 2% (n=4) never stated their frequency of using their mobile phone whenever they wanted to view their bank statement.

Table 4.3 illustrates that 36% (n=65) who were the majority stated that they always used a mobile phone when receiving money by means of electronic transfers, 32% (n=58) stated that they often used their mobile phone for receiving electronic money, 24% (n=43) of the respondents stated that they sometimes also used their mobile phone for the same purpose as the others, 7% (n=12) respondents rarely used their mobile phone for receiving money sent through the electronic money transfer platforms, while 1% (n=2) of the respondents never used a mobile phone as a medium of receiving money, with the other 1% (n=2) not stating whether they had at any point used a mobile phone to receive money or not.

Table 4.3 shows that the majority of the respondents represented by 32% (n=59) stated that they always used their mobile phone for sending funds, 24% (n=43) of the respondents stated that they often used their mobile phone for the purpose of sending money, 29% (n=52) also did in some instances use their mobile phone as a medium of sending money to someone, 10% (n=18) rarely used their mobile phone in order to send money to someone, 3% (n=6) of the respondents never used a mobile phone to send money to others, with only 2% (n=4) not stating whether they used their mobile phone when sending funds to someone.

4.2.2 Key Payment Systems Used by Students

The following figures reveal the payment systems used by students in higher learning institutions when paying mandatory academic obligations.

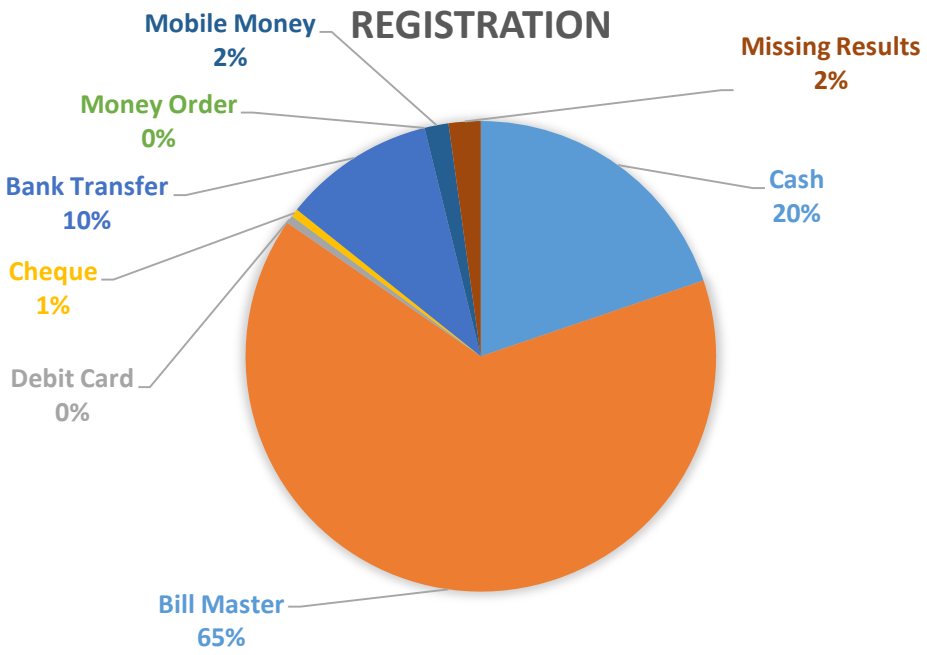


Figure 4.6. Payment Systems for Registration

The payment systems utilized by students to pay for registration are depicted in Figure 4.6. 20% (n=36) used cash, 65% (n=118) who were the majority used bill muster, 1% (n=1) used the debit card, another 1% (n=1) used a cheque, 10% (n=19) used bank transfers, no respondent 0% (n=0) used the money order platform, 2% (n=3) used mobile money method, with 2% (n=4) of the respondents not responding to the question.

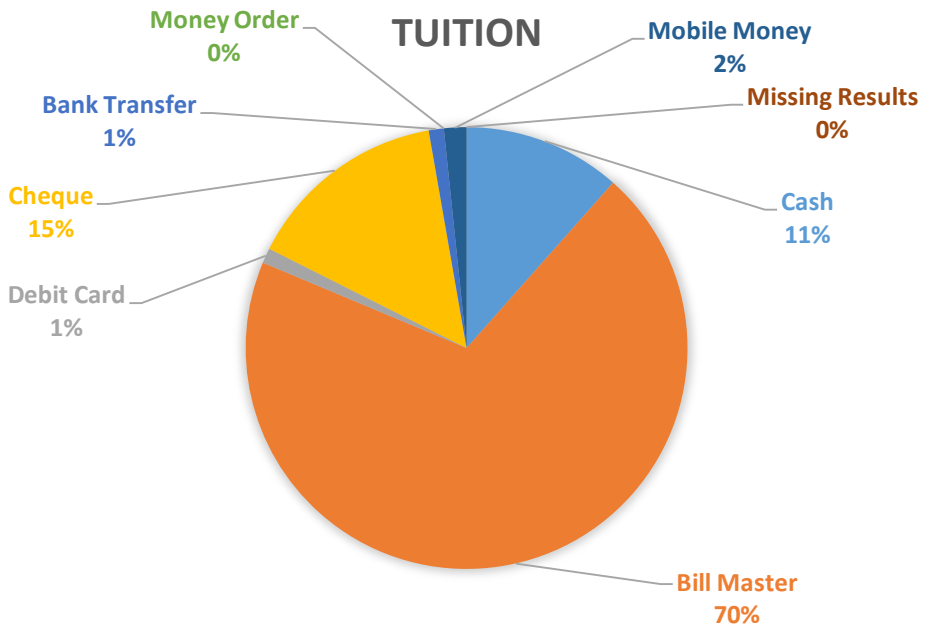


Figure 4.8. Payment Systems for Tuition Fees

Figure 4.8 illustrates the payment systems used by students to pay for tuition fees. 11% (n=21) used cash, 70% (n=127) who were the majority used bill muster, 1% (n=1) used a debit card, 15% (n=27) used a cheque, 1% (n=2) used bank transfers, no respondent (0%, n=0) used the money order method, while 2% (n=3) used mobile money method.

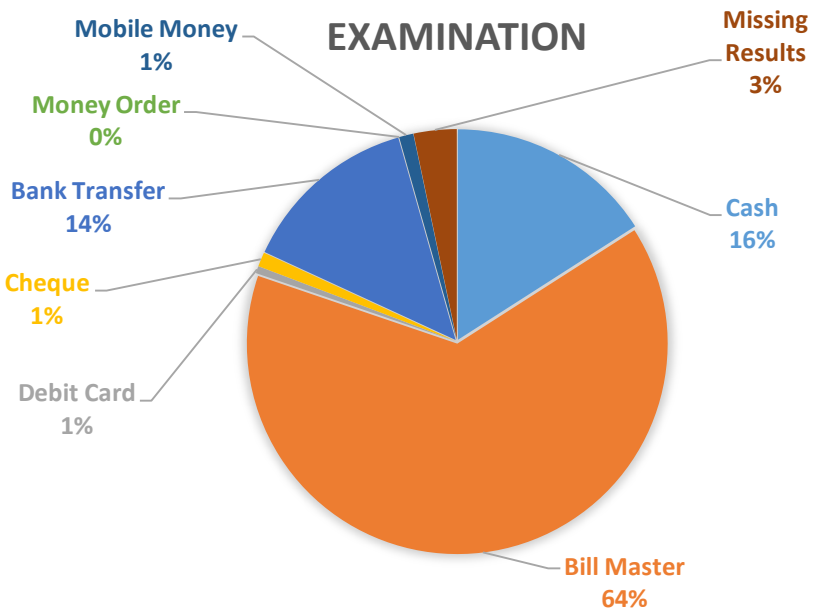


Figure 4.7. Payment Systems for Examination Fees

The payment systems utilized by students to pay for examination costs are depicted in Figure 4.7. 16% (n=29) used cash, 64% (n=117) who were the majority used bill muster, 1% (n=1) used a debit card, another 1% (n=2) used a cheque, 14% (n=25) used bank transfers, no respondent (0%, n=0) used the money order method, 1% (n=2) used mobile money method, whereas 5% (n=9) did not respond to the question.

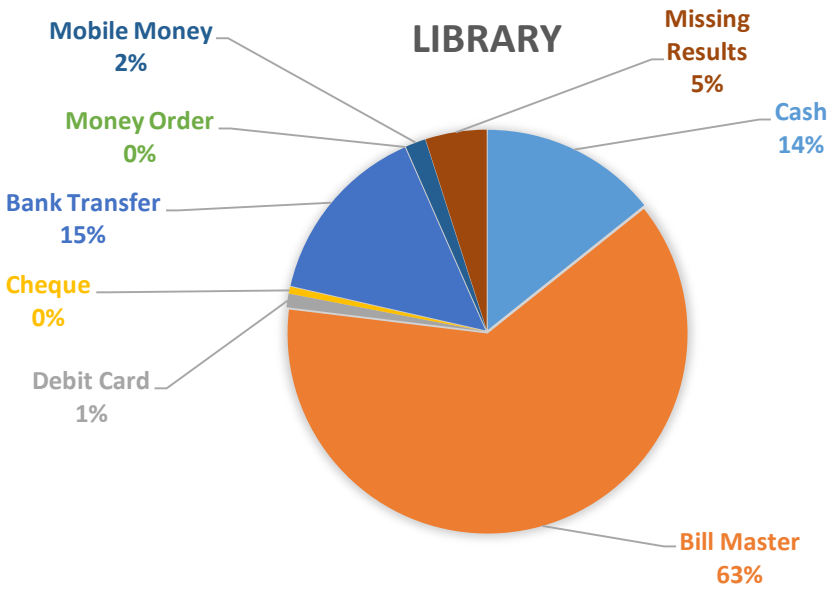


Figure 4.9. Payment Systems for Library Fees

Students pay library fees in a variety of ways as shown in Figure 4.9. 14% (n=26) used cash, 63% (n=114) who were the majority used bill muster, 1% (n=1) used a debit card, another 1% (n=2) used a cheque, 15% (n=27) used bank transfers, no respondent (0%, n=0) used the money order method, 2% (n=3) used mobile money method, while 5% (n=9) did not respond to the question

4.2.3 Challenges Faced by Students

The following figures demonstrate the challenges faced by students when using the current payment systems.

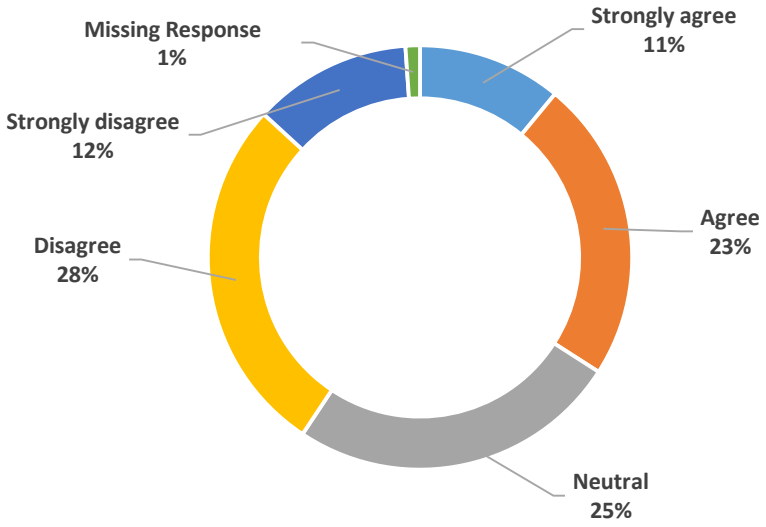


Figure 4.10 Distribution of Designated Banks

Figure 4.10 illustrates the assertion by students of whether banks designated by higher institutions of learning were evenly distributed in rural and urban areas. 12% (n=20) strongly agreed to the claim that the designated banks were evenly distributed in both rural and urban areas, 23% (n=42) agreed to the same, 25% (n=46) maintained a neutral position on the same, 28% (n=50) who were the majority disagreed to the claim, 12% (n=22) strongly disagreed with the assertion, while the other 1% (n=2) did not respond to the question.

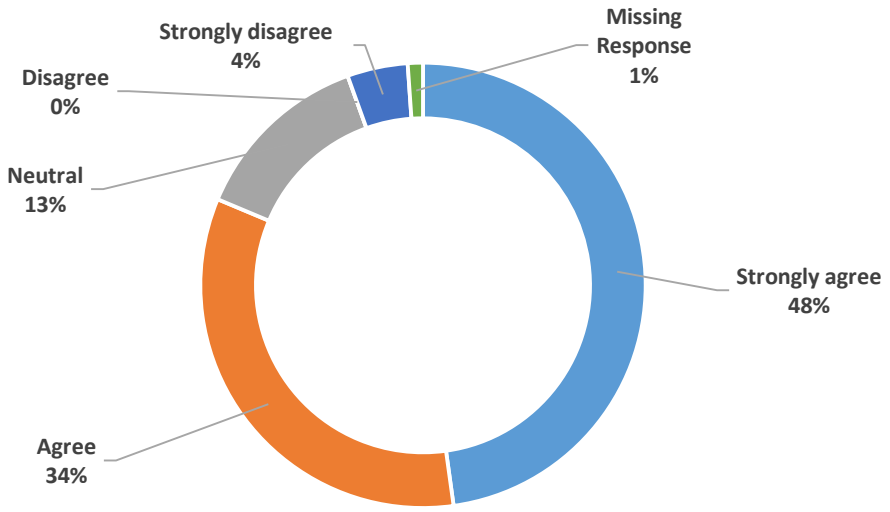


Figure 4.11. Long Queues and Overcrowding in Banks

Figure 4.11 demonstrates the conviction by students that designated banks were characterized by long unbearable queues. 48% (n=87) who were the majority strongly agreed to the assertion, 34% (n=61) agreed to the same, 13% (n=24) maintained a neutral position on the same, 4% (n=8) disagreed to the assertion, while the other 1% (n=2) did not respond to the question.

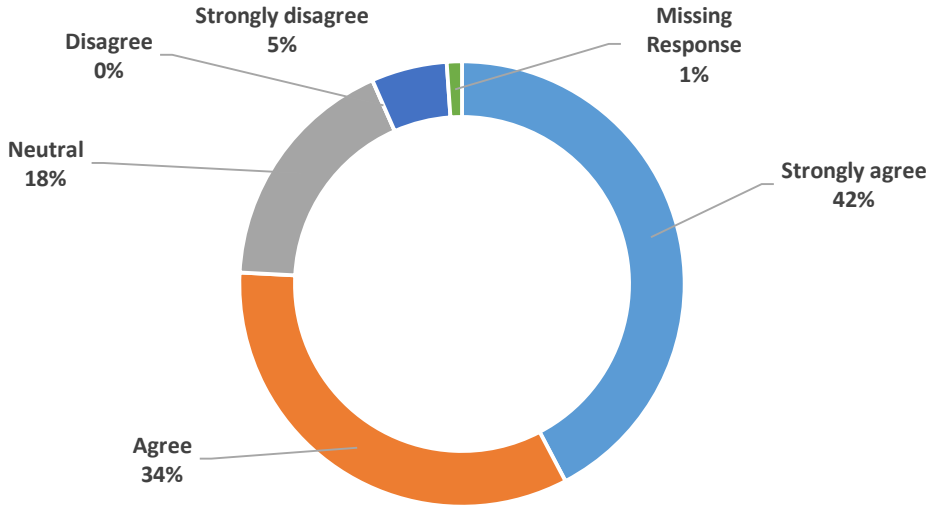


Figure 4.12. Loss of Time in Banks

Figure 4.12 depicts the affirmation by students that designated banks are characterized by unbearable loss of time whilst waiting to be attended to. 42% (n=77) who made the majority strongly agreed to the claim, 34% (n=61) agreed to the same, 18% (n=32) maintained a neutral position on the same, 5% (n=10) disagreed to the claim, whereas the other 1% (n=2) did not respond to the question.

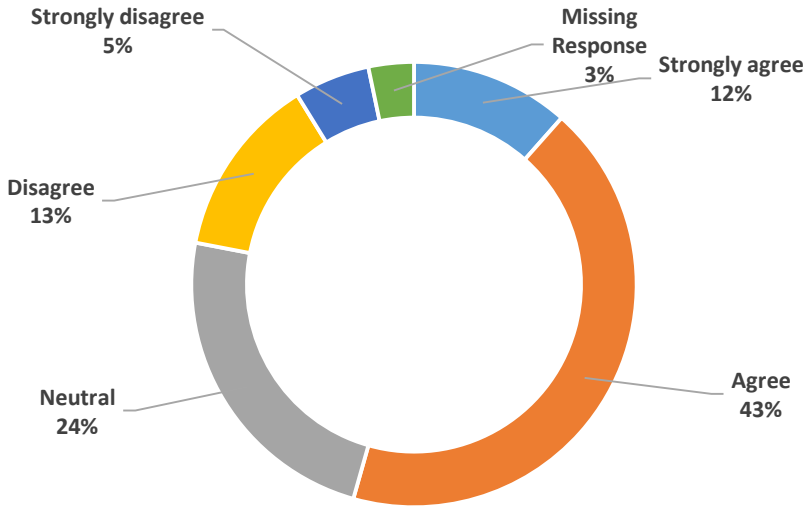


Figure 4.13. Theft or Abuse of Student Information

Figure 4.13 illustrates students' strong belief that there was a risk of abuse or theft of personally identifiable information. 12% (n=21) of the respondents strongly agreed to the assertion, 43% (n=78) who were the majority also agreed to the assertion, 24% (n=43) had a neutral position, 13% (n=24) of the respondents disagreed to the assertion, 5% (n=10) strongly disagreed to the assertion, while the other 3% (n=6) did not state their position.

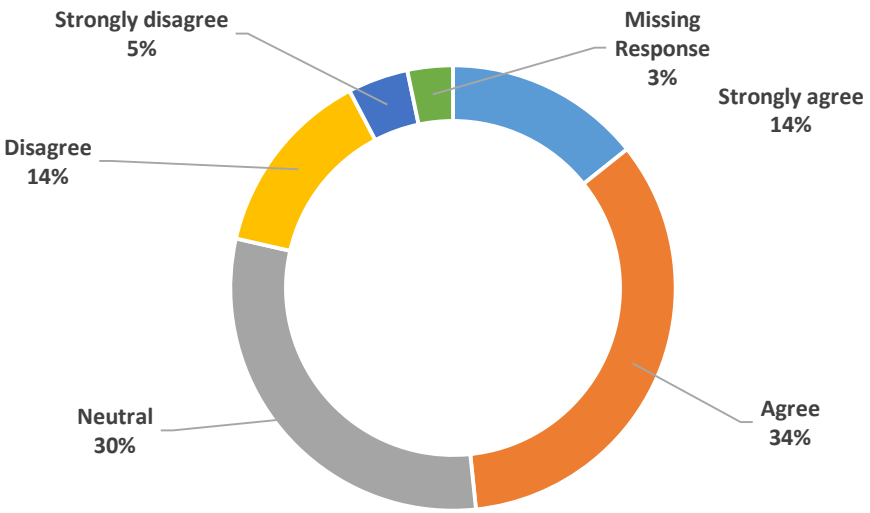


Figure 4.14. Theft or Abuse of Payment Information

`.

4.2.4 Perceived Usefulness

4.2.4.1 Usefulness of Mobile Wallets

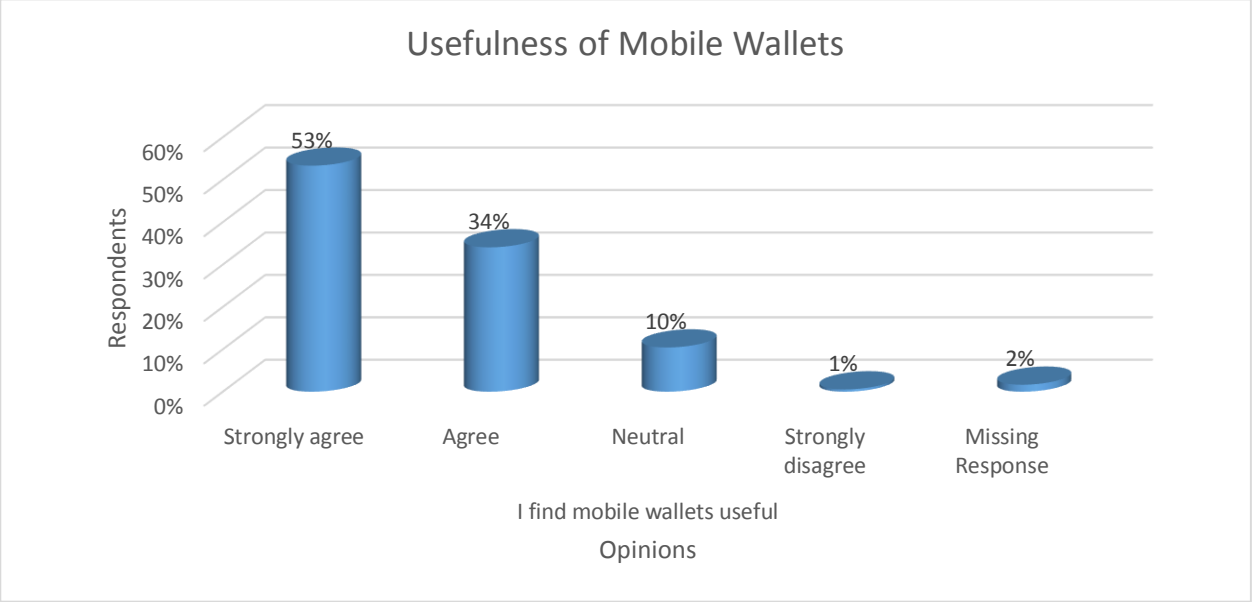


Figure 4.15. Usefulness of Mobile Wallets

Figure 4.15 shows whether the respondents found the utilisation of mobile wallets as being useful or not. Most of the responded represented by 53% (n=97) strongly agreed to finding utilisation of mobile wallet as being useful to them, 34% (n=62) agreed to the same, 10% (n=19) had a neutral position on the same, 1% (n=1) strongly disagreed to finding mobile wallets useful to them, while 2% (n=3) never gave a response on their position.

4.2.4.1 Mobile Payment System Usage and Its Potential Influence on Enhancing Effectiveness in Making Payments

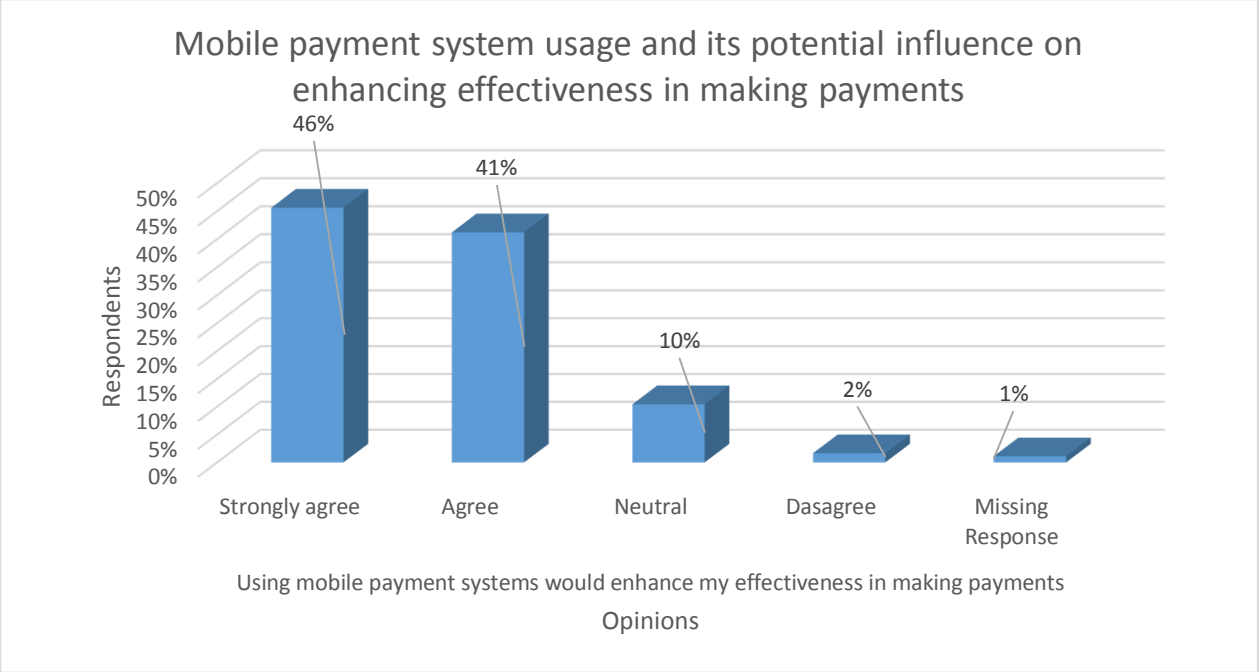


Figure 4.16. Mobile payment system usage and its potential influence on enhancing effectiveness in making payments

Figure 4.16 shows whether the respondents were of the view that using mobile payment systems would enhance their effectiveness in making payments or not. 46% (n=83) of the respondents who made the majority strongly agreed to the assertion that using mobile payment systems would enhance their effectiveness in making payments, 41% (n=75) agreed to the same, 10% (n=19) had a neutral position on the same, 2% (n=3) strongly disagreed to the assertion, whereas 1% (n=2) never gave a response on their position.

4.2.4.2 Usage of Mobile Payment Systems and Its Potential Ease to the Respondents' Ability to Manage and Facilitate Various Payments

Table 4.4 shows whether the respondents were of the view that using mobile payment systems would make it easier for them to manage and make payments.

Table 4.4. Usage of mobile payment systems and its potential ease to the respondents' ability to manage and facilitate various payments

Usage of mobile payment systems and its potential ease the respondents' ability to manage and facilitate various payments			
Assertion	**Response**	**Percent**	**Frequency**
Using mobile payment systems would make it easier for me to manage and make payments	Strongly agree	58%	105
	Agree	34%	61
	Neutral	6%	11
	Disagree	2%	4
	Missing Response	1%	1
	Total	100%	182

When respondents were questioned on whether using mobile payment systems would make it easier for them to manage and make various payments, 58% (n=105) of the respondents who made the majority strongly agreed to the assertion that using mobile payment systems would make it easier for them to manage and make various payments, 34% (n=61) agreed to the same, 6% (n=11) had a neutral position on the same, 2% (n=4) strongly disagreed to the assertion, whereas 1% (n=2) of the respondents never gave a response on their position.

4.2.5 Perceived Ease of Use

4.2.5.1 Ease of Registration for a Mobile Wallet

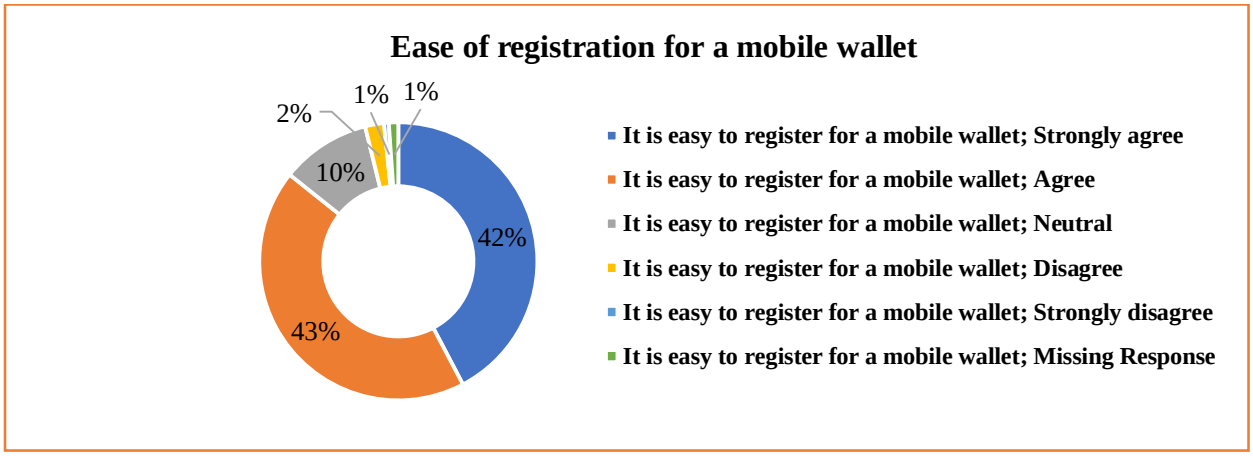


Figure 4.17. Ease of registration for a mobile wallet

Figure 4.17 shows the view that respondents had with regards to the ease of registration for a mobile wallet account. Most of the respondents 43% (n=79) agreed to the assertion that it was easy

for them to register for a mobile wallet account, 42% (n=77) disagreed to the assertion, 10% (n=19) had a neutral position, 2% (n=4) disagreed to the assertion, 1% (n=1) strongly disagreed to the same, while the other 1% (n=1) did not state their position.

4.2.5.2 Ease of Facilitating Transactions When Using Mobile Wallet

Table 4.5. Ease of facilitating transactions when using mobile wallet

Ease of facilitating transactions when using mobile wallet			
Assertion	**Response**	**Percent**	**Frequency**
It is easy to carry out transactions using a mobile wallet (start and finish transaction)	Strongly agree	43%	79
	Agree	40%	73
	Neutral	13%	23
	Disagree	2%	4
	Strongly disagree	1%	2
	Missing Response	1%	1
	Total	**100%**	**182**

Table 4.5 shows the view that respondents had on the ease of facilitating transactions when using mobile wallets. Most of the respondents 43% (n=79) agreed to the assertion that it was easy for them to carry out transactions using a mobile wallet (start and finish transactions), 40% (n=73) agreed to the assertion, 13% (n=23) had a neutral position, 2% (n=4) disagreed to the assertion, 1% (n=2) strongly disagreed to the same, while the other 1% (n=1) did not state their position.

4.2.5.3 Few Steps Required When Carrying Out Transactions

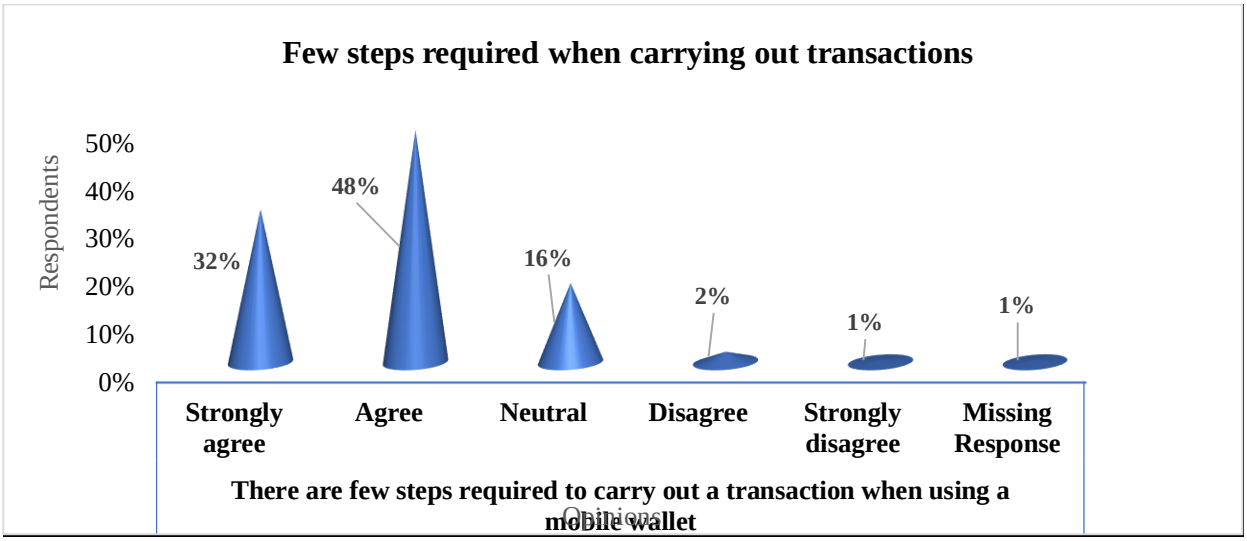


Figure 4.18. Few steps required when carrying out transactions using mobile wallets

Figure 4.18 shows whether respondents were in agreement with the assertion that there were few steps required for one to carry out a transaction. 32% (n=58) of the respondents strongly agreed to the assertion that there were few steps required to carry out a transaction when using a mobile wallet, most of the respondents 48% (n=88) agreed to the assertion, 16% (n=30) had a neutral position on the same, 2% (n=4) disagreed to the assertion, 1% (n=1) of the respondents strongly disagreed to the assertion, while the other 1% (n=1) did not state their position.

4.2.5.4 Ease of Error Reversal When Using Mobile Wallets

Table 4.6. Ease of Error Reversal when using mobile wallets

Ease of error reversal when using mobile wallets			
Assertion	**Response**	**Percent**	**Frequency**
Errors can be easily reversed when using mobile wallets	Strongly agree	13%	24
	Agree	22%	40
	Neutral	36%	66
	Disagree	21%	39
	Strongly disagree	5%	9
	Missing Response	2%	4
	Total	**100%**	**182**

Table 4.6 shows whether respondents were of the view that errors could be easily reversed when using a mobile wallet. 13% (n=24) of the respondents strongly agreed that errors could easily be reversed when using mobile wallets, 22% (n=40) agreed to the same assertion, 36% (n=66) who were the majority had a neutral position on the same, 21% (n=39) disagreed to the assertion, 5% (n=9) strongly disagreed to the assertion, whereas the other 2% (n=4) did not state their position.

4.2.5.5 Respondents' Take on How Clear and Understandable Interactions Involving Mobile Wallets' Operations

Table 4.7. Respondents' take on how clear and understandable interactions involving mobile wallets' operations

Respondents' comprehension of mobile wallets' operations			
Assertion	**Response**	**Percent**	**Frequency**
Interactions with mobile wallet is clear and understandable	Strongly agree	25%	46
	Agree	44%	80
	Neutral	24%	43
	Disagree	4%	8
	Strongly disagree	2%	3
	Missing Response	1%	2
	Total	**100%**	**182**

Table 4.7 shows whether respondents were of view that interactions with mobile wallets were clear and understandable. 25% (n=46) of the respondents strongly agreed to the assertion that interactions involving mobile wallets' operations were clear and understandable, 44% (n=80) who were the majority agreed to the same assertion, 24% (n=43) had a neutral position on the same, 4% (n=8) disagreed to the assertion, 2% (n=3) strongly disagreed to the assertion, while the other 1% (n=2) did not state their position.

4.2.6 Perceived Costs

4.2.6.1 Fairness of Registration Fee for Opening a Mobile Wallet Account

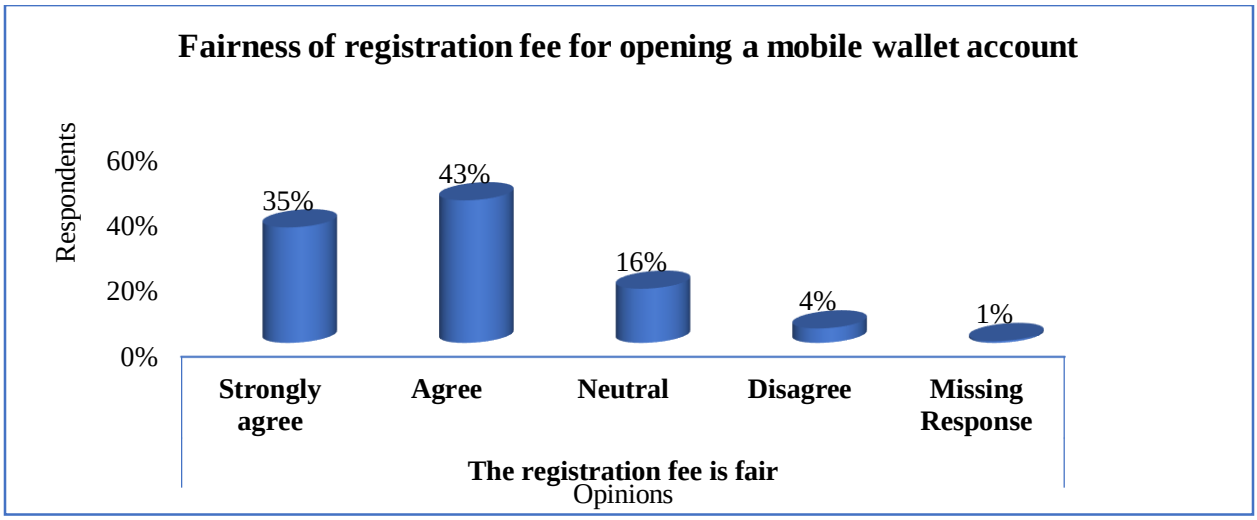


Figure 4.19. Fairness of registration fee for opening a mobile wallet account

Figure 4.19 shows whether the fees for opening a mobile wallet account by the respondents were fair or not. 35% (n=64) of the respondents strongly agreed to the assertion that the registration fee for opening a mobile wallet account was fair, 43% (n=79) who were the majority also agreed to the same, 16% (n=30) had a neutral position on the same, 4% (n=8) of the respondents disagreed to the assertion, whereas the other 1% (n=1) did not state their position.

4.2.6.2 Fairness of Transaction Cost for Using a Mobile e-Wallet

Table 4.8. Fairness of transaction cost for using a mobile e-wallet

Fairness of transaction cost for using a mobile e-wallet			
Assertion	**Response**	**Percent**	**Frequency**
The transaction cost is fair	Strongly agree	22%	40
	Agree	38%	70
	Neutral	29%	53
	Disagree	9%	17
	Strongly disagree	1%	1
	Missing Response	1%	1
	Total	**100%**	**182**

Table 4.8 shows whether the transaction cost for using a mobile e-wallet was fair or not. 22% (n=40) of the respondents strongly agreed to the assertion that the transaction cost for using a mobile e-wallet was fair, 38% (n=70) who were the majority also agreed to the same, 29% (n=53) had a neutral position on the same, 9% (n=17) of the respondents disagreed to the assertion, 1% (1) strongly disagreed to the assertion, while the other 1% (n=1) did not state their position.

4.2.6.3 Emotional or Physical Harm Emanating from Mobile Wallets Usage

Table 4.9. Emotional or physical harm emanating from mobile wallet usage

Emotional or physical harm emanating from using mobile wallet usage			
Assertion	**Response**	**Percent**	**Frequency**
There is no emotional or physical harm when using a mobile wallet	Strongly agree	29%	52
	Agree	37%	68
	Neutral	25%	45
	Disagree	7%	13
	Strongly disagree	1%	2
	Missing Response	1%	2
	Total	**100%**	**182**

Table 4.9 shows whether respondents experienced any emotional or physical harm due to usage of mobile wallets. 29% (n=52) of the respondents strongly agreed to the assertion that there is no emotional or physical harm when using a mobile wallet, 37% (n=68) who were the majority agreed to the assertion, 25% (n=45) had a neutral position on the same, 7% (n=13) of the respondents disagreed to the assertion, 1% (n=1) strongly disagreed to the assertion, whereas the other 1% (n=1) did not state their position.

4.2.7 Social Influence

4.2.7.1 Social Status Stemming from Using Mobile Wallet

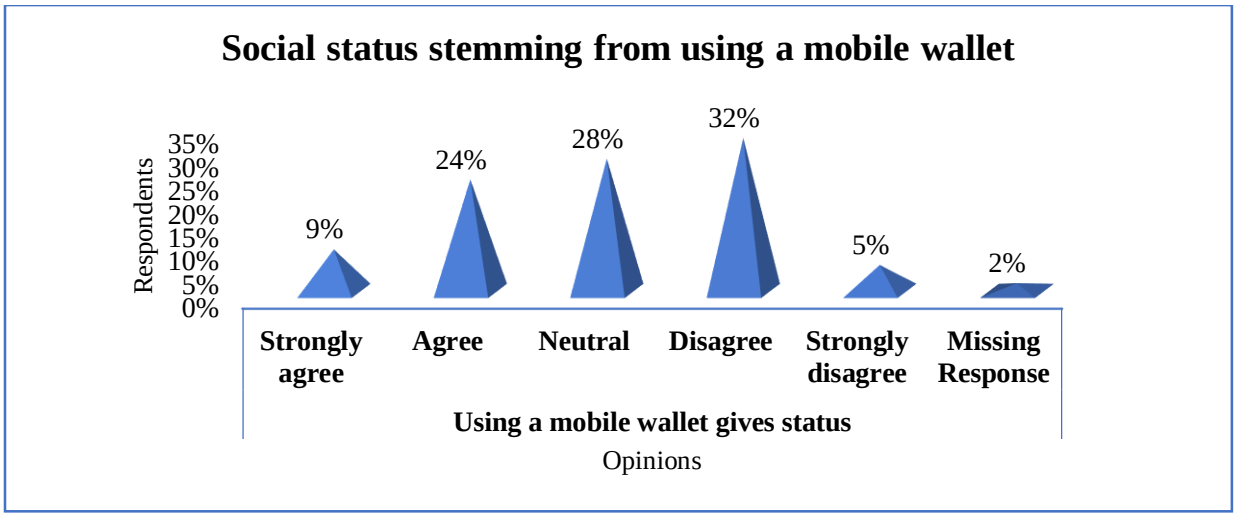


Figure 4.20. Social status stemming from using a mobile wallet

Figure 4.20 shows whether the respondents were of the view that using a mobile wallet gave them some higher social status or not. 9% (n=16) of the respondents strongly agreed to the assertion that using a mobile wallet gave them a higher social status, 24% (n=43) agreed to the stated assertion, 28% (n=51) had a neutral position on the same, 32% (n=59) who made the majority disagreed to the assertion, 5% (n=10) strongly disagreed to the same, while the other 2% (n=4) did not state their position.

4.2.7.2 Improvement in Social Interaction and Usage of Mobile Wallet

Table 4.10. Improvement in Social Interaction and Usage of Mobile Wallet

Improvement in Social Interaction and Usage of Mobile Wallet			
Assertion	**Response**	**Percent**	**Frequency**
Using a mobile wallet improves social interaction	Strongly agree	14%	26
	Agree	31%	56
	Neutral	28%	51
	Disagree	19%	35
	Strongly disagree	5%	10
	Missing Response	2%	4
	Total	**100%**	**182**

Table 4.10 shows whether respondents were in agreement with the assertion that using a mobile wallet improved social interactions or not. 14% (n=26) of the respondents strongly agreed to the assertion that using a mobile wallet improved social interactions, 31% (n=56) who were the majority agreed to the stated assertion, 28% (n=51) had a neutral position on the same, 19% (n=35) disagreed to the assertion, 5% (n=10) strongly disagreed to the same, while the other 2% (n=4) did not state their position.

4.2.7.3 Fashion and Usage of Mobile Wallets

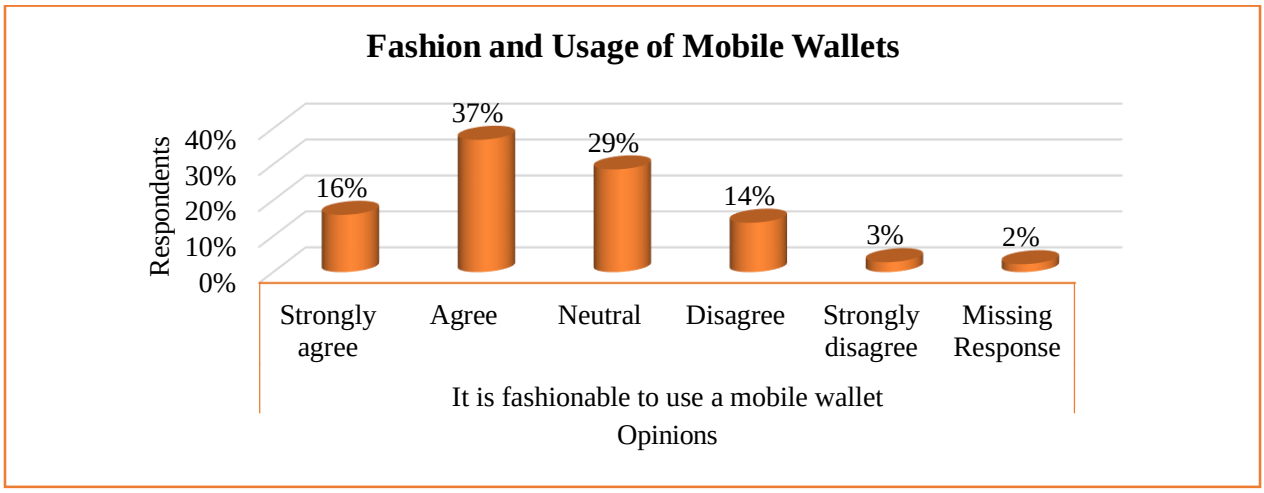


Figure 4.21. Fashion and Usage of Mobile Wallets

Figure 4.21 shows whether respondents agreed to the assertion that it was fashionable to use mobile wallets. 16% (n=29) of the respondents strongly agreed to the assertion that using a mobile wallet was fashionable, 37% (n=67) who were the majority also agreed to the sentiments of the assertion, 29% (n=52) had a neutral position on the same, 14% (n=25) of the respondents disagreed to the assertion, 3% (n=5) strongly disagreed to the assertion, while the other 2% (n=4) did not state their position.

4.2.7.4 Usage of Mobile Wallets by the Respondents' Peers and Family Members

Table 4.11. Usage of mobile wallets by the respondents' peers and family members

Usage of mobile wallets by the respondents' peers and/or family members			
Assertion	**Response**	**Percent**	**Frequency**
Mobile wallets are used by my peers (classmates or friends) and family members	Strongly agree	37%	68
	Agree	41%	75
	Neutral	10%	19
	Disagree	6%	11
	Strongly disagree	3%	6
	Missing Response	2%	3
	Total	**100%**	**182**

Table 4.11 shows whether the respondents agreed to the assertion that mobile wallets were also being used by their peers and family members. 37% (n=68) of the respondents agreed to the assertion that mobile wallets were being used by their peers and/or family members, 41% (n=75) who were the majority also agreed to the assertion, 10% (n=19) had a neutral position on the same, 6% (n=11) of the respondents disagreed to the assertion, 3% (n=6) strongly disagreed to the assertion, while the other 2% (n=2) did not state their position.

4.2.8 Perceived Risk

4.2.8.1 Risk of Abuse or Theft of Users' Information during Usage of Mobile Wallets

Table 4.12. Risk of abuse or theft of users' information during usage of mobile wallets

Risk of abuse or theft of users' information during usage of mobile wallets			
Assertion	**Response**	**Percent**	**Frequency**
The risk of abuse or theft of users' information (e.g., name of user, NRC, payment amount) is high when using mobile payment service	Strongly agree	12%	21
	Agree	43%	78
	Neutral	24%	43
	Disagree	13%	24
	Strongly disagree	5%	10
	Missing Response	3%	6
	Total	**100%**	**182**

Table 4.12 shows whether respondents agreed with the assertion that the risk of abuse or theft of users' information was high when using mobile payment services. 12% (n=21) of the respondents

strongly agreed to the assertion, 43% (n=78) who were the majority also agreed to the assertion, 24% (n=43) had a neutral position, 13% (n=24) of the respondents disagreed to the assertion, 5% (n=10) strongly disagreed to the assertion, while the other 3% (n=6) did not state their position.

4.2.8.2 Risk of Abuse or Theft of Billing Information during Usage of Mobile Wallets

Table 4.13. Risk of abuse or theft of billing information during usage of mobile wallets

Risk of abuse or theft of billing information during usage of mobile wallets			
Assertion	**Response**	**Percent**	**Frequency**
The risk of abuse or theft of billing information (e.g., credit card number, bank account data) is high when using mobile payment services	Strongly agree	14%	26
	Agree	34%	62
	Neutral	30%	55
	Disagree	14%	25
	Strongly disagree	4%	8
	Missing Response	3%	6
	Total	**100%**	**182**

Table 4.13 shows whether respondents agreed with the assertion that the risk of abuse or theft of the billing information was high when using mobile payment services. 14% (n=21) of the respondents strongly agreed to the assertion, 34% (n=62) who were the majority also agreed to the assertion, 30% (n=55) had a neutral position on the same, 14% (n=25) of the respondents disagreed to the assertion, 5% (n=8) strongly disagreed to the claim of the assertion, while the other 3% (n=6) did not state their position.

4.2.9 Perceived Trust

4.2.9.1 Trustworthiness of the Service Provider

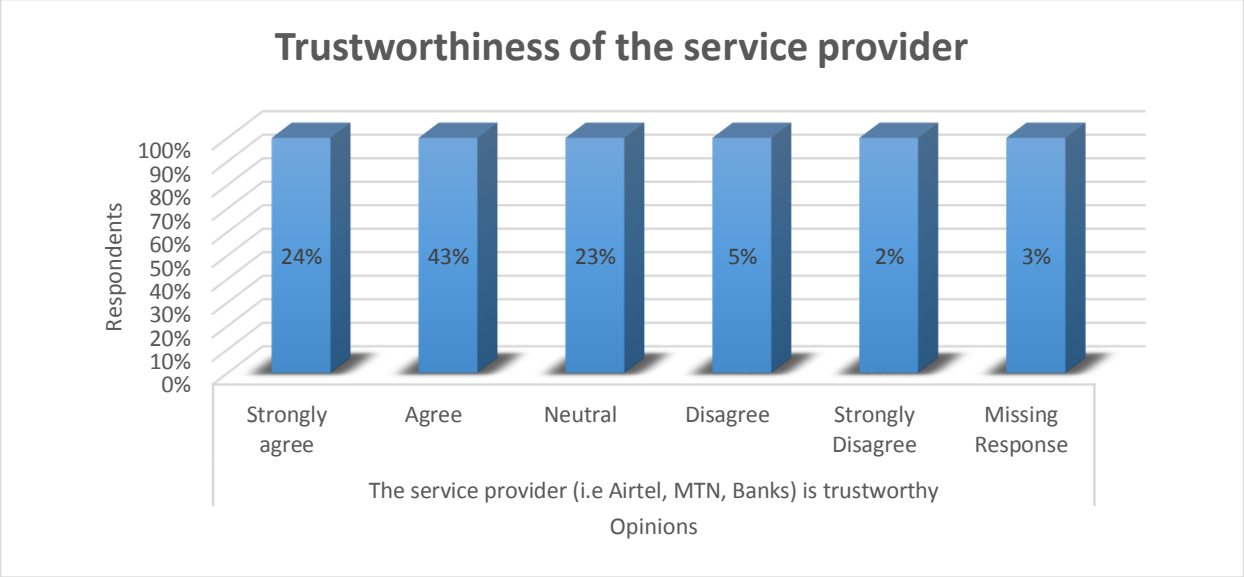


Figure 4.22. Trustworthiness of the Service Provider

Figure 4.22 reveals whether or not the respondents trusted their service providers. 24% (n=21) of the respondents agreed to the assertion that their service providers (Airtel, MTN, Banks) were trustworthy, 43% (n=78) who were the majority also agreed to the assertion, 23% (n=42) had a neutral position on the same, 5% (n=9) of the respondents disagreed to the assertion, 2% (n=3) strongly disagreed to the claim of assertion, while the other 3% (n=6) did not state their position.

4.2.9.2 Refunding of Wrong Transaction

Table 4.14. Refunding of Wrong Transaction by Service Provider

Refunding of wrong transactions by service provider			
Assertion	**Response**	**Percent**	**Frequency**
Wrong transactions can be easily refunded	Strongly agree	10%	19
	Agree	16%	29
	Neutral	38%	69
	Disagree	26%	47
	Strongly disagree	5%	9
	Missing Response	5%	9
	Total	**100%**	**182**

Table 4.14 shows whether the respondents agreed to the assertion that wrong transactions were easily refunded by their service providers. 10% (n=19) of the respondents strongly agreed to the assertion that their service providers were quick to reimburse incorrect transactions, 16% (n=29) agreed to the same assertion, 38% (n=69) who made the majority took a neutral position by neither agreeing nor denying to the assumption of the assertion, 26% (n=47) disagreed to the same, 5% (n=9) strongly agreed to the assertion, with another 5% (n=9) did not respond to the question.

4.2.9.3 Cashing of Transaction by Respondent

Table 4.15. Cashing of Transaction by Respondent

Cashing of Transaction by Respondent			
Assertion	**Response**	**Percent**	**Frequency**
	Strongly agree	26%	48
Whenever a transaction is directed to me, no one else can accept/cash it other than myself	Agree	40%	73
	Neutral	16%	30
	Disagree	13%	23
	Strongly agree	1%	2
	Missing Response	3%	6
	Total	**100%**	**182**

Table 4.15 reveals whether or not the respondents agreed to the assertion that whenever a transaction was directed to them, no one else could accept/cash it other than themselves. 26% (n=48) of the respondents strongly agreed to the assertion that whenever a transaction was directed at the respondent, no one else could accept/cash it other than themselves, 40% (n=73) who were the majority respondents agreed to the same assertion, 16% (n=30) took a neutral position by neither agreeing nor denying the assumption of the assertion, 13% (n=23) disagreed to the same, 1% (n=2) strongly disagreed to the assertion, with 3% (n=6) of the respondents did not respond to the question.

4.2.9.4 Privacy Concerns Arising from the Usage of Mobile Wallets

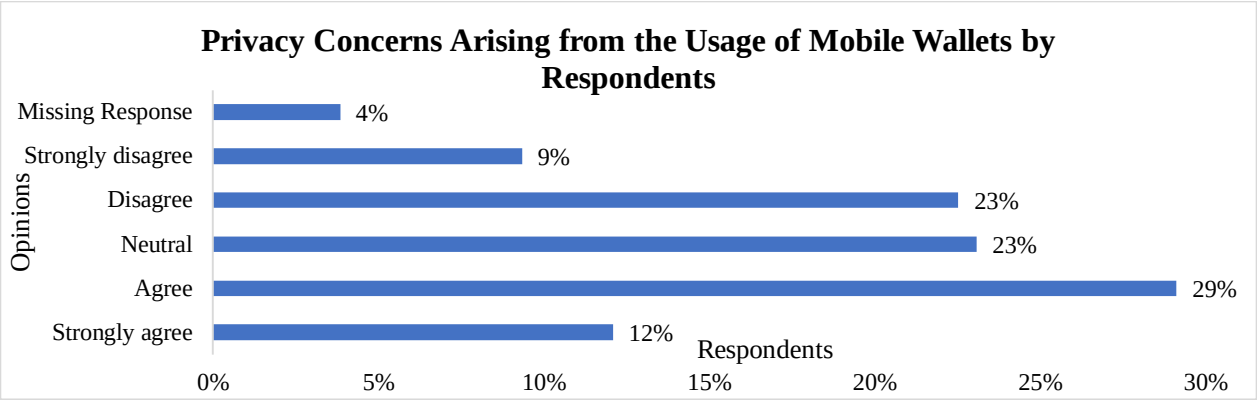


Figure 4.23. Privacy concerns arising from the usage of mobile wallets by respondents

Figure 4.23 shows whether or not the respondents agreed to the assertion that they had no privacy concerns that arose from using mobile wallets. 12% (n=22) of the respondents strongly agreed to the assertion that there were no privacy concerns that arose from using mobile wallets, 29% (n=53) who were the majority agreed to the same assertion, 23% (n=42) took a neutral position, 23% (n=42) disagreed to the assertion, 9% (n=17) strongly disagreed to the assertion and 4% (n=6) of the respondents did not respond to the question.

4.2.9.5 Trustworthiness of Mobile Payment Systems

Table 4.16. Trustworthiness of Mobile Payment Systems

Trustworthiness of Mobile Payment Systems			
Assertion	**Response**	**Percent**	**Frequency**
I trust mobile payment systems as being secure	Strongly agree	18%	32
	Agree	38%	70
	Neutral	29%	52
	Disagree	9%	17
	Strongly disagree	3%	5
	Missing Response	3%	6
	Total	**100%**	**182**

Table 4.16 shows if the respondents agreed with the assertion that mobile payment systems were secure. 18% (n=32) of the respondents strongly agreed to the assertion that they trusted the mobile payment systems as being secure, 38% (n=70) who were the majority agreed to the same assertion,

29% (n=52) took a neutral position by neither agreeing nor denying the assumption of the assertion, 9% (n=17) disagreed to the assertion, 3% (n=5) strongly disagreed to the assertion and 3% (n=6) of the respondents did not respond to the question.

4.2.10 Expectancy

4.2.10.1 Mobile Payment Systems as an Avenue for Paying Tuition and Other Fees in Higher Learning Institutions

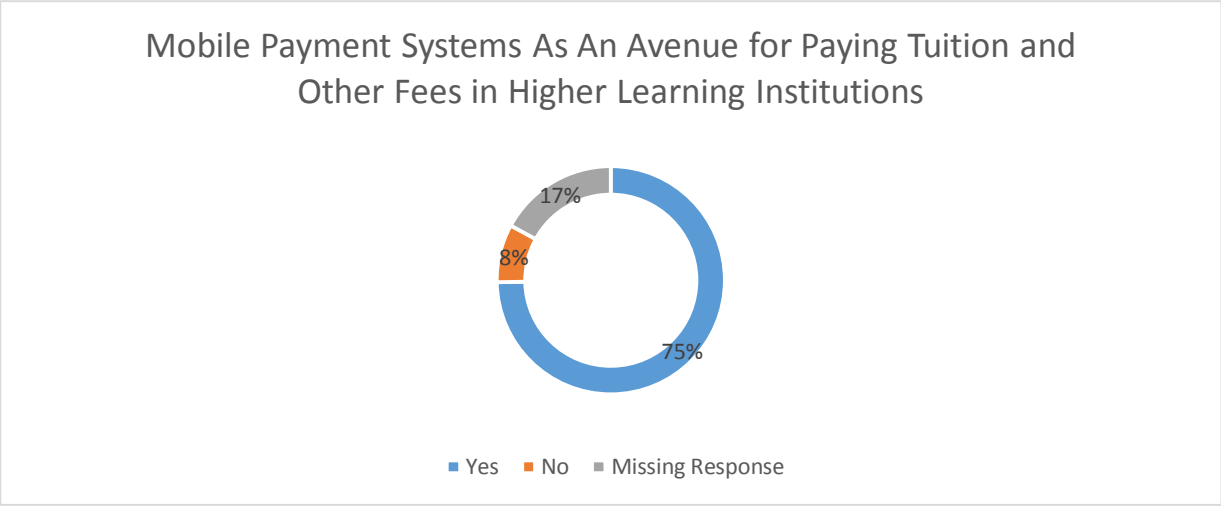


Figure 4.24. Mobile payment system as an avenue for paying tuition and other fees in Higher learning institutions

Figure 4.24 shows whether respondents believed that mobile payment systems should be used to pay tuition and other expenses at higher education institutions. Most of the respondents represented by 75% (n=136) agreed to the usage of mobile payment systems in higher learning institutions when paying tuition and other fees, 8% (n=15) disagreed, while the other 17% (n=31) did not respond to the question.

4.3 Inference Statistics

In order to test the research's hypotheses ($H_0 1, H_0 2, H_0 3, H_0 4, H_0 5, H_0 6$ and $H_0 7$), the Multinomial Logistic Regression Likelihood Tests model was run so as to investigate the

relationship among the variables. The results in Table 4.17 shows the estimation of the effect that the independent variables had on the dependent variable.

Table 4.17. Multinomial Logistic Regression's Likelihood Ratio Test Results

Dependent Variable: Utilisation of mobile e-wallets by respondents					
Method: Multinomial Logistic Regression's Likelihood Ratio Tests					
Sample Size: 182 respondents					
Independent Variables: I. Mobile wallets are useful (perceived usefulness) II. Easy to carry out transactions using mobile wallets (perceived ease of use); III. Transaction costs on mobile wallets are fair IV. Mobile wallets are used by most of my peers (social norm) V. Risk of abuse or theft of user's information when using e-wallets (perceived risk) VI. Gender of respondent VII. Age group					
Effect	**Model Fitting Criteria – 2 Log Likelihood of Reduced Model**	**Likelihood Ratio Tests**			
		Chi-Square	**df**	**Sig.**	**Result**
Intercept	124.262[a]	.000	0	.	
Perceived Usefulness (Mobile wallets are useful)	132.325	8.062	4	.089	$H_0$1 rejected
Perceived Ease of Use (Easy to execute transactions using mobile wallets)	134.417	10.155	4	.038	$H_0$2 accepted
Perceived Cost (Transaction costs incurred from mobile wallet usage are fair)	129.295	5.032	4	.284	$H_0$3 rejected
Social Norm (Mobile wallets are used by most of my peers)	130.977	6.715	4	.152	$H_0$4 rejected
Perceived Risk (Risk of abuse or theft of user's information when using mobile wallets)	127.597	3.335	4	.503	$H_0$5 rejected
Gender of Respondent	137.770	13.508	4	.009	$H_0$6 accepted
Age Group	140.534	16.271	16	.434	$H_0$7 rejected

Table 4.17 shows the findings of the Multinomial Logistic Regression Estimator Model. The interpretations of the findings are stated below.

4.3.1 Multinomial Logistic Regression Likelihood Tests Results Analysis

4.3.1.1 Usefulness of Mobile e-Wallets (Perceived Usefulness)

At a 5% level of significance, the null hypothesis($H_0 1$), which stated that "usefulness of e-wallets does not influence the adoption of e-wallets by students" was not rejected. This is because the probability value (0.089) for the relationship between the variable "mobile e-wallets are useful" and the variable "utilisation of mobile e-wallets" was greater than 0.05. This meant that the research (alternative) hypothesis (usefulness of e-wallet influences the adoption of mobile e-wallets by students) was not accepted.

4.3.1.2 Ease of Use of Mobile e-Wallets (Perceived Ease of Use)

At a 5% level of significance, the null hypothesis($H_0 2$), which stated that "ease of carrying out transactions using mobile e-wallets does not influence the adoption of e-wallets by students" was rejected. This is because the probability value (0.038) for the relationship between the variable "easy to carry out transactions using mobile wallets" and the variable "utilisation of mobile e-wallets" was less than 0.05. This meant that the research (alternative) hypothesis (ease of carrying out transactions using mobile e-wallets influences the adoption of mobile e-wallets by students) was accepted.

4.3.1.3 Transaction Cost Incurred When Using Mobile e-Wallets (Perceived Cost)

At a 5% level of significance, the null hypothesis($H_0 3$), which stated that "transaction cost incurred when using mobile e-wallets does not influence the adoption of mobile e-wallets by students" was not rejected. This is because the probability value (0.284) for the relationship between the variable "transaction cost incurred from mobile wallet usage are fair" and the variable "utilisation of mobile e-wallets" was greater than 0.05. This meant that the research (alternative) hypothesis (transaction cost incurred when using mobile e-wallets does influence the adoption of mobile e-wallets by students) was not accepted.

4.3.1.4 Utilisation of Mobile e-Wallets Is Trending (Social Norm)

At a 5% level of significance, the null hypothesis($H_0 4$), which stated that "the current social norm of mobile e-wallet usage does not influence the adoption of mobile e-wallets by students" was not rejected. This is because the probability value (0.152) for the relationship between the variable "mobile e-wallets are used by most of my peers in my social circle" and the variable "utilisation of mobile e-wallets" was greater than 0.05. This meant that the research (alternative) hypothesis (the current social norm of mobile e-wallet usage does influence the adoption of mobile e-wallets by students) was not accepted.

4.3.1.5 Perceived Risk Associated with Mobile e-Wallet Utilisation

At a 5% level of significance, the null hypothesis($H_0 5$), which stated that "perceived risk associated with mobile e-wallet usage does not influence the adoption of e-wallets by students" was not rejected. This is because the probability value (0.503) for the relationship between the variable "risk of abuse or theft of user's information when using mobile e-wallets" and the variable "utilisation of mobile e-wallets" was greater than 0.05. This meant that the research (alternative) hypothesis (perceived risk associated with mobile e-wallet usage does influence the adoption of mobile e-wallets by students) was not accepted.

4.3.1.6 Effect of Gender on Users' Utilisation of Mobile e-Wallets

At a 5% level of significance, the null hypothesis($H_0 6$), which stated that "gender does not influence the adoption of mobile e-wallets by students" was rejected. This is because the probability value (0.009) for the relationship between the variable "gender of respondent (e-wallet user)" and the variable "utilisation of mobile e-wallets" was less than 0.05. This meant that the research (alternative) hypothesis (gender does influence the adoption of mobile e-wallets by students) was accepted.

4.3.1.7 Effect of Age on Users' Utilisation of Mobile e-Wallets

At a 5% level of significance, the null hypothesis($H_0 7$), which stated that " age does not influence the adoption of mobile e-wallets by students" was not rejected. This is because the probability

value (0.434) for the relationship between the variable "age of respondent (age of e-wallet user)" and the variable "utilisation of mobile e-wallets" was less than 0.05. This meant that the research (alternative) hypothesis (age does influence the adoption of mobile e-wallets by students) was not accepted.

4.3.2 Model Stability Test

The Deviance and Pearson chi-square Goodness of Fit tests were used to determine whether the parameters of the Multinomial Regression Model were stable. These tests are important for determining whether a model fits the data or not. Non-significant test results are indicators that the model fits the data.

Table 4.18. Model Stability Test

Goodness-of-Fit			
	Chi-Square	**df**	**Sig.**
Pearson	139.793	284	1.000
Deviance	95.587	284	1.000

Table 4.18 indicate that the model fits the data well. This is because the P-values for both Pearson Chi-Square test (1.00) and the Deviance Chi- Square test (1.00) was greater than 0.05, thus indicating non-significant results at a 5% level of significance.

4.4 System Implementation Results

4.4.1 Blockchain API

The RESTful API was the communication and data sharing mechanism between the numerous nodes and mobile e-wallet application. Authentication between the RESTful API and e-wallet mobile application was achieved using JSON Web Tokens. The token was generated and signed by the API when a user of the e-wallet mobile application signed up. The JSON Web Token was used by the mobile application as an authentication token when fetching and sending data to the endpoints of the API. Figure 4.25 shows an overview of the client server communication the API.

The API leveraged the inherent characteristics of Blockchain technologies as the core component.

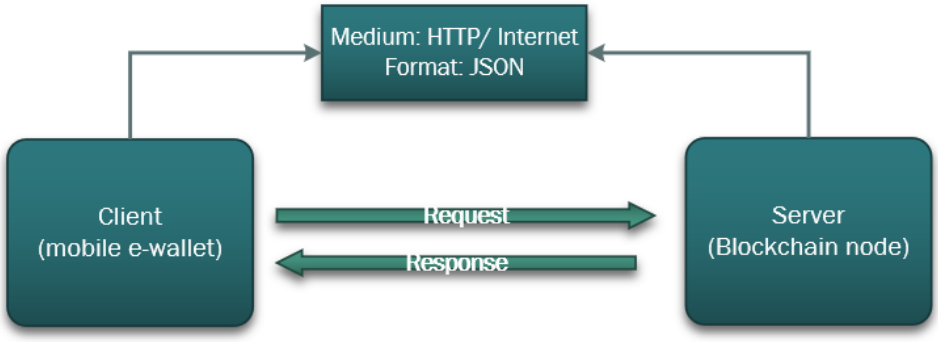


Figure 4.25. Client Server Communication

Blockchain was the underlying technology and data structure of the API. Figure 4.26 shows the JSON formatted output obtained from consuming one the API's endpoint using postman.

```
[
    {
        "timestamp": 1606461234754,
        "lastHash": "00000000000000000000000",
        "hash": "00b9924970ed999a43683c51cbda978f6a26c9e82c1e30c5d382c610c1bc5d71",
        "nonce": 0,
        "difficulty": 3,
        "data": []
    },
    {
        "timestamp": 1606461354922,
        "lastHash": "00b9924970ed999a43683c51cbda978f6a26c9e82c1e30c5d382c610c1bc5d71",
        "hash": "00a143df520611bbb56946d7e3978f8d65d1f249d68fe87e475c69643bb8c074",
        "nonce": 350,
        "difficulty": 2,
        "data": [
            {
                "id": "576f6f40-3080-11eb-8314-57fc37925ba4",
                "input": {
                    "timestamp": 1606461334582,
                    "sender_public_key": "0450ac88b4b69709c412ddc9ac7d4b05957697f114ca64c5d3d6f828a3b383c7054b066e9ab20afcdf01060ee887aa13a9e496c865a1e97d9e7743d0bc59268b5d",
                    "signature": "82ac15cdef3cb5c00d7c4a4c9f3ccacddc1880c2d52ae913c2d90adbf56625e0",
                    "amount_available": "7,000"
                },
                "outputs": [
                    {
                        "recipient_public_key": "043f7eab213d4999bd3b7ce2b61a627452622954728c48c84ee829c2db1fc07135a8b32be5d41bcde58c11e1222bd15fbee383ea970251ab4d96204256b4c4e6f3",
                        "fees": [
                            {
                                "fee_name": "Tuition fee",
                                "amount_paid": "5,907"
                            }
                        ]
                    },
                    {
                        "recipient_public_key": "0450ac88b4b69709c412ddc9ac7d4b05957697f114ca64c5d3d6f828a3b383c7054b066e9ab20afcdf01060ee887aa13a9e496c865a1e97d9e7743d0bc59268b5d",
                        "amount": "1,093"
                    }
                ]
            }
        ]
    }
]
```


Figure 4.26. RESTful API Output

A Blockchain contains a connected list of blocks, each containing a collection of transactions and is considered one of the data structures [29]. The first JSON object in the JSON array shows the first block called the genesis block. This was the block that was generated after initializing the Blockchain. The genesis block had meta-data such as the nonce which increases for every hash calculation, timestamp in seconds which referred to the time the block was created and the difficulty which was the hashing target then. In addition, the genesis block did not have a previous or last hash. Conventionally, the last hash for the genesis block was represented with all zeros. Nevertheless, the genesis block had its own harsh. The second JSON object in the JSON array shows the second block that proceeded the genesis block. Like the genesis, the second block had its own meta-data such as nonce, timestamp and difficulty. The last hash of the second block was identical to the hash of the genesis block. Therefore, genesis block and the second were

cryptographically linked through the hashes. Furthermore, the second block had its own hash which was generated based on the block's meta-data and data to store. As shown in Figure 4.26, transactions consisted of an input (where funds came from) and output (where funds were going) objects. Information about the sender was generated in the input of the transaction. Input information included a timestamp, sender's public key, the sender's balance, as well as the digital signature of the sender which was generated using the sender's private key. Digital signatures were similar to unique handwritten signatures, but with far more inherent security, so as to solve the problem of impersonation and tampering. The output object included recipient public key and a JSON array of fees being paid. The output object also included a transaction that specified the public key of the sender as the recipient key. This transaction is called Unspent Transaction Output (UTXO). UTXO refers to the amount of digital currency left after executing a transaction.

4.4.2 Blockchain Mobile Payment System Model

The following figures represent the model that was designed based on Blockchain. Figure 4.27 illustrates the home screen of the proposed mobile application with an open drawer menu. This

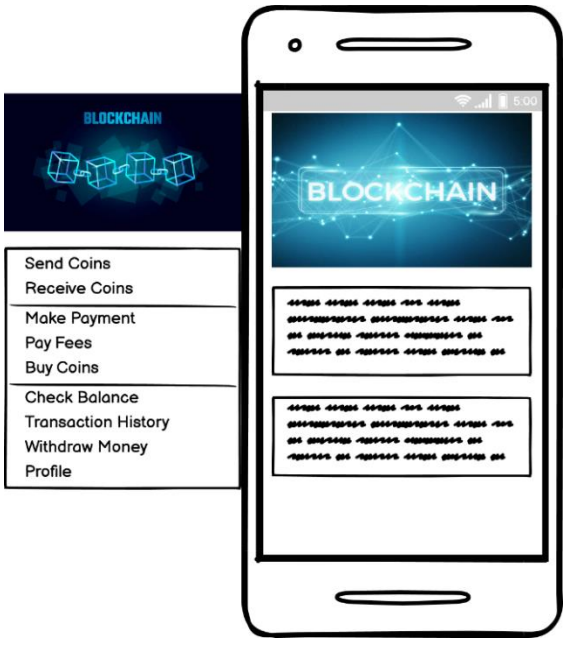


Figure 4.27. Home Screen

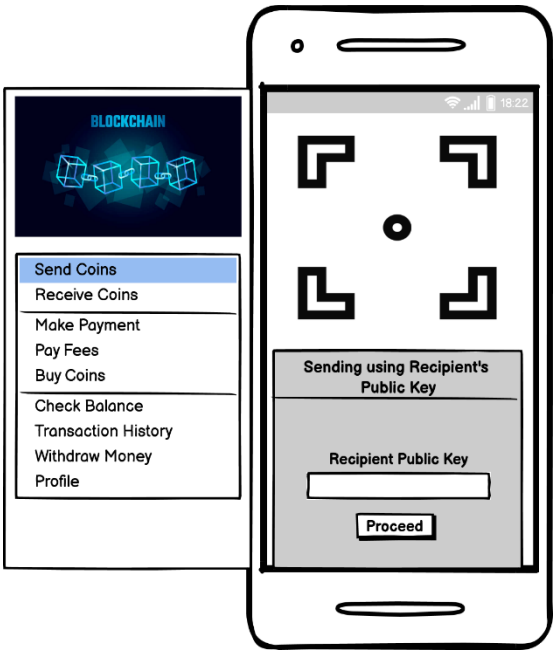


Figure 4.28. Send Coins Screen

was the screen that a student would view once authenticated.

Figure 4.28 shows the screen under the “send coins” menu option where a student could share or send their coins. The student could either scan the public key from the recipient's phone or type it into the input area.

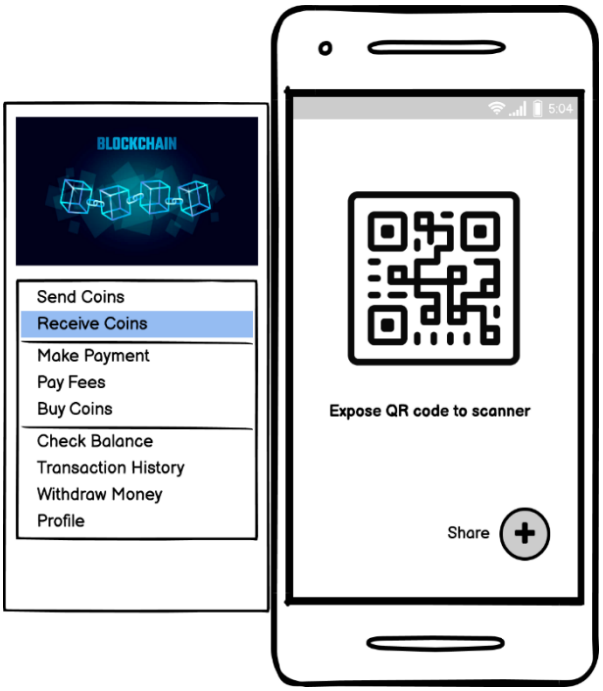


Figure 4.29. Receive Coins Screen

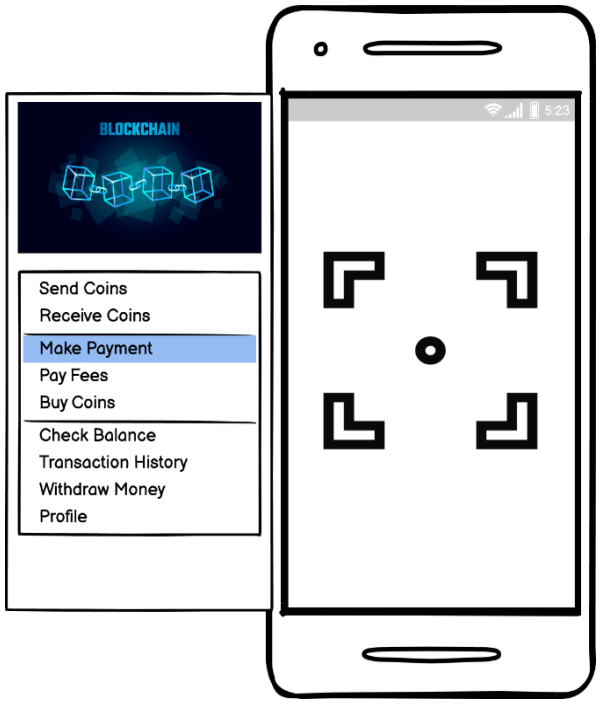


Figure 4.30. Make Payment Screen

Figure 4.29 depicts the screen under the “receive coins” menu option, where a student could either expose his or her public key via a QR code or share it via a messaging service like SMS, WhatsApp, or email.

Figure 4.30 illustrates the screen under the “make payment” menu option, where a student could scan the QR code displayed in the institution or merchant's premises to make a payment.

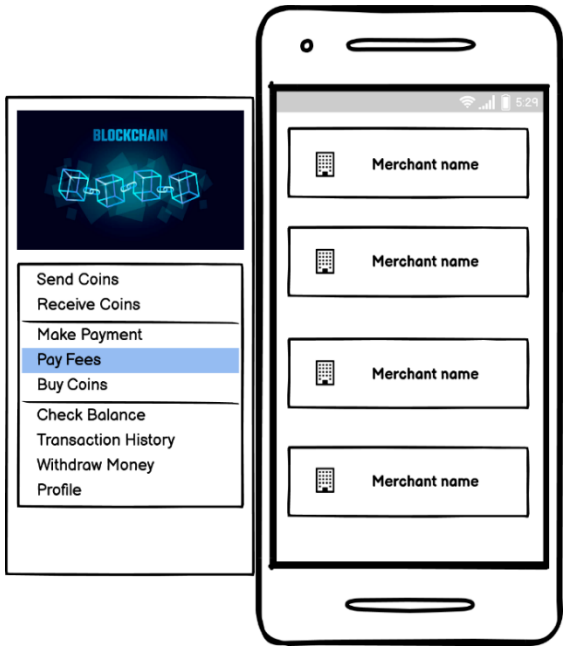


Figure 4.31. Pay Fees Screen

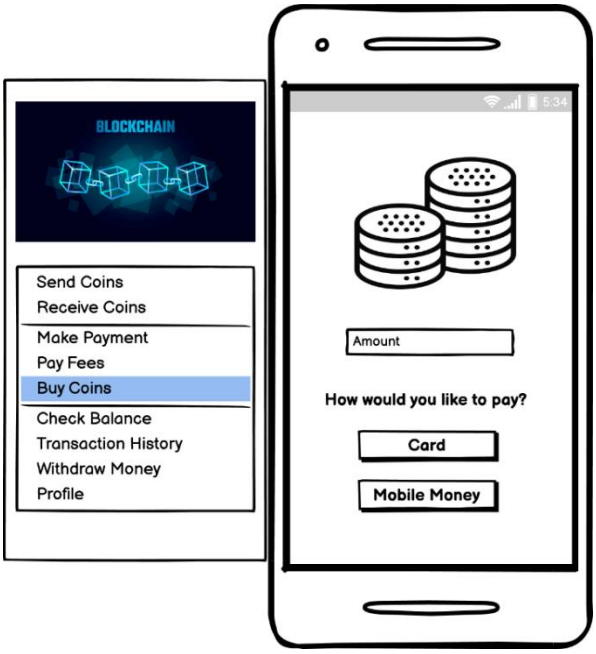


Figure 4.32. Buy Coins Screen

Figure 4.31 shows the screen under the "pay fees" menu option, where a student could make a payment for a merchant's predefined list of goods and services.

Figure 4.32 depicts the screen that appeared when a student selected the "buy coins" menu item, from which a student could acquire coins using a VISA Card or Mobile Money.

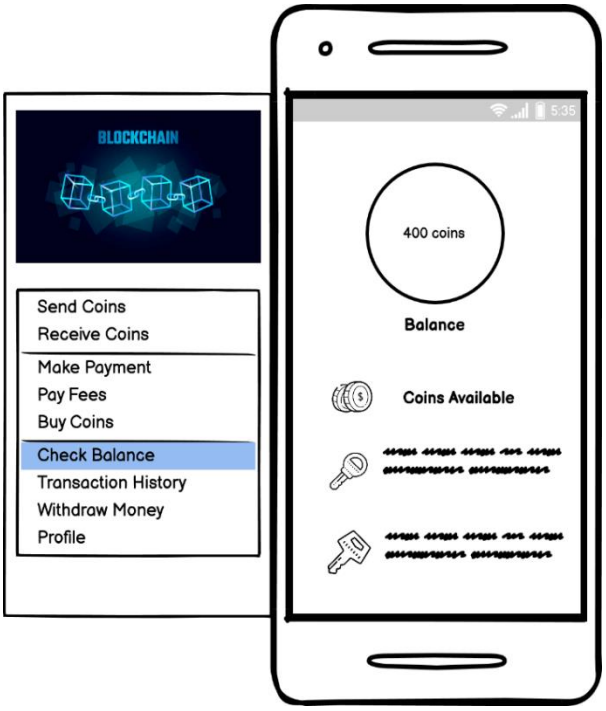


Figure 4.33. Check Balance Screen

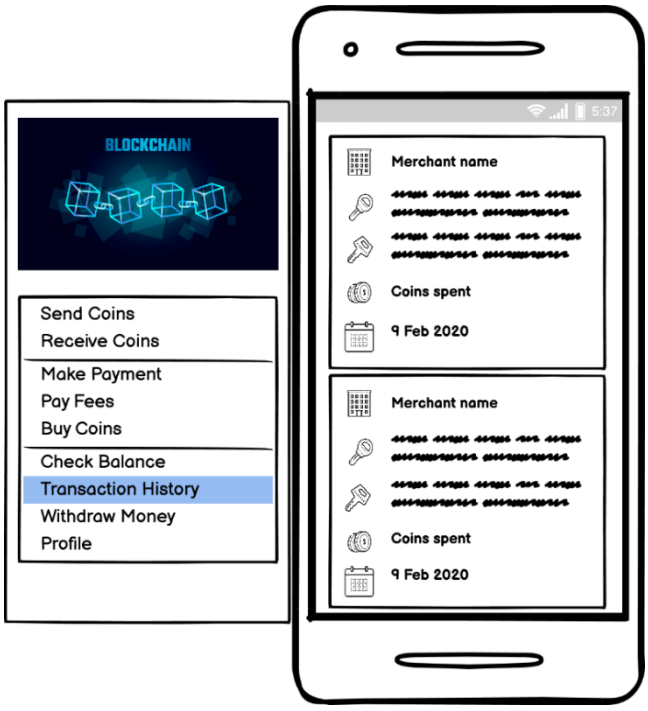


Figure 4.34. Transaction History Screen

Figure 4.33 displays the screen where a student could view his or her balance, an excerpt of his or her public key and an excerpt of his or her private key under the "check balance" menu option.

Figure 4.34 depicts the screen under the "transaction history" menu option, where a student could view his or her previous transactions. Furthermore, A student could view the recipient's name, recipient's public key, amount spent and date the transaction occurred.

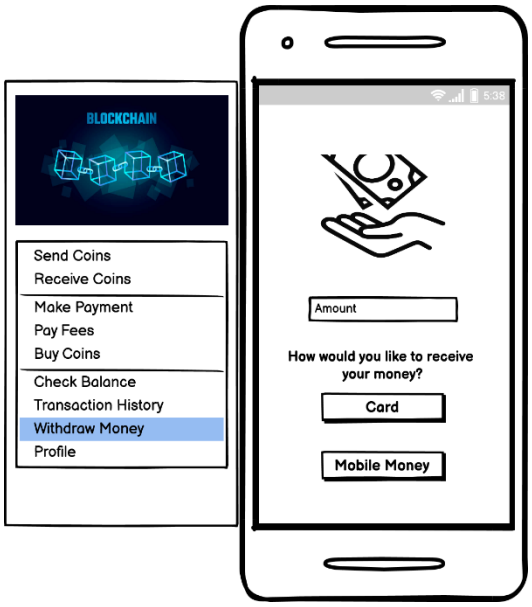


Figure 4.35. Withdraw Money Screen

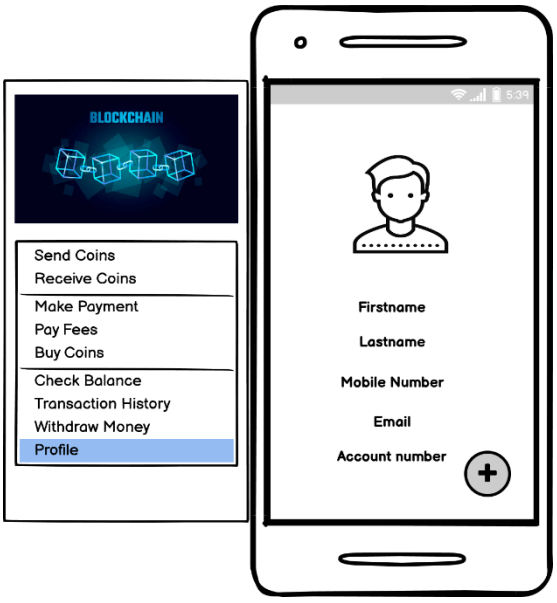


Figure 4.36. Profile Screen

Figure 4.35 depicts the screen under the "withdraw money" menu option, where a student could convert his or her coins to currency. The student would receive funds using either VISA card account or mobile money.

Figure 4.36 illustrates the screen under the "profile" menu option, where a student could view his or her details such as backdrop image, profile image, first name, last name, student number and mobile number.

4.4.3 Blockchain Mobile Payment System Prototype

The following figures represent the prototype that was developed based on the model.

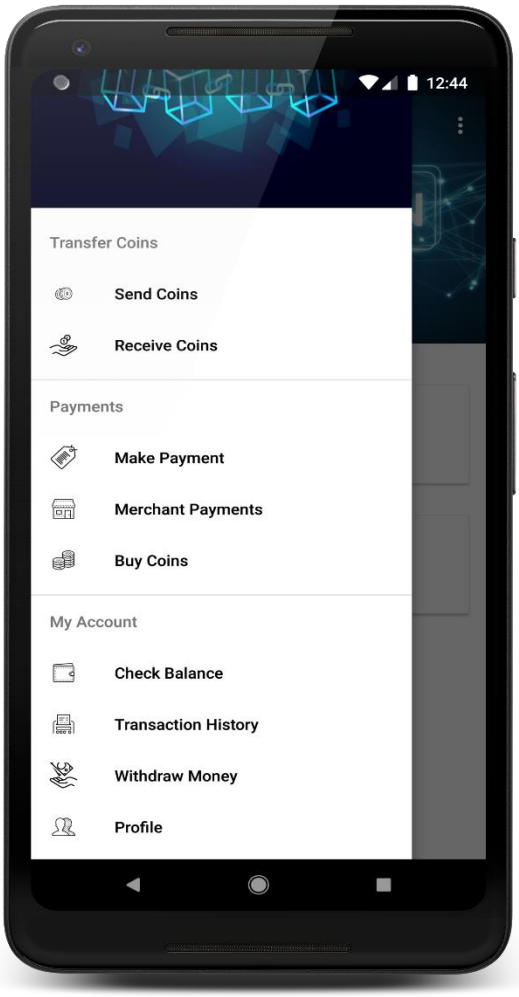


Figure 4.37. Home Screen

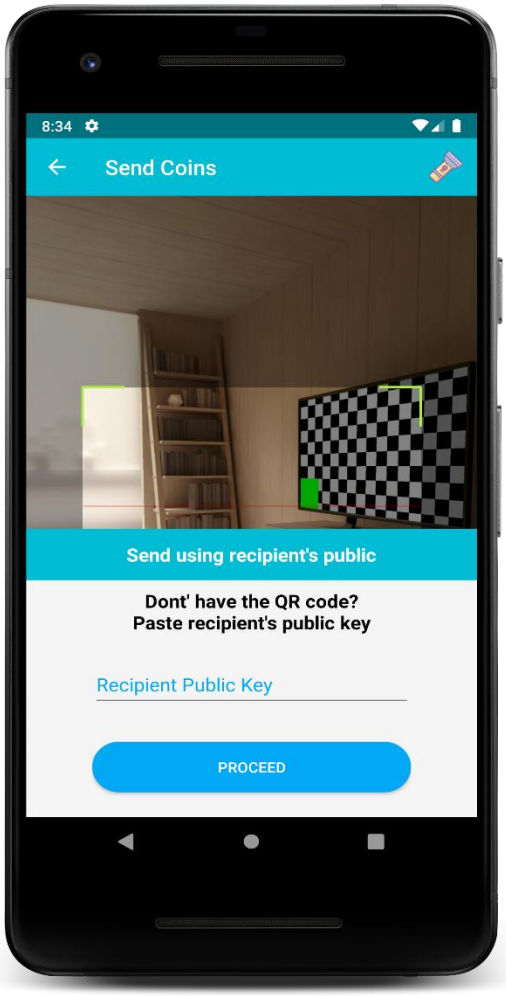


Figure 4.38. Send Coins

Figure 4.37 shows the home screen of the developed mobile application with an open drawer menu. The student would be able to navigate to various screens using the drawer menu options.

Figure 4.38 depicts the screen under the "send coins" menu option of the developed mobile application where a student could share or send their coins to a follower student. The student would either scan the public key from the recipient's phone or type it into the input field.

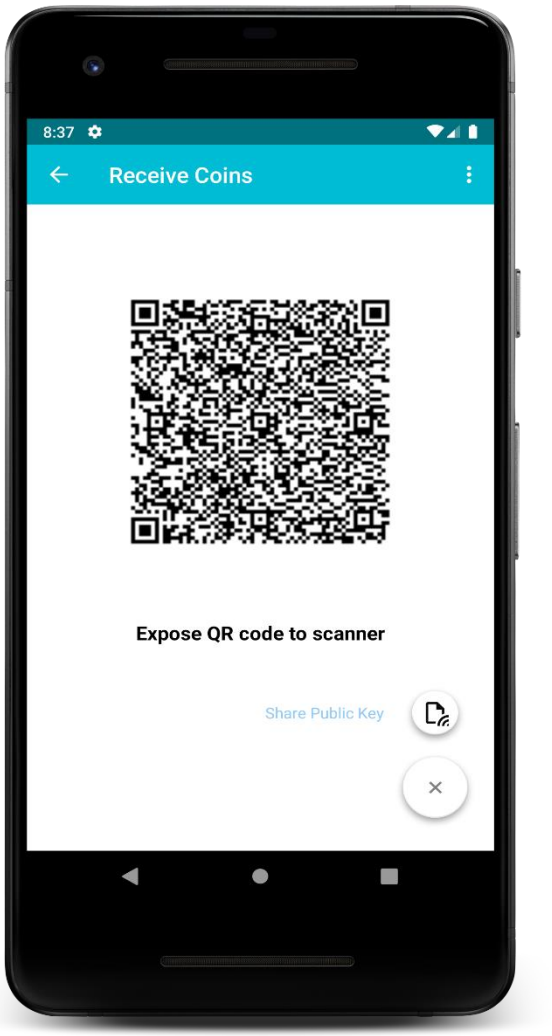


Figure 4.39. Receive Coins Screen

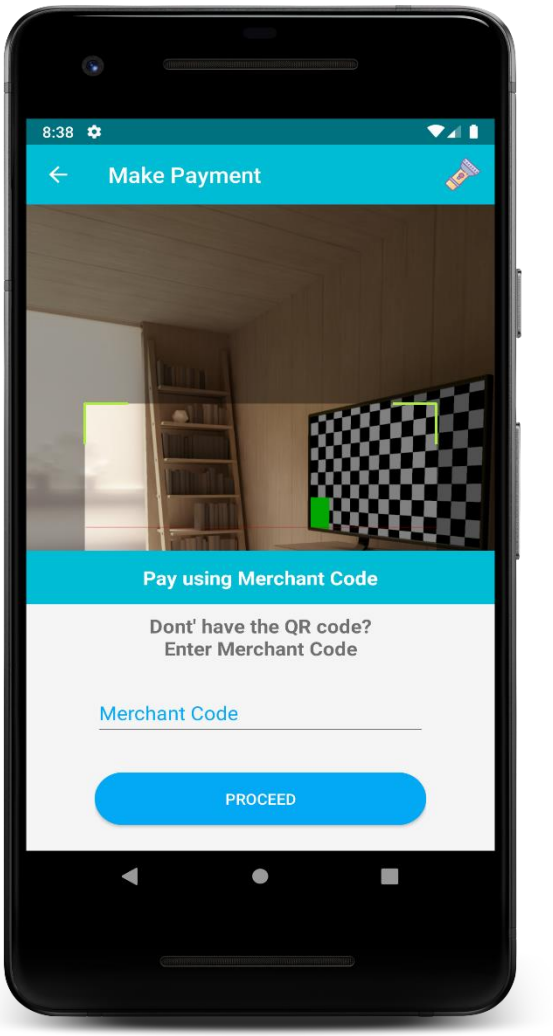


Figure 4.40. Make Payment Screen

Figure 4.39 illustrates the screen under the “receive coins” menu option of the developed mobile application where a student could either expose his or her public key via a QR code or share it via a messaging service like SMS, WhatsApp, or email.

Figure 4.40 demonstrates the screen under the “make payment” menu option of the developed mobile application where a student could scan the QR code displayed in the institution or merchant's premises or enter the merchant code to make a payment.

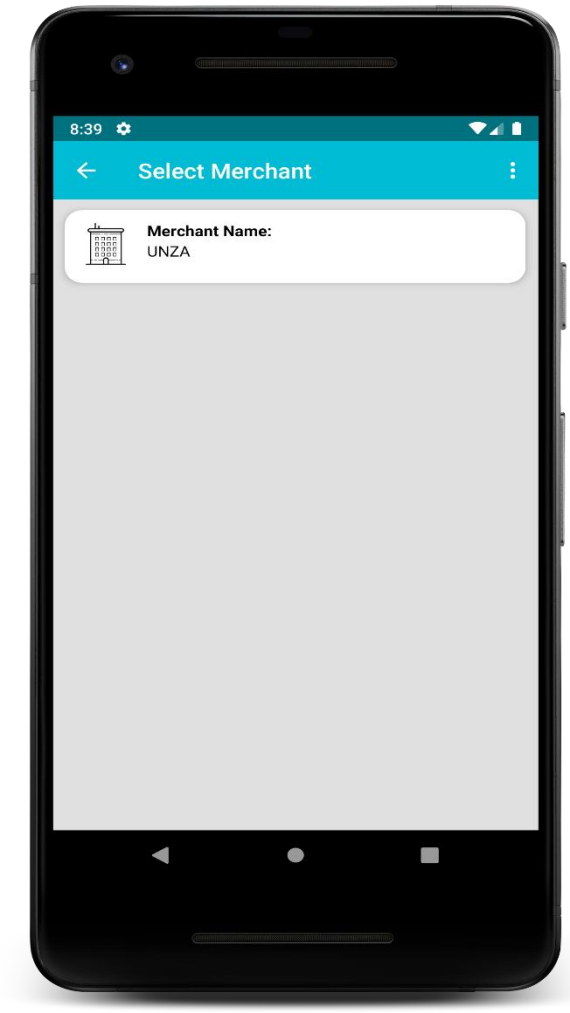


Figure 4.41. Pay Fees Screen

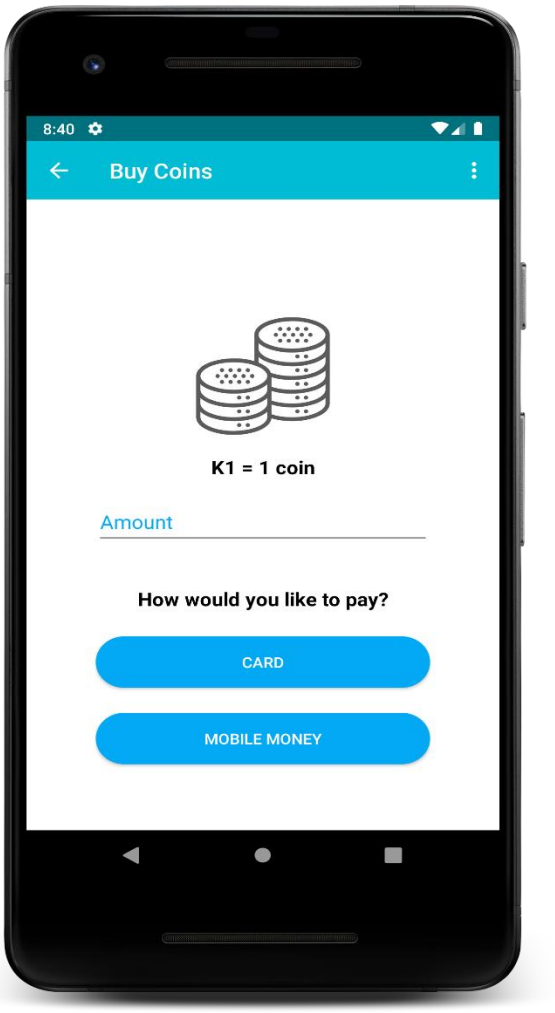
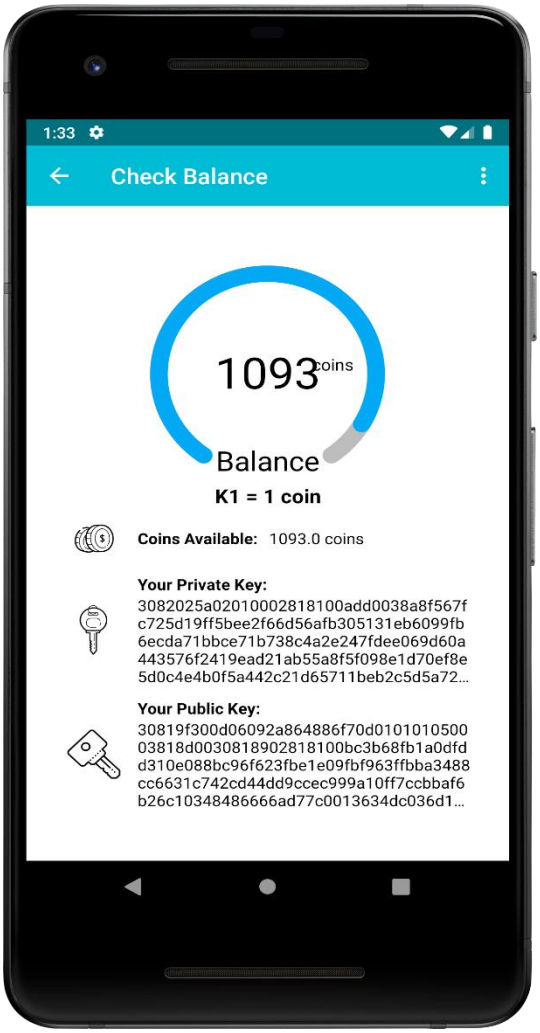


Figure 4.42. Buy Coins Screen

Figure 4.41 shows the screen under the “pay fees” menu option of the developed mobile application where a student could make a payment for a merchant's predefined list of goods and services.

Figure 4.42 depicts the screen of the developed mobile application that appeared when a student selected the “buy coins” menu item from which a student could acquire coins using a VISA Card or Mobile Money.



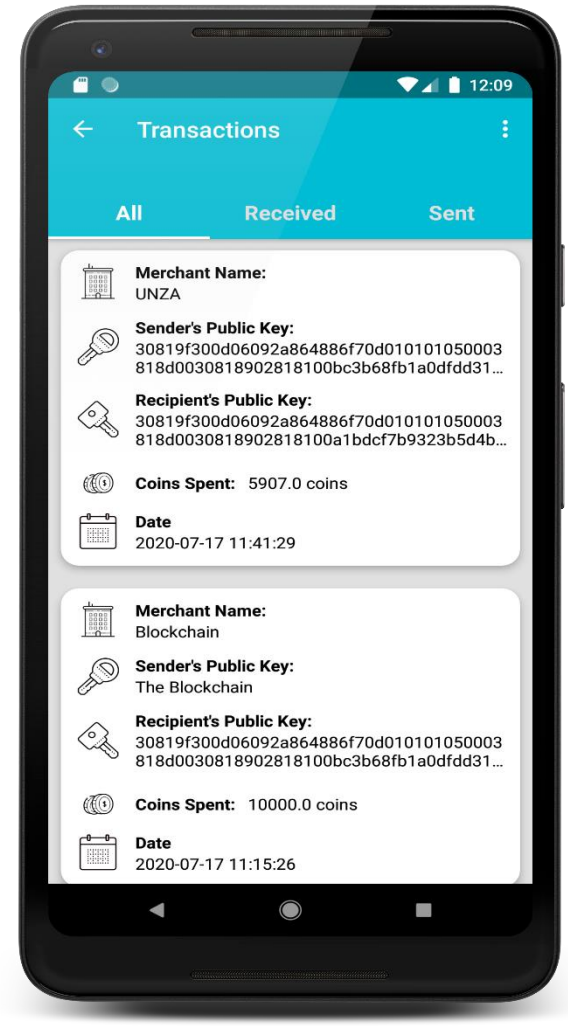


Figure 4.43. Check Balance Screen

Figure 4.44. Transaction History Screen

Under the "check balance" menu choice in Figure 4.43, a student could view his or her balance, an extract of his or her public key and an excerpt of his or her private key.

Figure 4.44 shows the screen of the developed mobile application where a student could view his or her previous transactions under the “transaction history” menu choice. A student would also see the recipient's name, public key, amount spent and the date as well as time of the transaction.

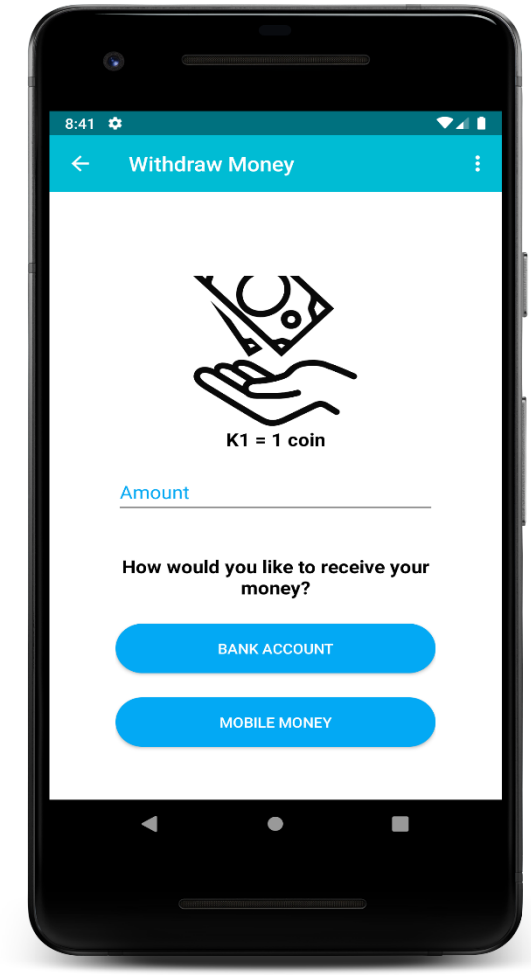


Figure 4.45. Withdraw Money Screen

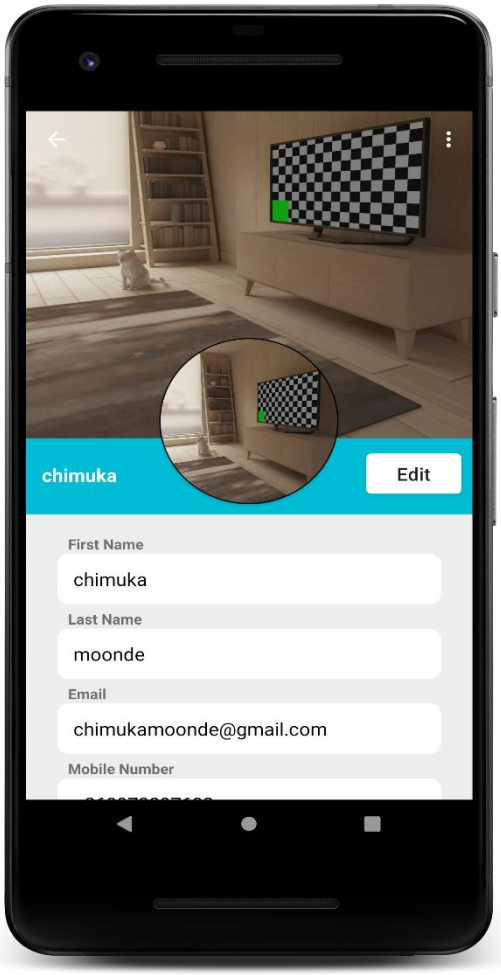


Figure 4.46. Profile Screen

Figure 4.45 shows the screen of the developed mobile application where a student could change his or her coins to currency under the “withdraw money” menu option. The student had the option of receiving funds by VISA card or mobile money.

Figure 4.46 shows the screen of the developed mobile application that appeared when a student selected the "profile" menu option, where he or she could view personal information such as first and surname names, student numbers and phone numbers.

4.5 Chapter Summary

This chapter presented the empirical results obtained from the questionnaire survey. It also provided the primary data analysis yielding the factor relationships among valuables identified in research questions. The Multinomial Regression's Likelihood Ratio test results in this chapter provide an output from which the hypotheses are validated and tested as will be discussed in Chapter 5. The results provided answers to the research questions through which objectives were met. In addition, this chapter illustrated the model and results of the developed components of Blockchain-based mobile payment system.

CHAPTER FIVE

DISCUSSION AND CONCLUSION

5.1 Introduction

This chapter discusses the findings of the study following the data presented in the previous chapter. It will follow a succinct approach with due cognizance to the research objectives. The interpretation will take two approaches. The first will begin by interpreting the findings as observed from the descriptive analysis and will be followed by the interpretation of inferential statistics where relations between the independent and dependent variable will be established. This chapter presents the conclusion of the study, recommendations for this study which are based on the study's findings and are in line with the research objectives and lastly, recommendations for future studies are also made.

5.2 Discussion of Results

5.2.1 Key Payment Systems Used by Students

The following reveals the payment systems used by students in higher learning institutions when paying mandatory academic obligations.

Figure 4.6. depicts the different payment methods that students used to pay for registration. Bill muster was the most popular payment option for registration, followed by cash and bank transfer, as shown in Figure 4.6. The finding that Bill Muster was the most widely utilized electronic payment system, is comparable to Mukonde's finding [17].

The payment systems utilized by students to pay for tuition fees are depicted in Figure 4.8. Bill muster was used by the majority of students, with cheque and cash ranking in second and third, respectively. These statistics support Mukonde's [17] claims that ZANACO's bill muster system was the most extensively used payment system.

Figure 4.7 depicts the payment systems used by students to pay for examination costs. The most preferred method was Bill muster, which was followed by cash and then bank transfer. The most

extensively used payment system, according to Mukonde's [17] findings, is ZANACO's bill muster system.

As indicated in Figure 4.9, students paid library fees in a variety of ways. The most preferred way was Bill muster, followed by bank transfer and cash. The finding that Bill Muster was the most widely utilized electronic payment system, is consistent with Mukonde's finding [17].

5.2.2 Challenges Faced by Students

The following describes the challenges faced by students when using the current payment systems.

Figure 4.10 illustrates the assertion by students of whether banks designated by higher institutions of learning were evenly distributed in rural and urban areas. Majority of the student were of the view that designated banks were not evenly distribution in rural and urban areas. As a result, students were forced to travel vast distances to reach the few designated banks. This is similar to Mukonde's [17] finding where students had difficulties as a result of a lack of access to payment platforms, such as banks, where individuals seeking financial services had to travel significant distances. For electronic payment, internet availability which was key for the transaction to be performed was at times not readily available.

Figure 4.11 demonstrates the conviction by students that designated banks were characterized by long unbearable queues. The rising number of students enrolled in higher education institutions resulted in long, inconvenient queues and extreme overcrowding in most financial institutions when it came to paying student fees. Figure 4.12 depicts the affirmation by students that designated banks were characterized by unbearable loss of time whilst waiting to be attended to. This was due to an overwhelming number of students attempting to pay students fees at the same time. These findings are similar to Mukonde's [17] and Singh's [108] findings where despite the efficiency of electronic payment systems, respondents complained that it was difficult and inconveniencing because students had to physically visit the bank which in most cases had long queues.

Figure 4.13 depicts students' significant belief that personally identifiable information could be abused or stolen. The safety of their personally identifiable information was a concern for the students. Students were scared that their personal information might be stolen or used

inappropriately. Figure 4.14 represents students' acknowledgement that payment and billing information, such as debit card numbers and bank account numbers, may be abused or stolen. Students were concerned about the security of their financial information. The realization that a malicious company or skilled individual could potentially gain access to transaction details at rest or in transit caused students to be concerned. These findings are consistent with that of Mukonde [17] and Adewole [109], who discovered that most students prefer cash over other modes of payment. The reason behind this was a lack of confidence in the electronic payment systems. The payment system architecture appeared to be such that acceptable service and timely consumer satisfaction were not guaranteed. Infrastructure failure was a typical occurrence, causing effective systems to be unfunctional. As a result, instead of being subjected to unnecessary difficulties, individuals choose to conduct transactions using cash.

5.2.3 Blockchain Mobile Payment System Model

UML diagrams such as Use-Case, Sequence, Class and Activity diagrams were used in the development of the proposed blockchain-based mobile payment system model. The UML diagrams were used to visually describe the proposed system, including its major actors, roles, actions, classes, to better understand, alter, maintain, or document system information. UML is a modern approach to modelling and documenting software. Use case diagrams were used to analyse the proposed system's high-level requirements. Figure 3.10 represent the use case diagram used in this study. Activity diagrams were used to describe the flow of different activities and actions. These can be both sequential and in parallel. Figure 3.11, Figure 3.12, Figure 3.13 and Figure 3.14 represent the activity diagrams used in this study. Sequence diagrams were used to describe the sequence of messages and interactions that happen between actors and objects. Figure 3.16, Figure 3.17, Figure 3.18, Figure 3.19 and Figure 3.20 represent the sequence diagrams used in this study. Class diagrams were used to show the static structure of the proposed system, including classes, their attributes and behaviours and the relationships between each class. Figure 3.15 represents the class diagram used in this study. In addition, Figure 4.27, Figure 4.28, Figure 4.29, Figure 4.30, Figure 4.31, Figure 4.32, Figure 4.33, Figure 4.34, Figure 4.35 and Figure 4.36 represent the mock ups used in development of the proposed system.

5.2.4 Blockchain Mobile Payment System Prototype

Figure 4.37,Figure 4.38, Figure 4.39, Figure 4.40, Figure 4.41, Figure 4.42, Figure 4.43, Figure 4.44, Figure 4.45 and Figure 4.46 shows the implemented e-wallet mobile application. Like a physical wallet, the mobile e-wallet Android application helped a student track how much digital currency he/she had. Furthermore, the e-wallet mobile application stored the student's private and public keys. The private key enabled the student to generate a unique digital signature to sign very exchange of digital currency between the student and the institution. The institution used the student's public key to verify the student's signature. A wallet's public key allowed other nodes or individuals to verify the digital signature generated by the private key of the wallet in the Blockchain network. Using the student public key, the institution decrypted the data presented by the signature. If the decrypted data did not match the data suggested, then the signature was deemed invalid. Likewise, the signature was valid if the decrypted data matched the proposed data. It was required that the signature undergoes verification to confirm whether the underlying transactional data was sent by the allegedly student to prevent system fraud. The public key also served as the public address of the wallet and was what other nodes or fellow students would use to send digital currency to the wallet. The public key was generated from the private key. The public key was a 2D point coordinate on an elliptic curve.

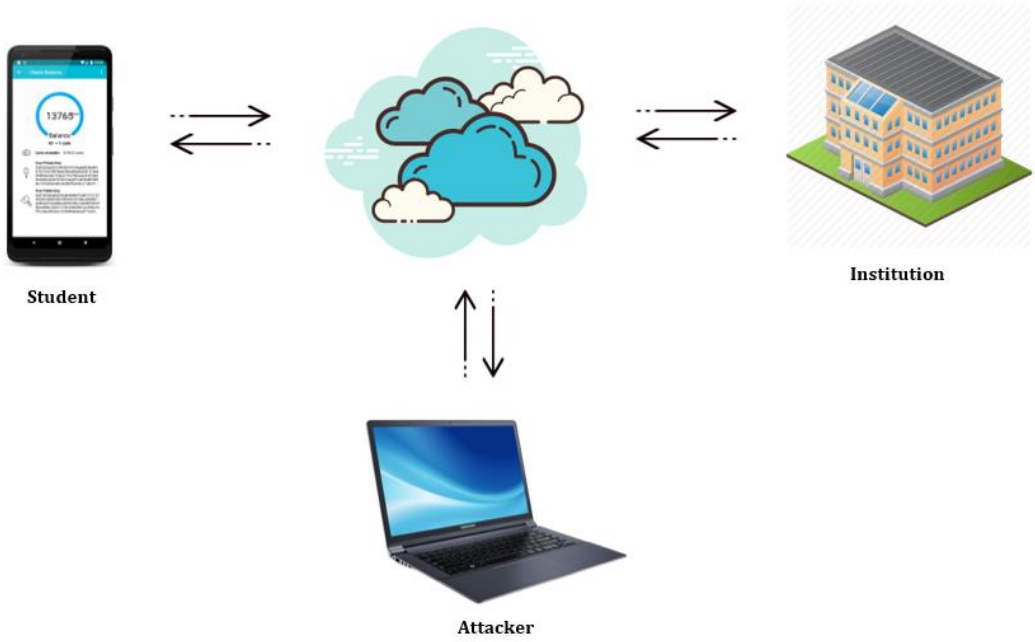


Figure 5.1. Communication via an unsecured channel

Figure 5.1 depicts the student and institution communication via an unsecured channel. In this study, the communication channel was the Internet. In an event that communication occurred in the presence of an attacker whose aim was to defeat of any security services provided to the student and institution, the attacker could attempt to read the traffic from the student to the institution, therefore learning the student's personal identifiable information as well as bank card or account information. In addition, the attacker could attempt to impersonate either the student or institution.

Careful analysis of the aforementioned scenarios shows the following underlying factors that required to be addressed in the implementation of the proposed payment system:

i. Confidentiality: keeping data secret from everyone, but those authorized to view it. Transactional data sent by the student using the e-wallet mobile application to the intuition should not be readable by the attacker.

ii. Data Integrity: ensuring that the transactional data sent through the unsecured channel is not altered by the attacker. The institution should be able to detect when the transactional data sent by the student using the e-wallet mobile application have been modified by the attacker.

iii. Data Origin Authentication: The institution should be able to check and verify that the transactional data supposedly sent by the student using the e-wallet mobile application did actually originate from the student.

iv. Entity Authentication: The institution should be convinced of the identity of the student.

v. Non-Repudiation: Preventing the student from denying transactions previously made. When the institution supposedly receives transactional data from the student, it should not only be convinced that the transaction came from the student, but it should be able to convince a neutral third party that the transaction came from the student. Therefore, the student should not be able to deny having made the transaction.

The highlighted fundamental security factors were addressed by adopting elliptic curve public-key encryption and signature in the implementation of the proposed system. With the help of the Blockchain, both the student and institution generated a pair of keys (*e*, *d*) consisting of a public key *e* and associated private key *d*. Each entity kept its private key a secret. Figure 5.2 illustrates an overview of the wallet public and private key.

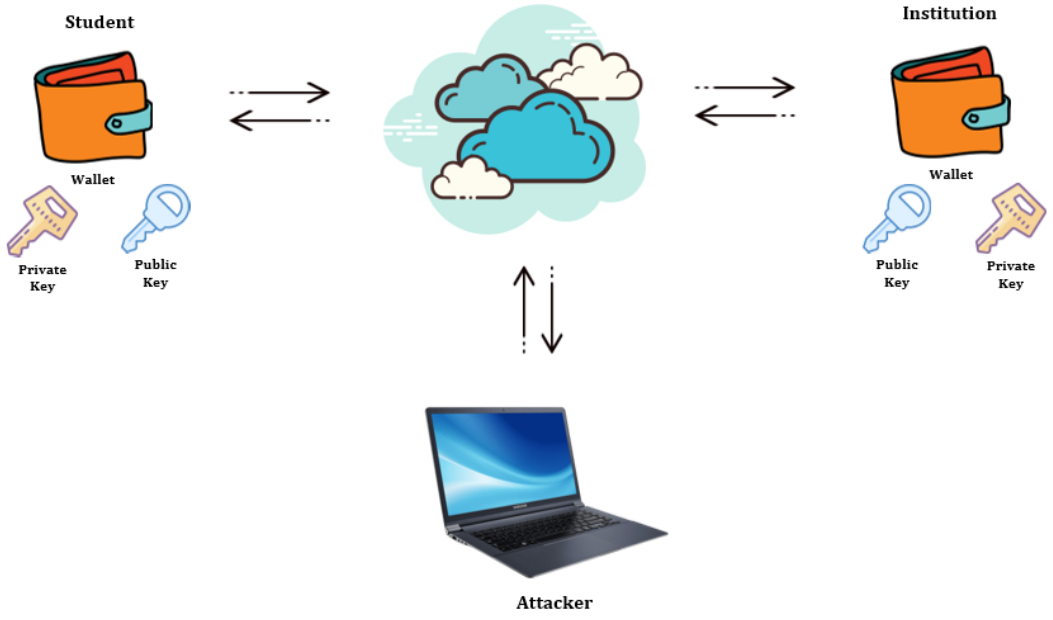


Figure 5.2. Wallet public and private keys

When a student needs to send transactional data to the institution, the e-wallet mobile application obtains a copy of the institution's public key $e_{institution}$. The e-wallet mobile application uses the encryption function ENCRYPT of elliptic curve public-key encryption scheme to compute the ciphertext c= ENCRYPT $e_{institution}$(transactional data). The e-wallet mobile application then sends c to the institution. The institution uses the decryption function DECRYPT and its private key $d_{institution}$ to recover the plaintext format of the transactional data, which are represented by m = DECRYPT $d_{institution}$(c), where c is the ciphertext that was received. An attacker with access to the copy of the institution's public cannot use the public key to decrypt the ciphertext sent from the student to the institution. The key pair has a property that is not computationally feasible to determine the private key only from the information of the public key.

A student using the e-wallet mobile application uses the signature generation algorithm SIGN of the digital signature scheme of the elliptic curve cryptography and their private key $d_{student}$ to compute the signature of the transactional data s = SIGN $d_{student}$(transactional data). The e-wallet mobile application sends the signed transactional data in ciphertext format to the institution. The institution obtains a copy of the student's public key $e_{student}$ and uses a signature verification algorithm to confirm that *s* was indeed generated from m and $d_{student}$. Since $d_{student}$ is only known by the student, the institution is assured that the transactional data did indeed originate from a particular student. More importantly, since verification requires only the non-secret quantities m and $e_{student}$, the signature *s* for the transactional data can also be verified by a third party who could settle disputes if the student denies having signed the transactional data. Figure 5.3 and Figure 5.4 summaries the use of elliptic curve public-key encryption and signature in the implementation of the proposed system.

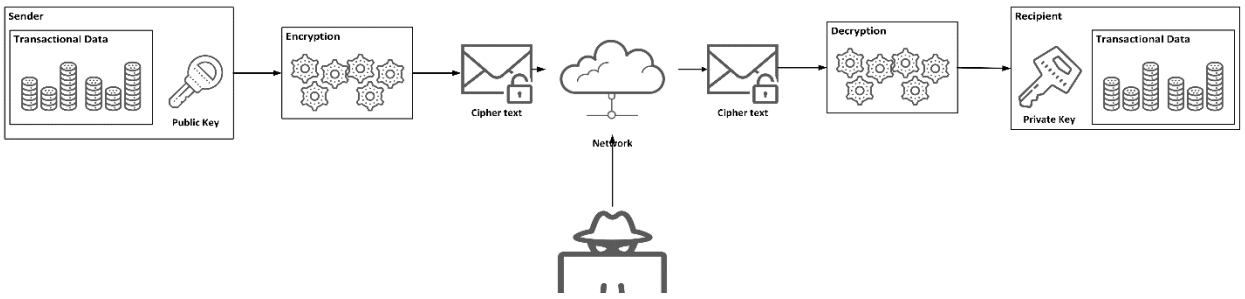


Figure 5.3. Summary of elliptic curve public-key encryption

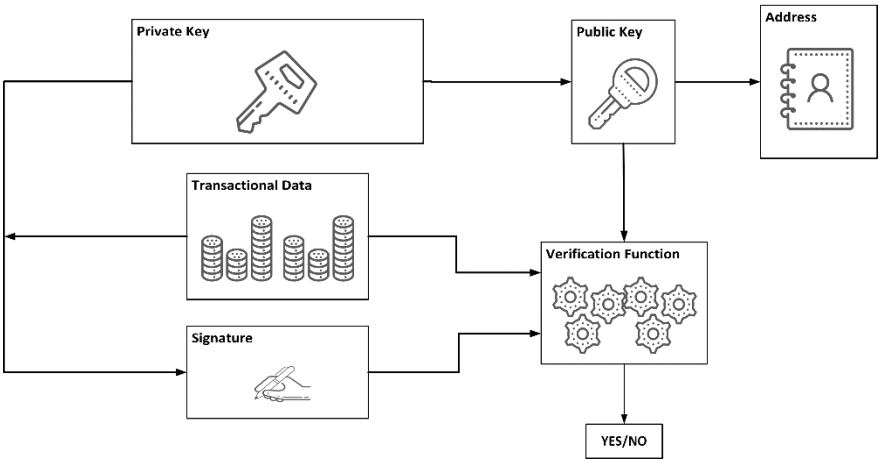


Figure 5.4. Summary of signature

Figure 5.5 shows a high-level overview of the proposed blockchain-based mobile payment system.

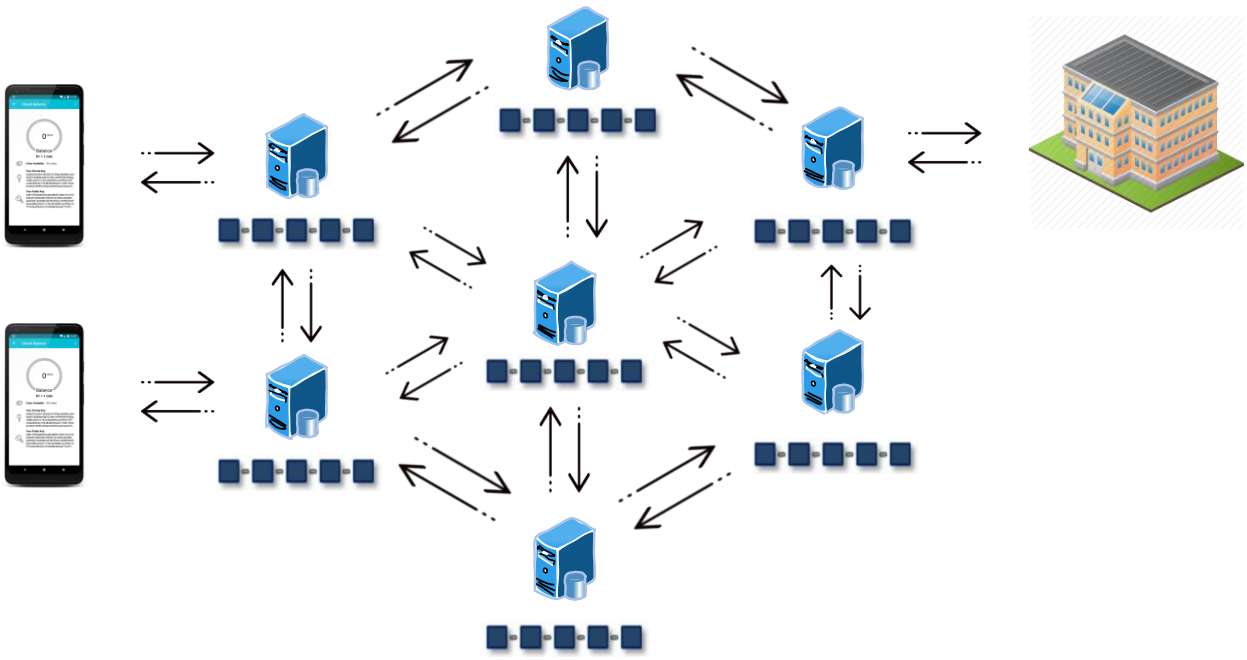


Figure 5.5. High-level overview of the proposed

This study adopted blockchain technology because blockchain creatively blends cryptography with a decentralized database in a novel way, allowing a blockchain to be decentralized, immutable and transparent all at once [12]. Additionally, this study adopted blockchain technology because blockchain is a distributed and decentralized ledger that is tamper-proof and preserves the growing array of data such as transactions. There is no centralized approach and no master computer. The ledger comprised of a chain of blocks linked to each other by cryptography [30]. Furthermore, the distributed and decentralized ledger was publicly shared across all the nodes of its network. This study adopted Proof-of-Work as the consensus protocol. By implementing the proof-of-work consensus protocol, each node of the network checked the validation of the block. The validated block was appended to the chain and the modified ledger was replicated through the permitted nodes of the chain. The consensus protocol replaced the requirement of a trusted third party or the central authority [36]. Permissioned Blockchain were used in this research, which ran a Blockchain among a group of known and identified different instances of an Ubuntu server located in different regions.

The blockchain consisted of multiple blocks of data chained together like the links of a physical chain [110]. Blocks were a storage of data on the blockchain network. Once a block was added to

the chain of blocks that preceded it, it became irreversible. Every block was given a unique value that looked like a random string of characters. The random string of characters is called the hash since it was generated from a hash function that creates a unique output for every unique input that it receives [32]. The unique hash was generated based on the metadata about the block and the data that was in the block. There was also one more very crucial data point used to generate the hash of a new block, namely the unique hash of the previous block. The unique hash of the previous block was also used as part of the input that the new block used to generate its hash. This means that the previous block was an integral part of creating the hash value of the new block.

5.2.5 Respondents' Level of Knowledge in ICT and Experience

5.2.5.1 Description of Knowledge or Skill in ICT usage

The researcher was interested in knowing how knowledgeable the respondents were in the usage of the internet, computers, tablets or iPads and mobile phones as well as interested in measuring their skills on utilising the same on a Likert scale. The findings showed that the ICT device which most respondents (66%, 121 out of 182) were mainly knowledgeable of was the mobile phone. When measuring their level of skills in using the mobile phones, the findings showed that all respondents who agreed to being knowledgeable in using ICT also possessed very good skills in using them. Furthermore, the researcher also established that the second and third most known and utilised ICT device were the computers with 52%, 94 out of 182 of the respondents agreeing to having knowledge of what computers were and also possessed good skills in using the same and the internet respectfully with 44%, 80 out of 182 of the respondents agreeing to having knowledge of what the Internet was and also possessed good skills in using the same. This finding was appreciated in that it gave a justification as to why it was more preferable to develop a mobile payment system which would run on mobile phones than other platforms because most of the potential users were mainly familiar with mobile phones and possessed very good skills using them, as such they may not find challenges using the proposed mobile payment system which will be running on their mobile phones.

5.2.5.2 Period of Using Some Selected ICT by the Respondents

When asked the period of time that the respondents had been using the form of ICT stated above, the study's finding showed that the form of ICT that most respondents (93%, 170 out of 182) had been using for a period of more than 2 years was a mobile phone, which was seconded by the Internet (91%, 166 out of 182) which had also been used by the respondents for a period of more than two years and taking the third position was the usage of the computer where 75% (137 out of 182) of the respondents also agreed to using a computer for a period of more than two years. This finding indicated that the sampled respondents had quiet some significant experience in using some selected ICT devices, for this reason, using the Blockchain-based payment system would not be such a challenge because of the fair experience that the study's respondents had been using ICT.

5.2.6 Factors Influencing the Utilisation of Mobile e-Wallets by the Study's Respondents

5.2.6.1 Demographic Factors

5.2.6.1.1 Effect of Gender on Users' Utilisation of e-Wallets

In this study, one of the characteristics investigated as a possible determinant of e-wallet adoption was gender. The decision to utilize this variable was based on research undertaken by Venkatesh et al., [57] who used gender as a possible determinant factor of technology adoption in their extended TAM2 model, which they later called the UTAUT model.

According to this study findings, the gender distribution of the sampled respondents was practically even, with a little discrepancy of 2%, with females accounting for 51.9 % (92 out of 182) and males accounting for 48.1 % (90 out of 182). Because no sex had an unfair representation over the other, the gender distribution in this study decreased gender bias, making the inferences more credible.

The null hypothesis($H_0 6$), which stated that "gender does not influence the adoption of e-wallets by students" was rejected when the hypothesis was tested at a 5% level of significance to see whether gender significantly influenced the adoption of e-wallets. This was due to the fact that the probability value (0.009) for the relationship between the variables "respondent gender" and

"mobile e-wallet usage" was less than 0.05. This suggested that the research (alternative) hypothesis (gender does influence the adoption of mobile e-wallets by students) was accepted.

According to the findings, it is critical for designers and developers of mobile e-wallets to consider the numerous concerns originating from gender differences, as this has a significant impact on consumers' decisions to use one e-wallet over another. This discovery is unsurprising, given that many products and services offered by corporate institutions, such as banks, are deliberately tailored to cater to the preferences of one gender over the other. As a result, e-wallet software designers and developers must incorporate features in e-wallets that are intended to meet the particular preferences of consumers based on their gender if e-wallet apps are to achieve maximum adoption.

The finding that gender had a significant impact on users' technology adoption varies from that of Venkatesh et al., [111], who used an enhanced UTAUT model but found that gender did not have a significant impact on users' decision to adopt a particular technology.

5.2.6.1.2 Effect of Age on Users' Utilisation of e-Wallets

Another aspect that the researcher evaluated as a potential factor influencing student acceptance of e-wallets was age. This is because different age groups are associated with diverse abilities and interests, which may influence their willingness and capacity to use different technologies, such as payment system technologies, which are the subject of this study. In most cases, a younger population is more likely to be interested in experimenting with new technology than an older population. As a result, knowing whether the age distribution of the sampled respondents influences e-wallet adoption is important to e-wallet software designers and developers because it allows them to consider the interests of various age groups when developing the product, ensuring that no age group is disadvantaged over the other.

According to the findings, 31% (n=56) of the respondents were under the age of 20, 61 % (n=111) who made the majority were in the age group of 21-30 years, 6% (n=11) were in the age group of 31-40 years, 1% (n=2) were in the age group 41-50 years, and the remaining 1% (n=2) were in the age group 51-60 years. Therefore, this finding implies that the majority of the study's sampled

respondents were youths, who are more likely to be interested in adopting mobile payment systems for facilitating payments for their fees at the sampled higher learning institutions, as youths are often associated with experimenting with new technologies than students who have passed their youthful years.

The null hypothesis($H_0 7$), which stated that "age does not influence the adoption of the e-wallets by students" was not rejected when the hypothesis was tested at a 5% level of significance to see if age significantly influenced the adoption of e-wallets by students. This is due to the fact that the probability value (0.434) for the relationship between the variables "respondent age" and "usage of mobile e-wallets" was greater than 0.05. As a result, the research (alternative) hypothesis (age influences student's use of mobile e-wallets) was rejected.

The finding stated above showed that the age of mobile e-wallet users had no bearing on their adoption of e-wallet technologies. This meant that anyone, regardless of age, could utilize the mobile wallet technology. When it came to the adoption of e-wallets, no specific age group or age group had an advantage over another age group. Hence the implication of the finding that age did not significantly influence the adoption of mobile payment systems.

The finding that age had no significant influence on users' adoption of technology is comparable to that of Venkatesh et al., [111] who used an extended UTAUT model for their study and found that age of technology users did not have a significant impact on technology adoption.

5.2.6.2 Perceived Usefulness and Utilisation of e-Wallets

One of the factors that the researcher assumed would influence the respondents' adoption of e-wallets was the perceived usefulness of e-wallets. According to the study's findings, most of the respondents represented by 58% (105 out of 182) strongly agreed that using e-wallets made it easier for them to manage and make various payments, while 34 % (n=61) concurred. On average, 91% of respondents (166 out of 182) agreed with the stated assumption. As a result of the survey, perceived usefulness was identified as one of the variables that drove respondents to use some of the current e-wallets on the market.

The null hypothesis($H_0 1$), which stated that "usefulness of e-wallets does not influence the adoption of the e-wallets by students" was not rejected at a 5% level of significance. This is due to the fact that the probability value (0.089) for the association between the variables "mobile e-wallets are useful" and "usage of mobile e-wallets" was greater than 0.05. This means that the research (alternative) hypothesis (usefulness of e-wallet influences the uptake of mobile e-wallets by students) was rejected.

According to the findings, there is no statistically significant association between the variable usefulness of mobile e-wallets and the variable use of mobile e-wallets by respondents. Despite the fact that statistics showed that there was no significant relationship between the two variables, statistics suggest that the relationship between the two variables was quite strong such that the null hypothesis ($H_0 1$) could have been rejected if it was to be tested at a 10% level of significance. As a result, the researcher contends that anyone considering designing and developing a mobile e-wallet must ensure that the mobile e-wallet includes features that will make it so helpful to consumers if it is to penetrate the market and be embraced. This submission is based on the findings of other researchers such as Akturan and Tezcan, [64] Phonthanukitithaworn [69] and Mallat, et al. [66] who all found a substantial relationship between perceived usefulness and usage of payment systems, at a 5% level of significance.

5.2.6.3 Perceived Ease of Use and Utilisation of e-Wallets

The study also assumed that perceived ease of use influenced the respondents' adoption of the various e-wallets on the market. The researcher chose a few variables to use as a proxy for evaluating the ease of use of e-wallets. These variables include the ease of facilitating transactions when using e-wallets, the ease of registering for an e-wallet, the steps required when carrying out transactions, the ease of reversing errors when using mobile wallets, and respondents' perceptions of how clear and understandable instructions involving mobile wallets' usage were.

When asked which of the above variables better characterized the ease of use of e-wallets, the majority of respondents 80% (146 out of 182) agreed that minimal steps necessary when carrying out transactions best reflected the ease of use when using mobile e-wallets. The other variables that described the ease of use that respondents experienced when using e-wallets was ease of

facilitating transactions and ease of registration for a mobile wallet account, both of which were represented by 43% (79 out of 182) as the second-best variable. As a result, it can be concluded that the majority of respondents found e-wallets to be simple to use. However, e-wallet service providers must address several concerns, such as the ease of reversing transactions, because most users have had difficulty reversing transactions when errors occurred during transaction execution.

The null hypothesis($H_0 2$), which stated that "ease of carrying out transactions using mobile e-wallets does not influence the adoption of the e-wallets by users" was rejected when test at a 5% level of significance. This is because the relationship between the variables 'simple to carry out transactions using mobile e-wallets' and 'use of mobile e-wallets' had a probability value (0.038) which was less than 0.05. This means that the study (alternative) hypothesis (ease of carrying out transactions using mobile e-wallets influences the adoption of mobile e-wallets by students) was accepted.

Having established that a significant relationship existed, the researcher concluded that if designers and developers of mobile payments technology are to attract the large numbers of users for their mobile e-wallet technologies, they should always endeavour to develop technologies which are so easy to use by users as this will enable their technology to receive massive appreciation by the users, hence in turn significantly enhancing its adoption as well.

This finding suggests that if an e-wallet is simple to use or user friendly, it is more likely to be accepted. This is due to the fact that complicated e-walllets tend to consume more time and effort for users as they try to figure out how to make and receive payments. This decreases the user's propensity to use a specific e-wallet again in the future, when simple and easy-to-use solutions are available that can serve a similar function and facilitate payments in a less complicated manner. These findings are similar to those established by Nag and Gilitwala [53], Schierz, et al. [55] and Sripalawat, et al. [68], where they also found a significant relationship between the ease of use of technology and the adoption of technology by its users.

5.2.6.4 Perceived Costs and Utilisation of e-Wallets

The perceived cost incurred when using e-wallets was an aspect that the researcher considered had an impact on the respondents' adoption of e-wallets. Two variables related to the perceived cost of using e-wallets were chosen as substitutes for measuring the perceived costs of utilizing e-wallet services. The variables chosen were the cost of registering for a mobile e-wallet account and the transaction cost incurred for using a mobile e-wallet.

The study found that 35% (64 out of 182) of respondents strongly agreed that the registration fee for obtaining a mobile wallet account was reasonable, with the 43% (n=79) who were the majority also agreeing to the same. As a result, on average, 78 percent (143 out of 182) of respondents thought the fee of opening an e-wallet account was reasonable. Affordability of e-wallet account opening could be one of the aspects that encouraged customers to use e-wallets in the first place.

When asked if the transaction cost for using a mobile e-wallet was fair or not, the majority of respondents (110 out of 182) agreed that the transaction cost was reasonable. This indicates that the majority of those polled were unaffected by the transaction costs of using e-wallets. As a result, it was concluded that the existing transaction costs for executing transactions using e-wallets are affordable enough to sustain the market's use of e-wallets.

When the null hypothesis($H_0 3$), which stated that “transaction cost incurred when using mobile e-wallets does not influence the adoption of e-wallets by students” was tested at a 5% level of significance, it was not rejected. This was attributable to the fact that the probability value (0.284) for the relationship between the variables "transaction costs incurred from mobile wallet usage" and "mobile e-wallet usage" was greater than 0.05. This means that the research (alternative) hypothesis (fair transaction costs incurred when using mobile e-wallets have an impact on student uptake of mobile e-wallets) was not accepted.

The relevance of this discovery was that students' usage of mobile e-wallets stemmed from other criteria identified as having a significant impact on their decision to use the e-wallets, not by the fact that the cost of completing transactions using e-wallets was affordable. As a result, the study concluded that the current transaction fees borne by mobile e-wallet users were insignificant to

influence their decision to either use or not use mobile e-wallets. Users could continue to use e-wallets without giving much regard to transaction charges because they were not significant enough to influence their decision.

This conclusion, however, contradicted Mallat‘s [72] assertion, which argued that if the cost of a payment transaction is passed on to customers, it has a direct impact on consumer adoption of mobile payments. However, the findings were comparable to those of Dahlberg, et al. [73] who found that transaction cost was not a significant factor influencing the use of mobile payment technology in their study.

5.2.6.5 Social Influence and Utilisation of e-Wallets

Social influence, according to the researcher, was another factor that influenced the respondents' adoption of e-wallets. For the purposes of substituting the generalised social influence variable, the researcher used four variables. The variables were: improved social interaction as a result of utilizing a mobile e-wallet, e-wallet usage as a fashionable trend in society, and e-wallet usage by the respondents' friends and family members. The researcher assumed that any of the characteristics mentioned had an impact on the study's respondents' adoption of e-wallets.

When asked if the variable "status resulting from the use of e-wallets" influenced their adoption of e-wallets, the data revealed that 32% (59 out of 182) of respondents disagreed. When asked if better social interactions through mobile wallets influenced their use of e-wallets, 31% (56 out of 182) agreed. Furthermore, when asked if the use of e-wallets as a popular trend in society influenced their use of the e-wallets, 37% (67 out of 182) agreed. Finally, when asked if the use of e-wallets by respondents' peers and family members influenced their use of e-wallets, the majority of respondents 78% (143 out of 182) agreed that having peers and family members use e-wallets influenced their use of e-wallets.

According to the findings, the biggest social factor that may have influenced the respondents' use of e-wallets on the market was the influence they received from their friends and family members who had previously used wallets. The respondents' support for the other variables under social

factors was substantially lower, hence they were not evaluated as potential social factors impacting the use of e-wallets on the market.

When the null hypothesis($H_0 4$), which stated that "the current social norm of mobile e-wallet usage does not influence the adoption of e-wallets by students" was tested at a 5% level of significance, it was not rejected. This was because the probability value (0.152) for the relationship between the variable "most of my peers and family member use mobile e-wallets" and the variable "utilisation of mobile e-wallets" was greater than 0.05. This meant that the research (alternative) hypothesis (current social norm of mobile e-wallet usage does influence the adoption of mobile e-wallets by students) was not accepted.

This result revealed that students were not using mobile e-wallets because it was fashionable to do so.Having peers (colleagues, acquaintances, and friends) who use mobile e-wallets did not necessarily inspire the students to consider using e-wallets, but rather their own convictions drove them to use e-wallets. This finding, however, contradicts the findings of Riquelme and Rose [80], and Schepers and Wetzels [81] who suggest that social norms have a significant impact on information technology system adaption and use.

5.2.6.6 Perceived Risk and Utilisation of Mobile e-Wallets

The perception of risk was also considered as a possible source of impact for mobile e-wallet adoption. The misuse or theft of users' personal information while using mobile e-wallets, or the misuse or theft of users' billing information by either hackers or service providers, were examples of perceived risk in this study.

In determining whether respondents' use of e-wallets exposed them to the two dangers mentioned, the majority of respondents 43% (78 out of 182) agreed that using mobile e-wallets exposed them to risk factors such as abuse or theft of users' information. The participants were also asked if using mobile e-wallets put them at danger of billing information being misused or stolen. The findings of the survey revealed that 30% of the respondents (55 out of 182) took a neutral stance by not indicating whether or not they were exposed to the danger, implying that a considerable number of the respondents were unsure whether or not they were exposed to the risk.

When the null hypothesis($H_0 5$), which stated that "perceived risk associated with mobile e-wallet usage does not influence the adoption of e-wallets by students" was tested at a 5% level of significance, it was not rejected. This was due to the fact that the probability value (0.503) for the relationship between the variables "risk of abuse or theft of user's information while using mobile e-wallets" and "usage of mobile e-wallets" was higher than 0.05. This means that the research (alternative) hypothesis (consumers' perceptions of risk associated with mobile e-wallet use influences their adoption of mobile e-wallets) was rejected.

This finding indicates that the risks of using mobile e-wallets have no impact on their adoption. This suggested that the risks currently associated with mobile e-wallet usage were insignificant to justify customers being so hesitant when using mobile e-wallets due to fears of their information being stolen or abused by hackers or mobile e-wallet service providers. Therefore, concluding that there are currently no significant risks associated with mobile e-wallet usage that are adversely affecting e-wallet users, and commending e-wallet service providers for instilling confidence in their users about the security they provide to prevent user information from being stolen or abused by third parties. E-wallet service providers, on the other hand, should continue to invest more in maintaining proper security for their users' information because hackers are always creating new and sophisticated methods for obtaining data from e-wallet service providers for a variety of nefarious reasons.

These findings on the impact of perceived risk on the adoption and use of mobile e-wallet innovations differ from those of Lockett and Littler [76], and Lesa and Tembo [112], who found that perceived risks of an innovation are inversely related to the adoption of mobile phone based direct banking services in their studies.

5.3 Conclusion

The aim of this study was to identify the key payment systems that students use in higher learning institutions in Lusaka and Central province in Zambia and the challenges faced by students when using these payment systems. Furthermore, explore the factors affecting adoption of e-wallets among students so as to design and develop a mobile payment system based on Blockchain for higher learning institutions in Zambia that will have a high uptake by students.

In order to determine the possible determinants of e-wallet adoption, the study used a proposed conceptual model that derived its constructs from TAM and UTAUT. Seven potential variables of e-wallet adoption among students in higher education institutions were evaluated.

The findings of the study showed that just two variables (one proposed by the TAM and the other suggested by the UTAUT) significantly influenced the students' adoption of e-wallets at a 5% level of significance using the Multinomial Logistic Regression's Likelihood Ratio Tests. These variables are the user's gender and perceived ease of use. It was also discovered that one TAM-suggested variable came very near to being a major factor of e-wallet usage; this is because it would have yielded a statistically significant result at a 10% level of significance. Perceived usefulness was the variable in question.

As a result, it has been recommended that designers and developers of e-wallet applications for students strive to make them as simple to use as possible, because complicated applications are not well received by users in this market. Additionally, when developing mobile e-wallet solutions, it is critical for developers to consider the numerous preferences that appeal differently to each gender of the product's consumers, as gender plays a big part in influencing the consumers' decision to use or not use payment systems.

The initiative to implement a Blockchain-based mobile payment system was spurred by the awareness of how the payment of student fees is undeniably ineffective, expensive and time-consuming. In addition, the increase in the number of students studying in higher education institutions often results in long stressful queues and severe overcrowding when paying student fees in most financial institutions. Students are expected to use the proposed payment system to pay their respective higher educational institution tuition fees and other student fees. Furthermore, students will be able to utilize the suggested payment system to pay for goods and services provided by the university as well as other vendors on campus.

5.4 Recommendations

5.4.1 Recommendations from the Study's findings

Following the findings from this study, it would be recommended that:

(i) Given that perceived ease of use has a substantial impact on student acceptance of e-wallets, it is recommended that designers and developers of e-wallet solutions for use by students strive to make them as simple to use as possible, because complicated applications are not appreciated by consumers in this market. By doing so, the likelihood of consumers appreciating and using e-wallets products will be high.

(ii) Since the findings also indicated a strong relationship between perceived usefulness and utilisation the e-wallets by the student, it can also be recommended that the developers ensure to make their e-wallet application to be as useful to the intended users as possible if they are to have their products significantly adopted by the targeted market.

(iii) It is also critical for mobile e-wallet developers to consider the unique preferences that appeal to each gender when developing e-wallet solutions, as gender plays a vital role in influencing users' decisions to use or not use the payment system. This can be accomplished by creating alternate user interfaces, such as one with colours that appeal primarily to female users and the other with colours that attract primarily to male users.

(iv) To encourage students to use e-wallets, higher education institutions should consider offering discounts, cash back, and gifts.

5.4.2 Recommendations for Future Studies

(i) Since this study had a relatively smaller sampled size, other scholars are encouraged to conduct a similar study but should instead consider including a relatively larger sample size.

(ii) Other scholars should consider sampling various districts in different provinces of Zambia so that the results can be easily generalized, instead of only considering two provinces as was the case in this study.

(iii)The study's findings revealed that the prevalence of neutral replies was particularly high when it came to perceived cost and risk concerns; as a result, this finding opens the door for further investigation of cost and risk as issues that require more consideration.

(iv) In order to promote interoperability between the proposed system and telecommunications firms, banks and microfinance institutions, a field for further studies would include the design and implementation of a RESTful API. Furthermore, consider the provision of desired features for clearing and settlement of account to account (A2A) interoperability transactions.

5.5 Chapter Summary

This chapter started by giving an overview of the chapter. It has presented a conclusion, made recommendations based on the study's findings and has also made recommendations to be considered by other scholars intending to conduct similar studies in the future have also been made, these recommendations stem from some of the limitations which this study had and the researcher hopes other future researchers will overcome such challenges in their future studies.

REFERENCES

[1] D. Flood, T. West and D. Wheadon, "Trends in Mobile Payments in Developing and Advanced Economies," *Bulleting for the 3rd Quarter. Sydney: Reserve Bank of Australia,* 2013.

[2] M. Awad, "Vodacom Tanzania's M-Pesa Hits 4.4 Million Users. IT News Africa," 2012.

[3] A. J. Levitin, "Pandora's Digital Box: The Promise and Perils of Digital Wallets," vol. 166, no. 2, 2018.

[4] Y. U. Chandra, Ernawaty and Suryanto, "Bank vs telecommunication E-Wallet: System analysis, purchase, and payment method of GO-mobile CIMB Niaga and T-Cash Telkomsel," *International Conference on Information Management and Technology (ICIMTech),* 2017.

[5] E. Sakalauskas, J. Muleravicius and I. Timofejeva, "Computational Resources for Mobile E-wallet System with Observers," *Electronics,* 2017.

[6] C. Pénicaud, "State of the Industry: Results from the 2012 Global Mobile Money Adoption Survey," 2013.

[7] N. Davidson and C. Penicaud, "State of the Industry: Results from 2011 Global Mobile Modey Adoption Survey," GSMA — Mobile Money for the Unbanked, 2012.

[8] G. Demombynes and A. Thegeya, "Kenya's Mobile Revolution and the Promise of Mobile Savings," *World Bank Policy Research Working Paper No. 5988,* 2012.

[9] N. Naghavi, "State of the Industry Report on Mobile Money 2019," GSMA, 2020.

[10] S. K. Andersson-Manjang and N. Naghavi, "State of the Industry Report on Mobile Money 2021," GSMA — Mobile Money for the Unbanked, 2021.

[11] M. Mwewa, EFFECTIVENESS OF THE STUDENT'S ELECTRONIC PAYMENT SYSTEM: A CASE STUDY OF THE UNIVERSITY OF ZAMBIA, 2018.

[12] W. Werapun, T. Arpornthip, E. Sangiamkul, R. Wetprasit and T. Karode, "A Blockchain-based Renewable Energy Investment Management Platform: Decentralized Sustainable Development (DeSDev)," *Journal of Computer Science,* vol. 16, no. 11, pp. 1657-1668, 2020.

[13] C. Moonde and J. Phiri, "An Investigation of the Factors Influencing the Utilization of E-wallets in Higher Learning Institutions Using Technology Acceptance Model," *ZAPUC International Conference Proceedings,* 2020.

[14] C. Moonde and J. Phiri, "Cryptocurrency Payments Implementation Based on Blockchain Technologies in Addressing Covid-19 in Higher Learning Institutions," *Proceedings of the 2nd African International Conference on Industrial Engineering and Operations Management,* 2020.

[15] C. Moonde and J. Phiri, "An Investigation of the Factors Influencing the Utilization of E-Wallets in Higher Learning Institutions in Zambia Using Technology Acceptance Model," *Zambia ICT Journal,* vol. 5, no. 1, 2021.

[16] C. Moonde and J. Phiri, An Investigation of Factors Influencing the Adoption of e-Wallets, 1 ed., LAP LAMBERT Academic Publishing, 2021, p. 52.

[17] M. Mwewa, "Effectiveness of the Student's Electronic Payment System: A Case Study of the University of Zambia," The University of Zambia, 2018.

[18] N. Lwanga, A. Justus and R. Sekibira, Online Fees Payment System for Makerere University, 2014.

[19] C. C. Benson, C. Niehaus, M. Mashayekhi, N. Clotteau, T. Zimmer, B. Antunes, Y. Grin, P. Potgieser, Q. Nguyen, Q. Wright, N. Feingold and A. Sathnur, "Financial Inclusion," *ITU-T Focus Group Digital Financial Services,* 2017.

[20] C. C. Benson, C. Niehaus, M. Mashayekhi, N. Clotteau, T. Zimmer, B. Antunes, Y. Grin, P. Potgieser, Q. Nguyen, G. Wright, N. Feingold and A. Sathnur, "The Digital Financial Services Ecosystem," *ITU-T Focus Group on Digital Financial Services,* 2016.

[21] R. Martin and V. Mauree, "Commonly Identified Consumer Protection Themes," *Focus Group Technical Report,* 2016.

[22] M. A. Nandhi, "Effects of Mobile Banking on the Savings Practices of Low Income Users," *Working paper,* 2012.

[23] F. Deloitte, *Value of connectivity: Economic and social benefits of expanding internet access,* Deloitte UK Economic Consulting, 2014.

[24] L. Braniff, "schools-africa-arent-taking-advantage-mobile-money-why," 2017. [Online]. Available: cgap.org/blog/schools-africa-arent-taking-advantage-mobile-money-why. [Accessed 23 August 2020].

[25] V. Mauree and K. Butler, DFS Security Assurance Framework, International Telecommunication Union (ITU), 2019.

[26] L. J. Zhao, S. Fan and J. Yan, "Overview of business innovations and research opportunities in blockchain and introduction to the special issue," *Financ Innov,* vol. 2, no. 28, 2016.

[27] S. Haber and W. S. Stornetta, "How to Time-Stamp a Digital Document," *Journal of Cryptology,* vol. 3, no. 2, pp. 99-111, 1991.

[28] F. Mvula, S. Tembo and J. Phiri, "A Blockchain based Mobile Money Interoperability Scheme," *International Journal of Advanced Computer Science and Applications (IJACSA),* vol. 11, no. 1, 2020.

[29] D. M. E.-D. M. Hussein, M. H. N. Taha and N. E. M. Khalifa, "A Blockchain Technology Evolution Between Business Process Management (BPM) and Internet-of-Things (IoT)," *International Journal of Advanced Computer Science and Applications (IJACSA),* vol. 9, no. 8, 2018.

[30] W. N. W. Muhamad, N. A. M. Razali, M. Wook, K. K. Ishak, N. M. Zainudin, N. A. Hasbullah and S. Ramli, "Evaluation of Blockchain-based Data Sharing Acceptance among Intelligence Community," *International Journal of Advanced Computer Science and Applications(IJACSA),* vol. 11, no. 12, 2020.

[31] M. Labrador and W. Hou, "Security Mechanism for Vehicle Identification and Transaction Authentication in the Internet of Vehicle (IoV) Scenario: A Blockchain Based Model," *Journal of Computer Science,* vol. 15, no. 2, pp. 249-257, 2019.

[32] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," *Decentralized Business Review,* 2008.

[33] A. Grech and A. F. Camilleri, "Blockchain in Education," Publications Office of the European Union, 2017.

[34] R. Collins, "Blockchain-A-New-Architecture-for-Digital-Content," 2016. [Online]. Available: http://www.econtentmag.com/Articles/Editorial/Commentary/Blockchain-A-New-Architecture-for-Digital-Content-114161.htm. [Accessed 1 August 2020].

[35] M. Memon, S. S. Hussain, U. A. Bajwa and A. Ikhlas, "Blockchain Beyond Bitcoin: Blockchain Technology Challenges and Real-World Applications," *International Conference on Computing, Electronics & Communications Engineering (iCCECE),* pp. 29-34, 2018.

[36] S. Yaqoob, M. M. Khan, R. Talib, A. D. Butt, S. Saleem, F. Arif and A. Nadeem, "Use of Blockchain in Healthcare: A Systematic Literature Review," *International Journal of Advanced Computer Science and Applications (IJACSA),* vol. 10, no. 5, 2019.

[37] S. Underwood, "Blockchain beyond bitcoin," *Communications of the ACM,* vol. 59, no. 11, pp. 15-17, 2016.

[38] J. Yli-Huumo, D. Ko, S. Choi, S. Park and K. Smolander, "Where is current research on blockchain technology? a systematic review," *PloS one,* vol. 11, no. 10, 2016.

[39] Z. Zheng, S. Xie, H.-N. Dai, X. Chen and H. Wang, "Blockchain challenges and opportunities: A survey," *International Journal of Web and Grid Services,* vol. 14, no. 4, pp. 352-375, 2018.

[40] V. Gatteschi, F. Lamberti, C. Demartini, C. Pranteda and V. Santamaría, "Blockchain and Smart Contracts for Insurance: Is the Technology Mature Enough?," *Future Internet,* vol. 10, no. 20, 2018.

[41] H. Kakavand and N. Kost De Sevres, "The Blockchain Revolution: An Analysis of Regulation and Technology Related to Distributed Ledger Technologies," *Luther Systems,* 2016.

[42] 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," 2017.

[43] S. G. Fashoto, F. Uzoka, M. Ameen and M. Mabayoje, "Development of e-wallet system for Tertiary institution in a Developing country," *GESJ: Computer Science and Telecommunications,* vol. 3, no. 49, 2016.

[44] A. I. Al-Alawi, A. H. Al-Hammam, S. S. Al-Alawi and E. I. AlAlawi, "The Adoption of E-Wallets: Current Trends and Future Outlook," *Innovative Strategies for Implementing FinTech in Banking*, pp. 242-262, 2021.

[45] A. Daragmeh, J. Sági and Z. Zéman, "Continuous Intention to Use E-Wallet in the Context of the COVID-19 Pandemic: Integrating the Health Belief Model (HBM) and Technology Continuous Theory (TCT)," *Journal of Open Innovation,* vol. 7, no. 2, 2021.

[46] N. Jonker, C. van der Cruijsen, M. Bijlsma and W. Bolt, "Pandemic Payment Patterns," *TILEC Discussion Paper No. 2020-033,* 2020.

[47] R. Pal and S. K. Bhadada, "Cash, currency and COVID-19," *Postgraduate Medical Journal,* vol. 96, no. 1137, pp. 427-428, 2020.

[48] F. Davis, "Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology," *MIS quarterly,* no. 13, pp. 319-340, 1989.

[49] V. Venkatesh and F. D. Davis, "A theoretical extension of the technology acceptance model: Four longitudinal field studies," *Management Science,* vol. 46, no. 2, pp. 186-204, 2000.

[50] P. N. Soneka and J. Phiri, "A Model for Improving E-Tax Systems Adoption in Rural Zambia Based on the TAM Model," *Open Journal of Business and Management,* no. 7, pp. 908-918, 2019.

[51] D. Gefen, E. Karahanna and D. W. Straub, "Trust and TAM in online shopping: an integrated model," *MIS Quarterly,* vol. 27, no. 1, pp. 51-90, 2003.

[52] J. W. Moon and Y. G. Kim, "Extending the TAM for a world-wide-web context," *Information & Management,* vol. 38, pp. 217-230, 2001.

[53] A. K. Nag and B. Gilitwala, "E-wallet- Factors Affecting Its Intention to Use," *International Journal of Recent Technology and Engineering (IJRTE),* vol. 8, no. 4, 2019.

[54] K. Masinge, Factors influencing the adoption of mobile banking services at the Bottom of the Pyramid in South Africa, (Master of Business Administration), University of Pretoria, 2010.

[55] P. G. Schierz, O. Schilke and B. W. Wirtz, "Understanding consumer acceptance of mobile payment services: An empirical analysis," *Electronic Commerce Research and Applications,* vol. 9, no. 3, pp. 209-216, 2010.

[56] S. Assegaff, "A Literature Review: Acceptance Models for e-learning Implementation in Higher Institution," *International Conference on Advances in Education Technology (ICAET-14),* 2015.

[57] V. Venkatesh, M. G. Morris, F. D. Davis and G. B. Davis, "User Acceptance of Information Technology: Toward a Unified View," *MIS Quarterly,* no. 27, pp. 425-478, 2003.

[58] I. Ajzen and M. Fishbein, "Understanding attitudes and predicting social behavior," *Englewood Cliffs,* 1980.

[59] A. A. Taiwo and A. G. Downe, "The theory of user acceptance and use of technology (UTAUT): A meta-analytic review of empirical findings," *Journal of Theoretical & Applied Information Technology,* vol. 49, no. 1, 2013.

[60] W. Ibidunmoye, "Identification of Factors Influencing the Adoption of Mobile Payments : A qualitative research study on the Swish mPayment App," 2018.

[61] D. E. Wasitarini and W. Tritawirasta, “Assessing users' acceptance toward a closed access Library Service System using the UTAUT model: A case study at the National Library of Indonesia,” *Information Technology Systems and Innovation (ICITSI),* pp. 1-4, 2015.

[62] Y. Sok Foon and B. Yin-Fah, “Internet banking adoption in Kuala Lumpur: an application of UTAUT model,” *International Journal of Business and Management,* vol. 6, no. 4, p. 161, 2011.

[63] R. H. Shroff, C. C. Deneen and M. W. Eugenia, “Analysis of the technology acceptance model in examining students’ behavioural intention to use an e-portfolio system,” *Australasian Journal of Educational Technology,* vol. 27, no. 4, pp. 600-618, 2011.

[64] U. Akturan and N. Tezcan, “Mobile banking adoption of the youth market: Perceptions and intentions,” 2012.

[65] J. H. Cheong, M. C. Park and J. H. Hwang, “Mobile payment adoption in Korea: Switching from credit card,” *ITS 15th Biennial Conference,* pp. 4-7, 2004.

[66] N. Mallat, M. Rossi, V. K. Tuunainen and A. Öörni, “The impact of use context on mobile services acceptance: The case of mobile ticketing,” *Information & Management,* vol. 46, no. 3, p. 190–195, 2009.

[67] D. H. Shin, “Modeling the interaction of users and mobile payment system: Conceptual framework,” *International Journal of Human-Computer Interaction,* vol. 26, no. 10, pp. 917-940, 2010.

[68] J. Sripalawat, M. Thongmak and A. Ngramyarn, "M-banking in metropolitan Bangkok and a comparison with other countries," *The Journal of Computer Information Systems,* vol. 51, no. 3, pp. 67-76, 2011.

[69] C. Phonthanukitithaworn, C. Sellitto and M. Fong, "User Intentions to Adopt Mobile Payment Services: A Study of Early Adopters in Thailand," *Journal of Internet Banking and Commerce,* vol. 20, no. 1, 2015.

[70] M. Amberg, M. Hirschmeier and J. Wehrmann, "The Compass Acceptance Model for the Analysis and Evaluation of Mobile Information Systems," *International Journal for Mobile Communications (IJMC),* 2003.

[71] P. Luarn and H. Lin, "Towards an understanding of the behavioral intention to use mobile banking," *Computers in Human Behavior,* vol. 21, pp. 873-891, 2005.

[72] Mallat, N., "Exploring consumer adoption of mobile payments – A qualitative study," *The Journal of Strategic Information Systems,* vol. 16, no. 4, pp. 413-432, 2007.

[73] T. Dahlberg, J. Gou and J. Ondrus, "A critical review of mobile payment research," *Electronic Commerce Research and Applications,* vol. 14, no. 5, pp. 265-284, 2015.

[74] P. Gerrard and B. J. Cunningham, "The diffusion of Internet banking among Singapore consumer," *International Journal of Bank Marketing,* vol. 21, no. 1, pp. 16-28, 2003.

[75] N. Suki, "An Empirical Study of Factors Affecting the internet Banking Adoption among Malaysian Consumers," *Journal of internet Banking and commerce,* vol. 15, no. 2, pp. 4-8, 2010.

[76] A. Lockett and D. Littler, "The adoption of direct banking services," *Journal of Marketing Management,* vol. 13, pp. 791-811, 1997.

[77] I. Ajzen and M. Fishbein, Belief, attitude, intention and behaviour: An introduction to theory and research, MA: Addison-Wesley, 1975.

[78] P. E. Pedersen and R. Ling, "Mobile end-user service adoption studies: A selective review," *Scandinavian Journal of Information Systems,* vol. 14, no. 1, pp. 3-17, 2002.

[79] S. Taylor and A. P. Todd, "Understanding information technology usage: A test of computing models," *Information Systems Research,* vol. 6, no. 2, p. 144–176, 1995.

[80] H. E. Riquelme and E. R. Rosa, "The moderating effect of gender in the adoption of mobile banking," *International Journal of Bank Marketing,* vol. 28, no. 5, p. 328–341, 2010.

[81] J. Schepers and M. Wetzels, "A meta-analysis of the technology acceptance model: Investigating subjective norm and moderation effects," *Information & Management,* vol. 44, no. 1, pp. 90-103, 2007.

[82] W. Wood and S. Li, "The empirical analysis of technology camel," *Issues in Information Systems,* vol. 6, no. 2, pp. 154-160, 2005.

[83] S. Li, R. Glass and H. Records, "The Influence of Gender on New Technology Adoption and Use–Mobile Commerce," *Journal of Internet Commerce,* vol. 7, no. 2, pp. 270-289, 2008.

[84] R. K. Rainer, K. Laosethakul and M. K. Astone, "Are gender perceptions of computing changing over time," *Journal of Computer Information Systems Summer,* vol. 43, no. 4, p. 108–114, 2003.

[85] S. Sarker and J. D. Wells, "Understanding mobile handheld device use and adoption," *Communications of the ACM,* vol. 46, no. 12, pp. 35-40, 2003.

[86] P. E. Pedersen, "Adoption of mobile Internet services: An exploratory study of mobile commerce early adopters," *Journal of organizational computing and electronic commerce,* vol. 15, no. 3, pp. 203-222, 2005.

[87] L. Zhou, L. Dai and D. Zhang, "On-line shopping acceptance model – A critical survey of consumer factors in on-line shopping," *Journal of Electronic Commerce Research,* vol. 8, no. 1, p. 41–62, 2007.

[88] N. Hughes and S. Lonie, "M-PESA: Mobile Money for the "Unbanked" Turning Cellphones into 24-Hour Tellers in Kenya," *Innovations: Technology, Governance, Globalization,* vol. 2, no. 1-2, pp. 64-81, 2007.

[89] M. Hinz, "M-PESA: The Best of Both Worlds," *BBVA,* pp. 1-5, 2014.

[90] K. Singh, S. Mandal and A. Mahanti, "Opportunity Analysis: The Story of Paytm During Demonetisation," in *Sixth National Conference for Case Studies (COGNOSCO)*, 2017.

[91] T. Joshi, S. S. Gupta and N. Rangaswamy, "Digital Wallets 'Turning a Corner' for Financial Inclusion: A Study of Everyday PayTM Practices in India," *IFIP Advances in Information and Communication Technology,* vol. 552, pp. 280-293, 2019.

[92] Pandy, S. M. and Crowe, M., “Choosing a Mobile Wallet,” *The Consumer Perspective*, 2017.

[93] D. Williams, “Encrypted Website Payments,” in *Pro PayPal E-Commerce*, 2007, pp. 55-57.

[94] O. Ghag and S. Hegde, “A Comprehensive Study of Google Wallet as an NFC Application,” *International Journal of Computer Applications,* vol. 58, no. 16, pp. 37-42, 2012.

[95] M. Roland, J. Langer and J. Scharinger, “Applying Relay Attacks to Google Wallet,” *International Workshop on Near Field Communication (NFC),* pp. 1-6, 2013.

[96] J. H. Huh, S. Verma, S. S. V. Rayala, R. B. Bobba, K. Beznosov and H. Kim, “I Don't Use Apple Pay Because It's Less Secure: Perception of Security and Usability in Mobile Tap-and-Pay,” *NDSS Symposium 2017,* 2017.

[97] E. Bruce, Apple Pay Essentials, Packt Publishing Ltd, 2016.

[98] D. Choi and Y. Lee, “Eavesdropping One-Time Tokens Over Magnetic Secure Transmission in Samsung Pay,” *10th USENIX Workshop on Offensive Technologies (WOOT 16). USENIX Association,* 2016.

[99] D. Choi and Y. Lee, “Eavesdropping of Magnetic Secure Transmission Signals and Its Security Implications for a Mobile Payment Protocol,” *IEEE,* vol. 6, pp. 42687-42701, 2018.

[100] ZICTA, "ICT Survey Report – Households and Individuals," ZICTA, 2015.

[101] M. Saunders, P. Lewis and A. Thornhill, "Research Methods for Business," *Harlow: Pearson,* 2016.

[102] H. Taherdoost, "Sampling Methods in Research Methodology; How to Choose a Sampling Technique for Research," *International Journal of Academic Research in Management (IJARM),* vol. 5, no. 2, pp. 18-27, 2016.

[103] A. R. Hevner, "Object-Oriented System Development Methods," *Advances in Computers,* vol. 35, pp. 135-198, 1992.

[104] L. A. Maciaszek, Requirements Analysis and System Design, Addison-Wesley, 2007.

[105] E. Merah, A. Laghrour, N. Messaoudi, H. Saidi and A. Chaoui, "Design of ATL Rules for Transforming UML 2 Communication Diagrams into Büchi Automata," *International Journal of Software Engineering and Its Applications,* vol. 7, no. 2, 2013.

[106] L. D. Singh and K. M. Singh, "Implementation of Text Encryption using Elliptic Curve Cryptography," *Procedia Computer Science,* vol. 54, pp. 73-82, 2015.

[107] D. Hankerson, A. Menezes and S. Vanstone, Guide to Elliptic Curve Cryptography, Springer, 2004.

[108] P. Singh, N. Supriya and M. Joshna, "Issues and challenges of electronic payment systems," *International Journal for Research in Management and Pharmacy,* vol. 2, no. 9, pp. 25-30, 2013.

[109] A. Adewole, "Consumer Payment System and the Challenge of Confidence in National Payment System of Developing Countries: A Case Study of Nigeria," *Mediterranean Journal of Social Sciences,* vol. 6, no. 2, p. 568, 2015.

[110] H. F. Atlam and G. B. Wills, "Technical aspects of blockchain and IoT," *Advances in Computers,* vol. 115, pp. 1-39, 2019.

[111] V. Venkatesh, J. Y. Thong and X. Xu, "Consumer acceptance and use of information technology: Extending the unified theory of acceptance and use of technology," *MIS Quarterly,* vol. 36, no. 1, pp. 157-178, 2012.

[112] E. Lesa and S. Tembo, "Study on Factors Affecting Mobile Payment Systems Diffusion in Zambia," *Management,* vol. 6, no. 2, pp. 36-45, 2016.

[113] Zeinab, M., "Determinants of Mobile Money Adoption: Europe - Middle East - North African," *Regional Conference of the International Telecommunications Society (ITS),* 2019.

[114] Ann Alexander, C. and Wang, L., "Blockchain: Methods, Applications and Technology Progress," *American Journal of Engineering and Applied Sciences,* vol. 12, no. 1, pp. 30-38, 2019.

[115] Akturan, U. and Tezcan, N., "Mobile banking adoption of the youth market: Perceptions and intentions," 2012.

[116] W. Penard and T. V. Werkhoven, Cryptography in Context, 2008.

[117] S. E. Traif, I. E. Alshihabi, A. Ajlan, A. Bubshait and A. Razzaque, "Adoption of FinTech by Students in Higher Education Institutions," *Innovative Strategies for Implementing FinTech in Banking*, 2021.

[118] S. M. Pandy and M. Crowe, "Choosing a Mobile Wallet: The Consumer Perspective," Federal Reserve Bank of Boston, 2017.

[119] L. A. Maciaszek, Requirements analysis and system design: developing information systems with UML, Addison Wesley, 2001.

[120] F. Mvula, A conceptual secure blockchain based settlement and clearing house for mobile financial services in Zambia, 2020.

APPENDICES

Appendix A: Ethical Approval

THE UNIVERSITY OF ZAMBIA
DIRECTORATE OF RESEARCH AND GRADUATE STUDIES

Great East Road Campus | P.O. Box 32379 | Lusaka 10101 | **Tel:** +260-290 258/291 777
Fax: (+260) 211 290 258/253 952 | **Email:** director.drgs@unza.zm | **Website:** www.unza.zm

APPROVAL OF STUDY

REF No. NASREC: 2021-APR-008

13th May, 2021

Mr. Chimuka Moonde
Principal Investigator
C/o School of Natural Sciences
LUSAKA

Dear Mr. Moonde

"SECURE MOBILE PAYMENT SYSTEM BASED ON BLOCHAIN FOR HIGHER INSTITUTIONS OF LEARNING"

Reference is made to your submission for ethical approval of the study captioned above.

The University Of Zambia Natural and Applied Sciences Research Ethics Committee IRB resolved to approve this study and your participation as Principal Investigator for a period of one year.

Review Type	**Ordinary Review**	Approval No. **NASREC:2021:APR-008**
Approval and Expiry Date	Approval Date: 13th May, 2021	Expiry Date: 12th May, 2022
Protocol Version and Date	Version-Nil	-
Information Sheet, Consent Forms and Dates	• English.	To be provided
Consent form ID and Date	• Version	To be provided
Recruitment Materials	Nil	Nil

Towards Improving Service and Excellence in High Education Beyond Fifty Years

Specific conditions will apply to this approval. As Principal Investigator it is your responsibility to ensure that the contents of this letter are adhered to. If these are not adhered to, the approval may be suspended. Should the study be suspended, study sponsors and other regulatory authorities will be informed.

Conditions of Approval

- No participant may be involved in any study procedure prior to the study approval or after the expiration date.
- All unanticipated or Serious Adverse Events (SAEs) must be reported to NASREC within 5 days.
- All protocol modifications must be approved by NASREC prior to implementation unless they are intended to reduce risk (but must still be reported for approval). Modifications will include any change of investigator/s or site address.
- All protocol deviations must be reported to NASREC within 5 working days.
- All recruitment materials must be approved by NASREC prior to being used.
- Principal investigators are responsible for initiating Continuing Review proceedings. HSSRECwill only approve a study for a period of 12 months.
- It is the responsibility of the PI to renew his/her ethics approval through a renewal application to NASREC.
- Where the PI desires to extend the study after expiry of the study period, documents for study extension must be received by NASREC at least 30 days before the expiry date. This is for the purpose of facilitating the review process. Documents received within 30 days after expiry will be labelled "late submissions" and will incur a penaltyfee of K500.00. No study shall be renewed whose documents are submitted for renewal 30 days after expiry of the certificate.
- Every 6 (six) months a progress report form supplied by The University of Zambia Humanities and Social Sciences Research Ethics Committee as an IRB must be filled in and submitted to us. There is a penalty of K500.00 for failure to submit the report.
- When closing a project, the PI is responsible for notifying, in writing or using the Research Ethics and Management Online (REMO),both NASREC and the National Health Research Authority (NHRA) when ethics certification is no longer required for a project.
- In order to close an approved study, a Closing Report must be submitted in writing or through the REMO system. A Closing Report should be filed when data collection has ended and the study team will no longer be using human participants or animals or secondary data or have any direct or indirect contact with the research participants or animals for the study.
- Filing a closing report (rather than just letting your approval lapse) is important as it assists NASREC in efficiently tracking and reporting on

projects. Note that some funding agencies and sponsors require a notice of closure from the IRB which had approved the study and can only be generated after the Closing Report has been filed.

- A reprint of this letter shall be done at a fee.
- All protocol modifications must be approved by NASREC by way of an application for an amendment prior to implementation unless they are intended to reduce risk (but must still be reported for approval). Modifications will include any change of investigator/s or site address or methodology and methods. Many modifications entail minimal risk adjustments to a protocol and/or consent form and can be made on an Expedited basis (via the IRB Chair). Some examples are: format changes, correcting spelling errors, adding key personnel, minor changes to questionnaires, recruiting and changes, and so forth. Other, more substantive changes, especially those that may alter the risk-benefit ratio, may require Full Board review. In all cases, except where noted above regarding subject safety, any changes to any protocol document or procedure must first be approved by NASREC before they can be implemented.

Should you have any questions regarding anything indicated in this letter, please do not hesitate to get in touch with us at the above indicated address.

On behalf of NASREC, we would like to wish you all the success as you carry out your study.

Yours faithfully,

Dr. E. Mwanaumo

CHAIRPERSON
THE UNIVERSITY OF ZAMBIA NATURAL AND APPLIED SCIENCES
RESEARCH ETHICS COMMITTEE IRB

cc Director, Directorate of Research and Graduate Studies
Assistant Registrar (Research), Directorate of Research and Graduate Studies
Acting Senior Administration (R), Directorate of Research and Graduate Studies

Appendix B: Publications

1. C. Moonde and J. Phiri, "An Investigation of the Factors Influencing the Utilization of E-wallets in Higher Learning Institutions Using Technology Acceptance Model," ZAPUC International Conference Proceedings, 2020.
2. C. Moonde and J. Phiri, “Cryptocurrency Payments Implementation Based on Blockchain Technologies in Addressing Covid-19 in Higher Learning Institutions,” Proceedings of the 2nd African International Conference on Industrial Engineering and Operations Management, 2020.
3. C. Moonde and J. Phiri, “An Investigation of the Factors Influencing the Utilization of E-Wallets in Higher Learning Institutions in Zambia Using Technology Acceptance Model,” Zambia ICT Journal, vol. 5, no. 1, 2021.
4. C. Moonde and J. Phiri, “An Investigation of Factors Influencing the Adoption of e-Wallets in Higher Learning Institutions in Zambia Using TAM,” LAP LAMBERT Academic Publishing, 2021.
5. C. Moonde and J. Phiri, “Addressing Covid-19 in Higher Education Institutions with a Blockchain-Based Mobile Payment System,” In: Silhavy, R. (eds) Software Engineering Perspectives in Systems. CSOC 2022. Lecture Notes in Networks and Systems, vol 501. Springer, 2022.

Appendix C: Questionnaire

The University of Zambia

School of Natural Sciences

SECURE MOBILE PAYMENT SYSTEM BASED ON BLOCKCHAIN FOR HIGHER INSTITUTIONS OF LEARNING

Chimuka Moonde (Student ID: 2018248898)

MSc. Computer Science

For more information or any queries, kindly get in touch on 0973297682

Dear Respondent,

My name is Chimuka Moonde, am a student at the University of Zambia. I am conducting a study on: "***Designing and Developing of a Secure Mobile Payment System Based on Blockchain for Higher Institutions of Learning."***

You have been purposefully selected to provide information for the topic indicated above. The information being collected is purely for academic purposes as such, it will be treated with maximum confidentiality. Subsequently, you are not supposed to indicate your name or any personal information that can lead to revealing of your identity. Please note there is no right or wrong answers to these questions, we are interested in knowing what you think.

Your co-operation will be greatly appreciated.

For more information or any queries, kindly get in touch with the following:

Principal Investigator
Chimuka Moonde
0973297682
chimukamoonde@gmail.com
Project Supervisor
Dr. Jackson Phiri,
Computer Science Department,
University of Zambia.
jackson.phiri@cs.unza.zm

Section A: Demographic profile (Please tick [√])

1. Gender:
   Male [ ] Female [ ]

2. Marital Status:
   Single [ ] Married [ ] Divorced [ ]

3. What is your age group?
   20 or under [ ] 21-30 [ ] 31-40 [ ] 41-50 [ ] 51-60 [ ] 61 and above [ ]

4. What is the highest level of education you have completed?
   High School [ ] Certificate [ ] Diploma [ ]
   Bachelor degree [ ] Master's degree [ ] Doctoral (Ph.D) degree [ ]

5. What level of education are you currently pursuing?
   Certificate [ ] Diploma [ ] Bachelor degree [ ]
   Master's degree [ ] Doctoral (Ph.D) degree [ ]

6. Please state the program and school under which you are pursuing your education?
   _____

Section B: ICT Knowledge and Experience (Please tick [√])

7. How would you describe your knowledge or skills with the following?

	Very good	Good	Moderate	Poor	Very poor
Internet					
Computers (laptops or desktops)					
Tablets or iPad					
Mobile phones					

8. For how long have you been using the following?

	Don't use	Less than 1 year	1-2 years	More than 2 years
Internet				
Computers (laptops or desktops)				
Tablets or iPad				
Mobile phones				

9. How frequently do you use your mobile phone to carry out the following tasks?

	Always	Often	Sometimes	Rarely	Never
Check Account Balance					
View Bank Statement					
Receive money from family or friends					
Send money to family or friends					
Bill payments:					
MultiChoice (GOtv and DStv)					
ZESCO Prepaid units					
Water Prepaid units					
Taxes and Govt Institutions					
Goods and services					
School fees					

10. How familiar are you with the following mobile wallets?

	I am currently an active or frequent user	I have used it in the past or have an account	I have used or considered using it	I have only heard of it but never used it	I have never heard of it
Airtel Money					
MTN money					
ZamKwacha / ZamPay					
Zanaco ZeeWallet					
FNB eWallet					
Barclays CashSend					
Tenga mobile wallet					
Zoona					

Perceived Usefulness

11. To what extent do you agree with the following statements about mobile wallets?

	Strongly agree	Agree	Neutral	Disagree	Strongly disagree
I find mobile wallets useful					
Using mobile payment systems would enhance my effectiveness in making payments.					
Using mobile payment systems would make it easier for me to manage and make payments.					

Perceived Ease of Use

12. How much do you agree or disagree with the following statements about mobile wallets?

	Strongly agree	Agree	Neutral	Disagree	Strongly disagree
It is easy to register for a mobile wallet					
It is easy to carry out a transaction (start and finish transaction)					
There are few steps required to carry out a transaction					
Errors can be easily reversed					
Interaction with mobile wallet is clear and understandable					
Instructions and documentations are helpful and clear					

Perceived Cost

13. To what extent do you agree with the following statements about mobile wallets?

	Strongly agree	Agree	Neutral	Disagree	Strongly disagree
The registration fee is fair					
The transaction cost is fair					
There is no emotional or physical harm when using a mobile wallet					

Social Influence

14. How much do you agree or disagree with the following statements about mobile wallets?

	Strongly agree	Agree	Neutral	Disagree	Strongly disagree
Using a mobile wallet gives status					
Using a mobile wallet improves social interaction					
It is fashionable to use a mobile wallet					
Mobile wallets are used by my peers (classmates or friends) and parents					

Perceived Risk

15. To what extent do you agree with the following statements about mobile wallets?

	Strongly agree	Agree	Neutral	Disagree	Strongly disagree
The risk of abuse or theft of user's information (e.g., name of user, NRC, payment amount) is low when using mobile payment services					

The risk of abuse or theft of billing information (e.g., credit card number, bank account data) is low when using mobile payment services					

Perceived Trust

16. To what extent do you agree with the following statements about mobile wallets?

	Strongly agree	Agree	Neutral	Disagree	Strongly disagree
The service provider (i.e. Airtel, MTN, Banks) is trustworthy					
Wrong transactions can be easily refunded					
Whenever a transaction is directed to me, no one else can accept/cash it other than myself					
I have no privacy concerns using a mobile wallet					
I trust mobile payment systems to be secure.					

Experience

17. To what extent do you agree that the following reasons contribute to the poor usage of mobile wallets?

	Strongly agree	Agree	Neutral	Disagree	Strongly disagree
Complicated Registration Process					
Preference to use banks					
Lack of Trust in mobile wallets					
Difficult to use mobile wallets					
Lack of mobile phone					
Unaware of mobile wallet					
Service charges of mobile wallets					

18. How familiar are you with the following payment methods?

	I am currently an active or frequent user	I have used it in the past	I have used or considered using it	I have only heard of it, but never used it	I have never heard of it
Cash					
Bill Master					
Debit Card (VISA Card)					
Cheque					
Bank Transfer					
Money Order					

Mobile money					

19. Which payment method do you use to pay for the following?

	Cash	Bill Master	Debit Card	Cheque	Bank Transfer	Money Order	Mobile Money
Registration							
Tuition							
Examination							
Medical							
Accommodation							
Library							
Recreation							
Internet							
Maintenance							
Student Union							

20. How easy or difficult is it to use the following payment methods to pay for your tuition and other fees?

	Very easy	Somewhat easy	Neutral	Somewhat difficult	Very difficult
Cash					
Bill Master					
Debit Card					
Cheque					
Bank Transfer					
Money Order					
Mobile money					

21. Payment of tuition and other fees is mostly done at an accepted bank chosen by the institution. To what extent do you agree that the following statements

	Strongly agree	Agree	Neutral	Disagree	Strongly disagree
Accepted banks are easily accessible					
Accepted banks are evenly distributed in rural and urban areas					
You have to travel a long distance to access an accepted bank					
Accepted bank is characterized with long queues					

Time spent waiting to be attended to is unbearable					
I am assisted when filling in the deposit form/document					

Expectancy

22. Is having a mobile payment system for your institution, one way of resolving some of the challenges experienced when paying your tuition and other fees?

    Yes [ ] No [ ]

23. To what extent do you agree that the following statements

	Strongly agree	Agree	Neutral	Disagree	Strongly disagree
A mobile payment system can be an **alternative** choice payment method					
A mobile payment system can **substitute** the current main method					
A mobile payment can **support** the current main payment method					
A mobile payment system is not necessary					

24. How important are the following factors in making your decision to use a mobile payment system?

	Very important	Somewhat important	Neutral	Somewhat unimportant	Very unimportant
Pricing (transaction fee, service fee)					
Convenience in making payments					
Ease of use					
Secured personal information					
Secured transaction					
Secured privacy					
Usefulness of mobile payment system					

Thank you very much for taking the time to complete our survey. We sincerely appreciate your response and time. Your feedback will help us to design and develop a more secure mobile payment solution.